

## **Application Data Sheet**

### **Application Information**

|                                 |                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------|
| Application number::            |                                                                                       |
| Filing Date::                   | Herewith                                                                              |
| Application Type::              | Regular                                                                               |
| Subject Matter::                | Utility                                                                               |
| Suggested classification::      |                                                                                       |
| Suggested Group Art Unit::      |                                                                                       |
| CD-ROM or CD-R??::              |                                                                                       |
| Number of CD disks::            |                                                                                       |
| Number of copies of CDs::       |                                                                                       |
| Sequence Submission::           |                                                                                       |
| Computer Readable Form (CRF)?:: |                                                                                       |
| Number of copies of CRF::       |                                                                                       |
| Title::                         | Method and System for Dynamic Network<br>Intrusion Monitoring, Detection and Response |
| Attorney Docket Number::        | 022133-000520US                                                                       |
| Request for Early Publication:: | No                                                                                    |
| Request for Non-Publication::   | No                                                                                    |
| Suggested Drawing Figure::      |                                                                                       |
| Total Drawing Sheets::          | 9                                                                                     |
| Small Entity?::                 | No                                                                                    |
| Latin name::                    |                                                                                       |
| Variety denomination name::     |                                                                                       |
| Petition included?::            | No                                                                                    |
| Petition Type::                 |                                                                                       |
| Licensed US Govt. Agency::      |                                                                                       |
| Contract or Grant Numbers One:: |                                                                                       |
| Secrecy Order in Parent Appl.:: | No                                                                                    |

**Applicant Information**

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: US  
Status:: Full Capacity  
Given Name:: Bruce  
Middle Name::  
Family Name:: Schneier  
Name Suffix::  
City of Residence:: Minneapolis  
State or Province of Residence:: MN  
Country of Residence:: US  
Street of Mailing Address:: 101 East Minnehaha Parkway  
City of Mailing Address:: Minneapolis  
State or Province of mailing address:: Mn  
Country of mailing address:: US  
Postal or Zip Code of mailing address:: 55419

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: US  
Status:: Full Capacity  
Given Name:: Andrew  
Middle Name:: H.  
Family Name:: Gross  
Name Suffix::  
City of Residence:: San Jose  
State or Province of Residence:: CA  
Country of Residence:: US  
Street of Mailing Address:: 1055 Coleman Road, #2309  
City of Mailing Address:: San Jose  
State or Province of mailing address:: CA  
Country of mailing address:: US  
Postal or Zip Code of mailing address:: 95123

Applicant Authority Type:: Inventor  
Primary Citizenship Country:: US  
Status:: Full Capacity  
Given Name:: Jonathan  
Middle Name:: D.  
Family Name:: Callas  
Name Suffix::  
City of Residence:: Mountain View  
State or Province of Residence:: CA  
Country of Residence:: US  
Street of Mailing Address:: 1781 Wema Way  
City of Mailing Address:: San Jose  
State or Province of mailing address:: CA  
Country of mailing address:: US  
Postal or Zip Code of mailing address:: 95124

#### **Correspondence Information**

Correspondence Customer Number:: 20350

#### **Representative Information**

Representative Customer Number:: 20350

#### **Domestic Priority Information**

|                                |                                                                          |                          |                      |
|--------------------------------|--------------------------------------------------------------------------|--------------------------|----------------------|
| Application::                  | Continuity Type::                                                        | Parent Application::     | Parent Filing Date:: |
| This Application<br>09/766,343 | Continuation of<br>An Appn claiming<br>benefit under 35 USC<br>119(e) of | 09/766,343<br>60/190,326 | 01/19/01<br>03/16/00 |

#### **Assignee Information**

Assignee Name:: Counterpane Internet Security, Inc.  
Street of mailing address:: 1090 La Avenida  
City of mailing address:: Mountain View  
State or Province of mailing address:: CA  
Country of mailing address:: US  
Postal or Zip Code of mailing address:: 94043

**PATENT APPLICATION**

**METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND RESPONSE**

Inventor(s): Bruce Schneier, a citizen of The United States, residing at  
101 East Minnehaha Parkway  
Minneapolis, MN 55419

Andrew H. Gross, a citizen of The United States, residing at  
1055 Coleman Road, #2309  
San Jose, CA 95123

Jonathan D. Callas, a citizen of The United States, residing at  
1781 Wema Way  
San Jose, CA 95124

Assignee: Counterpane Internet Security, Inc.  
1090A La Avenida  
Mountain View, CA 94043

Entity: Large

## **METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE**

### **CROSS-REFERENCE TO RELATED APPLICATIONS**

[0001] This application is a continuation application of and claims priority from U.S. Non-Provisional Patent Application Serial No. 09/766,343 filed January 19, 2001 (Attorney Docket No. 022133-000510US) which claims priority from and is a non-provisional of U.S. Provisional Patent Application No. 60/190,326, filed March 16, 2000 (Attorney Docket No. 022133-000500US), the entire disclosures of these applications are incorporated herein by reference for all purposes.

### **FIELD OF THE INVENTION**

[0002] This invention relates generally to network security and, more specifically, to methods and systems for dynamic network intrusion monitoring, detection and response.

### **BACKGROUND OF THE INVENTION**

[0003] Most computer and network security products focus on prevention. Firewalls prevent unauthorized traffic from entering a company's internal network; authentication mechanisms prevent unauthorized persons from logging on to a company's computers; and encryption prevents unauthorized persons from reading files. But because such products cannot be relied upon to work perfectly, and because security bugs may exist in other software or hardware, complete network security also requires monitoring, detection and response in the event of a breach.

[0004] An effective monitoring, detection and response system should be designed not to replace a customer's system administrators but to augment their abilities. System administrators normally do not have the time or ability to read through large amounts of constantly updated audit information, looking for attacks on their systems. They also do not have the time to continuously monitor hacker activities, looking out for new tactics, tools and trends. Finally, they do not have the time to become experts on every kind of intrusion and to maintain that expertise.

[0005] A monitoring, detection and response system that employs human intelligence, uses trained personnel in the loop, and takes advantage of security intelligence and other knowledge databases can provide customer system administrators the advice and coaching they need, when they need it, to help them repel attacks and maintain network integrity and uptime. While automatic defenses may work against automated attacks, they are at a disadvantage against an intelligent attack, against which is needed the kind of intelligent defense offered by the present invention.

#### BRIEF SUMMARY OF THE INVENTION

[0006] The present invention offers methods and systems for dynamic network intrusion monitoring, detection and response. In an exemplary implementation, these methods and systems may be used to deploy and provide a managed security monitoring service (the “MSM service”) that monitors a customer’s network activity using a probe or “sentry” system, collects status data from monitored components, filters or otherwise analyzes the collected data for activity possibly implicating security concerns, alerts and transmits information about such activity to trained security analysts working at secure operations centers (“SOCs”), and then guides the security analysts and customer through an appropriate response (with appropriate follow-up, if necessary).

[0007] The MSM service is not intended to replace but to supplement, and thereby render more effective, a customer’s existing preventive security products. Such products, which can include firewalls, servers, routers, intrusion detection systems, and other security products, can generate millions of lines of audit information each day. Buried in all that information may be the footprints of ongoing network attacks or intrusions. The MSM service can help filter and analyze all of that audit information in effectively real time to detect such attacks or intrusions.

[0008] Once a possible attack or intrusion (referred to more generally as an “incident” or “event”) is detected, its characteristics and particulars may then be examined and analyzed by trained security analysts continuously monitoring the customer’s network to further understand the incident and eliminate false positives. In analyzing the incident, security analysts can draw upon information and knowledge contained in a variety of databases, including but not limited to security intelligence databases containing information about the characteristics of various hacker techniques and tools and known vulnerabilities in various operating systems and commercial software products and hardware devices. If necessary,

security analysts can escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage. In effect, the MSM service acts as a defensive shield for a customer's network.

- 5 [0009] In an exemplary embodiment, the MSM service may allow for customization and complex data analysis. For example, the service may be customized, either dynamically or off-line, to accommodate network-specific needs and to reflect feedback received about the demonstrated efficacy of a real world response to an actual event. Furthermore, data filtering and analysis can include cross-product analysis, which allows the probe/sentry system to  
10 correlate and recognize such multiple sensor readings as reflecting the same happening. Such features ensure that the invention is capable of the rapid refinement necessary to combat network attacks.

[0010] The specific components of an exemplary implementation of the MSM service would likely include the following:

- 15 [0011] A. Security Analysts: Security analysts are personnel specializing in the analysis of network attacks. In an exemplary embodiment, such analysts would perform only such analysis and thus develop the most extensive knowledge in the field. In addition, given their access to sensitive customer information, security analysts would preferably pass background checks and be bonded to provide extra assurance for customers of the MSM service.
- 20 [0012] B. Security Intelligence: In an exemplary implementation, the expertise, knowledge and capabilities of MSM service security analysts can be supplemented by a variety of knowledge databases containing detailed information helpful for investigating, evaluating and responding to incidents. Security intelligence databases can contain information about, among other things, the characteristics of various network hardware and  
25 software products, known vulnerabilities of such products, the use and characteristics of various hacker tools, and known effective and ineffective responses to various kinds of attacks. Such databases could be continually updated by the MSM service by, for example, monitoring hacker forums, reviewing security analysts' incident reports, and evaluating customer audit data for new attack footprints.
- 30 [0013] C. Secure Operations Centers ("SOCs"): MSM service security analysts would preferably work in secure operations centers. To ensure the security of their customer networks, the SOCs should be connected to these networks preferably through

cryptographically secured tunnels (also called “pipes” or “pathways”). Furthermore, the SOC’s should provide no other interconnection with these pipes and should themselves be physically hardened against attack. Although single SOC operation is possible, multiple, geographically separated SOC’s can be used to provide redundancy and additional capacity for increased traffic or failure of one of the SOC’s.

**[0014] D. Probe/Sentry System:** The invention generally incorporates one or more probe/sentry systems that may collect data from a variety of software products and hardware to which they are attached. Such systems are preferably located within the customer’s firewall and may collect such data from essentially any product or device that can be configured to provide data to a remote device. Once the probe/sentry system collects the data, it then filters or otherwise analyzes such data and then transmits noteworthy information, preferably via a secure connection, in the form of “sentry messages” to a gateway system (described below in section E) at a SOC. Preferably, the system can perform preliminary analysis of the resulting data, either by simple filtering, cross-correlation, cross-analysis, or other means to reduce the immense volume of raw data into core information worthy of further analysis.

**[0015] E. Gateway System:** The invention may also include one or more gateway systems that serve a “gatekeeper” function in linking the probe/sentry systems to a SOC. Two possible functions of such a gateway system are (1) to reformat, add, or delete information to incoming messages from the probe/sentry systems (“sentry messages”) to ensure maximum utility of the output “gateway messages” and (2) to allow mutual “pulse monitoring” by the gateway and probe systems of their counterparts to ensure that each system is continuously operational. This latter function might allow probe/sentry systems to initiate contact with a redundant gateway system to ensure that each probe/sentry system is continuously connected to a SOC at all times.

**[0016] F. The “SOCRATES” Problem and Expertise Management System:** In an exemplary embodiment, security analysts at a SOC work in concert with the “SOCRATES”<sup>1</sup> problem and expertise management system to categorize, prioritize, investigate and respond to customer incidents or “problems.” The SOCRATES system, among other things, collects and formats gateway messages into “problem tickets” (each of which represents a discrete security-related event or incident of possible intrusive activity happening on a customer’s

---

<sup>1</sup> “SOCRATES” is an acronym standing for Secure Operations Center Responsive Analyst Technical Expertise System.

network), associates with each such ticket information useful for problem investigation, resolution and response, presents such tickets to security analysts for handling, and generally serves as a repository of useful information and procedures. Preferably, in the process of orchestrating the management of problem tickets, the SOCRATES system continuously  
5 augments problem-solving tools such as tables which tie symptoms to technology, symptoms to diagnosis, or vulnerability to diagnosis. This continuous improvement allows the invention to take full advantage of specialized nature of the monitoring system.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0017] FIG. 1 is an overview of the system architecture of an exemplary embodiment of the  
10 present invention.

[0018] FIG. 2 is a system overview of an exemplary embodiment of a probe/sentry system in an exemplary embodiment of the present invention.

[0019] “SOCRATES” is an acronym standing for Secure Operations Center Responsive Analyst Technical Expertise System.

15 [0020] FIG. 3 is a system overview of an exemplary embodiment of a gateway system in an exemplary embodiment of the present invention.

[0021] FIG. 4 is a system overview of an exemplary embodiment of a problem and expertise management system in an exemplary embodiment of the present invention.

[0022] FIG. 5 is a flowchart illustrating an exemplary implementation of incident handling  
20 by a security analyst in an exemplary embodiment of the present invention.

[0023] FIG. 6 is a diagram illustrating exemplary escalation paths for various types of escalation in an exemplary embodiment of the present invention.

[0024] FIG. 7 is a flowchart illustrating an exemplary implementation of a customer call handling procedure for a customer call arising from an existing problem ticket, in an  
25 exemplary embodiment of the present invention.

[0025] FIG. 8 is a flowchart illustrating an exemplary implementation of a customer call handling procedure for a customer cold call due to something the customer found on the customer’s own network, in an exemplary embodiment of the present invention.

[0026] FIG. 9 is a flowchart illustrating an exemplary implementation of a problem workflow in an exemplary embodiment of the present invention.

[0027] **Appendix A** provides specific details pertaining to an exemplary system for the transfer of information between customer networks and gateway systems (the “Pipes Protocol”).

[0028] **Appendix B** provides possible configuration details for an exemplary embodiment of the problem and expertise management system.

[0029] **Appendix C** provides details regarding the scope and structuring of information that might be retained and utilized by an exemplary embodiment of the problem and expertise management system.

#### DETAILED DESCRIPTION OF THE INVENTION

[0030] FIG. 1 is a overview of the systems in an MSM service exemplary implementation of the present invention. FIG. 1 is divided into two portions, components and systems that operate on the customer site (that is, within the customer’s firewall) and components and systems that operate within the SOC (that is, within the SOC firewall). A single SOC can monitor and service multiple customer sites, and a single customer site can be monitored by multiple probe/sentry systems. For ease in understanding, this discussion assumes a single SOC servicing a single customer site being monitored by a single probe/sentry system.

[0031] Probe/sentry system **2000**, which can be implemented in software or hardware or a combination of software and hardware, monitors sensors attached to customer network **1000** for evidence of potential security-related events happening on network **1000**. Such sensors can include firewalls and intrusion detection systems **1010**, commercially available sensors and agents **1020**, decoys and honeypots **1030** (monitored devices or programs specifically and solely designed to attract the attention of, and thereby expose, a would-be intruder), and custom sensors and agents **1040**. More generally, probe/sentry system **2000** can monitor and collect information from any network component (whether software or hardware or a combination of both) that can be configured to send or provide to it status data (including audit log data and other audit information) concerning the status of network **1000** and its components.

[0032] Both sensors and agents can monitor network components. However, while typically a sensor passively receives status data and audit information from network

components set up to send such information to the sensor, an agent is designed to actively seek such information from the components it is monitoring. Sensors may include scanning engines, syslog data providers (including devices such as routers and firewalls), Simple Mail Transfer Protocol (“SMTP”) sensors, Simple Network Management Protocol (“SNMP”)

5 sensors and SNMP traps. SNMP sensors generally require polling and may require additional software provided by the MSM service, whereas SNMP traps generally send data directly, without prompting. Sensors and agents may be customized for the particular needs of a customer’s network, for example, to provide information not provided by those sensors and agents that are commercially available. Commercial security products and devices that may  
10 be attached to a customer’s network include the following manufacturers and products: NFR, ISS, NETA (McAfee, Gauntlet, Cybercop), NetRanger (Cisco), Dragon, Checkpoint, Lucidian, Symantec, Cisco, Nortel, 3Com, Lucent, Livingston, Tripwire and Centrax.

[0033] Probe/sentry system **2000** collects and filters (positively and/or negatively) or otherwise analyzes the constantly updated status data it receives from sensors, using a set of  
15 rules and/or filters looking for evidence or “footprints” of unauthorized intrusions. The collected status data can either remain in the customer’s hands or be provided to MSM service personnel for further analysis (e.g., cross-customer analysis). The software and filters of probe/sentry system **2000**, in a preferred embodiment, may be adaptive or, alternatively, may be manually updated offline or dynamically (that is, during actual operation). In a  
20 preferred embodiment, such updates can be sent from the SOC to the probe/sentry system and signed, verified and then securely installed. In a preferred embodiment, probe/sentry system **2000** can also manage updates to other customer software, including antivirus signature files and software, firewall software, and router software. Such updates can be controlled by communications and resource coordinator **2060** within probe/sentry system **2000**.

25 [0034] Noteworthy data possibly indicating an unauthorized intrusion or other security-related event are formatted by probe/sentry system **2000** into “sentry messages,” which are then sent via “Pipes” communications system **3000** (referred to hereafter as “Pipes **3000**”) to gateway system **4000** at the SOC.

[0035] In a preferred embodiment, Pipes 3000 provides an encrypted, secure  
30 communications path and message protocol for messages sent back and forth between probe/sentry system **2000** at the customer site and gateway system **4000** at the SOC. The Pipes protocol preferably runs inside a Transport Layer Security (“TLS”) session or other

protected path. Either side can send individual messages containing identification information and a payload. Messages, in an exemplary embodiment, can be limited to a maximum size of, for example, 64k bytes in length. Larger messages could be sent fragmented across several messages with acknowledgements. **Appendix A** provides specific technical information pertaining to an exemplary Pipes protocol.

[0036] Pipes **3000** may be used to manage bandwidth consumption at both ends and can be used by the SOC to send software updates to probe/sentry system **2000**. Message flow through Pipes **3000** can be controlled by means of (i) a client program or process running on the probe/sentry end to service queues of incoming messages from and outgoing messages to the SOC; and (ii) a server program or process running on the gateway end to service queues of incoming messages from and outgoing messages to various probe/sentry systems. In an exemplary embodiment, a public key infrastructure (“PKP”) scheme using OpenSSL-based TLS and Digital Signature Standard (“DSS”) certificates can be used to authenticate both ends of Pipes **3000** as well as the messages being passed back and forth. For example, web delivery of customer network status reports, as well as certain customer requests, might be authenticated. In addition, Pipes **3000** can include a bootstrap protocol to support its initial installation as well as a recovery protocol to support recovery in the event of a probe/sentry or gateway failure.

[0037] An exemplary architecture for Pipes **3000** is as follows. A process on the probe/sentry runs as root. This process can keep its control information in a certain directory. To send a message, another process on the probe/sentry can send this root process a Transmission Control Protocol (“TCP”) connection on, for example, 127.0.0.1 port XYZ and emit a message in “Pipes User Message Format.” A response may then be sent back to the Pipes client indicating success, failure, or enqueued. The Pipes client can maintain a context for the SOC to which it is currently connected. Possible states include “connected” and “attempting to connect.” Preferably, the Pipes client should always be connected to a SOC (or attempting to connect). The Pipes client also preferably runs a loop with selects and sleeps such that it processes input from its SOC and from clients on the local machine. The root process running on the probe/sentry can use, for example, port 443 to behave as a normal TLS (SSL) client and can also listen on port 468 (“photuris”). The root process should be started before everything else, so the probe/sentry filtering subsystem can talk to it. A process running on the gateway should listen to port 443. When it gets a call, it should fork a child process that handles the probe/sentry. There should therefore be one process per

probe/sentry, although each gateway might be associated with a few hundred or more probe/sentries. There should also be a port 468 connection to the probe/sentry system communications and resource coordinator.

[0038] Pipes **3000** may be implemented using a variety of different mechanisms, depending on the customer's needs. One possible mechanism uses a secure Internet connection implemented using, for example, a Virtual Private Network ("VPN"), SSL/TLS, Secure Shell ("SSH"), IP Security ("IPsec") or other techniques. Other alternatives include using leased lines, dial-up lines, or even wireless point-to-point systems. The most demanding customer might employ all of these, with multiple cellular connections (each with a different provider) so that a failure of one cellular provider would not result in missing an alert. In one embodiment, Internet connections could be used predominantly, with slower, alternative connections as backup in case of failure, although some customers might want high priority alerts to be delivered over a cellular link so as not to reveal information to an attacker.

[0039] Additional security considerations for Pipes **3000** include the following:

- use of TLS
- authentication handles based on, for example, signatures
- PKI bootstrap
- threat model
- losses of connections to Sentry or Gateway
- Sentry or Gateway integrity compromises

[0040] Additional possible alternative implementations of Pipes **3000** include the following:

- use of *openssl s\_server* and *s\_client* as skeletons
- use of dss' certificates
- use of *redfish* in place of triple data encryption standard ("TDES") as encryption algorithms
- bandwidth manager last
- dump messages in input queue for starters

- syslog interface

[0041] Sentry messages sent by probe/sentry system **2000** through Pipes **3000** are received by gateway system **4000** at the SOC and transformed into gateway messages. Such transformation may include reformatting of the data in the sentry messages and/or appending of additional data. (TABLES 6 and 8 of **Appendix C** provide forms which might be incorporated into SOCRATES **6000** for storing information regarding formatting of messages sent to and from various gateway systems **4000**.) The gateway messages are then forwarded, via internal network **5000**, on to problem and expertise management (“SOCRATES”) system **6000** (hereafter referred to as “SOCRATES **6000**”). Gateway system **4000**, as well as SOCRATES system **6000**, can be implemented in software or hardware or a combination of software and hardware.

[0042] SOCRATES **6000** manages the problem resolution process, including (i) storing, managing and processing various kinds of information useful for problem resolution and response; and (ii) generating, from received gateway messages and other information, “problem tickets” representing potential security-related happenings on the customer’s network. The kinds of information managed by SOCRATES **6000**, which can be stored in various databases **6020**, can include security intelligence, customer information, and problem resolution information. TABLE 1 of **Appendix C** provides a more detailed listing of the types of databases which might be employed in an embodiment of SOCRATES **6000**. TABLES 2-19 of **Appendix A** provide possible information which might be incorporated into such databases.

[0043] MSM service security analysts receive problem tickets for handling access information useful for problem investigation, resolution and response, and otherwise interface with SOCRATES **6000** via security analyst consoles **6010**. For security reasons, consoles **6010** can be configured so that a given security analyst can have only a limited ability to look at data and/or perform tasks (for example, the security analyst might be given access to only the keyboard and monitor of each terminal and/or token-based authentication might be required for access to systems). In an exemplary embodiment, each security analyst at a SOC sits at a console **6010**, and each console **6010** has three terminals, two secure internal SOC terminals and one secure external terminal. The external terminal can provide secure access to the Internet and to the MSM service’s corporate network. The internal SOC terminals can be connected to secure, fully-redundant computers containing, among other things,

SOCRATES **6000**, a web browser for internal pages, an operations guide, and training materials. Depending on requirements, software for consoles **6010** could be written in Java for easy porting to a wide variety of hardware or be based on certain preexisting commercially available software (for example, automated call database software).

- 5    **[0044]**   The operation of SOCRATES **6000** can be controlled by operating procedures **6030**, which can be tailored to specific customers' needs. Such operating procedures can include, for example, specifying which customer contacts should be notified about what types of events during which hours of the day and how to respond to certain types of attacks.

(TABLE 4 of **Appendix C** suggests a database form capable of providing such information.)

- 10   **Workflow** functionality and business rules may also be developed using the SOCRATES system. Such rules can be implemented, for example, using a combination of active links, macros and filters. (TABLES 20-22 of **Appendix C** provide examples of possible resources that might be implemented on an embodiment of SOCRATES **6000**.)

- [0045]**   SOCRATES **6000** can generate a variety of reports for customers or internal use through report generation module **6040**. For example, a current report may be sent to and accessed directly from probe/sentry system **2000**. This report can be web-based and can include the status of the probe/sentry system, the status of open tickets and detailed log information. A weekly report could include incident summaries, open ticket summaries, details on critical and suspicious events, and sensor reports, and could be emailed to the primary customer contact. The weekly report could also include trend analysis of data covering monthly, quarterly and "to-date" data collections and could contain a variety of report sections, including ticket summary (including accumulation of events by type for the week, month, quarter, year), critical tickets summary, top ten events (including weekly, monthly, broken down by event type), known attackers list, top ten targets list, IP watch list (including attack occurrences broken down by day and time), probe/sentry statistics, and known device list.

- [0046]**   Report formats can include paper, email or web-based delivery in approximately real time. For security reasons, in a preferred embodiment, web-based connections for delivery of reports can be cryptographically protected, and sending and receipt of such reports authenticated using digital certificates.

**[0047]**   SOCRATES **6000** can send alerts **6050** to MSM service personnel or customer contacts. Such alerts can be delivered by a wide variety of means including email, pager,

telephone and cellular phone depending on a variety of factors, including the customer's needs, the configuration of the MSM service for the particular customer and contractual terms in a service level agreement. In a preferred embodiment, SOCRATES **6000** can maintain audit logs of all alerts issued, for tracking and other purposes.

5    **[0048]** FIG. 2 is a system overview of an exemplary embodiment of a probe/sentry system. One or more such systems can be installed at each customer site to monitor the customer's network and network components. (A database of all network components monitored by such probe/sentry systems may be stored by SOCRATES **6000** in a database similar to that suggested in TABLE 7 of **Appendix C**.) Data collected by sensors **1010**, **1020**, **1030** and  
10   **1040** (note that four sensors are shown solely by way of example and are not meant to limit the scope of the invention) are collated by sensor data collator **2010**. Once collated, the data is first filtered by negative filtering subsystem **2020**, which discards uninteresting information, and then by positive filtering subsystem **2030**, which selects possibly interesting information and forwards it to communications and resource coordinator **2060**. Data neither  
15   discarded by negative filtering subsystem **2020** nor selected out as interesting by positive filtering subsystem **2030** form the "residue," which is sent to anomaly engine **2050** for further analysis. Anomaly engine **2050** determines what residue information may be worthy of additional analysis and sends such information to communications and resource coordinator **2060** for forwarding to the SOC. Negative filtering, positive filtering, and residue analysis  
20   are examples of data discrimination analyses, other types of which are well-known to those skilled in the art.

**[0049]** Communications and resource coordinator **2060** creates sentry messages out of the interesting status data and forwards those messages on to gateway system **4000** via Pipes **3000**. In a preferred embodiment, each sentry message has a sentry identification number  
25   (uniquely identifying the sending sentry) as well as a message identification number (identifying the type of problem). (TABLE 6 of **Appendix C** suggests other information that might be included in such a message.) Communications and resource coordinator **2060** can also manage software updates to probe/sentry system **2000**, such as updates to filtering subsystems **2020** and **2030**, sent by the SOC. Communications and resource coordinator  
30   **2060** can also monitor a "heartbeat" passing between probe/sentry system **2000** and gateway system **4000**.

[0050] Pipes client 3010 on the probe/sentry end handles sentry messages generated by communications and resource coordinator 2060 and sends those messages through Pipes 3000 on to gateway system 4000. Pipes client 3010 also services queues of incoming messages from and outgoing messages to the SOC.

5 [0051] Customer reporting subsystem 2040 allows a customer to, among other things, check the status of problems that are being worked on by security analysts at the SOC. The SOC can have the ability to push web pages onto probe/sentry system 2000 at the customer's site via Pipes 3000. These pages then are directed by communications and resource coordinator 2060 to customer reporting subsystem 2040. Preferably, a customer, once  
10 authenticated, can view such pages using any browser.

[0052] Network response subsystem 2070 can, among other things, process and execute requests originating from the SOC designed to mitigate or, terminate various attacks. For example, network response subsystem 2070 might be requested by the SOC via Pipes 3000 to not allow a certain IP address to access the customer's network for the next 10 minutes. Such  
15 a "fix" might be sufficient to stop a transient attack, such as someone repeatedly trying to log in to the customer's network.

[0053] Execution integrity monitor 2080 (which may have a redundant backup) monitors the functioning of each of the components of probe/sentry system 2000 and communicates with the SOC via Pipes 3000 in the event that it detects any malfunction.

20 [0054] FIG. 3 is a system overview of an exemplary embodiment of a gateway system. Sentry messages from probe/sentry system 2000, travel through Pipes 3000, arrive first at Pipes server 3020 (which manages queues of messages incoming from and outgoing to various probe/sentry systems) and then are passed to communications and management coordinator 4020. Sentry update manager 4010 manages updates, such as software and/or  
25 filter updates, to probe/sentry system 2000. Communications and management coordinator 4020 converts sentry messages into gateway messages. Analyst problem reporting interface 4040 then passes these gateway messages on to SOCRATES 6000 via internal network 5000.

[0055] FIG. 4 is a system overview of an exemplary embodiment of a "SOCRATES" problem and expertise management system. The SOCRATES system is a consolidated  
30 system used to manage customers' problems and the supporting data helpful in resolving such problems. It provides security analysts at a SOC a single, integrated system with which to track information concerning, for example, problems, companies, people, contacts, tools,

and installed network components and known vulnerabilities. In an exemplary embodiment, the SOCRATES system can include the following capabilities:

- communications with probe/sentry systems;
- email integration;
- 5     • access and authority management;
- escalation and notification management;
- report development;
- probe/sentry management through gateway systems;
- distributed database;
- 10    • generation of web-based reports;
- addition of servers (as required);
- call desk/telephone system integration;
- paging integration; customer surveys; and service level agreement functionality.

[0056] In an exemplary implementation, processing of gateway messages by SOCRATES

15    **6000** proceeds as follows. Gateway messages arrive at SOCRATES **6000** from gateway system **4000** via internal network **5000**. SOCRATES **6000** first creates from these gateway messages “event records,” which can be stored in problem/event database **6021**. Event records may then be linked with other event records stored in problem/event database **6021** and with information from a variety of databases (including customer information from client information database **6022** and problem resolution information from problem/event resolution database **6023**) to form “problem tickets,” which are then opened and displayed on security analyst consoles **6010** to security analysts for handling. (Appendix C provides more detail on information that might be included in the client information database **6022** (see TABLES 3, 4, 7, and 9), the problem/event resolution database **6023** (see TABLES 13, 14, 18, and 19) , and problem tickets (see TABLE 10)). Alternatively, event records reflecting a problem already reflected in an existing and open problem ticket may simply be linked to such open ticket. Redundancy of the SOCRATES system may be achieved by connecting

SOCRATES **6000** to SOCRATES Duplicate **8000** via secure private network connection **7000**.

[0057] Problem/event resolution database **6023** can include, among other things, a database of vulnerabilities. Such a database of vulnerabilities can contain a table or “form” having an entry for each known vulnerability. Vulnerability intelligence may be developed in-house or acquired from outside sources and maintained within the SOCRATES system. In the event vulnerability information from more than one outside source is duplicative or conflicting, the SOCRATES system can maintain a table or “form” for each vendor of vulnerability information. For a more detailed description of possible embodiments, refer to TABLES 11 and 17 in **Appendix C**.

[0058] FIG. 5 is a flowchart showing an exemplary implementation of incident handling by a security analyst. In step **500**, a security analyst is notified by his or her console that a problem ticket has arrived. In step **505**, the security analyst picks up the ticket, and in step **510**, he or she begins to investigate it. If more information is needed from the customer (step **515**), the analyst can contact the customer to get such information (step **520**). (A preferred embodiment of the invention may contain forms that provide pertinent information about the customer and its contacts, as provided by way of example in TABLES 3, 4 and 9 of **Appendix C**). Otherwise, in step **525**, the analyst determines whether he or she can handle the ticket or whether the ticket needs to be escalated. If the ticket needs to be escalated (step **530**), the ticket can be transferred to another analyst (or security engineer) for investigation (step **510**). Once an analyst (or security engineer) is capable of handling the ticket, he or she determines, in step **535**, the symptoms, vulnerabilities and recommended solutions associated with the ticket. For example, the analyst (or security engineer) may use SOCRATES **6000** to match the observed symptoms of the attack to a known vulnerability. The analyst (or security engineer) can then search SOCRATES **6000** and its associated security intelligence and other databases for possible solutions. In step **540**, the analyst (or security engineer) determines an appropriate response level, and in step **545**, he or she initiates such a response.

[0059] By knowing the vulnerability, a security analyst should be able to properly respond to the customer, at a response level commensurate with the severity level of the incident. In a preferred embodiment, responses should be predetermined to the extent possible (for example, effective responses to identical incidents in the past can be repeated) in order to shorten response time. For security reasons, in a preferred embodiment, all

customer communications should be initiated from within the SOC. Responses to events of differing severity levels might proceed as follows:

Interesting Events: The customer is provided online and/or weekly reports.

Security-Relevant Events: The security analyst sends an encrypted email alert to the customer contact detailing the type of event, ticket number, symptoms, vulnerability and possible solutions for resolving the incident. The email alert can also include a URL to a secure website where the customer (after authentication) can access further detailed information.

Suspicious Events: The security analyst initiates a phone call to the customer contact. If the customer contact is not available, the analyst leaves a message and proceeds to call the next customer contact. Once a customer contact is on the phone with the security analyst, a customer contact authentication process begins. If authentication is successful, the security analyst can inform the customer of the incident and offer solutions to resolve the problem. An encrypted e-mail message can also be sent to the customer informing him of the incident and possible solutions.

Critical Events: The security analyst initiates a phone call to the customer contact. If customer contact is not available, the analyst leaves a message and proceeds to call the next customer contact. Once a customer contact is on the phone with the security analyst, a customer contact authentication process can begin. If authentication is successful, the security analyst can inform the customer of the incident and offer solutions to resolve the problem. After speaking with the primary contact, the security analyst can initiate another phone call to the customer management contact. The analyst can then inform the customer management contact about the incident and relate to whom the analyst previously reported the incident. An encrypted e-mail message can also be sent to the customer contact and customer management contact informing them of the incident, possible solutions and whom the analyst contacted about the incident.

**[0060]** Once the problem has been dealt with and resolved, the analyst, in step **550**, enters details of the incident, along with the associated symptoms, vulnerabilities and solutions into SOCRATES **6000** and then closes the ticket (step **555**). (TABLES 12, 17, and 5 of **Appendix C** provides more detail on information that might be included regarding symptoms, vulnerabilities, and diagnoses, respectively.)

[0061] Following ticket closure (for example, one or two days later), MSM service customer service personnel can send to the customer an incident survey to get the customer's comments regarding how the incident was handled. In addition, a phone call may be placed to customers whose tickets were critical in nature to make sure the incident was resolved and to get a final "all clear." When all issues have been resolved, customer service can stamp a complete closure on the ticket. An authenticated customer acknowledgment can be required before a critical or suspicious ticket is closed. If unresolved issues are discovered or there are problems that occurred due to the solutions provided by the security analyst, customer service can immediately reopen the ticket, route the call to a security engineer, and inform the appropriate SOC manager that the ticket needs immediate handling.

[0062] FIG. 6 is a diagram illustrating exemplary escalation scenarios for various types of escalation (incident, customer service and technical support) in an exemplary embodiment of the present invention. For problem resolution purposes, an incident may be escalated from security analysts to senior security analysts to security engineers and finally to the network intelligence and engineering organizations of the MSM service itself. Where customer service issues arise, escalation may proceed from the security analysts to the customer service organization of the MSM service to MSM service and customer management. Where technical support issues arise, escalation may proceed from a security engineer to the network intelligence and engineering organizations of the MSM service to the customer service organization of the MSM service. If necessary, customer service can coordinate with MSM service and customer management to arrange for outsourced field engineering personnel to provide any necessary technical support, including on-site support.

[0063] Escalations are primarily intended to prevent open problems from going unrecognized. Escalation procedures should therefore be designed to identify those open problems that may have been overlooked or that require additional attention. Ideally, the number of open problems that satisfy this condition should be relatively low and represent the exception rather than the rule.

[0064] Escalations may be of various types, including time-based and event-driven. Time-based escalations can be intended to capture problems that have remained in a particular state beyond a specified period of time. Event-based escalations can be designed to trigger immediately when a predefined condition is met. When escalation criteria are met, workflow procedures can be defined to perform one or more actions. Examples of such actions include:

- sending notification of the problem to the appropriate group or individual;
  - reassigning the problem;
  - escalating from first level support to second level support to manager of the day;
  - escalating to upper management;
- 5      • generating a report for the problem; and
- incrementing or decrementing the priority of the problem.

[0065] In the case of a time-based escalation, guidelines may be established for the maximum amount of time that a problem can remain unresolved before specific actions are taken. Normally, a solution cannot be guaranteed within a specific time frame but, in a preferred embodiment, support personnel can represent that within a certain amount of time, the problem will either be resolved or escalated by bringing additional resources to bear.

[0066] Escalation procedures can help ensure that the time frames for problem resolution are being met and that no problem remains unresolved. These timeframes can be built into the SOCRATES system with predetermined triggers that automatically escalate an incident based on the length of time it goes without valid resolution. For example, escalation in the form of notifying the assigned-to group might be required if a problem remains in an “open” or “assigned” state for longer than 60 minutes.

[0067] Operating procedures for the MSM service can also include procedures for handling incoming calls of various types. Possible call types can include incident-related calls, customer service related calls, technical support-related calls and sales related calls. Incident related calls can include customer callbacks due to an existing problem ticket (for example, returning a security analyst’s call, calling regarding ticket closure or calling requesting more support on an incident) and customer cold calls (for example, reporting an incident not flagged by the probe/sentry system and sent to the SOC).

[0068] FIG. 7 is a flowchart illustrating an exemplary implementation of a customer call handling procedure for a call arising from an existing problem ticket. In step 700, an incoming call is screened by a customer service representative or an analyst. In one embodiment, incoming calls during business hours could be first answered by a customer service representative, while calls after business hours could be directly routed to security analysts at the SOC. In step 705, the representative or analyst gathers information about the

customer and the nature of the call. In step 710, the call is transferred to the analyst who originally responded to the problem ticket, if he or she is available (step 715). If not, the customer may be given a choice to leave a message for the originating analyst .or be routed to another available security analyst within the same SOC (step 720). If another analyst is  
5 available at the same SOC (step 725), he or she can process the ticket (step 730). Otherwise, the customer can be routed to an analyst at another SOC, who will then process the ticket (step 735). After processing is complete, the ticket is closed (step 740).

**[0069]** FIG. 8 is a flowchart illustrating an exemplary implementation of a customer call handling procedure for a cold call resulting from an event that a customer has found on its  
10 own network. In step **800**, the call is screened by a customer service representative or analyst, who, in step **805**, gathers information about the customer and the nature of the call. In a preferred embodiment, the call is then transferred to the customer's home SOC. If there is no available security analyst in the customer's home SOC, the call may be routed to an available security analyst in another SOC. In step **810**, the analyst checks the appropriate  
15 SOCRATES database to make sure there are no open or closed tickets for the incident being reported. If there is an open ticket (step **815**), the analyst will proceed to process the ticket (step **820**). If there are no open or closed tickets pertaining to this incident, the analyst will proceed to open a new ticket (step **825**). In step **830**, the analyst gathers information from and authenticates the customer. In step **835**, the analyst gathers symptom information. In  
20 step **840**, the analyst determines whether he or she can handle the ticket. If not, the ticket may be escalated to the next level in accordance with FIG. 6, for example, to a security engineer (step **845**). In step **850**, the analyst (or security engineer) analyzes the ticket and matches symptoms to vulnerabilities to possible solutions. In step **855**, the analyst (or security engineer) calls the customer to provide possible solutions, and, in step **860**, places  
25 the customer in a "watch state." In step **865**, the analyst (or security engineer) tries to determine from the information provided by the customer why the probe/sentry system on the customer's site failed to capture the event, and, in step 870, he or she informs the next level escalation of any problem with the functioning of the probe/sentry system. In 875, the analyst (or security engineer) determines whether the solutions provided have solved the  
30 problem and whether the customer is now in an "all clear" state. If yes, in step **880**, the ticket can be closed.

**[0070]** Customer service related calls can include customer relationship calls (for example, customer complaints, customer comments, and other customer satisfaction related calls),

change management calls (for example, requests to change contact information, requests to change filters, requests to add or remove services, requests or notifications regarding movement of equipment and change orders) and information requests (for example, questions regarding current services, report requests, services requests and questions regarding future services). Customer service related calls may be processed similarly to other calls. In an exemplary embodiment, processing of customer service related calls could begin with opening a ticket. Customer service personnel would then gather information from the customer for authentication and then process the ticket according to the customer's needs. If the call required escalation, customer service could escalate the call to the appropriate team or management person best suited to handle the situation. Customer service would then follow up with the team or management person until the situation was resolved. At this point, the ticket could be closed.

**[0071]** Technical support related calls can include (i) customers calling the SOC for general support of their security devices and (ii) customers calling the SOC due to failures in their networks resulting from solutions provided by the SOC. An exemplary response protocol for the first type of call might be as follows: First, the security analyst opens a ticket, gathers all customer information required, and notes any questions the customer may have. The security analyst then determines if he or she can handle all of the customer's inquiries. If not, the ticket is escalated to a security engineer. The security analyst or security engineer then will answer all of the customer's questions to the best of their ability. If the customer requires in-depth product support of a product not supplied by the MSM service, the security analyst or security engineer can advise the customer to contact the manufacturer of the product for more detailed technical support. At this point, the security analyst or security engineer can proceed to close the ticket.

**[0072]** An exemplary response protocol for the second type of technical support related call might be as follows: Any call from a customer reporting a network failure due to a solution provided by the MSM service can immediately be escalated to a security engineer. The security engineer will help the customer to the best of his or her ability. If the security engineer cannot help the customer over the phone and the customer requires an on-site visit, the ticket is escalated to customer service. Customer service then determines how best to serve the customer. The ticket may require a security engineer to go to the customer's site. Alternatively, the ticket may be referred to a business partner of the MSM service for an on-site visit. When an "all clear" signal is received from the customer, customer service will

proceed to close the ticket, prior to which all details about the incident and responses, including any solutions implemented, should be logged into SOCRATES **6000**.

[0073] Sales related calls can include calls from potential customers inquiring about the MSM service. Such calls may be processed similarly to other calls. In an exemplary embodiment, processing of an incoming sales call could start with opening a ticket. The customer service representative or security analyst should gather information from the new or potential customer and forward it to sales. The security analyst or customer service representative should also log the name of the sales representative and the time and date the call was referred to sales.

[0074] FIG. 9 is a flowchart illustrating, in greater detail, an exemplary implementation of the problem ticket generation and handling process. In step **900**, the probe/sentry sends information about noteworthy events on the customer's network, in the form of sentry messages, to the gateway system at the SOC. Each sentry message is tagged with a sentry identification number ("sentry ID") and a message identification number ("message ID"). Message IDs reflect the nature of events happening on the customer's network, such that substantially identical events (for example, multiple incorrect logins to the same server) will result in identical message IDs.

[0075] In step 902, a gateway message or "event record," still tagged with the same sentry ID and message ID, is created by the gateway system at the SOC. In step **904**, a decision can be made to create a new problem ticket if the severity of the gateway message/event record is greater than some threshold (for example, "interesting") and the sentry ID and the message ID are different from that of any already opened problem ticket. If the sentry ID and message ID are identical to that of an already opened problem ticket, a message will, in step **906**, be written to an event log and the aggregation count associated with the particular problem ticket will be incremented by one.

[0076] In step 910, a problem ticket is created. In a preferred embodiment, the majority of problem tickets will be created automatically by SOCRATES **6000** as a result of gateway messages spawned by sentry messages sent from the probe/sentry system. Problem tickets may also be created manually (step **908**) by a security analyst or other SOCRATES operator using a SOCRATES form. The status of problem ticket may be set to one of a number of states. Once created, the status of the problem ticket is set to "open" (step 912) and, in step 914, the default assigned-to group is notified. In step **916**, if the problem ticket cannot be

assigned, an escalation notification is generated, in step **918**, and assignment is reattempted. Once assigned, the status of the problem ticket is set, in step **920**, to “assigned.” In step 922, if the assigned security analyst (or “operator”) is not working on the problem, the problem can be escalated, in step 924, until the problem is being worked on, at which point the status is set, in step 926, to “in progress.” In step **928**, the security analyst checks customer contact information, vulnerability information and previous cases involving similar incidents in a search for possible solutions. In step 930, the security analyst decides whether communication with a customer contact is necessary. If yes, in steps 932, 934 and 936, the security analyst tries to reach the customer contact through various avenues until he or she is successful or all avenues have been exhausted. If all avenues have been exhausted, the ticket status is set, in step 938, to “pending,” and the security analyst will check such pending tickets periodically (step 940). If the security analyst is able to reach the customer contact or communication with the customer is unnecessary, problem resolution can continue. The security analyst works on the problem until the problem is ready to resolve (step 942). During this time, the status of the problem ticket is set by the operator or analyst to “ongoing” (steps 944 and **946**). Once the problem is ready to resolve, the security analyst changes the status of the problem to “resolved” (steps 948 and **950**). In step 952, the ticket is closed, either automatically, by escalation setting the status to “closed” (step **954**) or manually, by the security analyst setting the status to “closed” (step 956). In step **958**, the ticket is closed.

#### **[0077] Modifications, Enhancements and Alternate Embodiments**

**[0078]** The foregoing has described various aspects of an exemplary implementation of the present invention, directed at monitoring, detecting and responding to computer network intrusions. Those skilled in the art will realize, however, that the present invention is usable generally for (i) monitoring of any system; (ii) filtering the data from the monitoring for noteworthy events happening in or affecting any system; (iii) alerting human beings to any such noteworthy events; and (iv) providing for a response by human beings to any such alert.

**[0079]** As one example, the present method could be applied to providing security monitoring, detection and response for a residence or business. For example, such a service might monitor alarm or other status data, filter such data for security-related events, alert a human being upon such a security-related event, and provide for a human response to the alert.

[0080] Therefore, it is intended that the scope of the invention be limited only by the claims appended below.

WHAT IS CLAIMED IS:

1                   1.       A method of operating a probe as part of a security monitoring system  
2 for a computer network, comprising:

3                   a)       collecting status data from at least one monitored component of said  
4 network;

5                   b)       identifying potentially security-related events pertaining to said  
6 network by analyzing said status data;

7                   c)       transmitting information about said identified events to an analyst  
8 associated with said security monitoring system;

9                   d)       receiving feedback at the probe based on empirically-derived  
10 information reflecting operation of said security monitoring system in a manner customized  
11 to said network; and

12                  e)       dynamically modifying an analysis capability of said probe during  
13 operation thereof based on said received feedback in a manner customized to said network.

1                   2.       The method of claim 1, wherein said identifying step includes  
2 performing a multi-stage analysis of said status data.

1                   3.       The method of claim 2, wherein said multi-stage analysis includes  
2 performing a discrimination analysis on said status data.

1                   4.       The method of claim 3, wherein the discrimination analysis includes  
2 positive filtering.

1                   5.       The method of claim 3, wherein the discrimination analysis includes  
2 negative filtering.

1                   6.       The method of claim 3, wherein the discrimination analysis includes  
2 filtering followed by an analysis of post-filtering residue.

1                   7.       The method of claim 2, wherein said multi-stage analysis includes  
2 analysis at the probe and analysis at a secure operations center configured to receive data  
3 from said probe.

- 1                   8.       The method of claim 1, wherein said identifying step includes  
2 aggregating and synthesizing said status data at the probe.
- 1                   9.       The method of claim 8, wherein said identifying step includes cross-  
2 correlating data across said monitored components.
- 1                   10.      The method of claim 8, wherein said identifying step includes  
2 analyzing the frequency of occurrence of said events.
- 1                   11.      The method of claim 1, further comprising after said step (c),  
2 performing further computer-based analysis at a secure operations center configured to  
3 receive data from said probe.
- 1                   12.      The method of claim 11, wherein said computer-based analysis  
2 includes aggregating, synthesizing, and presenting alerts on an ensemble basis.
- 1                   13.      The method of claim 11, wherein said identifying step includes cross-  
2 correlating data across said monitored components.
- 1                   14.      The method of claim 11, wherein said identifying step includes  
2 analyzing the frequency of occurrence of said events.
- 1                   15.      The method of claim 11, wherein said computer-based analysis  
2 includes cross-probe correlation.
- 1                   16.      The method of claim 1, further comprising instantaneously self-tuning  
2 said probe based on previously collected status data.
- 1                   17.      The method of claim 1, wherein said dynamic modifying step includes  
2 consideration of non-real-time information from ongoing security research efforts.
- 1                   18.      The method of claim 1, wherein said receiving feedback step occurs in  
2 substantially real time.
- 1                   19.      A computer-readable medium whose contents cause a computer system  
2 to operate a probe as part of a security monitoring system for a computer network, by  
3 performing “the steps of:

- a) collecting status data from at least one monitored component of said network;
- b) identifying potentially security-related events pertaining to said network by analyzing said status data;
- c) transmitting information about said identified events to an analyst associated with said security monitoring system;
- d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system in a manner customized to said network; and
- e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback in a manner customized to said network.

20. The computer-readable medium of claim 19, wherein said identifying step includes performing a multi-stage analysis of said status data.

21. The computer-readable medium of claim 20, wherein said multi-stage analysis includes performing a discrimination analysis on said status data.

22. The computer-readable medium of claim 21, wherein the discrimination analysis includes positive filtering.

23. The computer-readable medium of claim 21, wherein the discrimination analysis includes negative filtering.

24. The computer-readable medium of claim 21, wherein the discrimination analysis includes filtering followed by an analysis of post-filtering residue.

25. The computer-readable medium of claim 20, wherein said multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from said probe.

26. The computer-readable medium of claim 19, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

27. The computer-readable medium of claim 26, wherein said identifying step includes cross-correlating data across said monitored components.

1                   28.     The computer-readable medium of claim 26, wherein said identifying  
2 step includes analyzing the frequency of occurrence of said events.

1                   29.     The computer-readable medium of claim 19, further comprising after  
2 said step (c), performing further computer-based analysis at a secure operations center  
3 configured to receive data from said probe.

1                   30.     The computer-readable medium of claim 29, wherein said computer-  
2 based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble  
3 basis.

1                   31.     The computer-readable medium of claim 29, wherein said identifying  
2 step includes cross-correlating data across said monitored components.

1                   32.     The computer-readable medium of claim 29, wherein said identifying  
2 step includes analyzing the frequency of occurrence of said events.

1                   33.     The computer-readable medium of claim 29, wherein said computer-  
2 based analysis includes cross-probe correlation.

1                   34.     The computer-readable medium of claim 19, further comprising  
2 instantaneously self-tuning said probe based on previously collected status data.

1                   35.     The computer-readable medium of claim 19, wherein said dynamic  
2 modifying step includes consideration of non-real-time information from ongoing security  
3 research efforts.

1                   36.     The computer-readable medium of claim 19, wherein said receiving  
2 feedback step occurs in substantially real time.

1                   37.     A security monitoring system for a computer network, comprising  
2 a) a plurality of sensors for monitoring components of said network;  
3 at least one secure operations center configured to receive and analyze  
4 potentially security-related event data from at least one probe; and  
5 at least one probe, wherein said probe is configured to  
6 collect status data from at least one sensor monitoring at least one component  
7 of said network;

8                    identify potentially security-related events pertaining to said network by  
9   analyzing said status data;  
10                  transmit information about said identified events to an analyst associated with  
11   said secure operations center;  
12                  receive feedback based on empirically-derived information reflecting  
13   operation of said security monitoring system in a manner customized to said network; and  
14                  dynamically modify an analysis capability of said probe during operation  
15   thereof based on said received feedback in a manner customized to said network.

1                  38.     The security monitoring system of claim 37, wherein said probe is  
2   configured to identify potentially security-related events by performing a discrimination  
3   analysis on said status data.

1                  39.     The security monitoring system of claim 38, wherein said probe is  
2   configured to identify potentially security-related events by performing a positive filter  
3   discrimination analysis on said status data.

1                  40.     The security monitoring system of claim 38, wherein said probe is  
2   configured to identify potentially security-related events by performing a negative filter  
3   discrimination analysis on said status data.

1                  41.     The security monitoring system of claim 37, wherein said probe and  
2   said secure operations center are configured to identify potentially security-related events by  
3   performing a multi-stage analysis of said status data.

1                  42.     The security monitoring system of claim 41, wherein said multi-stage  
2   analysis includes analysis at the probe and analysis at said secure operations center.

1                  43.     The security monitoring system of claim 37, wherein' said secure  
2   operations center is configured to identify potentially security-related events by performing a  
3   computer-based analysis of said potentially security-related event data received from said  
4   probe.

1                  44.     The security monitoring system of claim 43, wherein said computer-based  
2   analysis is configured to correlate data from different probes.

## **METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE**

### **ABSTRACT OF THE DISCLOSURE**

A probe attached to a customer's network collects status data and other audit information from monitored components of the network, looking for footprints or evidence of unauthorized intrusions or attacks. The probe filters and analyzes the collected data to identify potentially security-related events happening on the network. Identified events are transmitted to a human analyst for problem resolution. The analyst has access to a variety of databases (including security intelligence databases containing information about known vulnerabilities of particular network products and characteristics of various hacker tools, and problem resolution databases containing information relevant to possible approaches or solutions) to aid in problem resolution. The analyst may follow a predetermined escalation procedure in the event he or she is unable to resolve the problem without assistance from others. Various customer personnel can be alerted in a variety of ways depending on the nature of the problem and the status of its resolution. Feedback from problem resolution efforts can be used to update the knowledge base available to analysts for future attacks and to update the filtering and analysis capabilities of the probe and other systems.

60895773 v1

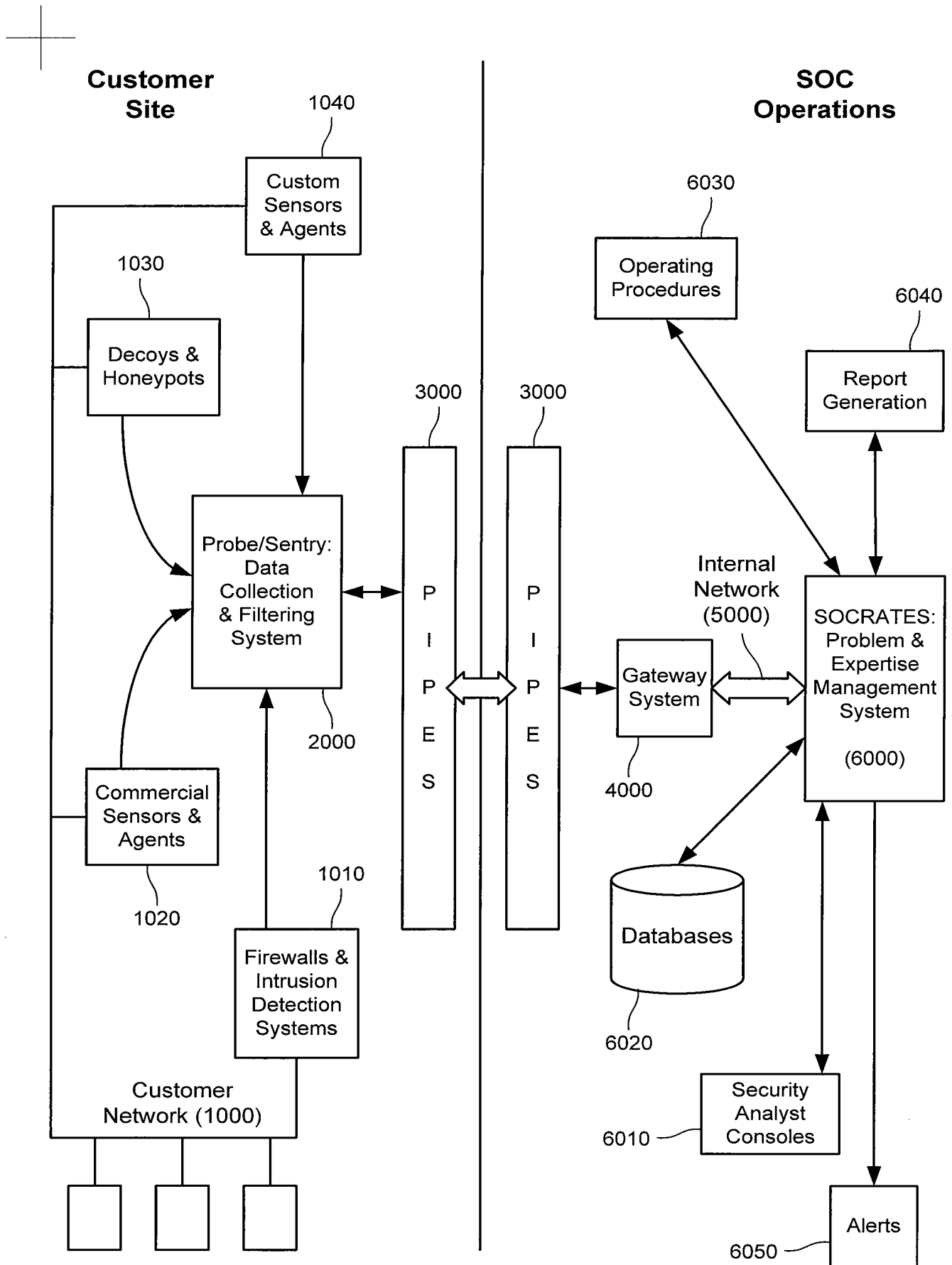


FIG. 1

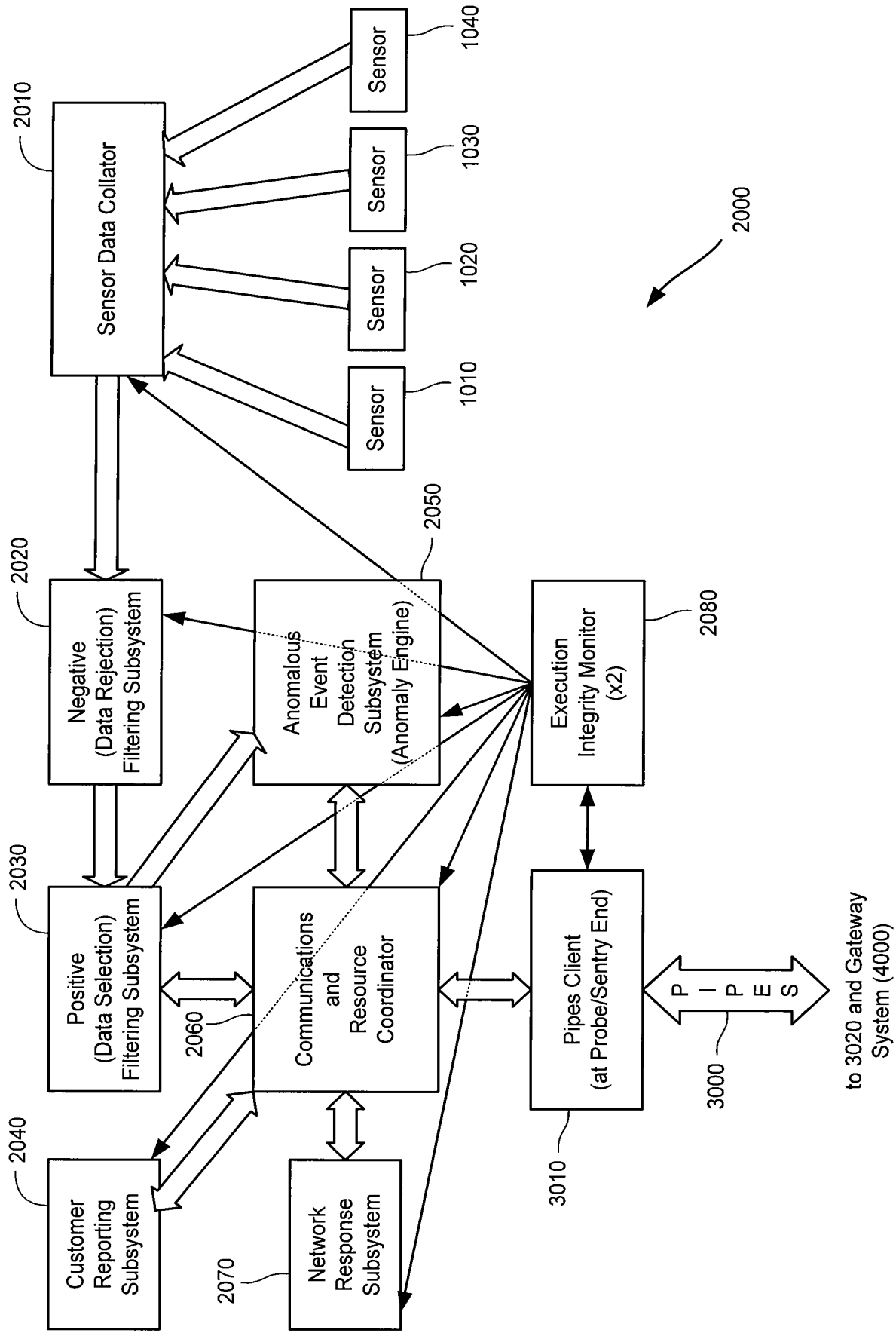


FIG. 2

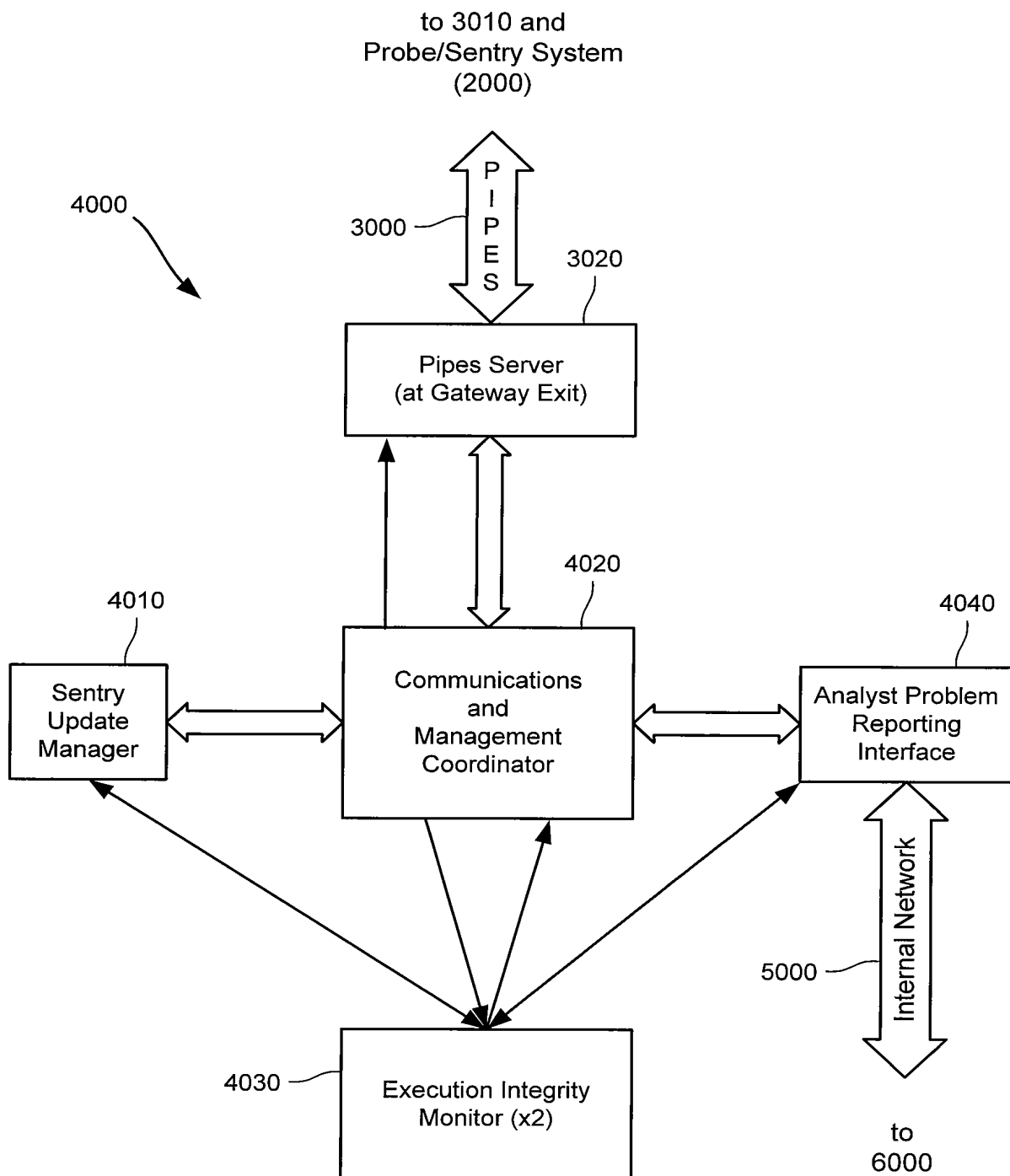


FIG. 3

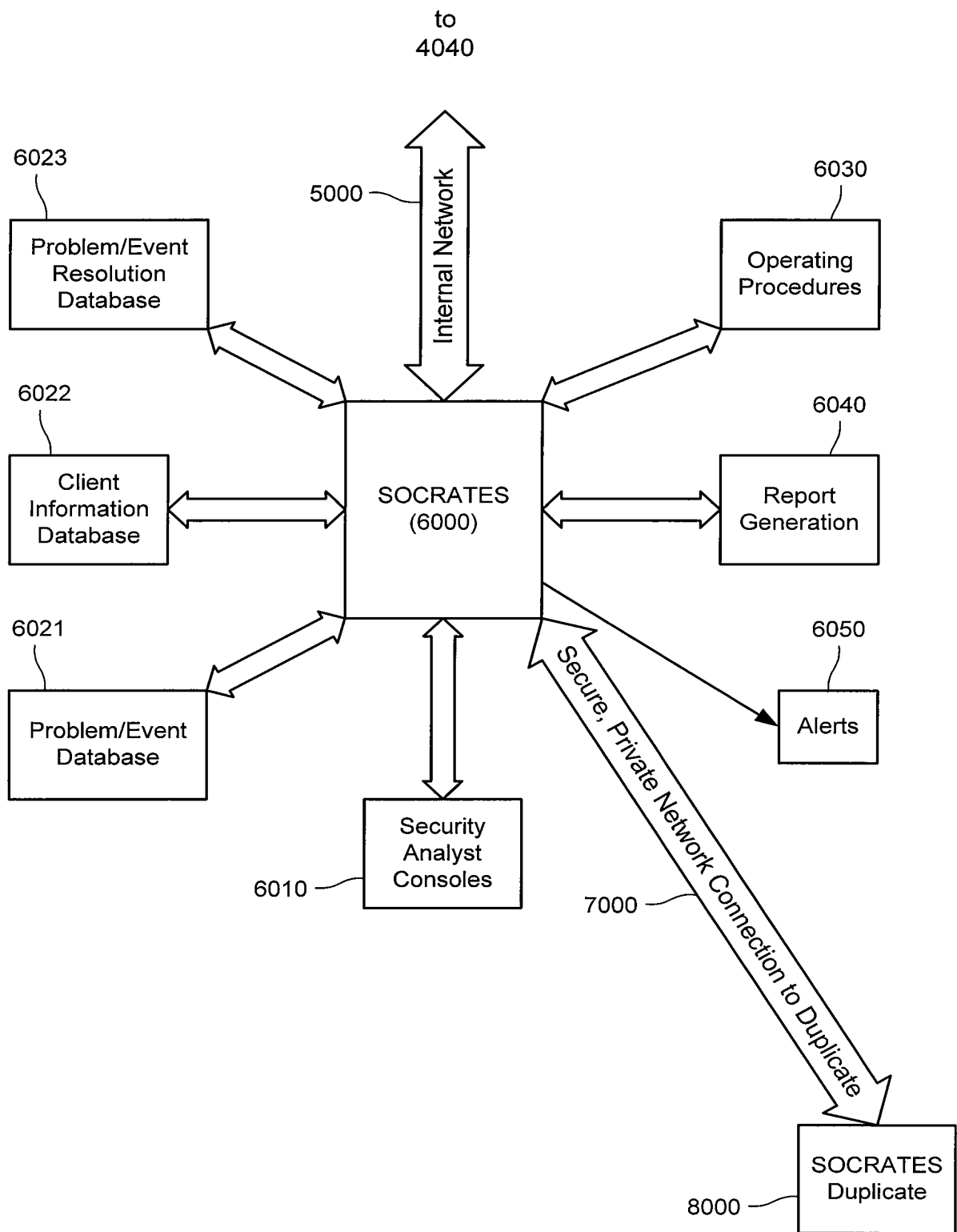


FIG. 4

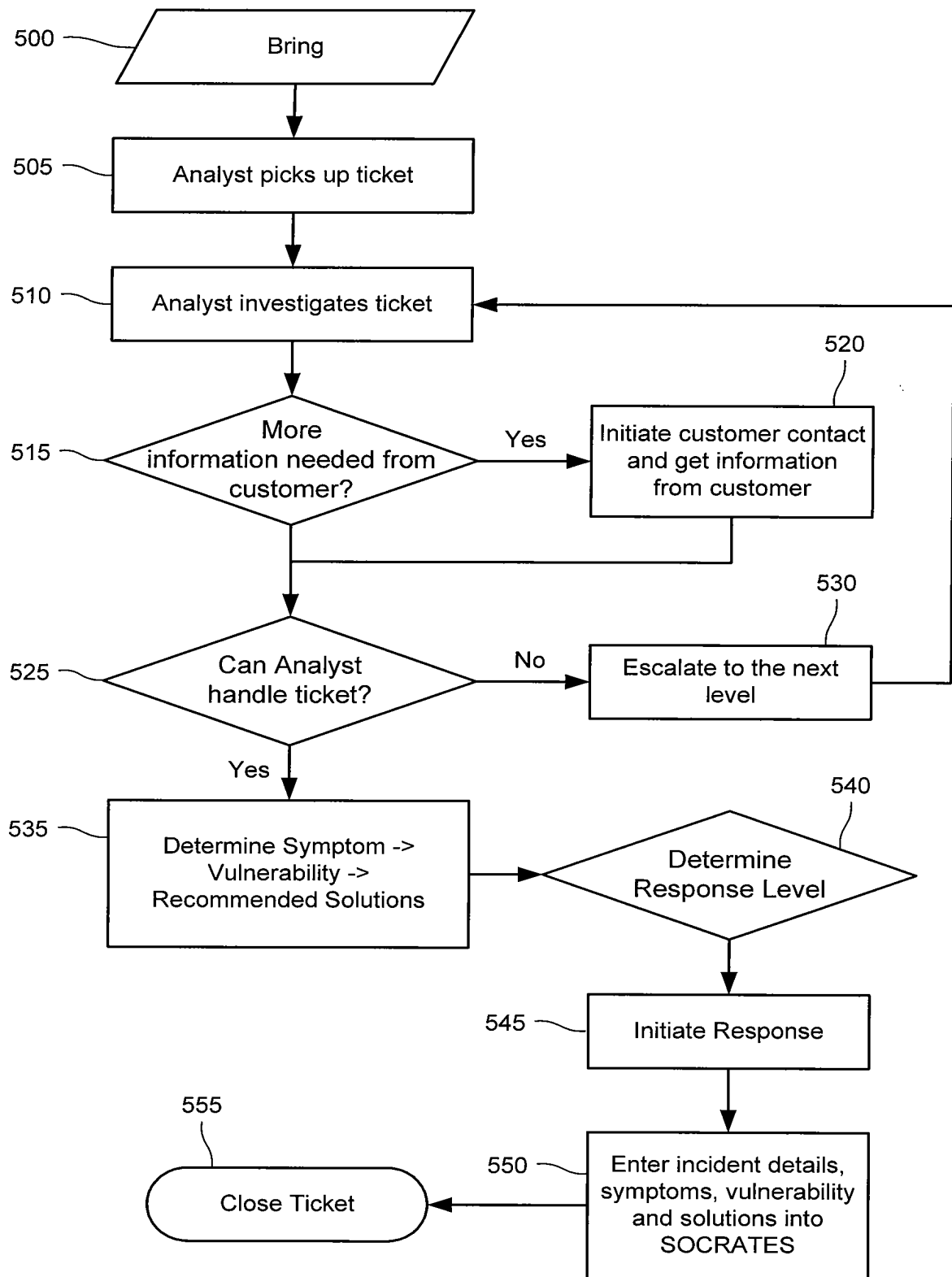
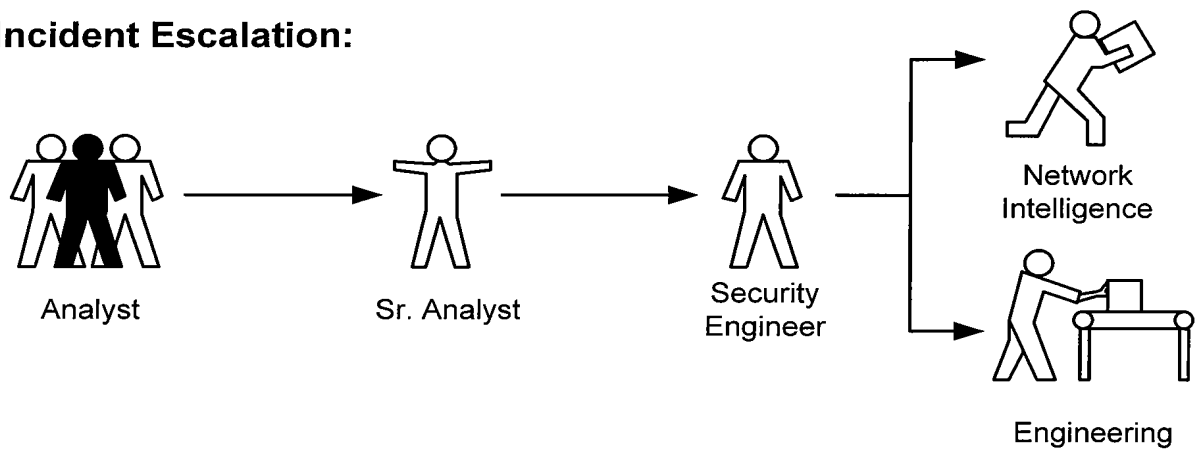
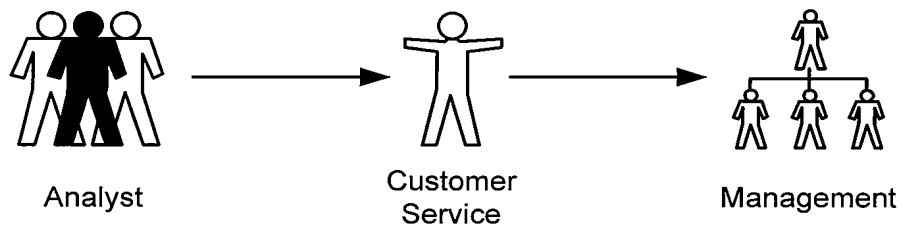


FIG. 5

### Incident Escalation:



### Customer Service Escalation:



### Technical Support Escalation:

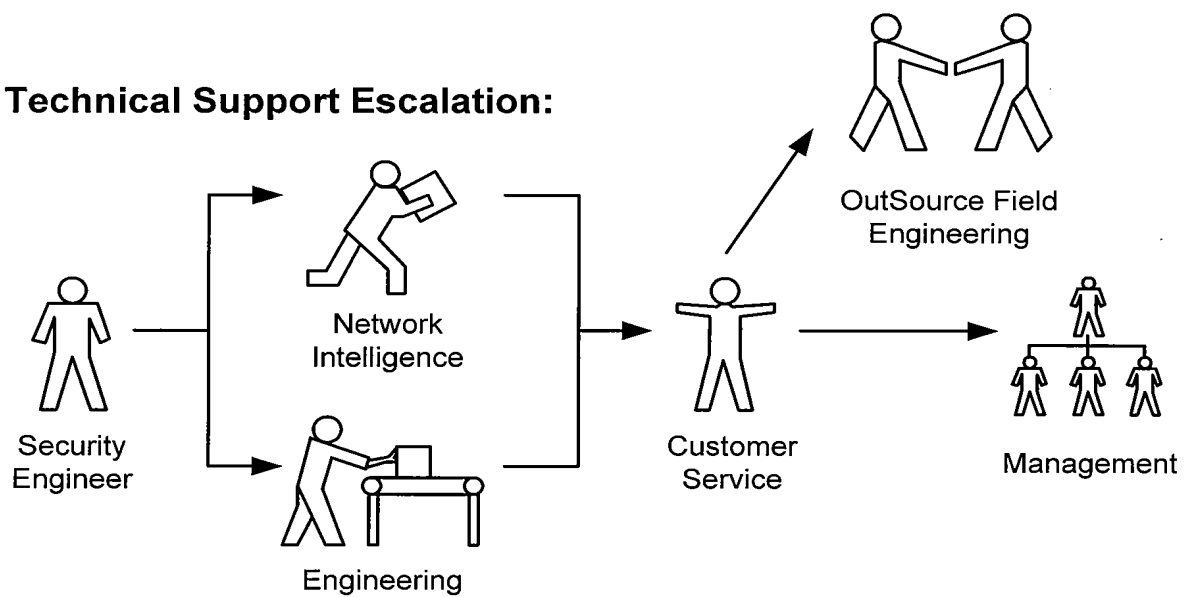


FIG. 6

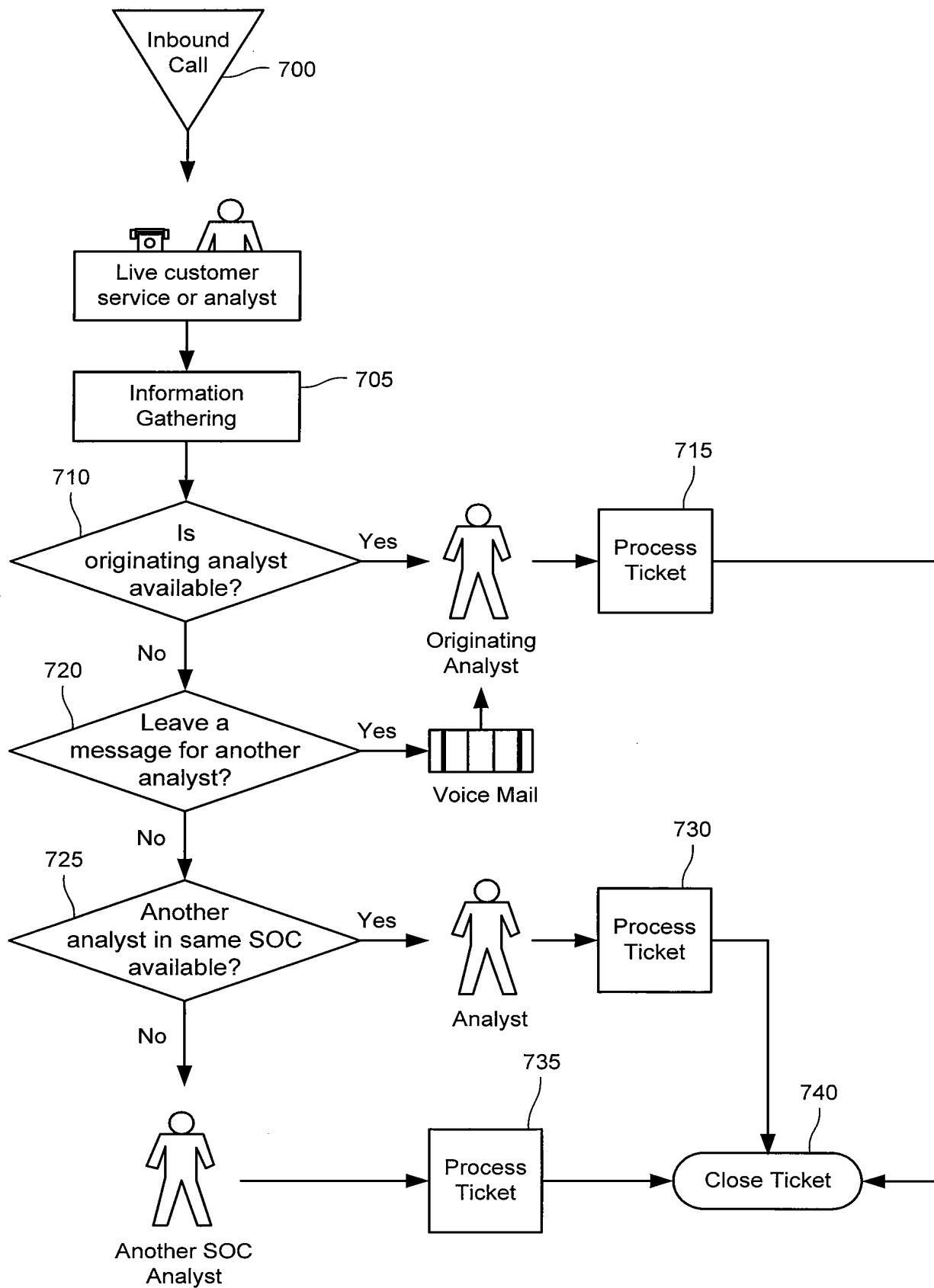


FIG. 7

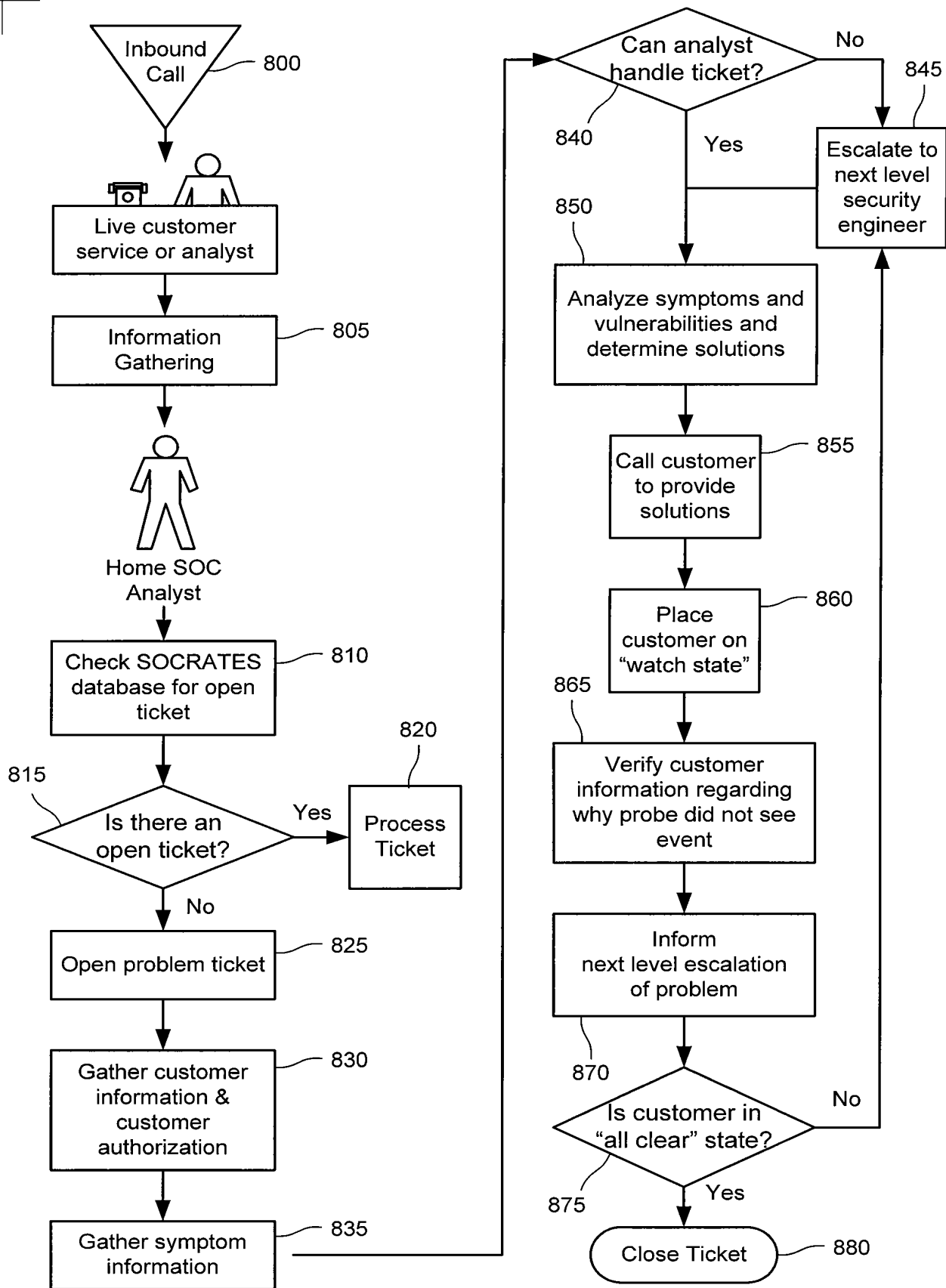
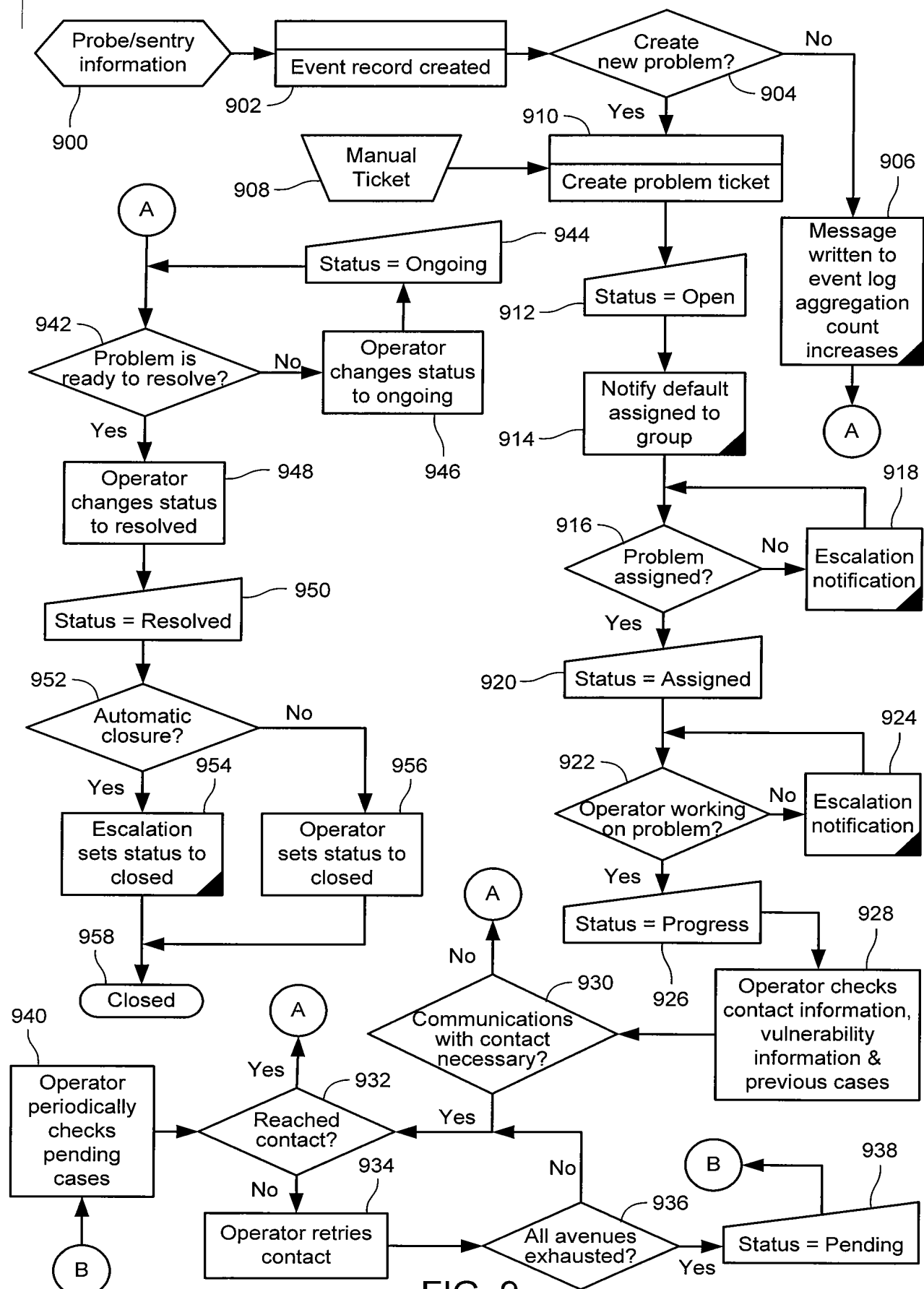


FIG. 8B



Docket No.  
028490-0007

# Declaration and Power of Attorney For Patent Application

## English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**Method and System for Dynamic Network Intrusion Monitoring, Detection and Response**

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on January 19, 2001 as United States Application No. or PCT International Application Number 09/766,343 and was amended on n/a

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

n/a

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

|                          |                |
|--------------------------|----------------|
| 60/190,326               | March 16, 2000 |
| (Application Serial No.) | (Filing Date)  |
| _____                    | _____          |
| (Application Serial No.) | (Filing Date)  |
| _____                    | _____          |
| (Application Serial No.) | (Filing Date)  |

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

|                          |               |                                            |
|--------------------------|---------------|--------------------------------------------|
| n/a                      |               |                                            |
| (Application Serial No.) | (Filing Date) | (Status)<br>(patented, pending, abandoned) |
| _____                    | _____         | _____                                      |
| (Application Serial No.) | (Filing Date) | (Status)<br>(patented, pending, abandoned) |
| _____                    | _____         | _____                                      |
| (Application Serial No.) | (Filing Date) | (Status)<br>(patented, pending, abandoned) |

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

**Ronald S. Laurie, Reg. No. 25,431**

**Joseph Yang, Ph.D., Reg. No. 41,387**

**Frederick D. Kim, Ph.D., Reg. No. 38,513**

**Thomas R. Lane, Reg. No. 42,781**

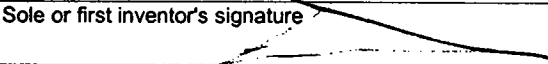
**Stacey J. Farmer, Ph.D., Reg. No. 42,526**

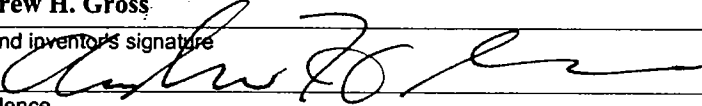
**Robert B. Beyers, Ph.D., Reg. No. 46,552**

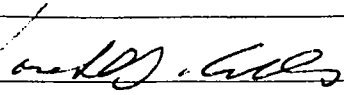
**Daniel J. Lin, Reg. No. P-47,750**

Send Correspondence to: **Robert B. Beyers, Ph.D.**  
**Skadden, Arps, Slate, Meagher & Flom LLP**  
**525 University Avenue**  
**Palo Alto, California 94301**

Direct Telephone Calls to: *(name and telephone number)*  
**Robert B. Beyers, Ph.D. - (650) 470-4500**

|                                                                                                                           |                        |
|---------------------------------------------------------------------------------------------------------------------------|------------------------|
| Full name of sole or first inventor<br><b>Bruce Schneier</b>                                                              |                        |
| Sole or first inventor's signature<br> | Date<br><b>3/24/01</b> |
| Residence<br><b>101 East Minnehaha Parkway, Minneapolis, MN 55419</b>                                                     |                        |
| Citizenship<br><b>U.S.A.</b>                                                                                              |                        |
| Post Office Address<br><b>same as above</b>                                                                               |                        |
|                                                                                                                           |                        |

|                                                                                                                    |                          |
|--------------------------------------------------------------------------------------------------------------------|--------------------------|
| Full name of second inventor, if any<br><b>Andrew H. Gross</b>                                                     |                          |
| Second inventor's signature<br> | Date<br><b>23 Feb 01</b> |
| Residence<br><b>1055 Coleman Road, #2309, San Jose, CA 95123</b>                                                   |                          |
| Citizenship<br><b>U.S.A.</b>                                                                                       |                          |
| Post Office Address<br><b>same as above</b>                                                                        |                          |
|                                                                                                                    |                          |

|                                                                                                                 |                          |
|-----------------------------------------------------------------------------------------------------------------|--------------------------|
| Full name of third inventor, if any<br><b>Jonathan D. Callas</b>                                                |                          |
| Third inventor's signature<br> | Date<br><b>7 Mar '01</b> |
| Residence<br><b>1781 Wema Way, San Jose, CA 95124</b>                                                           |                          |
| Citizenship<br><b>U.S.A.</b>                                                                                    |                          |
| Post Office Address<br><b>same as above</b>                                                                     |                          |
|                                                                                                                 |                          |

|                                      |      |
|--------------------------------------|------|
| Full name of fourth inventor, if any |      |
| Fourth inventor's signature          | Date |
| Residence                            |      |
| Citizenship                          |      |
| Post Office Address                  |      |
|                                      |      |

|                                     |      |
|-------------------------------------|------|
| Full name of fifth inventor, if any |      |
| Fifth inventor's signature          | Date |
| Residence                           |      |
| Citizenship                         |      |
| Post Office Address                 |      |
|                                     |      |

|                                     |      |
|-------------------------------------|------|
| Full name of sixth inventor, if any |      |
| Sixth inventor's signature          | Date |
| Residence                           |      |
| Citizenship                         |      |
| Post Office Address                 |      |
|                                     |      |

**REVOCATION OF POWER OF  
ATTORNEY WITH  
NEW POWER OF ATTORNEY  
AND  
CHANGE OF CORRESPONDENCE ADDRESS**

|                        |                  |
|------------------------|------------------|
| Application Number     | 09/766,343       |
| Filing Date            | January 19, 2001 |
| First Named Inventor   | Schneier, Bruce  |
| Art Unit               | 2131             |
| Examiner Name          | Unassigned       |
| Attorney Docket Number | 022133-000510US  |

I hereby revoke all previous powers of attorney given in the above-identified application:

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint the practitioners associated with the Customer Number:

**20350**

☒ Please change the correspondence address for the above-identified application to:

☒ The address associated with  
Customer Number:

**20350**

OR

☐ Firm or  
Individual Name

Address

Address

City

State

ZIP

Country

Telephone

Fax

I am the:

☐ Applicant/Inventor.

☒ Assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

**SIGNATURE of Applicant or Assignee of Record**

Name

*Christopher Harris*

Signature

*[Signature]*

Date

*1/26/04*

Telephone

*(650) 404-2400*

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

☐ \*Total of \_\_\_\_\_ forms are submitted.

Attorney Docket No. 022133-000510US

**STATEMENT UNDER 37 CFR 3.73(b)**Applicant/Patent Owner: Bruce Schneier, et. al.Application No./Patent No.: 09/766,343Filed/Issue Date: January 19, 2001Entitled: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSECounterpane Internet Security, Inc., a Corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.  
The extent (by, percentage) of its ownership interest is \_\_\_\_\_%

in the patent application/patent identified above by virtue of either:

- A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 011845, Frame 0122, or for which a copy thereof is attached.

**OR**

- B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

1. From: \_\_\_\_\_ To : \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

2. From: \_\_\_\_\_ To : \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

3. From: \_\_\_\_\_ To : \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.☐ Copies of assignments or other documents in the chain of title are attached.

[NOTE: A separate copy (i.e., the original assignment document or a true copy of the original document) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.8]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

1/26/04  
Date(650) 404-2400  
Telephone numberChristopher Haems  
Typed or printed name[Signature]  
SignatureActing CFO  
Title



**UNITED STATES DEPARTMENT OF COMMERCE  
Patent and Trademark Office**

ASSISTANT SECRETARY AND COMMISSIONER  
OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

AUGUST 13, 2001

PTAS

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP  
JOSEPH YANG, PH.D.  
525 UNIVERSITY AVENUE  
PALO ALTO, CA 94301



\*101738486A\*

**UNITED STATES PATENT AND TRADEMARK OFFICE  
NOTICE OF RECORDATION OF ASSIGNMENT DOCUMENT**

THE ENCLOSED DOCUMENT HAS BEEN RECORDED BY THE ASSIGNMENT DIVISION OF THE U.S. PATENT AND TRADEMARK OFFICE. A COMPLETE MICROFILM COPY IS AVAILABLE AT THE ASSIGNMENT SEARCH ROOM ON THE REEL AND FRAME NUMBER REFERENCED BELOW.

PLEASE REVIEW ALL INFORMATION CONTAINED ON THIS NOTICE. THE INFORMATION CONTAINED ON THIS RECORDATION NOTICE REFLECTS THE DATA PRESENT IN THE PATENT AND TRADEMARK ASSIGNMENT SYSTEM. IF YOU SHOULD FIND ANY ERRORS OR HAVE QUESTIONS CONCERNING THIS NOTICE, YOU MAY CONTACT THE EMPLOYEE WHOSE NAME APPEARS ON THIS NOTICE AT 703-308-9723. PLEASE SEND REQUEST FOR CORRECTION TO: U.S. PATENT AND TRADEMARK OFFICE, ASSIGNMENT DIVISION, BOX ASSIGNMENTS, CG-4, 1213 JEFFERSON DAVIS HWY, SUITE 320, WASHINGTON, D.C. 20231.

RECORDATION DATE: 05/24/2001

REEL/FRAME: 011845/0122  
NUMBER OF PAGES: 4

BRIEF: ASSIGNMENT OF ASSIGNOR'S INTEREST (SEE DOCUMENT FOR DETAILS).

**ASSIGNOR:**

SCHNEIER, BRUCE

DOC DATE: 02/21/2001

**ASSIGNOR:**

GROSS, ANDREW H.

DOC DATE: 02/23/2001

**ASSIGNOR:**

CALLAS, JONATHAN D.

DOC DATE: 03/07/2001

**ASSIGNEE:**

COUNTERPANE INTERNET SECURITY,  
INC.

3031 TISCH WAY  
SAN JOSE, CALIFORNIA 95128

SERIAL NUMBER: 09766343  
PATENT NUMBER:

FILING DATE: 01/19/2001  
ISSUE DATE:

**SASM&F**

**DOCKETED**

8-27-01 *jea*

AUG 20 2001

**RECEIVED**

011845/0122 PAGE 2

JOANN STEWART, EXAMINER  
ASSIGNMENT DIVISION  
OFFICE OF PUBLIC RECORDS

REC

06-04-2001

Packet No.: 028490-0007

U.S. DEPARTMENT OF COMMERCE  
Patent and Trademark Office



Tab settings → → → ▼ ▼

101738486

To the Honorable Commissioner of Patents and Trademarks. Please return the attached original documents or copy thereof.

1. Name of conveying party(ies):

Bruce Schneier  
Andrew H. Gross  
Jonathan D. Callas

5-2401

2. Name and address of receiving party(ies):

Name: Counterpane Internet Security, Inc.

Internal Address: \_\_\_\_\_

MAY 24 2001

Street Address: 3031 Tisch Way

City: San Jose State: CA ZIP: 95128

Additional names(s) of conveying party(ies) ☐ Yes ☒ No

3. Nature of conveyance:

- ☒ Assignment ☐ Merger  
☐ Security Agreement ☐ Change of Name  
☐ Other \_\_\_\_\_

Execution Date: 02/21/2001; 02/23/2001; and 03/07/2001

Additional name(s) & address(es) attached? ☐ Yes ☒ No

4. Application number(s) or registration numbers(s):

If this document is being filed together with a new application, the execution date of the application is: \_\_\_\_\_

A. Patent Application No.(s)

09/766,343

B. Patent No.(s)

Additional numbers attached? ☐ Yes ☒ No

5. Name and address of party to whom correspondence concerning document should be mailed:

Name: Joseph Yang, Ph.D.

Internal Address: Skadden, Arps, Slate, Meagher

& Flom LLP

06/04/2001 6TON11 00000047 09766343

01 FC:581 40.00 DR

Street Address: 525 University Avenue

City: Palo Alto State: CA ZIP: 94301

6. Total number of applications and patents involved: 1

7. Total fee (37 CFR 3.41):.....\$ 40.00

☒ Enclosed - Any excess or insufficiency should be credited or debited to deposit account

☐ Authorized to be charged to deposit account

8. Deposit account number:

19-2385

DO NOT USE THIS SPACE

9. Statement and signature.

To the best of my knowledge and belief, the foregoing information is true and correct and any attached copy is a true copy of the original document.

Robert B. Beyers

Robert B. Beyers

May 24, 2001

Name of Person Signing

Signature

Date

Total number of pages including cover sheet, attachments, and document: 3

## **ASSIGNMENT OF PATENT APPLICATION**

THIS ASSIGNMENT, by Bruce Schneier, Andrew H. Gross and Jonathan D. Callas (hereinafter referred to as "the Assignors"), residing at 101 East Minnehaha Parkway, Minneapolis, Minnesota 55419; 1055 Coleman Road, #2309, San Jose, California 95123 and 1781 Wema Way, San Jose, California 95124; respectively, witnesseth:

WHEREAS, the Assignors have invented certain new and useful improvements in "Method for Dynamic Network Intrusion Monitoring, Detection and Response" set forth in an application for Letters Patent of the United States

\_\_\_ having an oath or declaration executed on even date herewith;  
X bearing Serial No. 09/766,343 and filed on January 19, 2001; and

WHEREAS, Counterpane Internet Security, Inc., a corporation duly organized under and pursuant to the laws of Delaware and having its principal place of business at 3031 Tisch Way, San Jose, California 95128 (hereinafter referred to as "the Assignee"), is desirous of acquiring the entire right, title and interest in and to said inventions and said application for Letters Patent of the United States, and in and to any Letters Patent or Patents, United States or foreign, to be obtained therefor and thereon.

NOW, THEREFORE, in consideration of One Dollar (\$1.00) and other good and sufficient consideration, the receipt of which is hereby acknowledged, the Assignors have sold, assigned, transferred and set over, and by these presents do sell, assign, transfer and set over, unto the Assignee, its successors, legal representatives and assigns, the entire right, title and interest in and to the above-mentioned inventions, application for Letters Patent and any and all Letters Patent or Patents of the United States of America and all foreign countries that may be granted therefor and thereon, and in and to any and all divisions, continuations, continuations-in-part and substitutes of said application, and reissues and extensions of said Letters Patent or Patents, and all rights, together with all priority rights, under any of the international conventions, unions, agreements, acts and treaties, including all future international conventions, unions, agreements, acts and treaties, the same to be held and enjoyed by the Assignee, for its own use and behoof and the use and behoof of its successors, legal representatives and assigns, to the full end of the term or terms for which Letters Patent or Patents may be granted, as fully and entirely as the same would have been held and enjoyed by the Assignors had this sale and assignment not been made;

AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives and assigns, that, at the time of execution and delivery of these presents, the Assignors are the sole and lawful owners of the entire right, title and interest in and to the inventions and application for Letters Patent above-mentioned, and that the same are unencumbered, and that the Assignors have good and full right and lawful authority to sell and convey the same in the manner herein set forth;

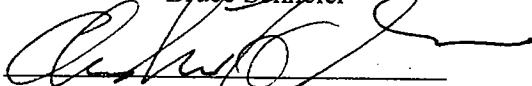
AND for the same consideration, the Assignors hereby covenant and agree to and with the Assignee, its successors, legal representatives and assigns, that the Assignors will, whenever counsel of the Assignee, or the counsel of its successors, legal representatives and assigns, shall advise that any proceeding in connection with said inventions or said application for Letters Patent, or any proceeding in connection with Letters Patent for said inventions in any country, including interference proceedings, is

lawful and desirable, or that any division, continuation, continuation-in-part or substitute of any application for Letters Patent, or any reissue or extension of any Letters Patent to be obtained thereon, is lawful and desirable, sign all papers and documents, take all lawful oaths, testify in any legal or quasi legal proceedings and do all acts necessary or required to be done for the procurement, maintenance, enforcement and defense of Letters Patent for said inventions, without charge to the Assignor, its successors, legal representatives and assigns, but at the cost and expense of the Assignee, its successors, legal representatives and assigns;

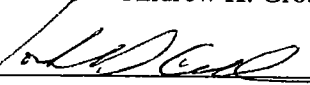
AND the Assignors hereby request the Commissioner of Patents to issue said Letters Patent of the United States to the Assignee as the Assignee of said inventions, the Letters Patent to be issued for the sole use and behoof of the Assignee, its successors, legal representatives and assigns.

Date 2/21/01 Name of Assignor 

Bruce Schnizer

Date 23 Feb 01 Name of Assignor 

Andrew H. Gross

Date 7 Mar 01 Name of Assignor 

Jonathan D. Callas

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**Applicant(s): **B. Schneier et al.**

Docket No.

**028490-0007**Serial No.  
**09/766,343**Filing Date  
**January 19, 2001**Examiner  
**Not Yet Assigned**Group Art Unit  
**2131**

Invention:

**Method for Dynamic Network Intrusion Monitoring, Detection and Response**

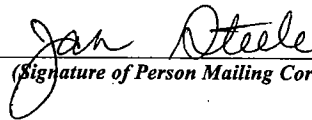
I hereby certify that this **Assignment of Patent Application and Recordation Form Cover Sheet**  
(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under  
37 CFR 1.10 in an envelope addressed to: The Commissioner of Patents and Trademarks, Washington, D.C.

20231-0001 on **May 24, 2001**  
(Date)

**Jan Steele**

(Typed or Printed Name of Person Mailing Correspondence)



(Signature of Person Mailing Correspondence)

**EL 728 498 616 US**

("Express Mail" Mailing Label Number)

**Note: Each paper must have its own certificate of mailing.**

Skadden, Arps, Slate, Meagher & Flom LLP  
525 University Avenue  
Palo Alto, California 94301  
United States of America  
Telephone: (650) 470-4500  
Facsimile: (650) 470-4570

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 1266177                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Philip H. Albert/Paula Cunningham                                                  |
| <b>Filer Authorized By:</b>                 | Philip H. Albert                                                                   |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 20-OCT-2006                                                                        |
| <b>Filing Date:</b>                         |                                                                                    |
| <b>Time Stamp:</b>                          | 18:15:05                                                                           |
| <b>Application Type:</b>                    | Utility                                                                            |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description   | File Name               | File Size(Bytes) | Multi Part /.zip | Pages (if appl.) |
|-----------------|------------------------|-------------------------|------------------|------------------|------------------|
| 1               | Application Data Sheet | ADS_022133-000520US.pdf | 82398            | no               | 3                |

### Warnings:

|                                                 |                                                            |                                                      |              |            |    |
|-------------------------------------------------|------------------------------------------------------------|------------------------------------------------------|--------------|------------|----|
| <b>Information:</b>                             |                                                            |                                                      |              |            |    |
| This is not an USPTO supplied ADS fillable form |                                                            |                                                      |              |            |    |
| 2                                               |                                                            | Continuation_Application_02<br>2133-000520US.pdf     | 1878701      | yes        | 39 |
|                                                 | <b>Multipart Description/PDF files in .zip description</b> |                                                      |              |            |    |
|                                                 | <b>Document Description</b>                                |                                                      | <b>Start</b> | <b>End</b> |    |
|                                                 | Specification                                              |                                                      | 1            | 24         |    |
|                                                 | Claims                                                     |                                                      | 25           | 29         |    |
|                                                 | Abstract                                                   |                                                      | 30           | 30         |    |
|                                                 | Drawings                                                   |                                                      | 31           | 39         |    |
| <b>Warnings:</b>                                |                                                            |                                                      |              |            |    |
| <b>Information:</b>                             |                                                            |                                                      |              |            |    |
| 3                                               | Oath or Declaration filed                                  | Original_Declaration_and_P<br>OA_022133-000520US.pdf | 159916       | no         | 4  |
| <b>Warnings:</b>                                |                                                            |                                                      |              |            |    |
| <b>Information:</b>                             |                                                            |                                                      |              |            |    |
| 4                                               | Power of Attorney                                          | Revocation_of_POA_022133<br>-000520US.pdf            | 39158        | no         | 1  |
| <b>Warnings:</b>                                |                                                            |                                                      |              |            |    |
| <b>Information:</b>                             |                                                            |                                                      |              |            |    |
| 5                                               | Assignee showing of ownership per<br>37 CFR 3.73(b).       | Statement_373b_and_assig<br>nmt_022133-000520US.pdf  | 295439       | no         | 7  |
| <b>Warnings:</b>                                |                                                            |                                                      |              |            |    |
| <b>Information:</b>                             |                                                            |                                                      |              |            |    |
| <b>Total Files Size (in bytes):</b>             |                                                            |                                                      | 2455612      |            |    |

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING or 371(c)<br>DATE | GRP ART UNIT | FIL FEE REC'D | ATTY. DOCKET NO | DRAWINGS | TOT CLAIMS | IND CLAIMS |
|--------------------|--------------------------|--------------|---------------|-----------------|----------|------------|------------|
| 11/551,606         | 10/20/2006               | 2131         | 0.00          | 022133-000520US | 9        | 44         | 3          |

**CONFIRMATION NO. 1662**

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

**FILING RECEIPT**

Date Mailed: 11/21/2006

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

**Applicant(s)**

Bruce Schneier, Minneapolis, MN;  
Andrew H. Gross, San Jose, CA;  
Jonathan D. Callas, Mountain View, CA;

**Assignment For Published Patent Application**

Counterpane Internet Security, Inc., Mountain View, CA

**Power of Attorney:** The patent practitioners associated with Customer Number 20350

**Domestic Priority data as claimed by applicant**

This application is a CON of 09/766,343 01/19/2001  
which claims benefit of 60/190,326 03/16/2000

**Foreign Applications**

**If Required, Foreign Filing License Granted:** 11/20/2006

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is  
**US11/551,606**

**Projected Publication Date:** To Be Determined - pending completion of Missing Parts

**Non-Publication Request:** No

**Early Publication Request:** No

**Title**

Method and System for Dynamic Network Intrusion Monitoring, Detection and Response

**Preliminary Class**

726

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

---

**LICENSE FOR FOREIGN FILING UNDER****Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under

37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

#### **NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371 (c) DATE | FIRST NAMED APPLICANT | ATTORNEY DOCKET NUMBER |
|--------------------|------------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006             | Bruce Schneier        | 022133-000520US        |

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

CONFIRMATION NO. 1662  
FORMALITIES  
LETTER

Date Mailed: 11/21/2006

**NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION**

**FILED UNDER 37 CFR 1.53(b)**

*Filing Date Granted*

**Items Required To Avoid Abandonment:**

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.  
*Applicant must submit \$ 300 to complete the basic filing fee for a non-small entity. If appropriate, applicant may make a written assertion of entitlement to small entity status and pay the small entity filing fee (37 CFR 1.27).*

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - More than one figure is present and each figure is not labeled "Fig." with a consecutive Arabic numeral (1, 2, etc.) or an Arabic numeral and capital letter in the English alphabet (A, B, etc.)(see 37 CFR 1.84(u)(1)). See Figure(s) 8. A brief description of the several views of the drawings (see 37 CFR 1.74) should be added or amended to correspond to the corrected numbering of the figures. See also 37 CFR 1.77(b)(7).

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **\$1200** as a non-small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- To avoid abandonment, a surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.

**SUMMARY OF FEES DUE:**

Total additional fee(s) required for this application is **\$2330** for a non-small entity

- **\$300** Statutory basic filing fee.
- **\$130** Surcharge.
- The application search fee has not been paid. Applicant must submit **\$500** to complete the search fee.
- The application examination fee has not been paid. Applicant must submit **\$200** to complete the examination fee for a non-small entity.
- Total additional claim fee(s) for this application is **\$1200**
  - **\$1200** for **24** total claims over 20.

Replies should be mailed to:    Mail Stop Missing Parts  
                                                 Commissioner for Patents  
                                                 P.O. Box 1450  
                                                 Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.  
<https://portal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html>

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at <http://www.uspto.gov/ebc>.

---

***If you are not using EFS-Web to submit your reply, you must include a copy of this notice.***



Office of Initial Patent Examination (571) 272-4000, or 1-800-PTO-9199, or 1-800-972-6382  
PART 3 - OFFICE COPY

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on March 21, 2007.

PATENT  
Attorney Docket No.: 022133-000520US

TOWNSEND and TOWNSEND and CREW LLP

By: /Maureen Golob/  
Maureen Golob

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier

Application No.: 11/551,606

Filed: November 21, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Customer No.: 20350

Confirmation No. 1662

Examiner:

Technology Center/Art Unit:

PRELIMINARY AMENDMENT

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Prior to examination of the above-referenced application, please enter the  
following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this  
paper.

**Amendments to the Drawings** begin on page 6 of this paper and attached are replacement  
sheets.

**Remarks/Arguments** begin on page 7 of this paper.

**Appendices A through C** are attached after the **Remarks/Arguments** section following page 7  
of this paper.

An **Appendix** including amended drawing figures is attached following Appendices A through  
C.

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1. - 44. (Canceled).

45. (New) A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:

- a) a sensor coupled to collect status data from at least one monitored component of the network;
- b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
- c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
- d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
- e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

46. (new) The system of claim 45, wherein the identifying step includes performing a multi-stage analysis of the status data.

47. (New) The system of claim 46, wherein the multi-stage analysis includes performing a discrimination analysis on the status data.

48. (New) The system of claim 47, wherein the discrimination analysis includes positive filtering.

49. (New) The system of claim 47, wherein the discrimination analysis includes negative filtering.

50. (New) The system of claim 46, wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe.

51. (New) The system of claim 45, wherein the identifying step includes aggregating and synthesizing the status data at the probe.

52. (New) The system of claim 51, wherein the identifying step includes cross-correlating data across the monitored components.

53. (New) The system of claim 51, wherein the identifying step includes analyzing the frequency of occurrence of the events.

54. (New) The system of claim 45, further comprising after the step (c), a secure operations center coupled to perform further computer-based analysis and to receive data from the probe.

55. (New) The system of claim 54, wherein the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

56. (New) The system of claim 54, wherein the identifying step includes cross-correlating data across the monitored components.

57. (New) The system of claim 54, wherein the identifying step includes analyzing the frequency of occurrence of the events.

58. (New) The system of claim 54, wherein the computer-based analysis includes cross-probe correlation.

59. (New) The system of claim 45, further comprising instantaneously self-tuning the probe based on previously collected status data.

60. (New) The system of claim 45, wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

61. (New) The system of claim 45, wherein the receiving feedback step occurs in substantially real time.

62. (New) A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:

creating an event record for information received about an identified potentially security-related event occurring on the network;

correlating the event record with customer information and a symptom record;

using the correlated symptom record to link the event record to problem resolution information;

consolidating the event record, correlated customer information and symptom record, and linked problem resolution information into a problem ticket; and

providing the problem ticket to a security analyst console for analysis.

63. (New) The method of claim 62, further comprising:

correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and

linking the event record to an open problem ticket associated with the pre-existing event record.

64. (New) The method of claim 62, wherein the problem resolution information links the symptom to a diagnosis.

65. (New) The method of claim 62, wherein the problem resolution information links the symptom to a technology.

66. (New) The method of claim 62, further comprising:

correlating the event record with a vulnerability; and

using the correlated vulnerability to link the event record to problem resolution information.

67. (New) The method of claim 66, wherein the problem resolution information links the vulnerability to a diagnosis.

68. (New) The method of claim 66, wherein the problem resolution information links the vulnerability to a technology.

69. (New) The method of claim 62, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by filtering.

70. (New) The method of claim 62, further comprising:  
updating the problem resolution information after the potentially security-related event is resolved.

**Amendments to the Drawings:**

The attached sheet of drawings includes changes to Fig. 8. This sheet, which includes Fig. 8, replaces the original sheet including Fig. 8.

Attachment: Replacement Sheet

**REMARKS/ARGUMENTS**

Applicant encloses for Examiner's reference Appendix A, Appendix B and Appendix C as indicated on page 6 of the above application.

**CONCLUSION**

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

/Naya Chatterjee-Marathe/

Naya Chatterjee-Marathe  
Reg. No. 54,680

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400  
Fax: 415-576-0300  
Attachments  
NCM:mg  
61002555 v1

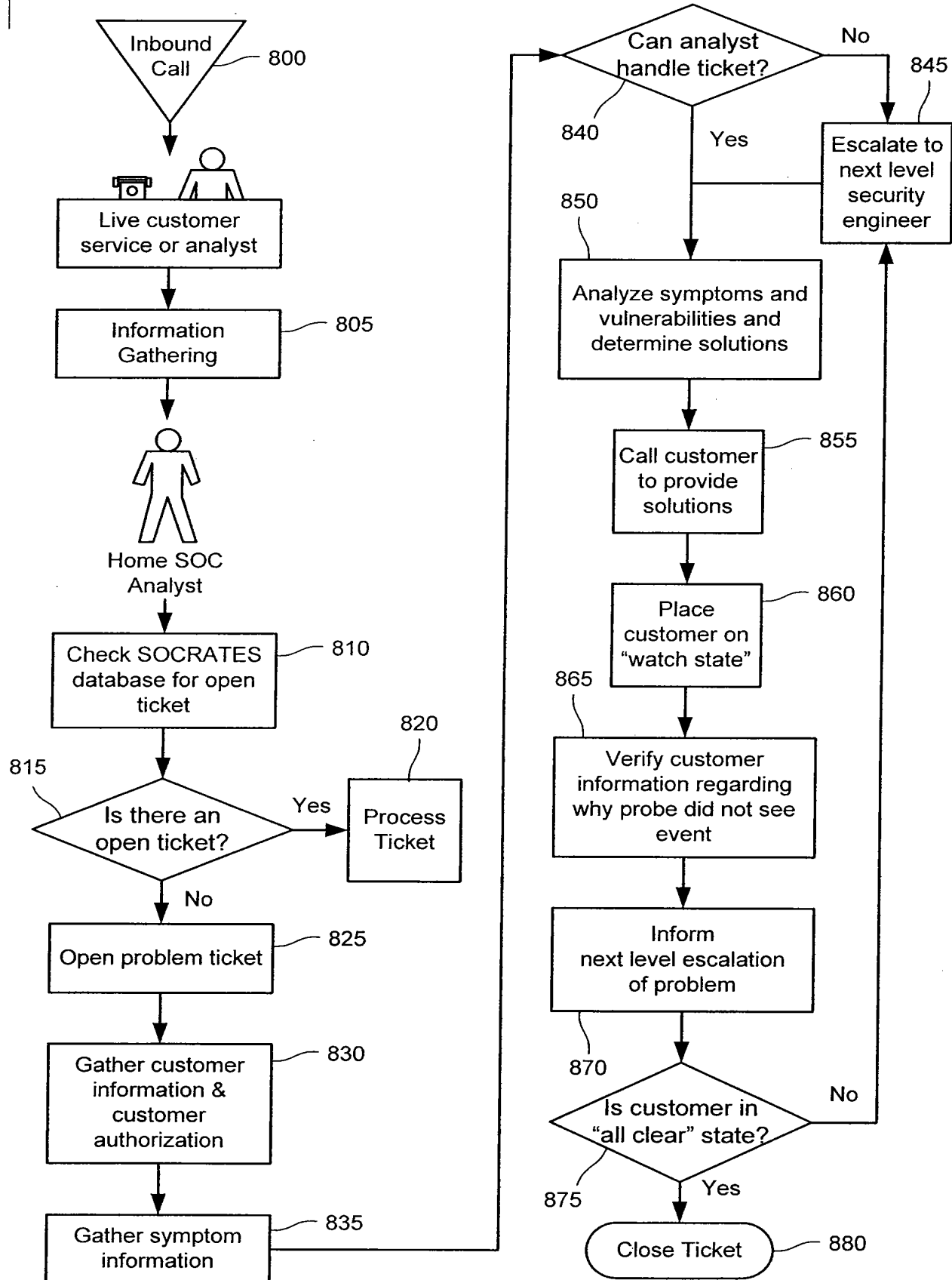


FIG. 8

## APPENDIX A

### Exemplary Pipes Protocol

#### Message Format

In a preferred embodiment, the Pipes message format should be easy to parse and human readable to the extent possible without interfering with parsing. Each header field can be separated by spaces. Values can be either printable hex (lower case for letters) or alphabetic mnemonics.

A message can consist of a fixed header followed by a body. An exemplary format for the header is as follows:

HHHH – length (printable hex, 4 characters, range 0..nn)  
SPACE – one character, hex 0x20  
HHHH – revision (printable hex, 4 characters)  
SPACE  
SSSS – sentry number (printable hex, 4 characters)  
SPACE  
HHHH – reference number (printable hex, 4 characters)  
SPACE  
STATUS – status code for each message  
SPACE  
KMAC value (always "X" for now)  
SPACE  
XXXX – opcode (4 printable ASCII characters)  
SPACE  
PAYLOAD – (length) bytes, in printable hex, max 2048 characters less header

#### Example Message

"001f0000 3333 1111 2222 X ALRT 12345678"

#### Notes

1. All the above fields should have spaces between them.
2. The first four-digit group is the length of everything after it (LENGTH) (the space through the end of "12345678").
3. The second four-digit group is the revision field (REVISION).

4. The third four-digit group is the probe/sentry number, which identifies a particular probe/sentry ("3333" in the example).
5. The fourth four-digit group is the reference number defined by the probe/sentry system (REFNUM)("1111" in the example).
6. The fifth four-digit group is the status number defined by the probe/sentry system (STATUS) ("2222" in the example).
7. The next one-digit field ("X") is the keyed Media Access Control (KMAC) value, if present. If not present, the value should be an "X."
8. The next field is the op code (OPCODE). For filter-related messages, it is always "ALRT."
9. The portion of the message after the space after "ALRT" is content-specific.

### Field Descriptions

REVISION – a version number, consisting of a major and a minor value. Minor revisions should be compatible with previous revisions within the same major number range.

LENGTH – the length in characters of the message that follows the header.

REFNUM – a reference number generated by the initiator of the message exchange. For PING and other multi-message exchanges, the REFNUM of the response should match the value in the request.

STATUS – a status code indicating the severity of the message. Messages are sorted in the hold queue according to priority (status codes numerically larger than *n* are sent first).

KMAC value – 'X' or 32 characters representing a 16 byte keyed MD5 hash of the entire message, including the header, with the KMAC (Keyed MAC) preset to zero.

OPCODE – printable value indicating the message operation code (i.e., "ALRT").

PAYLOAD – the core content of the message.

### Sample Payload Descriptions

#### ALERT

##### Opcode "ALRT"

This message is sent from the probe/sentry to the gateway by the probe/sentry filtering subsystem. An ALRT payload contains (after decoding to binary):

0..last – block of probe/sentry alert data

## INITIAL CONTACT

### Opcode "INIT"

This message is sent from the probe/sentry to the gateway when the probe/sentry first connects to the gateway. An INIT payload contains (after decoding to binary):

0..3 – connect type: 0000=normal, 0001=must-be-accepted

## INITIAL CONTACT ACK

### Opcode "INAK"

This message is sent from the gateway to the probe/sentry in response to an INIT.

0..3 – response status: 0000=ok/accepted, 0001=go away

Note: a "go away" response should not be acceptable if the probe/sentry used the "must be accepted" connect type.

## PING

### Opcode "PING"

This message is sent from (either end) to determine if the other end is alive. A PING payload contains (after decoding to binary):

0...last null terminated text data containing memory used, number of alerts sent, etc.

## PING ACK

### Opcode "PACK"

This message is sent in response to a PING. A PACK payload contains (after decoding to binary):

0..3 – first four bytes of PING message.

## TEST

### Opcode "TEST"

This message is sent from (either end) to respond to a test message. A TEST payload contains (after decoding to binary):

0..last test data

## TEST ACK

### Opcode "TSAK"

This message is sent from (either end) to respond to a test message. A TSAK payload contains (after decoding to binary):

0..3 first four bytes of the test message

## UPDATE EXECUTE

### Opcode "UPEX"

This message is sent from the gateway to the probe/sentry to cause an update to be executed. A UPEX payload contains (after decoding to binary):

0..last null terminated ASCII path, from root, of shell script to execute to force update

#### UPDATE EXECUTE ACK

Opcode "EXAK"

This message is sent from the probe/sentry to the gateway to acknowledge a UPEX message. An EXAK payload contains (after decoding to binary):

- 0..3 network byte order return code from script.

#### UPDATE FRAGMENT

Opcode "UFRG"

This message is sent from the gateway to the probe/sentry to send an update. An "update" is a file that may be stored in a directory such as "/MSM/update/<id>", where "id" is the id value from the message. A UFRG payload contains (after decoding to binary):

- 0..3 – network byte order offset within update

- 4..7 – ID of update

- 8..last – contents of update fragment

#### UPDATE FRAGMENT ACK

Opcode "UFAK"

This message is sent from the probe/sentry to the gateway to acknowledge a UFRG message. A UFAK payload contains (after decoding to binary):

- 0..3 network byte order offset of last byte of update received.

## **APPENDIX B**

The configuration details of one possible production environment for the SOCRATES system are as follows:

### **AR System Details**

AR System Version: 4.03  
AR Client Version: 4.03  
AR Admin Version: 4.03

### **H/W Platform Details**

Hardware: Sun Ultra Enterprise 450  
Operating System: Solaris 7.0  
Hard disk space: 256 GB  
Memory: 1 GB  
Disk Configuration: RAID 5 or RAID 10 (to be determined)  
# CPU's: 2 x 400mhz

### **Database Details**

Vendor: Oracle 8.x  
Allocated Disk Space: To be determined

### **Client Details**

Operating System: NT 4.0 Workstation  
Monitor Resolution: 1024 x 768

The configuration details of one possible development environment for the SOCRATES system are listed below:

### **AR System Details**

AR System Version: 4.03  
AR Client Version: 4.03  
AR Admin Version: 4.03

### **H/W Platform Details**

Hardware: Sun Ultra 10 Workstation  
Operating System: Solaris 7.0  
Hard disk space: 9 GB  
Memory: 1 GB  
Disk Configuration: To be determined  
# CPU's: 1 440mhz

### **Database Details**

Vendor: Oracle 8.x  
Allocated Disk Space: To be determined

## APPENDIX C

This appendix describes data categories and functionalities that may be employed in an exemplary embodiment of the SOCRATES system. Additional data categories are possible. Such data elements can be stored in forms, tables or other formats.

The tables provided in this appendix are organized as follows:

|              |                                                                       |
|--------------|-----------------------------------------------------------------------|
| TABLE 1      | Summary of data categories                                            |
| TABLES 2-19  | Summary of fields included in each data category described in TABLE 1 |
| TABLES 20-26 | Types of active links, filters, macros, notifications, etc.           |

In TABLES 2-19, the "field type" columns correspond to field types commonly employed in programming languages like C, Java, or Fortran.

TABLE 1. Data Categories

| Data Category (TABLE #) | Description                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Change Request (2)      | A request to make a change, including suggesting a new feature, changing an existing function, reporting a bug, or changing data.                                                                          |
| Company (3)             | Information about a company.                                                                                                                                                                               |
| Contacts (4)            | A matrix of Persons used to decide whom to contact and under what circumstances.                                                                                                                           |
| Diagnosis (5)           | The end result of the problem resolution process, for example an attack or a normal operating procedure that created warnings.                                                                             |
| Gateway Message (6)     | A received Message describing what happened.                                                                                                                                                               |
| Install (7)             | An installed device monitored by the MSM service.                                                                                                                                                          |
| Message (8)             | A type of Message that a gateway may send.                                                                                                                                                                 |
| Person (9)              | Information about a person.                                                                                                                                                                                |
| Problem Ticket (10)     | A consolidation of information regarding a specific set of happenings that may indicate an attack, such information including gateway messages, company information and security intelligence information. |

|                                 |                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SecurityFocusVulnerability (11) | Information about system vulnerabilities, which may be a combination of custom information and information provided by a commercial provider such as SecurityFocus.com. |
| Symptom (12)                    | An in-depth description of a Message. Many different Messages may indicate the same Symptom.                                                                            |
| SymptomToDiagnosis (13)         | Links Symptoms to Diagnoses.                                                                                                                                            |
| SymToTechnology (14)            | Links Symptoms to affected Technologies.                                                                                                                                |
| Technology (15)                 | An operating system, software product or hardware product that may play a role in security.                                                                             |
| TimeZone (16)                   | A representation, which may be text, of a particular time zone. The representation may be expressed as a number of hours representing the difference from GMT.          |
| Vulnerability (17)              | An exploitable weakness in a Technology.                                                                                                                                |
| VulnerabilityToDiagnosis (18)   | Links Vulnerabilities to Diagnoses.                                                                                                                                     |
| VulnToTechnology (19)           | Links Vulnerabilities to affected Technologies.                                                                                                                         |

TABLE 2. SOC:Change Request

| Name                               | Field Type        | Description                                                                                         |
|------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------|
| Status                             | Radio Button      | Possible states include: New, Assigned, Fixed, Rejected, Closed.                                    |
| Request Type                       | Radio Button      | Possible states include: Suggestion, Change Function, Bug, Required Missing Function, Data Request. |
| Brief Description                  | Char 64           | A brief description of the request.                                                                 |
| From, FromPersonName               | Char 15, Char 155 | Full name from Person record of person who made the request.                                        |
| Responsible, ResponsiblePersonName | Char 15, Char 155 | Full name from Person record of person who should administrate or be responsible for the request.   |
| Priority                           | Radio Button      | Possible states include: High, Medium, Low, Implement if Time Allows.                               |
| Memo                               | Diary             | A discussion of the problem.                                                                        |
| Attachments                        | Attachment        | Attached files relating to the problem                                                              |

TABLE 3. SOC:Company

| Name         | Field Type | Description                          |
|--------------|------------|--------------------------------------|
| CompanyID    | Char 15    | Unique ID for the Company.           |
| Company Name | Char 128   | Name of the Company.                 |
| Work Phone   | Char 30    | Telephone number for the front desk. |

|                   |            |                                                                                              |
|-------------------|------------|----------------------------------------------------------------------------------------------|
| Fax               | Char 30    | Main Company fax number.                                                                     |
| WebSite           | Char 255   | Corporate home page.                                                                         |
| Area Code         | Char 10    | Area Code used for geographic location.                                                      |
| ContactID         | Char 40    | Pointer to the Company Contacts record.                                                      |
| TimeZone Desc     | Char 255   | Character description of the Time Zone.                                                      |
| Time Zone         | Real       | Numeric offset from GMT.                                                                     |
| Region            | Char 30    | Company defined region.                                                                      |
| Site              | Char 30    | Company defined site.                                                                        |
| P.O. Box          | Char 10    | Post office box number.                                                                      |
| Street Number     | Char 10    | Street number.                                                                               |
| Street Name       | Char 65    | Street name.                                                                                 |
| Other Street Info | Char 65    | Address information other than Street Name and Street Number, for example, "100 Plaza East." |
| City              | Char 65    | City.                                                                                        |
| Country           | Char 65    | Country.                                                                                     |
| Zip Code          | Char 30    | Zip or postal code.                                                                          |
| Mailing Address   | Char 300   | Mailing address exactly as written on a post envelope.                                       |
| Memo              | Diary      | Pertinent notes for this record.                                                             |
| Attachments       | Attachment | Pertinent file attachments for this record.                                                  |

TABLE 4. SOC:Contacts

| Name                             | Field Type           | Description                                                                                                                            |
|----------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Contacts Unique ID               | Char 40              | Unique ID for the Contact                                                                                                              |
| Description1-10                  | Char 60              | Ten descriptions representing 10 different contact events. Each contact event can have, for example, 3 contacts and 3 contact methods. |
| Contact                          | Drop-Down List       | Either or Both. Indicates whether more than one contact must be contacted.                                                             |
| ContactIDA1-B10<br>ContactA1-B10 | Char 15,<br>Char 155 | Full name of the Contact Person.                                                                                                       |
| MethodA1-B10                     | Drop-Down List       | Method of communicating with Contact, including Phone, Page and Email.                                                                 |
| Memo                             | Diary                | Pertinent notes for this record.                                                                                                       |
| Attachments                      | Attachment           | Pertinent file attachments for this record.                                                                                            |

TABLE 5. SOC:Diagnosis

| Name | Field Type | Description |
|------|------------|-------------|
|------|------------|-------------|

|                                                                                   |                |                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Diagnosis ID                                                                      | Char 15        | Unique identifier for this record.                                                                                                                                                                   |
| Type                                                                              | Radio Button   | Operational Procedure, Attack, Configuration.                                                                                                                                                        |
| Name                                                                              | Char 60        | Name of particular diagnosis.                                                                                                                                                                        |
| DocumentationStatus                                                               | Drop-Down List | Possible states include: Named, Summarized, Described, Reviewed by NI(1), Reviewed by Technical Writer, Reviewed NI(2), Approved.                                                                    |
| Summary                                                                           | Char 0         | A summary description of the diagnosis which can used in an initial communication to the customer. The description can be somewhat of a "scripted" response the analyst can provide to the customer. |
| Impact                                                                            | Char 500       | A brief description of the impact the diagnosis has on the customer.                                                                                                                                 |
| Description                                                                       | Char 0         | A detailed description and discussion of the diagnosis.                                                                                                                                              |
| Severity<br>For Unknown Victim<br>For Known Victim<br>For Mission Critical Victim | Drop-Down List | Possible states include: Critical, Suspicious, Relevant, Interesting and Not Defined. Indicates severity for each category of installed device.                                                      |
| Recommendations                                                                   | Char 0         | Recommended courses of action. This can be broken out into more structured data.                                                                                                                     |
| Memo                                                                              | Diary          | Pertinent notes for this record.                                                                                                                                                                     |
| Confirmation                                                                      | Char 0         | What procedures could be done to confirm this is a correct diagnosis.                                                                                                                                |
| CounterEvidence                                                                   | Char 0         | What procedures could be done to confirm this is not the correct diagnosis.                                                                                                                          |
| Attachments                                                                       | Attachment     | Pertinent file attachments for this record.                                                                                                                                                          |

TABLE 6. SOC:Gateway Message

| Name             | Field Type | Description                                                                                   |
|------------------|------------|-----------------------------------------------------------------------------------------------|
| GatewayMessageID | Char 15    | Unique identifier for this record.                                                            |
| Company ID       | Char 15    | Pointer into the Company table.                                                               |
| Company Name     | Char 128   | Name of the Company responsible for the probe/sentry that sent the initiating sentry message. |
| Attacker IP      | Char 25    | IP address of the device that invoked this attack.                                            |
| Vcategory        | Drop Down  | Category of the Victim device.                                                                |
| Victim IP        | Char 25    | IP address of the Victim device.                                                              |
| Victim ID        | Char 45    | Pointer into the Install Table for the Victim device.                                         |
| Sensor IP        | Char 25    | IP address of the Sensor device that alerted the probe/sentry (e.g., firewall, IDS, etc.).    |

|                                             |                    |                                                                                                                                     |
|---------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Sensor ID                                   | Char 45            | Pointer into the Install Table for the Sensor.                                                                                      |
| Sentry IP                                   | Char 25            | IP address of the probe/sentry that monitored the Sensor.                                                                           |
| Sentry ID                                   | Char 45            | Pointer into the Install Table for the Sentry                                                                                       |
| Problem ID                                  | Char 15            | Pointer into the Problem Ticket Table for the Problem Ticket generated because of this Gateway Message.                             |
| Short Message                               | Char 255           | Message text sent by the Sentry.                                                                                                    |
| Long Message                                | Char 0             | Message text sent by the Sentry.                                                                                                    |
| Message ID                                  | Char 45            | Pointer into the Message Table indicating the type of message sent.                                                                 |
| SymptomID                                   | Char 45            | The Symptom linked to by the Message ID.                                                                                            |
| Symptom Name                                | Char 128           | The name of the above Symptom.                                                                                                      |
| Severity                                    | Drop-Down List     | Possible states include: Critical, Suspicious, Relevant, Interesting and Not Identified. May be derived from Symptom and Vcategory. |
| Sentry Hardware, Product, and OS            | Char 255           | Information regarding Sentry. Can be taken from the Install record pointed to by Sentry ID.                                         |
| Sensor Hardware, Product, and OS            | Char 255           | Information regarding Sensor. Can be taken from the Install record pointed to by Sensor ID.                                         |
| Victim Hardware, Product, and OS            | Char 255           | Information regarding Victim. Can be taken from the Install record pointed to by Victim ID.                                         |
| Desc1, Value1, Desc2, Value2, Desc3, Value3 | Char 64, Char 255  | Generic parameters sent by the probe/sentry.                                                                                        |
| Attack Time                                 | Date/Time          | Timestamp of when the attack occurred.                                                                                              |
| Attack uTime                                | Decimal            | Unix representation of the above time.                                                                                              |
| Sensor Time                                 | Date/Time          | Timestamp of when the sensor reported the attack.                                                                                   |
| Sensor uTime                                | Decimal            | Unix representation of the above time.                                                                                              |
| Gateway Time                                | Date/Time          | Timestamp of when the gateway reported the attack.                                                                                  |
| Sensor uTime                                | Decimal            | Unix representation of the above time.                                                                                              |
| Grouped Messages                            | Radio Button       | Yes or No. Indicates if this Message is one of a group of several messages of the same type.                                        |
| Group Count Start, Group Count uTime        | Date/Time, Decimal | When the probe/sentry started counting the messages in this group.                                                                  |
| Group Count Duration                        | Decimal            | How long (in, for example, milliseconds) the probe/sentry counted the messages in this group.                                       |
| Message Count                               | Integer            | How many messages the probe/sentry counted in this group.                                                                           |

TABLE 7. SOC:Install

| Name | Field Type | Description |
|------|------------|-------------|
|------|------------|-------------|

|                                                              |                      |                                                                                                                                                                                    |
|--------------------------------------------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Company ID                                                   | Char 15              | Pointer into the Company Table indicating the company that is being monitored.                                                                                                     |
| Company Name                                                 | Char 128             | Name of the Company.                                                                                                                                                               |
| Tag Number                                                   | Char 45              | Unique identifier for particular device.                                                                                                                                           |
| HardwareID,<br>HardwareName                                  | Char 15,<br>Char 255 | Pointer into Technology table representing the Hardware for this device.                                                                                                           |
| ProductID,<br>ProductName                                    | Char 15,<br>Char 255 | Pointer into Technology table representing the Product for this device.                                                                                                            |
| OSID, OSName                                                 | Char 15,<br>Char 255 | Pointer into Technology table representing the Operating System for this device.                                                                                                   |
| Status                                                       | Drop-Down List       | Possible states include: Ordered, Received, Being Assembled, Deployed, In Repair, Down, End of Life, Transferred, Delete, In Inventory, On Loan, Disposed.                         |
| Supported                                                    | Radio Button         | Yes or No. Indicates whether the MSM service supports this device. For probe/sentries this normally can be Yes; for Installs that point to probe/sentries this normally can be No. |
| Sentry                                                       | Radio Button         | Yes or No. Indicates whether or not this Install is a probe/sentry.                                                                                                                |
| Device IP                                                    | Char 25              | The IP address of this device.                                                                                                                                                     |
| Sentry ID                                                    | Char 45              | The Tag Number of the probe/sentry that this Device points to. May be left blank if this Install is a probe/sentry.                                                                |
| Machine Name                                                 | Char 64              | Name of the particular device.                                                                                                                                                     |
| Machine Category                                             | Drop-Down List       | Category of device, including Unknown, Known, and Mission Critical.                                                                                                                |
| Contact ID, Contact Name                                     | Char 15,<br>Char 40  | Pointer into the SOC:Contacts table for the contact matrix.                                                                                                                        |
| Received Date, Returned Date, Available Date, Installed Date | Date/Time            | A series of dates that can record the life of the Install.                                                                                                                         |
| CPU Serial Number, Monitor Serial Number                     | Char 64              | Vendor identifying numbers.                                                                                                                                                        |
| Accessories                                                  | Char 128             | A description of peripherals installed.                                                                                                                                            |
| Installer                                                    | Char 155             | The full name of the person that installed this device.                                                                                                                            |
| Owner                                                        | Char 155             | The full name of the person that owns this device.                                                                                                                                 |
| Department, Floor, Room, Cage                                | Char 65              | Identifying the location of the Installed device.                                                                                                                                  |
| Use Company Location                                         | Radio Button         | Yes or No. Indicates whether or not to use the company location information stored in the Company record.                                                                          |
| TimeZone Desc                                                | Char 255             | Character Description of the Time Zone.                                                                                                                                            |

|                                                                                                                          |            |                                                                               |
|--------------------------------------------------------------------------------------------------------------------------|------------|-------------------------------------------------------------------------------|
| Time Zone                                                                                                                | Real       | Numeric offset from GMT.                                                      |
| Region                                                                                                                   | Char 30    | Company defined region.                                                       |
| Site                                                                                                                     | Char 30    | Company defined site.                                                         |
| P.O. Box                                                                                                                 | Char 10    | Post office box number.                                                       |
| Street Number                                                                                                            | Char 10    | Street number.                                                                |
| Street Name                                                                                                              | Char 65    | Street name.                                                                  |
| Other Street Info                                                                                                        | Char 65    | Address information other than Street Name and Number (e.g., 100 Plaza East). |
| City                                                                                                                     | Char 65    | City.                                                                         |
| Country                                                                                                                  | Char 65    | Country.                                                                      |
| Zip Code                                                                                                                 | Char 30    | Zip or postal code.                                                           |
| Mailing Address                                                                                                          | Char 300   | The mailing address exactly as written on a post envelope.                    |
| Router Address, Subnet Mask, Ethernet Address, NATIP, SSH Port, Public Key, BIOS Password, Root Password, Other Password | Char       | Specific information about this Install.                                      |
| Memo                                                                                                                     | Diary      | Pertinent notes for this record.                                              |
| Attachments                                                                                                              | Attachment | Pertinent file attachments for this record.                                   |

TABLE 8. SOC:Message

| Name        | Field Type     | Description                                                                       |
|-------------|----------------|-----------------------------------------------------------------------------------|
| Message ID  | Char 45        | Sentry group defined identifier for a message.                                    |
| Symptom ID  | Char 45        | Pointer to the Symptom table.                                                     |
| Name        | Char 255       | Name of the message.                                                              |
| Service     | Char 30        | Service to which this message pertains.                                           |
| Type        | Drop-Down List | Type of message, including Drop, Forensic, Report, Alert.                         |
| Description | Char 255       | Description of message.                                                           |
| Pattern(s)  | Char 0         | The actual filter pattern(s). Each filter pattern can be separated by a new line. |
| Memo        | Diary          | Pertinent notes for this record.                                                  |

TABLE 9. SOC:Person

| Name      | Field Type | Description                        |
|-----------|------------|------------------------------------|
| PersonID  | Char 15    | Unique identifier for this person. |
| CompanyID | Char 15    | Pointer into the Company table.    |

|                                                              |                |                                                                                         |
|--------------------------------------------------------------|----------------|-----------------------------------------------------------------------------------------|
| Company Name                                                 | Char 128       | Name of the above Company.                                                              |
| Last Name                                                    | Char 65        | Last name.                                                                              |
| First Name                                                   | Char 65        | First name.                                                                             |
| MI                                                           | Char 5         | Middle initial.                                                                         |
| Full Name                                                    | Char 155       | The full name of this person in a particular format (e.g., first name first).           |
| Courtesy Title                                               | Drop-Down List | Possible states include: Mr., Ms., Mrs., Miss. or Dr.                                   |
| Title                                                        | Char 50        | The person's job title (e.g., on the person's business card).                           |
| Level                                                        | Radio Button   | Possible states include: Officer, VP, Director, Manager, Supervisor, Technician, Other. |
| Works in Support                                             | Radio Button   | Yes, No.                                                                                |
| Work Phone, Work Phone2, Fax, Fax2, Mobile Phone, Home Phone | Char 30        | Phone numbers that could be used to contact this person.                                |
| Email                                                        | Char 255       | Email address of this person.                                                           |
| CC:Email                                                     | Char 255       | Email address(es) of those to CC when emailing this person.                             |
| Area Code                                                    | Char 10        | Geographically identifies where this person is located.                                 |
| Pager Phone, Pager Email, Pager Pin, Pager Provider          | Char           | Pager information.                                                                      |
| Department, Floor, Room                                      | Char 65        | Location of this person.                                                                |
| Use Company Location                                         | Radio Button   | Yes or No. Indicates whether or not to use the location stored in the Company record.   |
| TimeZone Desc                                                | Char 255       | Character description of the Time Zone.                                                 |
| Time Zone                                                    | Real           | Numeric offset from GMT.                                                                |
| Region                                                       | Char 30        | Company defined region.                                                                 |
| Site                                                         | Char 30        | Company defined site.                                                                   |
| P.O. Box                                                     | Char 10        | Post office box number.                                                                 |
| Street Number                                                | Char 10        | Street number.                                                                          |
| Street Name                                                  | Char 65        | Street name.                                                                            |
| Other Street Info                                            | Char 65        | Address information other than Street Name and Number (e.g., 100 Plaza East).           |
| City                                                         | Char 65        | City.                                                                                   |
| Country                                                      | Char 65        | Country.                                                                                |
| Zip Code                                                     | Char 30        | Zip or postal code.                                                                     |
| Mailing Address                                              | Char 300       | Mailing address exactly as written on a post envelope.                                  |
| Memo                                                         | Diary          | Pertinent notes for this record.                                                        |

|             |            |                                             |
|-------------|------------|---------------------------------------------|
| Attachments | Attachment | Pertinent file attachments for this record. |
|-------------|------------|---------------------------------------------|

**TABLE 10. SOC:Problem Ticket**

| Name                                                      | Field Type        | Description                                                                                                                      |
|-----------------------------------------------------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------|
| Problem ID                                                | Char 15           | Unique identifier for this record.                                                                                               |
| Status                                                    | Drop-Down List    | Possible states include: Open, Assigned, In Progress, Pending, Ongoing, Resolved, Consolidated, Closed.                          |
| CompanyID                                                 | Char 15           | Pointer into the Company table.                                                                                                  |
| Company Name                                              | Char 128          | Name of the above Company.                                                                                                       |
| Priority                                                  | Char 2            | An identifier indicating what to work on first.                                                                                  |
| Pending Reason                                            | Drop-Down List    | Possible states: Waiting for Customer Callback, Problem is Being Monitored, Collecting Report Data, Reoccurring Normal Function. |
| Source                                                    | Drop-Down List    | Possible values: Gateway, Operator, Customer.                                                                                    |
| Caller, Caller Name                                       | Char 15, Char 155 | Full Name of the person who called. A record should also be made in Person.                                                      |
| Assigned Operator, AssignedOperatorName                   | Char 15, Char 155 | Full name of the analyst assigned to this problem.                                                                               |
| Sentry ID                                                 | Char 45           | Pointer to the Install record for the probe/sentry that reported this problem.                                                   |
| Sentry IP                                                 | Char 25           | IP address of the above probe/sentry                                                                                             |
| Linked Gateway Messages                                   | Table             | A table of all Gateway Messages linked to this problem.                                                                          |
| 1 <sup>st</sup> Symptom ID                                | Char 45           | Pointer into the Symptom table to the most relevant Symptom.                                                                     |
| 1 <sup>st</sup> Symptom Name                              | Char 65           | Name of the above Symptom                                                                                                        |
| Diagnoses with the above symptom                          | Table             | A table of all Diagnoses that are linked to 1 <sup>st</sup> Symptom ID.                                                          |
| Diagnosis ID                                              | Char 15           | Pointer into the Diagnosis table to proposed Diagnosis.                                                                          |
| Diagnosis Name                                            | Char 60           | Name of the above Diagnosis.                                                                                                     |
| Symptoms of this Diagnosis                                | Table             | A table of all symptoms linked to the Diagnosis ID.                                                                              |
| Attack Time                                               | Date/Time         | Timestamp of when the attack occurred                                                                                            |
| Sensor Time                                               | Date/Time         | Timestamp of when the sensor reported the attack                                                                                 |
| Gateway Time                                              | Date/Time         | Timestamp of when the gateway reported the attack                                                                                |
| Create Time                                               | Date/Time         | Timestamp of when the problem ticket was created                                                                                 |
| Resolved Time                                             | Date/Time         | Timestamp of when the problem ticket was resolved                                                                                |
| Sentry Delta, Gateway Delta, Create Delta, Resolved Delta | Integer           | The number of seconds between two consecutive timestamps. Useful to identify lags in the process.                                |
| Department, Floor,                                        | Char              | Can be copied from the probe/sentry record.                                                                                      |

|                                                                                                                                                  |            |                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------|------------|---------------------------------------------|
| Room, Cage, Region,<br>Site, Street Number,<br>Street Name, Other<br>Street Info, City,<br>State, Country, Zip<br>Code, Hardware,<br>Product, OS |            |                                             |
| Memo                                                                                                                                             | Diary      | Pertinent notes for this record.            |
| Attachments                                                                                                                                      | Attachment | Pertinent file attachments for this record. |

**TABLE 11. SOC:SecurityFocusVulnerability**

| Name                                                                                                                                                  | Field Type | Description                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Name                                                                                                                                                  | Char 255   | Name of the Vulnerability.                                                                                                             |
| LinksToVulnerability                                                                                                                                  | Char 40    | Pointer into the Vulnerability table.                                                                                                  |
| LinksToVulnName                                                                                                                                       | Char 255   | Name of the above Vulnerability.                                                                                                       |
| Bugtraq id                                                                                                                                            | Char 255   | SecurityFocus.com defined unique identifier for this Vulnerability.                                                                    |
| Object, Class, cve,<br>published, updated,<br>remote, local,<br>Vulnerable, Not<br>Vulnerable, Credit,<br>Discussion, Exploit,<br>Reference, Solution | Char       | SecurityFocus.com defined information fields as described in <a href="http://www.securityfocus.com">http://www.securityfocus.com</a> . |
| Memo                                                                                                                                                  | Diary      | Pertinent notes for this record.                                                                                                       |
| Attachments                                                                                                                                           | Attachment | Pertinent file attachments for this record.                                                                                            |

**TABLE 12. SOC:Symptom**

| Name                                                                                 | Field Type         | Description                                                                                                                             |
|--------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| SymptomID                                                                            | Char 45            | Unique identifier for this record.                                                                                                      |
| Name                                                                                 | Char 128           | Name of this Symptom.                                                                                                                   |
| Severity<br>For Unknown Victim<br>For Known Victim<br>For Mission Critical<br>Victim | Drop-<br>Down List | Possible values: Critical, Suspicious, Relevant, Interesting and Not Defined. Indicates severity for each category of installed device. |
| Description                                                                          | Char 255           | A lengthy description of this Symptom                                                                                                   |
| Memo                                                                                 | Diary              | Pertinent notes for this record.                                                                                                        |
| Attachments                                                                          | Attachment         | Pertinent file attachments for this record.                                                                                             |

TABLE 13. SOC:SymptomToDiagnosis

| Name           | Field Type     | Description                                                                                                       |
|----------------|----------------|-------------------------------------------------------------------------------------------------------------------|
| ID             | Char 15        | Unique identifier for the record.                                                                                 |
| Symptom ID     | Char 40        | Pointer to the Symptom record.                                                                                    |
| Symptom Name   | Char 255       | Name of the Symptom.                                                                                              |
| Diagnosis ID   | Char 15        | Pointer to the Diagnosis record.                                                                                  |
| Diagnosis Name | Char 255       | Name of the Diagnosis.                                                                                            |
| Closeness      | Drop-Down List | Possible values: Definitely Not Connected, Might Be Connected, Likely Connected, Connected, Definitely Connected. |

TABLE 14. SOC:SymToTechnology

| Name                             | Field Type           | Description                                                                                                                   |
|----------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Symptom ID, Symptom Name         | Char 40,<br>Char 255 | Pointer to the Symptom record.                                                                                                |
| Technology ID<br>Technology Name | Char 15,<br>Char 255 | The name of the Technology to which this Symptom is linked.                                                                   |
| Relationship                     | Drop-Down List       | Possible values: Confirmed Unrelated, "Low" Relationship, "Medium" Relationship, "High" Relationship, Confirmed Relationship. |

TABLE 15. SOC:Technology

| Name                                                                   | Field Type           | Description                                                                  |
|------------------------------------------------------------------------|----------------------|------------------------------------------------------------------------------|
| Technology ID                                                          | Char 15              | Unique identifier for this record.                                           |
| Category 1                                                             | Char 126             | Indicates most general level of categorization (e.g., hardware or software). |
| Category 2                                                             | Char 126             | Next category level (e.g., operating system, firewall, etc.).                |
| Category 3                                                             | Char 126             | Vendor and product (e.g., Microsoft Windows NT).                             |
| Category 4                                                             | Char 126             | Version number (e.g., 4.0).                                                  |
| Category 5                                                             | Char 126             | Service pack (e.g., SP5).                                                    |
| Name                                                                   | Char 255             | Can be a concatenation of Categories 3, 4, and 5.                            |
| VendorID, VendorName                                                   | Char 15,<br>Char 128 | Pointer to Company table indicating the vendor of this Technology.           |
| Product Number,<br>Description, Supplier<br>Name, Manufacturer<br>Name | Char                 | Recent information regarding how this Technology was purchased.              |

|             |            |                                             |
|-------------|------------|---------------------------------------------|
| Memo        | Diary      | Pertinent notes for this record.            |
| Attachments | Attachment | Pertinent file attachments for this record. |

TABLE 16. SOC:TimeZone

| Name  | Field Type | Description                        |
|-------|------------|------------------------------------|
| Name  | Char 60    | Text description of the time zone. |
| Value | Real       | Hours difference from GMT.         |

TABLE 17. SOC:Vulnerability

| Name                 | Field Type | Description                                                                                         |
|----------------------|------------|-----------------------------------------------------------------------------------------------------|
| Vulnerability ID     | Char 40    | Unique identifier for this Vulnerability.                                                           |
| Name                 | Char 80    | Full name of the Vulnerability.                                                                     |
| Summary              | Char 0     | Summary description of the Vulnerability.                                                           |
| Description          | Char 0     | Detailed technical description of the Vulnerability.                                                |
| AffectedTechnologies | Char 0     | A listing of affected Technologies and configurations.<br>This data can be additionally structured. |
| Memo                 | Diary      | Pertinent notes for this record.                                                                    |
| Attachments          | Attachment | Pertinent file attachments for this record.                                                         |

TABLE 18. SOC:VulnerabilityToDiagnosis

| Name               | Field Type | Description                          |
|--------------------|------------|--------------------------------------|
| ID                 | Char 15    | Unique identifier for the record.    |
| Vulnerability ID   | Char 40    | Pointer to the Vulnerability record. |
| Vulnerability Name | Char 255   | Name of the Vulnerability.           |
| Diagnosis ID       | Char 15    | Pointer to the Diagnosis record.     |
| Diagnosis Name     | Char 255   | Name of the Diagnosis.               |

TABLE 19. SOC:VulnToTechnology

| Name                                    | Field Type           | Description                                                                                                                   |
|-----------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Vulnerability ID,<br>Vulnerability Name | Char 30,<br>Char 255 | Pointer to the Vulnerability record.                                                                                          |
| Technology ID,<br>Technology Name       | Char 15,<br>Char 255 | Pointer to the Technology record.                                                                                             |
| Relationship                            | Drop-Down<br>List    | Possible values: Confirmed Unrelated, "Low" Relationship, "Medium" Relationship, "High" Relationship, Confirmed Relationship. |

TABLE 20. Active Links

| Name                                                      | Description                                                                                                                                                               |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SOC:CIPersonNameA1 – CIPersonNameB10                      | Retrieves a person's name based on ID.                                                                                                                                    |
| SOC:CIPushA1-CIPushB10                                    | Displays a highlighted contact's personal information at the bottom of the SOC:Contacts form.                                                                             |
| SOC:COContacts                                            | Runs the SOC:FindContacts macro when the Contacts button is pushed on the SOC:Company form.                                                                               |
| SOC:COContactsName                                        | Retrieves a contact's name based on ID.                                                                                                                                   |
| SOC:COGenerateMailingAddress                              | Concatenates Address, City, State, Country and Zip information into the Mailing Address field when the Generate Mailing Address button is pushed on the SOC:Company form. |
| SOC:COTimeZone                                            | Looks up a TimeZone value when a TimeZone name is selected on the SOC:Company form.                                                                                       |
| SOC:CTDisplayPersonRecord                                 | Runs the SOC:FindPerson macro when the GoTo the Full Person Record button is pushed on the SOC:Contacts form.                                                             |
| SOC:CRResponsiblePersonName                               | Retrieves the person's name based on ID.                                                                                                                                  |
| SOC:CRUpdateFrom                                          | Retrieves the person's name based on ID.                                                                                                                                  |
| SOC:DTDDisplayPersonRecord                                | Runs the Display Person Record macro.                                                                                                                                     |
| SOC:INCompanyID                                           | Looks up the CompanyID when a Company Name is selected on the SOC:Install form.                                                                                           |
| SOC:INContacts                                            | Runs the SOC:FindContacts macro when the Contacts button is pushed on the SOC:Install form.                                                                               |
| SOC:INContactsName                                        | Retrieves the contact's name based on ID.                                                                                                                                 |
| SOC:INCopyCompanyLocation                                 | Copies Company information into the SOC:Install form when the Copy Company Info button is pushed.                                                                         |
| SOC:INGenerateMailingAddress                              | Concatenates Address, City, State, Country and Zip information into the Mailing Address field when the Generate Mailing Address button is pushed on the SOC:Install form. |
| SOC:INHardwareName,<br>SOC:INOSName,<br>SOC:INProductName | Retrieves the Install's name based on ID.                                                                                                                                 |
| SOC:INTimeZone                                            | Looks up a TimeZone value when a TimeZone name is selected on the SOC:Install form.                                                                                       |
| SOC:INUseCompanyLocation                                  | Changes fields from read only to read write (and vice versa) when the Use Company Location radio button is selected on the SOC:Install form.                              |
| SOC:IPAssignedEngineerPerson                              | Retrieves the person's name based on ID.                                                                                                                                  |

|                              |                                                                                                                                                                                  |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SOC:IPCallerPersonName       | Retrieves the person's name based on ID.                                                                                                                                         |
| SOC:PECompanyID              | Looks up the CompanyID when a Company Name is selected on the SOC:Person form.                                                                                                   |
| SOC:PECopyCompanyLocation    | Copies Company information into the SOC:Person form when the Copy Company Info button is pushed.                                                                                 |
| SOC:PEGenerateFullName       | Concatenates First Name, Middle Initial and Last Name into the Full Name field when the Generate Full Name button is pushed on the SOC:Person form.                              |
| SOC:PEGenerateMailingAddress | Concatenates Address, City, State, Country and Zip information into the Mailing Address field with the Generate Mailing Address button is pushed on the SOC:Problem Ticket form. |
| SOC:PETimeZone               | Looks up a TimeZone value when a TimeZone name is selected on the SOC:Person form.                                                                                               |
| SOC:PRAssignedOperatorPerson | Retrieves the person's name based on ID.                                                                                                                                         |
| SOC:PRCallerPersonName       | Retrieves the person's name based on ID.                                                                                                                                         |
| SOC:PRCreateDelta            | Calculates Create Delta when Create Time changes on the SOC:Problem Ticket form.                                                                                                 |
| SOC:PRCreateDelta2           | Calculates Create Delta when Gateway Time changes on the SOC:Problem Ticket form.                                                                                                |
| SOC:PRDiagnosisName          | Looks up the Diagnosis ID when a Diagnosis Name is selected on the SOC:Problem Ticket form.                                                                                      |
| SOC:PRFillSentryInfo         | Sets the Sentry Location fields by looking up Sentry ID on Install.                                                                                                              |
| SOC:PRFillSentryInfo10       | Runs the clearflag macro so that the user is not prompted to save data when the user initially displays data.                                                                    |
| SOC:PRFindCompany            | Runs the SOC:FindCompany macro when the Company button is pushed on the SOC:Problem Ticket form.                                                                                 |
| SOC:PRFindContacts           | Runs the SOC:FindContacts macro when the Contacts button is pushed on the SOC:Problem Ticket form.                                                                               |
| SOC:PRFindSentry             | Runs the SOC:FindInstall macro when the Sentry button is pushed on the SOC:Problem Ticket form.                                                                                  |
| SOC:PRGatewayDelta           | Calculates Gateway Delta when Sensor Time changes on the SOC:Problem Ticket form.                                                                                                |
| SOC:PRGatewayDelta2          | Calculates Gateway Delta when the Gateway Time changes on the SOC:Problem Ticket form.                                                                                           |
| SOC:PRResolvedDelta          | Calculates Resolved Delta when Create Time changes on the SOC:Problem Ticket form.                                                                                               |
| SOC:PRResolvedDelta2         | Calculates Resolved Delta when Resolved Time changes on the SOC:Problem Ticket form.                                                                                             |
| SOC:PRSensorDelta            | Calculates Sensor Delta when Sensor Time changes on the SOC:Problem Ticket form.                                                                                                 |
| SOC:PRSensorDelta2           | Calculates Sensor Delta when Sensor Time changes on the SOC:Problem Ticket form.                                                                                                 |

|                               |                                                                                                  |
|-------------------------------|--------------------------------------------------------------------------------------------------|
| SOC:PRSymptomName             | Looks up the Symptom ID when the Symptom Name is selected from a menu.                           |
| SOC:SDDiagnosisName           | Looks up the Diagnosis ID when the Diagnosis Name is selected from a menu.                       |
| SOC:SDSymptomName             | Looks up the Symptom ID when the Symptom Name is selected from a menu.                           |
| SOC:SFVulnName                | Looks up the VulnID when the Vulnerability Name is selected from a menu.                         |
| SOC:STSymptomName             | Looks up the Symptom ID when the Symptom Name is selected from a menu.                           |
| SOC:STTechnologyName          | Retrieves the Technology's name based on ID.                                                     |
| SOC:TOGenerateToolNameFromCat | Concatenates Categories 3, 4, and 5 into the Technology Name field in the SOC:Technology form.   |
| SOC:TORtnOnCat1               | Creates the Category 2 menu based on the result of the Category 1 menu.                          |
| SOC:TORtnOnCat2               | Creates the Category 3 menu based on the result of the Category 2 menu.                          |
| SOC:TORtnOnCat3               | Creates the Category 4 menu based on the result of the Category 3 menu.                          |
| SOC:TORtnOnCat4               | Creates the Category 5 menu based on the result of the Category 4 menu.                          |
| SOC:VDDiagnosisName           | Looks up the Diagnosis ID when a Diagnosis Name is selected from a menu.                         |
| SOC:VDVulnerabilityName       | Looks up the VulnID when the Vulnerability Name is selected from a menu.                         |
| SOC:VTTechnologName           | Retrieves the technology's name based on ID.                                                     |
| SOC:VTVulnName                | Looks up the VulnID when the Vulnerability Name is selected from a menu.                         |
| SOC:VUFindSecurityFocusVuln   | Runs the FindSecurityFocusVulnerability macro when the Info from SecurityFocus button is pushed. |

**TABLE 21. Filters**

| Name                          | Description                                                                                                         |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------|
| SOC:GMSubmitEvent10-50        | A series of filters that extracts information for a SOC:GatewayMessage record and creates a new SOC:Problem Ticket. |
| SOC:PRAuditLog                | Provides a record of all field values each time a SOC:Problem Ticket is modified.                                   |
| SOC:PRFillLastMemo            | Fills in a character field with the last typed in memo from the memo field in SOC:Problem Ticket.                   |
| SOC:PRSetSentryEventProblemID | Sets the ProblemID field in SOC:GatewayMessage whenever a GatewayMessage creates a new Problem ID.                  |

TABLE 22. Macros

| Name                          | Description                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------|
| SOC:FindContacts              | Runs a search on SOC:Contacts for all entries matching an input ContactID.                   |
| SOC:FindPerson                | Runs a search of SOC:Person for all entries matching an input PersonID.                      |
| clearflag                     | Clears the change flag for the current form.                                                 |
| SOC:FindCompany               | Runs a search on SOC:Company for all entries matching an input CompanyID.                    |
| SOC:FindInstall               | Runs a search on SOC:Install for all entries matching an input Tag Number.                   |
| FindSecurityFocusVulnerabilty | Runs a search on SOC:SecurityFocusVulnerability for all entries matching an input bugtraqid. |

TABLE 23. Menus

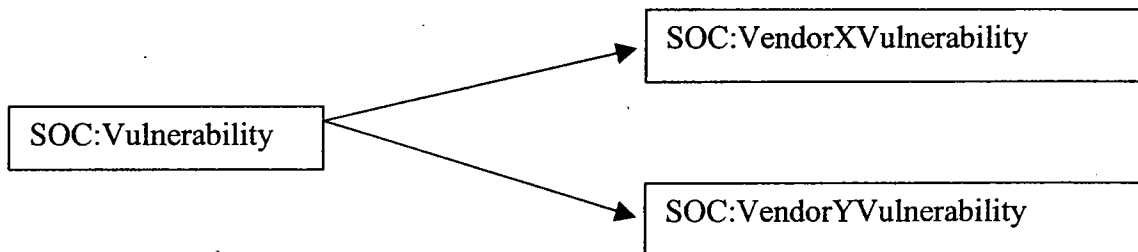
| Name                | Description                                                                                |
|---------------------|--------------------------------------------------------------------------------------------|
| SOC:Category1       | A list of categories describing this level of a specific Technology.                       |
| SOC:Category2       | A list of categories describing this level of a specific Technology.                       |
| SOC:Category3       | A list of categories describing this level of a specific Technology.                       |
| SOC:Category4       | A list of categories describing this level of a specific Technology.                       |
| SOC:Category5       | A list of categories describing this level of a specific Technology.                       |
| SOC:Company         | A list of Companies that return a Company Name when selected.                              |
| SOC:CompanyID       | A list of Companies that return a Company ID when selected.                                |
| SOC:Contacts        | A list of Contacts.                                                                        |
| SOC:Diagnosis       | A list of Diagnoses.                                                                       |
| SOC:Hardware        | A list of Technologies that have Category1="Hardware."                                     |
| SOC:Message         | A list of Messages.                                                                        |
| SOC:OperatingSystem | A list of Technologies that have Category1="Operating System."                             |
| SOC:Person          | A list of Persons.                                                                         |
| SOC:Problem         | A list of Problem Tickets.                                                                 |
| SOC:Product         | A list of Technologies that are do not have Category1="Hardware" or Category1 = "Operating |

|                     |                                               |
|---------------------|-----------------------------------------------|
|                     | System.”                                      |
| SOC:Sensor          | A list of all Installs that are not Sentries. |
| SOC:Sentry          | A list of all Installs that are Sentries.     |
| SOC:Symptoms        | A list of all Symptoms.                       |
| SOC:TimeZone        | A list of all TimeZones.                      |
| SOC:Tool            | A list of all Technologies.                   |
| SOC:Vulnerabilities | A list of all Vulnerabilities.                |

TABLE 24. Notifications

| Notify Individual/Group | Reason                 |
|-------------------------|------------------------|
| Assigned to Group       | Problem submitted.     |
| Assigned to Group       | Problem reassigned.    |
| Assigned to Group       | Escalation conditions. |

TABLE 25. Vulnerability Information



Vulnerability information from an outside vendor may be received in a variety of formats. An exemplary format is the following three column text table.

| Name             | Field Type   | Description                                                       |
|------------------|--------------|-------------------------------------------------------------------|
| ID               | Char 30      | Unique identifier for this vulnerability                          |
| Local            | Radio Button | The vulnerability is exploitable locally on the system or device. |
| Description      | Char 0       | A detailed description of the vulnerability.                      |
| Published        | Date/Time    | The date the vulnerability was made public.                       |
| Other fields ... | ...          | ...                                                               |

A vendor of vulnerability information can be required to specify fields. When specifying fields, the vendor should send the name of the field, a brief description of the field and the data type of the field. Some exemplary datatype rules are as follows:

- Always specify a length for a character field. Char 0 specifies a field that is 0-64MB of data in length. Use lengths that have a reasonable maximum size (e.g., less than 512 characters).
- Fields with a range of values should have those values listed under the type, for example (True, False), (Yes, No) and (Unlikely, Likely, Definite).
- Date/Time format is preferred for date and time values. If data cannot be sent in Date/Time format, then it can be sent as a character field.

In a preferred embodiment, each vendor of vulnerability information should send information in a format that can be imported into a SOCRATES database. One possible format is comma-separated values ("CSV") form. A SOCRATES form can be created and a CSV file with the header information can be sent to the vendor. The vendor can then email back a CSV file with the vulnerability data. This data should be made to adhere to certain rules, such as the following:

- The vendor must create a unique identifier for each row of data.
- On any given set of data, a row of data should be sent only once (no duplicate data in a CSV file).
- To change the data for a vulnerability, send an entire row of data for that unique identifier in a download file.
- The vendor may send the entire set of data in each CSV file or send only changes and updates. The decision may be left to the vendor.
- DateTime is sent in the standard "Month Day, Year" format, for example:  
"October 01, 1988"

#### TABLE 26. Naming Conventions

The SOCRATES system can employ naming conventions and standards to facilitate consistent workflow, easy to follow applications, and migration to new versions. For example, all SOCRATES forms and menus can be prefixed with the characters "SOC" followed by a full worded description. In addition, all active links and filters can be prefixed with the characters

"SOC" followed by an abbreviation for the attached form followed by a full worded description.

Exemplary abbreviations for each form can be as follows:

| Data Category                  | Abbreviation |
|--------------------------------|--------------|
| SOC:Change Request             | CR           |
| SOC:Company                    | CO           |
| SOC:Contacts                   | CI           |
| SOC:Diagnosis                  | DI           |
| SOC:Gateway Message            | GM           |
| SOC:Install                    | IN           |
| SOC:Message                    | ME           |
| SOC:Person                     | PE           |
| SOC:Problem Ticket             | PR           |
| SOC:SecurityFocusVulnerability | SF           |
| SOC:Symptom                    | SY           |
| SOC:SymptomToDiagnosis         | SD           |
| SOC:SymToTechnology            | ST           |
| SOC:Technology                 | TO           |
| SOC:TimeZone                   | TZ           |
| SOC:Vulnerability              | VU           |
| SOC:VulnerabilityToDiagnosis   | VD           |
| SOC:VulnToTechnology           | VT           |

## Electronic Patent Application Fee Transmittal

|                                         |                                                                                    |                 |               |                             |
|-----------------------------------------|------------------------------------------------------------------------------------|-----------------|---------------|-----------------------------|
| <b>Application Number:</b>              | 11551606                                                                           |                 |               |                             |
| <b>Filing Date:</b>                     | 20-Oct-2006                                                                        |                 |               |                             |
| <b>Title of Invention:</b>              | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |                 |               |                             |
| First Named Inventor/Applicant Name:    | Bruce Schneier                                                                     |                 |               |                             |
| <b>Filer:</b>                           | Nayantara Chatterjee-Marathe                                                       |                 |               |                             |
| <b>Attorney Docket Number:</b>          | 022133-000520US                                                                    |                 |               |                             |
| Filed as Large Entity                   |                                                                                    |                 |               |                             |
| <b>Utility Filing Fees</b>              |                                                                                    |                 |               |                             |
| <b>Description</b>                      | <b>Fee Code</b>                                                                    | <b>Quantity</b> | <b>Amount</b> | <b>Sub-Total in USD(\$)</b> |
| <b>Basic Filing:</b>                    |                                                                                    |                 |               |                             |
| Utility application filing              | 1011                                                                               | 1               | 300           | 300                         |
| Utility Search Fee                      | 1111                                                                               | 1               | 500           | 500                         |
| Utility Examination Fee                 | 1311                                                                               | 1               | 200           | 200                         |
| <b>Pages:</b>                           |                                                                                    |                 |               |                             |
| <b>Claims:</b>                          |                                                                                    |                 |               |                             |
| Claims in excess of 20                  | 1202                                                                               | 6               | 50            | 300                         |
| <b>Miscellaneous-Filing:</b>            |                                                                                    |                 |               |                             |
| Late filing fee for oath or declaration | 1051                                                                               | 1               | 130           | 130                         |

| Description                        | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|------------------------------------|----------|----------|--------|----------------------|
| Petition:                          |          |          |        |                      |
| Patent-Appeals-and-Interference:   |          |          |        |                      |
| Post-Allowance-and-Post-Issuance:  |          |          |        |                      |
| Extension-of-Time:                 |          |          |        |                      |
| Extension - 2 months with \$0 paid | 1252     | 1        | 450    | 450                  |
| Miscellaneous:                     |          |          |        |                      |
| Total in USD (\$)                  |          |          |        | 1880                 |

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 1612812                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Nayantara Chatterjee-Marathe                                                       |
| <b>Filer Authorized By:</b>                 |                                                                                    |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 21-MAR-2007                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 17:36:31                                                                           |
| <b>Application Type:</b>                    | Utility                                                                            |

### Payment information:

|                                                                                                                                                                                             |         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Submitted with Payment                                                                                                                                                                      | yes     |
| Payment was successfully received in RAM                                                                                                                                                    | \$ 1880 |
| RAM confirmation Number                                                                                                                                                                     | 771     |
| Deposit Account                                                                                                                                                                             | 201430  |
| The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:<br>Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17 |         |

### File Listing:

---

| Document Number              | Document Description                                | File Name                                 | File Size(Bytes) | Multi Part /.zip | Pages (if appl.) |
|------------------------------|-----------------------------------------------------|-------------------------------------------|------------------|------------------|------------------|
| 1                            |                                                     | 022133-000520US_Preliminary_Amendment.pdf | 101599           | yes              | 7                |
|                              | Multipart Description/PDF files in .zip description |                                           |                  |                  |                  |
|                              | Document Description                                |                                           | Start            | End              |                  |
|                              | Specification                                       |                                           | 1                | 1                |                  |
|                              | Claims                                              |                                           | 2                | 5                |                  |
|                              | Drawings                                            |                                           | 6                | 6                |                  |
|                              | Applicant Arguments/Remarks Made in an Amendment    |                                           | 7                | 7                |                  |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 2                            | Drawings                                            | 022133-000520US_Replacement_Fig_8.pdf     | 37072            | no               | 1                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 3                            | Appendix to the Specification                       | 022133-000520US_Appendix_A.pdf            | 320641           | no               | 4                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 4                            | Appendix to the Specification                       | 022133-000520US_Appendix_B.pdf            | 213142           | no               | 1                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 5                            | Appendix to the Specification                       | 022133-000520US_Appendix_C.pdf            | 1614613          | no               | 19               |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 6                            | Fee Worksheet (PTO-06)                              | fee-info.pdf                              | 8778             | no               | 2                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| Total Files Size (in bytes): |                                                     |                                           | 2295845          |                  |                  |

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 1612812                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Nayantara Chatterjee-Marathe                                                       |
| <b>Filer Authorized By:</b>                 |                                                                                    |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 21-MAR-2007                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 17:36:31                                                                           |
| <b>Application Type:</b>                    | Utility                                                                            |

### Payment information:

|                                                                                                                                                                                             |         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Submitted with Payment                                                                                                                                                                      | yes     |
| Payment was successfully received in RAM                                                                                                                                                    | \$ 1880 |
| RAM confirmation Number                                                                                                                                                                     | 771     |
| Deposit Account                                                                                                                                                                             | 201430  |
| The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:<br>Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17 |         |

### File Listing:

---

| Document Number              | Document Description                                | File Name                                 | File Size(Bytes) | Multi Part /.zip | Pages (if appl.) |
|------------------------------|-----------------------------------------------------|-------------------------------------------|------------------|------------------|------------------|
| 1                            |                                                     | 022133-000520US_Preliminary_Amendment.pdf | 101599           | yes              | 7                |
|                              | Multipart Description/PDF files in .zip description |                                           |                  |                  |                  |
|                              | Document Description                                |                                           | Start            | End              |                  |
|                              | Specification                                       |                                           | 1                | 1                |                  |
|                              | Claims                                              |                                           | 2                | 5                |                  |
|                              | Drawings                                            |                                           | 6                | 6                |                  |
|                              | Applicant Arguments/Remarks Made in an Amendment    |                                           | 7                | 7                |                  |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 2                            | Drawings                                            | 022133-000520US_Replacement_Fig_8.pdf     | 37072            | no               | 1                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 3                            | Appendix to the Specification                       | 022133-000520US_Appendix_A.pdf            | 320641           | no               | 4                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 4                            | Appendix to the Specification                       | 022133-000520US_Appendix_B.pdf            | 213142           | no               | 1                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 5                            | Appendix to the Specification                       | 022133-000520US_Appendix_C.pdf            | 1614613          | no               | 19               |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| 6                            | Fee Worksheet (PTO-06)                              | fee-info.pdf                              | 8778             | no               | 2                |
| Warnings:                    |                                                     |                                           |                  |                  |                  |
| Information:                 |                                                     |                                           |                  |                  |                  |
| Total Files Size (in bytes): |                                                     |                                           | 2295845          |                  |                  |

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**PATENT APPLICATION FEE DETERMINATION RECORD**

Substitute for Form PTO-875

Application or Docket Number

**11/551,606****APPLICATION AS FILED – PART I**

(Column 1)

(Column 2)

OR

**OTHER THAN  
SMALL ENTITY**

| FOR                                               | NUMBER FILED                                                                                                                                                                                                         | NUMBER EXTRA |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| BASIC FEE<br>(37 CFR 1.16(a), (b), or (c))        |                                                                                                                                                                                                                      |              |
| SEARCH FEE<br>(37 CFR 1.16(k), (l), or (m))       |                                                                                                                                                                                                                      |              |
| EXAMINATION FEE<br>(37 CFR 1.16(o), (p), or (q))  |                                                                                                                                                                                                                      |              |
| TOTAL CLAIMS<br>(37 CFR 1.16(i))                  | 26 minus 20 =                                                                                                                                                                                                        | * 6          |
| INDEPENDENT CLAIMS<br>(37 CFR 1.16(h))            | 2 minus 3 =                                                                                                                                                                                                          | * 0          |
| APPLICATION SIZE FEE<br>(37 CFR 1.16(s))          | If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR |              |
| MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j)) |                                                                                                                                                                                                                      |              |

| SMALL ENTITY |          |
|--------------|----------|
| RATE (\$)    | FEE (\$) |
|              |          |
|              |          |
|              |          |
| X\$ 25       |          |
| X\$100       |          |
|              |          |
| N/A          |          |
| TOTAL        |          |

OR

| RATE (\$) | FEE (\$)    |
|-----------|-------------|
|           | <b>300</b>  |
|           | <b>500</b>  |
|           | <b>200</b>  |
| X\$50     | <b>300</b>  |
| X\$200    |             |
|           |             |
| N/A       |             |
| TOTAL     | <b>1300</b> |

\* If the difference in column 1 is less than zero, enter "0" in column 2.

**APPLICATION AS AMENDED – PART II**

(Column 1)

(Column 2)

(Column 3)

OR

**OTHER THAN  
SMALL ENTITY**

| AMENDMENT A |                                                                 | CLAIMS<br>REMAINING<br>AFTER<br>AMENDMENT |       | HIGHEST<br>NUMBER<br>PREVIOUSLY<br>PAID FOR | PRESENT<br>EXTRA |
|-------------|-----------------------------------------------------------------|-------------------------------------------|-------|---------------------------------------------|------------------|
|             | Total<br>(37 CFR 1.16(i))                                       | *                                         | Minus | **                                          | =                |
|             | Independent<br>(37 CFR 1.16(h))                                 | *                                         | Minus | ***                                         | =                |
|             | Application Size Fee (37 CFR 1.16(s))                           |                                           |       |                                             |                  |
|             | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j)) |                                           |       |                                             |                  |

| SMALL ENTITY       |                             |
|--------------------|-----------------------------|
| RATE (\$)          | ADDI-<br>TIONAL<br>FEE (\$) |
| X =                |                             |
| X =                |                             |
|                    |                             |
| N/A                |                             |
| TOTAL<br>ADD'T FEE |                             |

OR

| RATE (\$)          | ADDI-<br>TIONAL<br>FEE (\$) |
|--------------------|-----------------------------|
| X =                |                             |
| X =                |                             |
|                    |                             |
| N/A                |                             |
| TOTAL<br>ADD'T FEE |                             |

| AMENDMENT B |                                                                 | CLAIMS<br>REMAINING<br>AFTER<br>AMENDMENT |       | HIGHEST<br>NUMBER<br>PREVIOUSLY<br>PAID FOR | PRESENT<br>EXTRA |
|-------------|-----------------------------------------------------------------|-------------------------------------------|-------|---------------------------------------------|------------------|
|             | Total<br>(37 CFR 1.16(i))                                       | *                                         | Minus | **                                          | =                |
|             | Independent<br>(37 CFR 1.16(h))                                 | *                                         | Minus | ***                                         | =                |
|             | Application Size Fee (37 CFR 1.16(s))                           |                                           |       |                                             |                  |
|             | FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j)) |                                           |       |                                             |                  |

| RATE (\$)          | ADDI-<br>TIONAL<br>FEE (\$) |
|--------------------|-----------------------------|
| X =                |                             |
| X =                |                             |
|                    |                             |
| N/A                |                             |
| TOTAL<br>ADD'T FEE |                             |

OR

| RATE (\$)          | ADDI-<br>TIONAL<br>FEE (\$) |
|--------------------|-----------------------------|
| X =                |                             |
| X =                |                             |
|                    |                             |
| N/A                |                             |
| TOTAL<br>ADD'T FEE |                             |

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

\*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| <b>PATENT APPLICATION FEE DETERMINATION RECORD</b><br>Substitute for Form PTO-875                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                               |                                  |                                    |               | Application or Docket Number<br><b>11/551,606</b> |                     | Filing Date<br><b>10/20/2006</b> |                     | <input type="checkbox"/> To be Mailed |                         |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------|---------------|---------------------------------------------------|---------------------|----------------------------------|---------------------|---------------------------------------|-------------------------|--|
| <b>APPLICATION AS FILED – PART I</b>                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                  | (Column 2)                         |               | SMALL ENTITY <input type="checkbox"/>             |                     | OR                               |                     | OTHER THAN SMALL ENTITY               |                         |  |
| FOR                                                                                                                                                                                                                                                                                                                                                                                                                                  | NUMBER FILED                                                                                                                                                                                                                  | NUMBER EXTRA                     | RATE (\$)                          | FEE (\$)      | RATE (\$)                                         | FEE (\$)            |                                  |                     |                                       |                         |  |
| <input type="checkbox"/> BASIC FEE<br>(37 CFR 1.16(a), (b), or (c))                                                                                                                                                                                                                                                                                                                                                                  | N/A                                                                                                                                                                                                                           | N/A                              | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |                         |  |
| <input type="checkbox"/> SEARCH FEE<br>(37 CFR 1.16(k), (l), or (m))                                                                                                                                                                                                                                                                                                                                                                 | N/A                                                                                                                                                                                                                           | N/A                              | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |                         |  |
| <input type="checkbox"/> EXAMINATION FEE<br>(37 CFR 1.16(o), (p), or (q))                                                                                                                                                                                                                                                                                                                                                            | N/A                                                                                                                                                                                                                           | N/A                              | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |                         |  |
| TOTAL CLAIMS<br>(37 CFR 1.16(i))                                                                                                                                                                                                                                                                                                                                                                                                     | minus 20 =                                                                                                                                                                                                                    | *                                | X \$                               | =             | OR                                                | X \$                | =                                |                     |                                       |                         |  |
| INDEPENDENT CLAIMS<br>(37 CFR 1.16(h))                                                                                                                                                                                                                                                                                                                                                                                               | minus 3 =                                                                                                                                                                                                                     | *                                | X \$                               | =             | OR                                                | X \$                | =                                |                     |                                       |                         |  |
| <input type="checkbox"/> APPLICATION SIZE FEE<br>(37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                    | If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s). |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |
| <input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |
| * If the difference in column 1 is less than zero, enter "0" in column 2.                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                               |                                  | TOTAL                              |               | TOTAL                                             |                     |                                  |                     |                                       |                         |  |
| <b>APPLICATION AS AMENDED – PART II</b>                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               | (Column 2)                       |                                    | (Column 3)    |                                                   | SMALL ENTITY        |                                  | OR                  |                                       | OTHER THAN SMALL ENTITY |  |
| AMENDMENT                                                                                                                                                                                                                                                                                                                                                                                                                            | 03/21/2007                                                                                                                                                                                                                    | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$)                                         | ADDITIONAL FEE (\$) | RATE (\$)                        | ADDITIONAL FEE (\$) |                                       |                         |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Total (37 CFR 1.16(i))                                                                                                                                                                                                        | * 26                             | Minus                              | ** 26         | = 0                                               | X \$                | =                                | OR                  | X \$50=                               | 0                       |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Independent (37 CFR 1.16(h))                                                                                                                                                                                                  | * 2                              | Minus                              | *** 3         | = 0                                               | X \$                | =                                | OR                  | X \$200=                              | 0                       |  |
| <input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |
| <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     | OR                               |                     |                                       |                         |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                               |                                  |                                    |               | TOTAL ADD'L FEE                                   |                     | OR                               | TOTAL ADD'L FEE     | 0                                     |                         |  |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               | (Column 2)                       |                                    | (Column 3)    |                                                   | SMALL ENTITY        |                                  | OR                  |                                       | OTHER THAN SMALL ENTITY |  |
| AMENDMENT                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                               | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$)                                         | ADDITIONAL FEE (\$) | RATE (\$)                        | ADDITIONAL FEE (\$) |                                       |                         |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Total (37 CFR 1.16(i))                                                                                                                                                                                                        | *                                | Minus                              | **            | =                                                 | X \$                | =                                | OR                  | X \$                                  | =                       |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Independent (37 CFR 1.16(h))                                                                                                                                                                                                  | *                                | Minus                              | ***           | =                                                 | X \$                | =                                | OR                  | X \$                                  | =                       |  |
| <input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |
| <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     | OR                               |                     |                                       |                         |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                               |                                  |                                    |               | TOTAL ADD'L FEE                                   |                     | OR                               | TOTAL ADD'L FEE     |                                       |                         |  |
| <p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p> |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |                         |  |

Legal Instrument Examiner:  
/Susan K. Ford/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on March 22, 2007.

PATENT  
Docket No.: 022133-000520US

TOWNSEND and TOWNSEND and CREW LLP

By: /Maureen Golob/  
Maureen Golob

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier

Application No.: 11/551,606

Filed: November 21, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Customer No. 20350

Examiner: Unassigned

Art Unit: Unassigned

Confirmation No. 1662

COMMUNICATION

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

On March 21, 2007, Applicant filed a Preliminary Amendment and accompanying documents in response to a Notice of Missing Parts of Application dated November 21, 2006.

Applicant also paid the fees required by the Notice of Missing Parts, together with the fee for a two-month extension of time. However, Applicant failed to file the Petition for Extension of Time at the time of filing.

Attached herewith is the required Petition for Extension of Time. Applicant respectfully requests that this Petition be entered in the file.

Bruce Schneier  
Application No.: 11/551,606  
Page 2

PATENT

Please contact the undersigned if there are any questions.

Respectfully submitted,

/Naya M. Chatterjee-Marathe/

Naya M. Chatterjee-Marathe  
Reg. No. 54,680

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, 8<sup>th</sup> Floor  
San Francisco, California 94111-3834  
Tel: (650) 326-2400  
Fax: (415) 576-0300  
NMC/mg

61011300 v1

| <b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b><br><br><b>FY 2006</b><br><i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Docket Number (Optional) 022133-000520US |                         |              |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|-------------------------|--------------|-------------------------|--|--------------------------------------------------------|-------|------|----------|--------------------------------------------------------------------|-------|-------|--------------|-----------------------------------------------------------|--------|-------|----------|----------------------------------------------------------|--------|-------|----------|----------------------------------------------------------|--------|--------|----------|
| Application Number 11/551,606                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Filed November 21, 2006                  |                         |              |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                          |                         |              |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| Art Unit                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Examiner                                 |                         |              |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <p>This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.</p> <p>The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;"></th> <th style="width: 15%; text-align: center;"><u>Fee</u></th> <th style="width: 15%; text-align: center;"><u>Small Entity Fee</u></th> <th style="width: 30%;"></th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> One month (37 CFR 1.17(a)(1))</td> <td style="text-align: center;">\$120</td> <td style="text-align: center;">\$60</td> <td>\$ _____</td> </tr> <tr> <td><input checked="" type="checkbox"/> Two months (37 CFR 1.17(a)(2))</td> <td style="text-align: center;">\$450</td> <td style="text-align: center;">\$225</td> <td>\$ 450 _____</td> </tr> <tr> <td><input type="checkbox"/> Three months (37 CFR 1.17(a)(3))</td> <td style="text-align: center;">\$1020</td> <td style="text-align: center;">\$510</td> <td>\$ _____</td> </tr> <tr> <td><input type="checkbox"/> Four months (37 CFR 1.17(a)(4))</td> <td style="text-align: center;">\$1590</td> <td style="text-align: center;">\$795</td> <td>\$ _____</td> </tr> <tr> <td><input type="checkbox"/> Five months (37 CFR 1.17(a)(5))</td> <td style="text-align: center;">\$2160</td> <td style="text-align: center;">\$1080</td> <td>\$ _____</td> </tr> </tbody> </table> <p><input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.</p> <p><input type="checkbox"/> A check in the amount of the fee is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input checked="" type="checkbox"/> The Director has already been authorized to charge fees in this application to a Deposit Account. The fees were paid on March 21, 2007.</p> <p><input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number <u>20-1430</u>. I have enclosed a duplicate copy of this sheet.</p> <p><b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b></p> <p>I am the</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <p><input type="checkbox"/> applicant/inventor.</p> <p><input type="checkbox"/> assignee of record of the entire interest. See 37 CFR 3.71.<br/>Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).</p> <p><input checked="" type="checkbox"/> attorney or agent of record. Registration Number <u>54,680</u></p> <p><input type="checkbox"/> attorney or agent under 37 CFR 1.34.<br/>Registration number if acting under 37 CFR 1.34 _____</p> </div> <div style="width: 35%; text-align: right;"> <p>March 22, 2007</p> <p>_____</p> <p>Date</p> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 60%;"> <p><u>/Naya Chatterjee-Marathe/</u></p> <p>Signature</p> <p><u>Naya Chatterjee-Marathe, Reg. No. 54,680</u></p> <p>Typed or printed name</p> </div> <div style="width: 35%; text-align: right;"> <p>650-326-2400</p> <p>_____</p> <p>Telephone Number</p> </div> </div> |                                          |                         | <u>Fee</u>   | <u>Small Entity Fee</u> |  | <input type="checkbox"/> One month (37 CFR 1.17(a)(1)) | \$120 | \$60 | \$ _____ | <input checked="" type="checkbox"/> Two months (37 CFR 1.17(a)(2)) | \$450 | \$225 | \$ 450 _____ | <input type="checkbox"/> Three months (37 CFR 1.17(a)(3)) | \$1020 | \$510 | \$ _____ | <input type="checkbox"/> Four months (37 CFR 1.17(a)(4)) | \$1590 | \$795 | \$ _____ | <input type="checkbox"/> Five months (37 CFR 1.17(a)(5)) | \$2160 | \$1080 | \$ _____ |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <u>Fee</u>                               | <u>Small Entity Fee</u> |              |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <input type="checkbox"/> One month (37 CFR 1.17(a)(1))                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | \$120                                    | \$60                    | \$ _____     |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <input checked="" type="checkbox"/> Two months (37 CFR 1.17(a)(2))                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | \$450                                    | \$225                   | \$ 450 _____ |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <input type="checkbox"/> Three months (37 CFR 1.17(a)(3))                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | \$1020                                   | \$510                   | \$ _____     |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <input type="checkbox"/> Four months (37 CFR 1.17(a)(4))                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | \$1590                                   | \$795                   | \$ _____     |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <input type="checkbox"/> Five months (37 CFR 1.17(a)(5))                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | \$2160                                   | \$1080                  | \$ _____     |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |
| <p>NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.</p> <p><input checked="" type="checkbox"/> Total of <u>1</u> forms are submitted.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                          |                         |              |                         |  |                                                        |       |      |          |                                                                    |       |       |              |                                                           |        |       |          |                                                          |        |       |          |                                                          |        |        |          |

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 1616655                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Nayantara Chatterjee-Marathe/Maureen Golob                                         |
| <b>Filer Authorized By:</b>                 | Nayantara Chatterjee-Marathe                                                       |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 22-MAR-2007                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 17:31:35                                                                           |
| <b>Application Type:</b>                    | Utility                                                                            |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description          | File Name                         | File Size(Bytes) | Multi Part /.zip | Pages (if appl.) |
|-----------------|-------------------------------|-----------------------------------|------------------|------------------|------------------|
| 1               | Miscellaneous Incoming Letter | 022133-000520US_Communication.pdf | 83005            | no               | 2                |

### Warnings:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                   |                                                    |        |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------------------------------------------|--------|----|---|
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                   |                                                    |        |    |   |
| 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Extension of Time | 022133-000520US_Petition_for_Extension_of_time.pdf | 107457 | no | 1 |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                   |                                                    |        |    |   |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                   |                                                    |        |    |   |
| <b>Total Files Size (in bytes):</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                   |                                                    | 190462 |    |   |
| <p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b><br/> <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b><br/> <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b><br/> <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p> |                   |                                                    |        |    |   |



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING or 371(c)<br>DATE | GRP ART UNIT | FIL FEE REC'D | ATTY. DOCKET NO | TOT CLAIMS | IND CLAIMS |
|--------------------|--------------------------|--------------|---------------|-----------------|------------|------------|
| 11/551,606         | 10/20/2006               | 2131         | 1430          | 022133-000520US | 26         | 2          |

**CONFIRMATION NO. 1662**

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

**UPDATED FILING RECEIPT**

Date Mailed: 03/30/2007

Receipt is acknowledged of this regular Patent Application. It will be considered in its order and you will be notified as to the results of the examination. Be sure to provide the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION when inquiring about this application. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please mail to the Commissioner for Patents P.O. Box 1450 Alexandria Va 22313-1450. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections (if appropriate).**

**Applicant(s)**

Bruce Schneier, Minneapolis, MN;  
Andrew H. Gross, San Jose, CA;  
Jonathan D. Callas, Mountain View, CA;

**Assignment For Published Patent Application**

Counterpane Internet Security, Inc., Mountain View, CA

**Power of Attorney:** The patent practitioners associated with Customer Number 20350

**Domestic Priority data as claimed by applicant**

This application is a CON of 09/766,343 01/19/2001 PAT 7,159,237  
which claims benefit of 60/190,326 03/16/2000

**Foreign Applications**

**If Required, Foreign Filing License Granted:** 11/20/2006

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is  
**US11/551,606**

**Projected Publication Date:** 07/12/2007

**Non-Publication Request:** No

**Early Publication Request:** No

**Title**

Method and System for Dynamic Network Intrusion Monitoring, Detection and Response

**Preliminary Class**

726

**PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES**

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

---

**LICENSE FOR FOREIGN FILING UNDER****Title 35, United States Code, Section 184****Title 37, Code of Federal Regulations, 5.11 & 5.15****GRANTED**

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under

37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

#### **NOT GRANTED**

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on May 2, 2007.

PATENT  
Attorney Docket No.: 022133-000520US

TOWNSEND and TOWNSEND and CREW LLP

By: /Maureen Golob/  
Maureen Golob

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier et al.

Application No.: 11/551,606

Filed: November 21, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Confirmation No.: 1662

Examiner: Unassigned

Art Unit: 2131

INFORMATION DISCLOSURE  
STATEMENT UNDER 37 CFR §1.97 and  
§1.98

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The references cited on attached form PTO/SB/08A and PTO/SB/08B are being called to the attention of the Examiner. In accordance with 37 CFR §1.98(d), copies of a number of the references can be found in Application No. 09/766,343, filed January 19, 2001 (Attorney Docket No. 022133-000510US). It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR §1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement.

However, if a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,

/Naya Chatterjee-Marathe/

Naya Chatterjee-Marathe  
Reg. No. 54,680

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400  
Fax: 650-326-2422  
NMC:tfw:mg  
61042835 v1

|                                                                                                                                               |   |    |                          |                        |                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------|---|----|--------------------------|------------------------|-----------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(Use as many sheets as necessary)</i> |   |    | <b>Complete if Known</b> |                        |                 |
|                                                                                                                                               |   |    | Application Number       | 11/551,606             |                 |
|                                                                                                                                               |   |    | Filing Date              | November 21, 2006      |                 |
|                                                                                                                                               |   |    | First Named Inventor     | Schneier, Bruce        |                 |
|                                                                                                                                               |   |    | Art Unit                 | 2131                   |                 |
|                                                                                                                                               |   |    | Examiner Name            | Unassigned             |                 |
| Sheet                                                                                                                                         | 1 | of | 3                        | Attorney Docket Number | 022133-000520US |

| U.S. PATENT DOCUMENTS |                          |                                          |                                |                                                    |                                                                                 |
|-----------------------|--------------------------|------------------------------------------|--------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------|
| Examiner<br>Initials* | Cite<br>No. <sup>1</sup> | Document Number                          | Publication Date<br>MM-DD-YYYY | Name of Patentee or<br>Applicant of Cited Document | Pages, Columns, Lines, Where<br>Relevant Passages or Relevant<br>Figures Appear |
|                       |                          | Number Kind Code <sup>2</sup> (if known) |                                |                                                    |                                                                                 |
|                       | 1                        | 5,440,723                                | 08-08-1995                     | Arnold et al.                                      |                                                                                 |
|                       | 2                        | 5,796,942                                | 08-18-1998                     | Esbensen                                           |                                                                                 |
|                       | 3                        | 5,909,493                                | 06-01-1999                     | Motoyama                                           |                                                                                 |
|                       | 4                        | 6,026,442                                | 02-15-2000                     | Lewis et al.                                       |                                                                                 |
|                       | 5                        | 6,088,804                                | 07-11-2000                     | Hill et al.                                        |                                                                                 |
|                       | 6                        | 6,119,236                                | 09-12-2000                     | Shipley                                            |                                                                                 |
|                       | 7                        | 6,125,390                                | 09-26-2000                     | Touboul                                            |                                                                                 |
|                       | 8                        | 6,182,226                                | 01-30-2001                     | Reid et al.                                        |                                                                                 |
|                       | 9                        | 6,205,551                                | 03-20-2001                     | Grosse                                             |                                                                                 |
|                       | 10                       | 6,298,445                                | 10-02-2001                     | Shostack et al.                                    |                                                                                 |
|                       | 11                       | 6,363,489                                | 03-26-2002                     | Comay et al.                                       |                                                                                 |
|                       | 12                       | 6,519,703                                | 02-11-2003                     | Joyce                                              |                                                                                 |
|                       | 13                       | 6,681,331                                | 01-20-2004                     | Munson et al.                                      |                                                                                 |
|                       | 14                       | 6,704,874                                | 03-09-2004                     | Porras et al.                                      |                                                                                 |

| FOREIGN PATENT DOCUMENTS |                       |                           |                     |                                   |                             |                                                 |                                                                           |                |
|--------------------------|-----------------------|---------------------------|---------------------|-----------------------------------|-----------------------------|-------------------------------------------------|---------------------------------------------------------------------------|----------------|
| Examiner Initials*       | Cite No. <sup>1</sup> | Foreign Patent Document   |                     |                                   | Publication Date MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear | T <sup>6</sup> |
|                          |                       | Country Code <sup>3</sup> | Number <sup>4</sup> | Kind Code <sup>5</sup> (if known) |                             |                                                 |                                                                           |                |
|                          |                       |                           |                     |                                   |                             |                                                 |                                                                           | <div></div>    |
|                          |                       |                           |                     |                                   |                             |                                                 |                                                                           |                |

|                       |  |                    |  |
|-----------------------|--|--------------------|--|
| Examiner<br>Signature |  | Date<br>Considered |  |
|-----------------------|--|--------------------|--|

<sup>1</sup> EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>2</sup> Applicant's unique citation designation number (optional). <sup>3</sup> Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>4</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>5</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>6</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>7</sup> Applicant is to place a check mark here if English language Translation is attached.

|                                                                                                                                        |   |    |   |                          |                   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--------------------------|-------------------|
| Substitute for form 1449B/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br>(Use as many sheets as necessary) |   |    |   | <b>Complete if Known</b> |                   |
|                                                                                                                                        |   |    |   | Application Number       | 11/551,606        |
|                                                                                                                                        |   |    |   | Filing Date              | November 21, 2006 |
|                                                                                                                                        |   |    |   | First Named Inventor     | Schneier, Bruce   |
|                                                                                                                                        |   |    |   | Art Unit                 | 2131              |
|                                                                                                                                        |   |    |   | Examiner Name            | Unassigned        |
| Sheet                                                                                                                                  | 2 | of | 3 | Attorney Docket Number   | 022133-000520US   |

| NON PATENT LITERATURE DOCUMENTS |                          |                                                                                                                                                                                                                                                                                             |                          |  |
|---------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--|
| Examiner<br>Initials *          | Cite<br>No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                             | T <sup>2</sup>           |  |
|                                 | 15                       | "FAQ: Network Intrusion Detection Systems," Version 0.3, Jan. 1, 1998, <a href="http://www.robertgraham.com/pubs/network-intrusion-detection.txt">http://www.robertgraham.com/pubs/network-intrusion-detection.txt</a> , downloaded Oct. 19, 2001, pp. 1-29.                                | <input type="checkbox"/> |  |
|                                 | 16                       | "Latest Network Management Products," (Product Information) <i>Communication News</i> , Jun. 2000, 2 pages total.                                                                                                                                                                           | <input type="checkbox"/> |  |
|                                 | 17                       | "Managed Security Services: Are They Right For You?" <i>ENT</i> , Nov. 22, 2000, 4 pages total.                                                                                                                                                                                             | <input type="checkbox"/> |  |
|                                 | 18                       | "Security Monitoring Services," <i>Information Week</i> , No. 792, June 26, 2000, p. 244.                                                                                                                                                                                                   | <input type="checkbox"/> |  |
|                                 | 19                       | BALASUBRAMANIYAN, J. S. et al., "An Architecture for Intrusion Detection Using Autonomous Agents," Center for Education and Research in Information Assurance and Security, CERIAS Technical Report May 1995, Jun. 11, 1998, pp. 1-19.                                                      | <input type="checkbox"/> |  |
|                                 | 20                       | BLACHARSKI, "Outsourcing Firewall Management -- Managed Firewall Services Prevent Security Burnouts -- Firewall Management Requires 24-Hour Vigilance. If You Can't Pull Round-the-Clock Guard Duty, Outsourcing May Be for You," <i>Network Magazine</i> , Vol. 60, Aug. 1, 2000, 6 pages. | <input type="checkbox"/> |  |
|                                 | 21                       | Citation details: "Automated Information System--(AIS) Alarm System," W. Hunteman, <a href="http://citeseer.nj.nec.com/context/1642652/0">http://citeseer.nj.nec.com/context/1642652/0</a> , downloaded Oct. 19, 2001, 1 page.                                                              | <input type="checkbox"/> |  |
|                                 | 22                       | COMPUTEL WHITE PAPERS, "Managed Security Monitoring," 2001, pp. 1-4.                                                                                                                                                                                                                        | <input type="checkbox"/> |  |
|                                 | 23                       | ESSEX, "E-Sleuths Make Net Safe for E-Commerce; RIPTech Stakes Its Claim in the Growing Market for Remotely Managed Security," <i>Computerworld</i> , Vol. 80, No. 1, Jun. 12, 2000, 2 pages.                                                                                               | <input type="checkbox"/> |  |
|                                 | 24                       | FRATTO, "RFP: Managed Firewall Services," <i>Network Computing</i> , Vol. 9, No. 20, p.68, Nov. 1, 1998, 12 pages total.                                                                                                                                                                    | <input type="checkbox"/> |  |
|                                 | 25                       | HUNTEMAN, W., "Automated Information System--(AIS) Alarm System," University of California, Los Alamos National Laboratory, In Proceedings of the 20th National Information Systems Security Conference, National Institute of Standards and Technology, Oct. 1997, pp. 1-12.               | <input type="checkbox"/> |  |

|                       |  |                    |  |
|-----------------------|--|--------------------|--|
| Examiner<br>Signature |  | Date<br>Considered |  |
|-----------------------|--|--------------------|--|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

|                                                                                                                                        |   |    |   |                          |                   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--------------------------|-------------------|
| Substitute for form 1449B/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br>(Use as many sheets as necessary) |   |    |   | <b>Complete if Known</b> |                   |
|                                                                                                                                        |   |    |   | Application Number       | 11/551,606        |
|                                                                                                                                        |   |    |   | Filing Date              | November 21, 2006 |
|                                                                                                                                        |   |    |   | First Named Inventor     | Schneier, Bruce   |
|                                                                                                                                        |   |    |   | Art Unit                 | 2131              |
|                                                                                                                                        |   |    |   | Examiner Name            | Unassigned        |
| Sheet                                                                                                                                  | 3 | of | 3 | Attorney Docket Number   | 022133-000520US   |

| NON PATENT LITERATURE DOCUMENTS |                          |                                                                                                                                                                                                                                                                                                                                                                                          |                          |  |
|---------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--|
| Examiner<br>Initials *          | Cite<br>No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                                                                                                                          | T <sup>2</sup>           |  |
|                                 | 26                       | M2 PRESSWIRE, "GTE Internetworking: GTE Internetworking Offers New Version of Its Site Patrol Managed Security Services," Sep. 3, 1999, pp. 1-3.                                                                                                                                                                                                                                         | <input type="checkbox"/> |  |
|                                 | 27                       | M2 PRESSWIRE, "ISS: ISS Acquires Netrex Secure Solutions," Aug. 31, 1999, 1 page.                                                                                                                                                                                                                                                                                                        | <input type="checkbox"/> |  |
|                                 | 28                       | MESSMER, "Security Needs Spawn Services Managed Detection Services Growing in Popularity," <i>Network World</i> , April 3, 2000, 1 page                                                                                                                                                                                                                                                  | <input type="checkbox"/> |  |
|                                 | 29                       | NEUMANN, P. G. et al., "Experience with Emerald to Date," Computer Science Laboratory, SRI International, 1st USENIX Workshop on Intrusion Detection and Networking Monitoring, Santa Clara, California, Apr. 11-12, 1999, pp. 73-80, <a href="http://www.csl.sri.com/users/neumann/det99.html">http://www.csl.sri.com/users/neumann/det99.html</a> , downloaded Oct. 19, 2001, pp. 1-9. | <input type="checkbox"/> |  |
|                                 | 30                       | PORRAS, P. A. et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Computer Science Laboratory, SRI International, 20th NISSC --Oct. 9, 1997 pp. 1-22 (version with legible text but no figures), pp. 1-13 (version with figures but illegible text)                                                                                                   | <input type="checkbox"/> |  |
|                                 | 31                       | REDSIREN, "Managed Solutions," downloaded from Internet << <a href="http://www.redsiren.com">http://www.redsiren.com</a> >>, p. 1-3 (Publication Date Unknown).                                                                                                                                                                                                                          | <input type="checkbox"/> |  |
|                                 | 32                       | RKON TECHNOLOGIES, downloaded from Internet << <a href="http://www.rkontechnologies.com">http://www.rkontechnologies.com</a> >> (Publication Date Unknown)                                                                                                                                                                                                                               | <input type="checkbox"/> |  |
|                                 | 33                       | SAVAGE, "Locking the Doors -- Denial of Services Attacks and Viruses Prime the Market For Security Solutions and Services," <i>Computer Reseller News</i> , Vol. 72, Sep. 25, 2000, 2 pages total.                                                                                                                                                                                       | <input type="checkbox"/> |  |
|                                 | 34                       | VPNTRUST: CONSULTING, "VPNTrust Services: Consulting" 1999, Technica Corporation, pp. 1-3.                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> |  |

|                       |  |                    |  |
|-----------------------|--|--------------------|--|
| Examiner<br>Signature |  | Date<br>Considered |  |
|-----------------------|--|--------------------|--|

<sup>1</sup> EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>2</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 1738872                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Nayantara Chatterjee-Marathe                                                       |
| <b>Filer Authorized By:</b>                 |                                                                                    |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 02-MAY-2007                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 18:22:35                                                                           |
| <b>Application Type:</b>                    | Utility                                                                            |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description                         | File Name               | File Size(Bytes) | Multi Part /.zip | Pages (if appl.) |
|-----------------|----------------------------------------------|-------------------------|------------------|------------------|------------------|
| 1               | Information Disclosure Statement (IDS) Filed | 022133-000520US_IDS.pdf | 280550           | no               | 5                |

### Warnings:

**Information:**

This is not an USPTO supplied IDS fillable form

**Total Files Size (in bytes):**

280550

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

| APPLICATION NUMBER | FILING OR 371(c) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | 022133-000520US        |

**CONFIRMATION NO. 1662**

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA94111-3834

**Title:** Method and System for Dynamic Network Intrusion Monitoring, Detection and Response

**Publication No.** US-2007-0162973-A1

**Publication Date:** 07/12/2007

**NOTICE OF PUBLICATION OF APPLICATION**

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at [www.uspto.gov](http://www.uspto.gov). The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at [www.uspto.gov](http://www.uspto.gov) using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

| APPLICATION NUMBER | FILING OR 371(c) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | 022133-000520US        |

**CONFIRMATION NO. 1662**

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA94111-3834

**Title:** Method and System for Dynamic Network Intrusion Monitoring, Detection and Response

**Publication No.** US-2007-0162973-A1

**Publication Date:** 07/12/2007

**NOTICE OF PUBLICATION OF APPLICATION**

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at [www.uspto.gov](http://www.uspto.gov). The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at [www.uspto.gov](http://www.uspto.gov) using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

**REQUEST FOR WITHDRAWAL  
AS ATTORNEY OR AGENT  
AND CHANGE OF  
CORRESPONDENCE ADDRESS**

|                        |                 |
|------------------------|-----------------|
| Application Number     | 11/551,606      |
| Application Date       | 10/20/2006      |
| First Named Inventor   | Schneier et al. |
| Art Unit               | 2131            |
| Examiner Name          | Unassigned      |
| Attorney Docket Number | 022133-000520US |

**To: Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450**

Please withdraw me as attorney or agent for the above identified patent application, and

- ☐ all the attorneys/agents of record
- ☐ all the attorneys/agents (with registration numbers) listed on the attached paper(s), or
- ☒ all the attorneys/agents associated with Customer Number **20350**

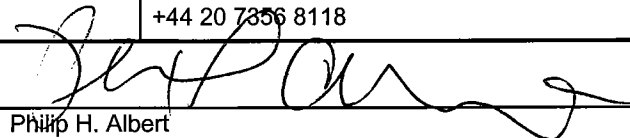
NOTE: This box can only be checked when the power of attorney of record in the application is to all the practitioners associated with a customer number.

The reasons for this request are: Client requests transfer of matter listed below.

**CORRESPONDENCE ADDRESS**

1. ☐ The correspondence address is NOT affected by this withdrawal.
2. ☒ Change the correspondence address and direct all future correspondence to:
- ☐ The address associated with Customer Number:

**OR**

|                                                             |                                                                                     |       |                  |                     |  |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------|-------|------------------|---------------------|--|
| <input checked="" type="checkbox"/> Firm or Individual Name | Roger Nash<br>BT Intellectual Property Department                                   |       |                  | roger.2.nash@bt.com |  |
| Address                                                     | ppC5, BT Centre<br>81 Newgate Street.                                               |       |                  |                     |  |
| City                                                        | London EC1A 7AJ                                                                     | State |                  | Zip                 |  |
| Country                                                     | UNITED KINGDOM                                                                      |       |                  |                     |  |
| Telephone                                                   | +44 20 7356 8118                                                                    |       | Fax              | +44 20 7600 6891    |  |
| Signature                                                   |  |       |                  |                     |  |
| Name                                                        | Philip H. Albert                                                                    |       | Registration No. | 35,819              |  |
| Date                                                        | January 17, 2008                                                                    |       | Telephone No.    | 650-326-2400        |  |

NOTE: Withdrawal is effective when approved rather than when received. Unless there are at least 30 days between approval of withdrawal and the expiration date of a time period for response or possible extension period, the request to withdraw is normally disapproved.

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 2756763                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Philip H. Albert/Susan Aikins                                                      |
| <b>Filer Authorized By:</b>                 | Philip H. Albert                                                                   |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 23-JAN-2008                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 16:27:39                                                                           |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)                                                        |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description | File Name                         | File Size(Bytes) /Message Digest                  | Multi Part /.zip | Pages (if appl.) |
|-----------------|----------------------|-----------------------------------|---------------------------------------------------|------------------|------------------|
| 1               | Change of Address    | Withdraw_Atty_022133-000520US.pdf | 40863<br>380bc4d91505a55a66297e94b6ebf58b0e1893a6 | no               | 1                |

### Warnings:

### Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

**New Applications Under 35 U.S.C. 111**

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

**National Stage of an International Application under 35 U.S.C. 371**

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

**New International Application Filed with the USPTO as a Receiving Office**

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE



Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
www.uspto.gov

TOWNSEND AND TOWNSEND  
AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

COPY MAILED

FEB 19 2008

OFFICE OF PETITIONS

In re Application of  
Bruce SCHNEIR, et al  
Application No. 11/551,606  
Filed: October 20, 2006  
Attorney Docket No. 022133-000520US

DECISION ON PETITION  
TO WITHDRAW  
FROM RECORD

This is a decision on the Request to Withdraw as attorney or agent of record under 37 C.F.R. § 1.36(b), filed January 23, 2008.

The request is **APPROVED**.

A grantable request to withdraw as attorney/agent of record must be signed by every attorney/agent seeking to withdraw or contain a clear indication that one attorney is signing on behalf of another/others. A request to withdraw will not be approved unless at least 30 (thirty) days would remain between the date of approval and the later of the expiration date of a time to file a response or the expiration date of the maximum time period which can be extended under 37 C.F.R. § 1.136(a).

The request was signed by attorney Philip H. Albert on behalf of all attorneys/agents of record associated with Customer Number 20350.

All attorneys/agents of record associated with Customer Number 20350 have been withdrawn.

Applicant is reminded that there is no attorney of record at this time.

The request to change the correspondence of record is not acceptable as the requested correspondence address is not that of: (1) the first named signing inventor; or (2) an intervening assignee of the entire interest under 37 C.F.R. 3.71. All future communications from the Office will be directed to the Assignee of the entire interest at the first copied address below until otherwise properly notified by the applicant.

There are no outstanding Office actions pending at the present time.

Telephone inquiries concerning this decision should be directed to the undersigned at 571-272-6735.

  
Diane Goodwyn  
Petitions Examiner  
Office of Petitions

cc: COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

ROGER NASH  
BT INTELLECTUAL PROPERTY DEPARTMENT  
PPC5, BT CENTRE  
81 NEWGATE STREET  
LONDON EC1A 7AJ  
UNITED KINGDOM



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | 022133-000520US        |

CONFIRMATION NO. 1662

POWER OF ATTORNEY NOTICE



20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

Date Mailed: 02/19/2008

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/23/2008.

- The withdrawal as attorney in this application has been accepted. Future correspondence will be mailed to the new address of record. 37 CFR 1.33.

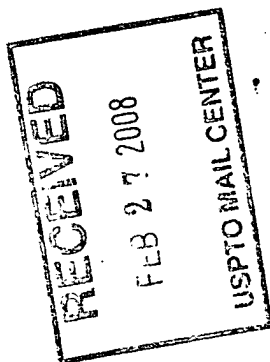
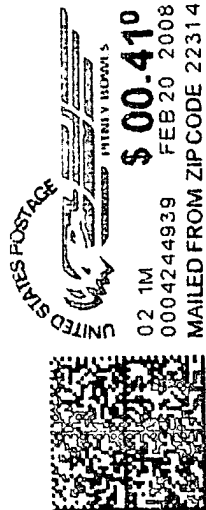
/dcgoodwyn/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

Organization MDW Bldg./Room 7A58  
UNITED STATES PATENT AND TRADEMARK OFFICE  
P.O. Box 1450  
Alexandria, Va. 22313-1450  
If Undeliverable Return In Ten Days

Official Business  
Penalty For Private Use, \$300

AN EQUAL OPPORTUNITY EMPLOYER



COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

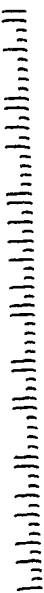
NIXIE

951 25 1 73 02123108

RETURN TO SENDER  
NOT DELIVERABLE AS ADDRESSED  
UNABLE TO FORWARD

BC: 22313145050 \*0217-02841-20-41

9512832541 0013  
2231301450





# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | 022133-000520US        |

**CONFIRMATION NO. 1662**

## POWER OF ATTORNEY NOTICE



\*OC000000028355481\*

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

Date Mailed: 02/19/2008

## NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/23/2008.

- The withdrawal as attorney in this application has been accepted. Future correspondence will be mailed to the new address of record. 37 CFR 1.33.

/dcgoodwyn/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents  
United States Patent and Trademark Office  
P.O. Box 1450  
Alexandria, VA 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

**TOWNSEND AND TOWNSEND  
AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834**

**COPY MAILED**

**FEB 19 2008**

**OFFICE OF PETITIONS**

In re Application of  
Bruce SCHNEIR, et al  
Application No. 11/551,606  
Filed: October 20, 2006  
Attorney Docket No. 022133-000520US

DECISION ON PETITION  
TO WITHDRAW  
FROM RECORD

This is a decision on the Request to Withdraw as attorney or agent of record under 37 C.F.R. § 1.36(b), filed January 23, 2008.

The request is **APPROVED**.

A grantable request to withdraw as attorney/agent of record must be signed by every attorney/agent seeking to withdraw or contain a clear indication that one attorney is signing on behalf of another/others. A request to withdraw will not be approved unless at least 30 (thirty) days would remain between the date of approval and the later of the expiration date of a time to file a response or the expiration date of the maximum time period which can be extended under 37 C.F.R. § 1.136(a).

The request was signed by attorney Philip H. Albert on behalf of all attorneys/agents of record associated with Customer Number 20350.

All attorneys/agents of record associated with Customer Number 20350 have been withdrawn.

Applicant is reminded that there is no attorney of record at this time.

The request to change the correspondence of record is not acceptable as the requested correspondence address is not that of: (1) the first named signing inventor; or (2) an intervening assignee of the entire interest under 37 C.F.R. 3.71. All future communications from the Office will be directed to the Assignee of the entire interest at the first copied address below until otherwise properly notified by the applicant.

There are no outstanding Office actions pending at the present time.

Telephone inquiries concerning this decision should be directed to the undersigned at 571-272-6735.



Diane Goodwyn  
Petitions Examiner  
Office of Petitions

cc: COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

ROGER NASH  
BT INTELLECTUAL PROPERTY DEPARTMENT  
PPC5, BT CENTRE  
81 NEWGATE STREET  
LONDON EC1A 7AJ  
UNITED KINGDOM



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | 022133-000520US        |

CONFIRMATION NO. 1662

POWER OF ATTORNEY NOTICE

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834



Date Mailed: 02/19/2008

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 01/23/2008.

- The withdrawal as attorney in this application has been accepted. Future correspondence will be mailed to the new address of record. 37 CFR 1.33.

/dcgoodwyn/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov



Bib Data Sheet

CONFIRMATION NO. 1662

|                                                                                                                                                                                                                                                                                                   |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <b>SERIAL NUMBER</b><br>11/551,606                                                                                                                                                                                                                                                                | <b>FILING OR 371(c) DATE</b><br>10/20/2006<br><b>RULE</b>                                                         | <b>CLASS</b><br>726           | <b>GROUP ART UNIT</b><br>2131                                                                                                                                                                                                                                                   | <b>ATTORNEY DOCKET NO.</b> |
| <b>APPLICANTS</b><br>Bruce Schneier, Minneapolis, MN;<br>Andrew H. Gross, San Jose, CA;<br>Jonathan D. Callas, Mountain View, CA;                                                                                                                                                                 |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| <b>** CONTINUING DATA *****</b><br>This application is a CON of 09/766,343 01/19/2001 PAT 7,159,237<br>which claims benefit of 60/190,326 03/16/2000                                                                                                                                              |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| <b>** FOREIGN APPLICATIONS *****</b>                                                                                                                                                                                                                                                              |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| <b>IF REQUIRED, FOREIGN FILING LICENSE GRANTED</b><br><b>** 11/20/2006</b>                                                                                                                                                                                                                        |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no<br>35 USC 119 (a-d) conditions <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after<br>met Allowance<br>Verified and Acknowledged _____<br>Examiner's Signature Initials |                                                                                                                   | <b>STATE OR COUNTRY</b><br>MN | <b>SHEETS DRAWING</b><br>9                                                                                                                                                                                                                                                      | <b>TOTAL CLAIMS</b><br>26  |
| <b>INDEPENDENT CLAIMS</b><br>2                                                                                                                                                                                                                                                                    |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| <b>ADDRESS</b><br>COUNTERPANE INTERNET SECURITY, INC.<br>3031 TISCH WAY<br>SAN JOSE, CA95128                                                                                                                                                                                                      |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| <b>TITLE</b><br>Method and System for Dynamic Network Intrusion Monitoring, Detection and Response                                                                                                                                                                                                |                                                                                                                   |                               |                                                                                                                                                                                                                                                                                 |                            |
| <b>FILING FEE RECEIVED</b><br>1430                                                                                                                                                                                                                                                                | FEES: Authority has been given in Paper<br>No. _____ to charge/credit DEPOSIT ACCOUNT<br>No. _____ for following: |                               | <input type="checkbox"/> All Fees<br><input type="checkbox"/> 1.16 Fees ( Filing )<br><input type="checkbox"/> 1.17 Fees ( Processing Ext. of time )<br><input type="checkbox"/> 1.18 Fees ( Issue )<br><input type="checkbox"/> Other _____<br><input type="checkbox"/> Credit |                            |



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 11/551,606      | 10/20/2006  | Bruce Schneier       |                     | 1662             |

7590 06/18/2009  
COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

|          |
|----------|
| EXAMINER |
|----------|

JACKSON, JENISE E

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2439

|           |               |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

06/18/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                                      |                                        |  |
|------------------------------|--------------------------------------|----------------------------------------|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>11/551,606 | <b>Applicant(s)</b><br>SCHNEIER ET AL. |  |
|                              | <b>Examiner</b><br>JENISE E. JACKSON | <b>Art Unit</b><br>2439                |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 21 March 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 45-70 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 45-68 and 70 is/are rejected.
- 7) ☒ Claim(s) 69 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |                                                                                        |                                                                   |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____                                                            | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION*****Double Patenting***

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 45-61 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-17 of U.S. Patent No. 7,159,237. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following rationale below:

3. Claim 45 of application 11/551606 discloses a system, and Claim 1 of Patent 7,159,237 discloses a method. It would have been obvious to include the system of application 11/551606 in Patent 7,159,237 that claims a method; the system performs certain steps/methods in order to perform security monitoring. Claim 45 of application 11/551606 discloses a sensor coupled to collect status data, and Claim 1 of Patent 7,159,237 discloses collecting status data. It would have been obvious to include a sensor of 11/551606 of application, in Patent 7159,237, in order

Art Unit: 2439

to have a device that can collect the status data of at least one monitored component of the network.

4. Claims 46-61 of application 11/551606 recite same limitations as claims 2-17 of Patent No. 7,159,237 respectively.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 62-68, 70 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson(5,970, 149)

7. As per claim 62, Johnson discloses a method of operating a secure operations center(i.e. secure dispatch control center)(see fig. 1 sheet 1) as part of a security monitoring system for a customer computer network(i.e. secure customer site, see fig. 1 sheet 1)(see col. 2, lines 46-61), comprising: creating an event record for information received about an identified potentially security-related event occurring on the network(see col. 2, lines 60-63, col. 3, lines 65-66, col. 4, lines 1-3); correlating the event record with customer information and a symptom record; using the correlated symptom record to link the event record to problem resolution information(see col. 2, lines 32-36, col. 5, lines 25-45); consolidating the event record, correlated customer information and symptom record, and linked problem resolution information into a problem ticket; and providing the problem ticket to a security analyst console for analysis(see col. 4, lines 9-20, col. 4, lines 39-40).

Art Unit: 2439

8. As per claim 63, Johnson discloses correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and linking the event record to an open problem ticket associated with the pre-existing event record(see col. 5, lines 25-45).

9. As per claim 64, Johnson discloses wherein the problem resolution information links the symptom to a diagnosis(col. 2, lines 32-36).

10. As per claim 65, Johnson discloses wherein the problem resolution information links the symptom to a technology(see col. 4, lines 65-67, col. 4, lines 1-5).

11. As per claim 66, Johnson discloses correlating the event record with vulnerability; and using the correlated vulnerability to link the event record to problem resolution information (see col. 2, lines 53-63).

12. As per claim 67, Johnson discloses wherein the problem resolution information links the vulnerability to a diagnosis (see col. 2, lines 32-36).

13. As per claim 68, Johnson discloses wherein the problem resolution information links the vulnerability to a technology(see col. 4, lines 65-67, col. 4, lines 1-5).

14. As per claim 70, Johnson discloses updating the problem resolution information after the potentially security-related event is resolved(see col. 5, lines 39-55).

Art Unit: 2439

***Claim Objections***

15. Claim 69 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 11/551,606

Page 6

Art Unit: 2439

June 11, 2009

/J. E. J./

Examiner, Art Unit 2439

/Michael J Simitoski/

Primary Examiner, Art Unit 2439

|                                   |                                       |                                                               |             |
|-----------------------------------|---------------------------------------|---------------------------------------------------------------|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/551,606 | Applicant(s)/Patent Under<br>Reexamination<br>SCHNEIER ET AL. |             |
|                                   | Examiner<br>JENISE E. JACKSON         | Art Unit<br>2439                                              | Page 1 of 1 |

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name              | Classification |
|---|---|--------------------------------------------------|-----------------|-------------------|----------------|
| * | A | US-5,970,149                                     | 10-1999         | Johnson, R. Brent | 714/46         |
|   | B | US-                                              |                 |                   |                |
|   | C | US-                                              |                 |                   |                |
|   | D | US-                                              |                 |                   |                |
|   | E | US-                                              |                 |                   |                |
|   | F | US-                                              |                 |                   |                |
|   | G | US-                                              |                 |                   |                |
|   | H | US-                                              |                 |                   |                |
|   | I | US-                                              |                 |                   |                |
|   | J | US-                                              |                 |                   |                |
|   | K | US-                                              |                 |                   |                |
|   | L | US-                                              |                 |                   |                |
|   | M | US-                                              |                 |                   |                |

**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--------------------------------------------------|-----------------|---------|------|----------------|
|   | N |                                                  |                 |         |      |                |
|   | O |                                                  |                 |         |      |                |
|   | P |                                                  |                 |         |      |                |
|   | Q |                                                  |                 |         |      |                |
|   | R |                                                  |                 |         |      |                |
|   | S |                                                  |                 |         |      |                |
|   | T |                                                  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|-------------------------------------------------------------------------------------------|
|   | U |                                                                                           |
|   | V |                                                                                           |
|   | W |                                                                                           |
|   | X |                                                                                           |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on May 2, 2007.

PATENT  
Attorney Docket No.: 022133-000520US

TOWNSEND and TOWNSEND and CREW LLP

By: /Maureen Golob/  
Maureen Golob

# **IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier et al.

Application No.: 11/551,606

Filed: November 21, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Confirmation No.: 1662

Examiner: Unassigned

Art Unit: 2131

INFORMATION DISCLOSURE  
STATEMENT UNDER 37 CFR §1.97 and  
§1.98

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The references cited on attached form PTO/SB/08A and PTO/SB/08B are being called to the attention of the Examiner. In accordance with 37 CFR §1.98(d), copies of a number of the references can be found in Application No. 09/766,343, filed January 19, 2001 (Attorney Docket No. 022133-000510US). It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR §1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /JJ/

Application No.: 11/551,606

Page 2

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement.

However, if a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,

/Naya Chatterjee-Marathe/

Naya Chatterjee-Marathe  
Reg. No. 54,680

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400  
Fax: 650-326-2422  
NMC:tfw:mg  
61042835 v1

|                                                                                                                                               |   |    |                          |                        |                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------|---|----|--------------------------|------------------------|-----------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(Use as many sheets as necessary)</i> |   |    | <b>Complete if Known</b> |                        |                 |
|                                                                                                                                               |   |    | Application Number       | 11/551,606             |                 |
|                                                                                                                                               |   |    | Filing Date              | November 21, 2006      |                 |
|                                                                                                                                               |   |    | First Named Inventor     | Schneier, Bruce        |                 |
|                                                                                                                                               |   |    | Art Unit                 | 2131                   |                 |
|                                                                                                                                               |   |    | Examiner Name            | Unassigned             |                 |
| Sheet                                                                                                                                         | 1 | of | 3                        | Attorney Docket Number | 022133-000520US |

| U.S. PATENT DOCUMENTS |                       |                                                             |                                |                                                    |                                                                                 |
|-----------------------|-----------------------|-------------------------------------------------------------|--------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------|
| Examiner Initials*    | Cite No. <sup>1</sup> | Document Number<br>Number Kind Code <sup>2</sup> (if known) | Publication Date<br>MM-DD-YYYY | Name of Patentee or<br>Applicant of Cited Document | Pages, Columns, Lines, Where<br>Relevant Passages or Relevant<br>Figures Appear |
|                       | 1                     | 5,440,723                                                   | 08-08-1995                     | Arnold et al.                                      |                                                                                 |
|                       | 2                     | 5,796,942                                                   | 08-18-1998                     | Esbensen                                           |                                                                                 |
|                       | 3                     | 5,909,493                                                   | 06-01-1999                     | Motoyama                                           |                                                                                 |
|                       | 4                     | 6,026,442                                                   | 02-15-2000                     | Lewis et al.                                       |                                                                                 |
|                       | 5                     | 6,088,804                                                   | 07-11-2000                     | Hill et al.                                        |                                                                                 |
|                       | 6                     | 6,119,236                                                   | 09-12-2000                     | Shipley                                            |                                                                                 |
|                       | 7                     | 6,125,390                                                   | 09-26-2000                     | Touboul                                            |                                                                                 |
|                       | 8                     | 6,182,226                                                   | 01-30-2001                     | Reid et al.                                        |                                                                                 |
|                       | 9                     | 6,205,551                                                   | 03-20-2001                     | Grosse                                             |                                                                                 |
|                       | 10                    | 6,298,445                                                   | 10-02-2001                     | Shostack et al.                                    |                                                                                 |
|                       | 11                    | 6,363,489                                                   | 03-26-2002                     | Comay et al.                                       |                                                                                 |
|                       | 12                    | 6,519,703                                                   | 02-11-2003                     | Joyce                                              |                                                                                 |
|                       | 13                    | 6,681,331                                                   | 01-20-2004                     | Munson et al.                                      |                                                                                 |
|                       | 14                    | 6,704,874                                                   | 03-09-2004                     | Porras et al.                                      |                                                                                 |

| FOREIGN PATENT DOCUMENTS |                       |                           |                     |                                   |                                |                                                    |                                                                                 |                |
|--------------------------|-----------------------|---------------------------|---------------------|-----------------------------------|--------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------|----------------|
| Examiner Initials*       | Cite No. <sup>1</sup> | Foreign Patent Document   |                     |                                   | Publication Date<br>MM-DD-YYYY | Name of Patentee or<br>Applicant of Cited Document | Pages, Columns, Lines,<br>Where Relevant Passages<br>or Relevant Figures Appear | T <sup>6</sup> |
|                          |                       | Country Code <sup>3</sup> | Number <sup>4</sup> | Kind Code <sup>5</sup> (if known) |                                |                                                    |                                                                                 |                |
|                          |                       |                           |                     |                                   |                                |                                                    |                                                                                 |                |
|                          |                       |                           |                     |                                   |                                |                                                    |                                                                                 |                |

|                    |                               |                 |            |
|--------------------|-------------------------------|-----------------|------------|
| Examiner Signature | /Jenise Jackson/ (06/11/2009) | Date Considered | 06/11/2009 |
|--------------------|-------------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /JJ/

61042835 VT

|                                                                                                                                        |   |    |   |                          |                   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--------------------------|-------------------|
| Substitute for form 1449B/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br>(Use as many sheets as necessary) |   |    |   | <b>Complete if Known</b> |                   |
|                                                                                                                                        |   |    |   | Application Number       | 11/551,606        |
|                                                                                                                                        |   |    |   | Filing Date              | November 21, 2006 |
|                                                                                                                                        |   |    |   | First Named Inventor     | Schneier, Bruce   |
|                                                                                                                                        |   |    |   | Art Unit                 | 2131              |
|                                                                                                                                        |   |    |   | Examiner Name            | Unassigned        |
| Sheet                                                                                                                                  | 2 | of | 3 | Attorney Docket Number   | 022133-000520US   |

| NON PATENT LITERATURE DOCUMENTS |                          |                                                                                                                                                                                                                                                                                             |                          |
|---------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Examiner<br>Initials *          | Cite<br>No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                             | T <sup>2</sup>           |
|                                 | 15                       | "FAQ: Network Intrusion Detection Systems," Version 0.3, Jan. 1, 1998, <a href="http://www.robertgraham.com/pubs/network-intrusion-detection.txt">http://www.robertgraham.com/pubs/network-intrusion-detection.txt</a> , downloaded Oct. 19, 2001, pp. 1-29.                                | <input type="checkbox"/> |
|                                 | 16                       | "Latest Network Management Products," (Product Information) <i>Communication News</i> , Jun. 2000, 2 pages total.                                                                                                                                                                           | <input type="checkbox"/> |
|                                 | 17                       | "Managed Security Services: Are They Right For You?" <i>ENT</i> , Nov. 22, 2000, 4 pages total.                                                                                                                                                                                             | <input type="checkbox"/> |
|                                 | 18                       | "Security Monitoring Services," <i>Information Week</i> , No. 792, June 26, 2000, p. 244.                                                                                                                                                                                                   | <input type="checkbox"/> |
|                                 | 19                       | BALASUBRAMANIYAN, J. S. et al., "An Architecture for Intrusion Detection Using Autonomous Agents," Center for Education and Research in Information Assurance and Security, CERIAS Technical Report May 1995, Jun. 11, 1998, pp. 1-19.                                                      | <input type="checkbox"/> |
|                                 | 20                       | BLACHARSKI, "Outsourcing Firewall Management -- Managed Firewall Services Prevent Security Burnouts -- Firewall Management Requires 24-Hour Vigilance. If You Can't Pull Round-the-Clock Guard Duty, Outsourcing May Be for You," <i>Network Magazine</i> , Vol. 60, Aug. 1, 2000, 6 pages. | <input type="checkbox"/> |
|                                 | 21                       | Citation details: "Automated Information System--(AIS) Alarm System," W. Hunteman, <a href="http://citeseer.nj.nec.com/context/1642652/0">http://citeseer.nj.nec.com/context/1642652/0</a> , downloaded Oct. 19, 2001, 1 page.                                                              | <input type="checkbox"/> |
|                                 | 22                       | COMPUTEL WHITE PAPERS, "Managed Security Monitoring," 2001, pp. 1-4.                                                                                                                                                                                                                        | <input type="checkbox"/> |
|                                 | 23                       | ESSEX, "E-Sleuths Make Net Safe for E-Commerce; RIPTech Stakes Its Claim in the Growing Market for Remotely Managed Security," <i>Computerworld</i> , Vol. 80, No. 1, Jun. 12, 2000, 2 pages.                                                                                               | <input type="checkbox"/> |
|                                 | 24                       | FRATTO, "RFP: Managed Firewall Services," <i>Network Computing</i> , Vol. 9, No. 20, p.68, Nov. 1, 1998, 12 pages total.                                                                                                                                                                    | <input type="checkbox"/> |
|                                 | 25                       | HUNTEMAN, W., "Automated Information System--(AIS) Alarm System," University of California, Los Alamos National Laboratory, In Proceedings of the 20th National Information Systems Security Conference, National Institute of Standards and Technology, Oct. 1997, pp. 1-12.               | <input type="checkbox"/> |

|                       |                               |                    |            |
|-----------------------|-------------------------------|--------------------|------------|
| Examiner<br>Signature | /Jenise Jackson/ (06/11/2009) | Date<br>Considered | 06/11/2009 |
|-----------------------|-------------------------------|--------------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

|                                                                                                                                        |   |    |   |                          |                   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--------------------------|-------------------|
| Substitute for form 1449B/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br>(Use as many sheets as necessary) |   |    |   | <b>Complete if Known</b> |                   |
|                                                                                                                                        |   |    |   | Application Number       | 11/551,606        |
|                                                                                                                                        |   |    |   | Filing Date              | November 21, 2006 |
|                                                                                                                                        |   |    |   | First Named Inventor     | Schneier, Bruce   |
|                                                                                                                                        |   |    |   | Art Unit                 | 2131              |
|                                                                                                                                        |   |    |   | Examiner Name            | Unassigned        |
| Sheet                                                                                                                                  | 3 | of | 3 | Attorney Docket Number   | 022133-000520US   |

| NON PATENT LITERATURE DOCUMENTS |                          |                                                                                                                                                                                                                                                                                                                                                                                          |                          |  |
|---------------------------------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--|
| Examiner<br>Initials *          | Cite<br>No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                                                                                                                          | T <sup>2</sup>           |  |
|                                 | 26                       | M2 PRESSWIRE, "GTE Internetworking: GTE Internetworking Offers New Version of Its Site Patrol Managed Security Services," Sep. 3, 1999, pp. 1-3.                                                                                                                                                                                                                                         | <input type="checkbox"/> |  |
|                                 | 27                       | M2 PRESSWIRE, "ISS: ISS Acquires Netrex Secure Solutions," Aug. 31, 1999, 1 page.                                                                                                                                                                                                                                                                                                        | <input type="checkbox"/> |  |
|                                 | 28                       | MESSMER, "Security Needs Spawn Services Managed Detection Services Growing in Popularity," <i>Network World</i> , April 3, 2000, 1 page                                                                                                                                                                                                                                                  | <input type="checkbox"/> |  |
|                                 | 29                       | NEUMANN, P. G. et al., "Experience with Emerald to Date," Computer Science Laboratory, SRI International, 1st USENIX Workshop on Intrusion Detection and Networking Monitoring, Santa Clara, California, Apr. 11-12, 1999, pp. 73-80, <a href="http://www.csl.sri.com/users/neumann/det99.html">http://www.csl.sri.com/users/neumann/det99.html</a> , downloaded Oct. 19, 2001, pp. 1-9. | <input type="checkbox"/> |  |
|                                 | 30                       | PORRAS, P. A. et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Computer Science Laboratory, SRI International, 20th NISSC --Oct. 9, 1997 pp. 1-22 (version with legible text but no figures), pp. 1-13 (version with figures but illegible text)                                                                                                   | <input type="checkbox"/> |  |
|                                 | 31                       | REDSIREN, "Managed Solutions," downloaded from Internet << <a href="http://www.redsiren.com">http://www.redsiren.com</a> >>, p. 1-3 (Publication Date Unknown).                                                                                                                                                                                                                          | <input type="checkbox"/> |  |
|                                 | 32                       | RKON TECHNOLOGIES, downloaded from Internet << <a href="http://www.rkontechnologies.com">http://www.rkontechnologies.com</a> >> (Publication Date Unknown)                                                                                                                                                                                                                               | <input type="checkbox"/> |  |
|                                 | 33                       | SAVAGE, "Locking the Doors -- Denial of Services Attacks and Viruses Prime the Market For Security Solutions and Services," <i>Computer Reseller News</i> , Vol. 72, Sep. 25, 2000, 2 pages total.                                                                                                                                                                                       | <input type="checkbox"/> |  |
|                                 | 34                       | VPNTRUST: CONSULTING, "VPNTrust Services: Consulting" 1999, Technica Corporation, pp. 1-3.                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> |  |

|                       |                               |                    |            |
|-----------------------|-------------------------------|--------------------|------------|
| Examiner<br>Signature | /Jenise Jackson/ (06/11/2009) | Date<br>Considered | 06/11/2009 |
|-----------------------|-------------------------------|--------------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

|                                                                                                                        |                                                |                                                                       |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b><i>Index of Claims</i></b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                                        | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

|   |                 |   |                   |   |                     |   |                 |
|---|-----------------|---|-------------------|---|---------------------|---|-----------------|
| ✓ | <b>Rejected</b> | - | <b>Cancelled</b>  | N | <b>Non-Elected</b>  | A | <b>Appeal</b>   |
| = | <b>Allowed</b>  | ÷ | <b>Restricted</b> | I | <b>Interference</b> | O | <b>Objected</b> |

| <input type="checkbox"/> <b>Claims renumbered in the same order as presented by applicant</b> |          | <input type="checkbox"/> <b>CPA</b> |  | <input type="checkbox"/> <b>T.D.</b> |  | <input type="checkbox"/> <b>R.1.47</b> |  |  |  |
|-----------------------------------------------------------------------------------------------|----------|-------------------------------------|--|--------------------------------------|--|----------------------------------------|--|--|--|
| CLAIM                                                                                         |          | DATE                                |  |                                      |  |                                        |  |  |  |
| Final                                                                                         | Original | 06/11/2009                          |  |                                      |  |                                        |  |  |  |
|                                                                                               | 45       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 46       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 47       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 48       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 49       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 50       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 51       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 52       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 53       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 54       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 55       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 56       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 57       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 58       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 59       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 60       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 61       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 62       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 63       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 64       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 65       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 66       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 67       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 68       | ✓                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 69       | O                                   |  |                                      |  |                                        |  |  |  |
|                                                                                               | 70       | ✓                                   |  |                                      |  |                                        |  |  |  |

|                                                                                                              |                                                |                                                                       |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b>Search Notes</b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                              | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

| SEARCHED |          |         |          |
|----------|----------|---------|----------|
| Class    | Subclass | Date    | Examiner |
| 726      | 3        | 6/11/09 | JJ       |
| 726      | 22-25    | 6/11/09 | JJ       |

| SEARCH NOTES                      |         |          |
|-----------------------------------|---------|----------|
| Search Notes                      | Date    | Examiner |
| West text search                  | 6/11/09 | JJ       |
| West class and text search        | 6/11/09 | JJ       |
| West inventor and assignee search | 6/11/09 | JJ       |
| Dialog non-patent lit search      | 6/11/09 | JJ       |

| INTERFERENCE SEARCH |          |      |          |
|---------------------|----------|------|----------|
| Class               | Subclass | Date | Examiner |
|                     |          |      |          |

|  |  |
|--|--|
|  |  |
|--|--|

## WEST Search History for Application 11551606

**Creation Date: 2009061118:05**

| Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | DB                                 | Op. | Plur. | Thes. | Date       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-----|-------|-------|------------|
| (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 06-11-2009 |
| ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) ) and (probe or sentry or scanner? or sensor? or honeypot)                                                                                                                                                                                                                                                                                                                                                                                                                          | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 06-11-2009 |
| (monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) )                                                                                                                                              | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 06-11-2009 |
| (sensor or filter\$5 or probe or sentry or black near box)near(collect\$5 or gather\$5)near(data or information or alert\$5 or event\$2) and ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 06-11-2009 |
| (transmit\$8 or send\$8 or transfer\$8 or forward\$8)near(information or data or alert\$2 or event\$2 or footprint\$2)near(dispatch\$5 or engineer or analyst or admin\$8 or support near person or help near desk\$4)                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 06-11-2009 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                    | OR  | YES   |       | 06-11-2009 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |    |     |  |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| ((sensor or filter\$5 or probe or sentry or black near box)near(collect\$5 or gather\$5)near(data or information or alert\$5 or event\$2) and (monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (((transmit\$8 or send\$8 or transfer\$8 or forward\$8)near(information or data or alert\$2 or event\$2 or footprint\$2)near(dispatch\$5 or engineer or analyst or admin\$8 or support near person or help near desk\$4) ) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD |    |     |  |            |
| (filter\$5 or separate)near(data or information or alert\$5 or event\$5 or footprint\$2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| (post near filter\$5 near residue)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| (keeping\$5 or say\$5)near(residue or left near over)near(alert\$2 or data or information or event\$2 or footprint\$2)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| (receiv\$5 or obtain\$5)near(feedback or results)near(probe or sensor? or sentry or black near box)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| ((receiv\$5 or obtain\$5)near(feedback or results)near(probe or sensor? or sentry or black near box) ) and ((filter\$5 or separate)near(data or information or alert\$5 or event\$5 or footprint\$2) )                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |

|                                                                                                                                               |                                    |    |     |  |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| (dynamically or real-time)near(modif\$8 or updat\$8 or chang\$8)near(probe or sentry or sensor? or black near box)near(feedback or result\$2) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/22.ccls.                                                                                                                                  | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/24.ccls.                                                                                                                                  | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/25.ccls.                                                                                                                                  | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/23.ccls.                                                                                                                                  | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/2.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)                     | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/3.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)                     | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 06-11-2009 |
| 726/6.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)                     | PGPB, USPT, EPAB, JPAB,            | OR | YES |  | 06-11-2009 |

|                                                                                                                             |                                                   |    |     |  |            |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
|                                                                                                                             | DWPI,<br>TDBD                                     |    |     |  |            |
| 726/15.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)  | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/208.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/209.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/223.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/224.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/225.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/226.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
|                                                                                                                             |                                                   | OR | YES |  | 06-11-2009 |

|                                                                                                                             |                                                   |    |     |  |            |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
| 709/227.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD |    |     |  |            |
| 709/228.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 709/229.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| Bruce near Schneier.in. and (secure near operations near center)                                                            | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| (Andrew near Gross.in.) and (secure near operations near center)                                                            | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| (Jonathan near Callas).in. and (secure near operations near center)                                                         | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| (Counterpane.as. and secure near operations near center)                                                                    | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| ((ticket) and (analyst or help near desk) and network ) and (intrusion)                                                     | PGPB,<br>USPT,<br>EPAB,<br>JPAB,                  | OR | YES |  | 06-11-2009 |

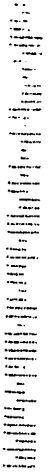
|                                                          |                                                   |    |     |  |            |
|----------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
|                                                          | DWPI,<br>TDBD                                     |    |     |  |            |
| ((ticket) and (analyst or help near desk) ) and network  | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| ((incident near log) ) and (analyst or help near desk)   | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| (problem near ticket\$2) and (help near desk or analyst) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |
| 726/3.ccls.                                              | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 06-11-2009 |

OFFICIAL BUSINESS  
PENALTY FOR PRIVATE USE, \$300

AN EQUAL OPPORTUNITY EMPLOYER

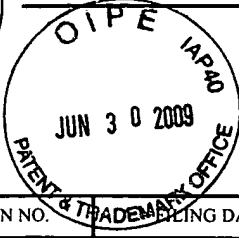


Department of Labor  
Equal Employment Opportunity Commission  
Washington, D.C. 20451  
Date: \_\_\_\_\_





# UNITED STATES PATENT AND TRADEMARK OFFICE



UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 11/551,606      | 10/20/2006  | Bruce Schneier       |                     | 1662             |

7590 06/18/2009  
COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

EXAMINER

JACKSON, JENISE E

ART UNIT PAPER NUMBER

2439

MAIL DATE DELIVERY MODE

06/18/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

|                              |                        |  |                     |  |
|------------------------------|------------------------|--|---------------------|--|
| <b>Office Action Summary</b> | <b>Application No.</b> |  | <b>Applicant(s)</b> |  |
|                              | 11/551,606             |  | SCHNEIER ET AL.     |  |
|                              | <b>Examiner</b>        |  | <b>Art Unit</b>     |  |
|                              | JENISE E. JACKSON      |  | 2439                |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 21 March 2007.
- 2a) ☐ This action is FINAL.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 45-70 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 45-68 and 70 is/are rejected.
- 7) ☒ Claim(s) 69 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |                                                                                        |                                                                   |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)            | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____                                                            | 6) <input type="checkbox"/> Other: _____                          |

## DETAILED ACTION

### *Double Patenting*

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 45-61 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-17 of U.S. Patent No. 7,159,237. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following rationale below:

3. Claim 45 of application 11/551606 discloses a system, and Claim 1 of Patent 7,159,237 discloses a method. It would have been obvious to include the system of application 11/551606 in Patent 7,159,237 that claims a method; the system performs certain steps/methods in order to perform security monitoring. Claim 45 of application 11/551606 discloses a sensor coupled to collect status data, and Claim 1 of Patent 7,159,237 discloses collecting status data. It would have been obvious to include a sensor of 11/551606 of application, in Patent 7159,237, in order

Art Unit: 2439

to have a device that can collect the status data of at least one monitored component of the network.

4. Claims 46-61 of application 11/551606 recite same limitations as claims 2-17 of Patent No. 7,159,237 respectively.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 62-68, 70 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson(5,970, 149)

7. As per claim 62, Johnson discloses a method of operating a secure operations center(i.e. secure dispatch control center)(see fig. 1 sheet 1) as part of a security monitoring system for a customer computer network(i.e. secure customer site, see fig. 1 sheet 1)(see col. 2, lines 46-61), comprising: creating an event record for information received about an identified potentially security-related event occurring on the network(see col. 2, lines 60-63, col. 3, lines 65-66, col. 4, lines 1-3); correlating the event record with customer information and a symptom record; using the correlated symptom record to link the event record to problem resolution information(see col. 2, lines 32-36, col. 5, lines 25-45); consolidating the event record, correlated customer information and symptom record, and linked problem resolution information into a problem ticket; and providing the problem ticket to a security analyst console for analysis(see col. 4, lines 9-20, col. 4, lines 39-40).

Art Unit: 2439

8. As per claim 63, Johnson discloses correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and linking the event record to an open problem ticket associated with the pre-existing event record(see col. 5, lines 25-45).
9. As per claim 64, Johnson discloses wherein the problem resolution information links the symptom to a diagnosis(col. 2, lines 32-36).
10. As per claim 65, Johnson discloses wherein the problem resolution information links the symptom to a technology(see col. 4, lines 65-67, col. 4, lines 1-5).
11. As per claim 66, Johnson discloses correlating the event record with vulnerability; and using the correlated vulnerability to link the event record to problem resolution information (see col. 2, lines 53-63).
12. As per claim 67, Johnson discloses wherein the problem resolution information links the vulnerability to a diagnosis (see col. 2, lines 32-36).
13. As per claim 68, Johnson discloses wherein the problem resolution information links the vulnerability to a technology(see col. 4, lines 65-67, col. 4, lines 1-5).
14. As per claim 70, Johnson discloses updating the problem resolution information after the potentially security-related event is resolved(see col. 5, lines 39-55).

***Claim Objections***

15. Claim 69 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 11/551,606

Page 6

Art Unit: 2439

June 11, 2009

/J. E. J./

Examiner, Art Unit 2439

/Michael J Simitoski/

Primary Examiner, Art Unit 2439

I hereby certify that this correspondence is being filed via  
EFS-Web with the United States Patent and Trademark Office  
on May 2, 2007

11551606 - GAU: 2439

PATENT

Attorney Docket No.: 022133-000520US

TOWNSEND and TOWNSEND and CREW LLP

By: /Maureen Golob/  
Maureen Golob

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application-of:

Bruce Schneier et al.

Application No.: 11/551,606

Filed: November 21, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Confirmation No.: 1662

Examiner: Unassigned

Art Unit: 2131

INFORMATION DISCLOSURE  
STATEMENT UNDER 37 CFR §1.97 and  
§1.98

Mail Stop Amendment  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The references cited on attached form PTO/SB/08A and PTO/SB/08B are being called to the attention of the Examiner. In accordance with 37 CFR §1.98(d), copies of a number of the references can be found in Application No. 09/766,343, filed January 19, 2001 (Attorney Docket No. 022133-000510US). It is respectfully requested that the cited references be expressly considered during the prosecution of this application, and the references be made of record therein and appear among the "references cited" on any patent to issue therefrom.

As provided for by 37 CFR §1.97(g) and (h), no inference should be made that the information and references cited are prior art merely because they are in this statement and no

**ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /JJ/**

Application No.: 11/551,606  
Page 2

representation is being made that a search has been conducted or that this statement encompasses all the possible relevant information.

Applicant believes that no fee is required for submission of this statement.

However, if a fee is required, the Commissioner is authorized to deduct such fee from the undersigned's Deposit Account No. 20-1430. Please deduct any additional fees from, or credit any overpayment to, the above-noted Deposit Account.

Respectfully submitted,

/Naya Chatterjee-Marathe/

Naya Chatterjee-Marathe  
Reg. No. 54,680

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400  
Fax: 650-326-2422  
NMC:tfw:mg  
61042835 v1

|                                                                                                                                               |   |    |                          |                        |                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------|---|----|--------------------------|------------------------|-----------------|
| Substitute for form 1449A/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br><i>(Use as many sheets as necessary)</i> |   |    | <b>Complete if Known</b> |                        |                 |
|                                                                                                                                               |   |    | Application Number       | 11/551,606             |                 |
|                                                                                                                                               |   |    | Filing Date              | November 21, 2006      |                 |
|                                                                                                                                               |   |    | First Named Inventor     | Schneier, Bruce        |                 |
|                                                                                                                                               |   |    | Art Unit                 | 2131                   |                 |
|                                                                                                                                               |   |    | Examiner Name            | Unassigned             |                 |
| Sheet                                                                                                                                         | 1 | of | 3                        | Attorney Docket Number | 022133-000520US |

| U.S. PATENT DOCUMENTS |                       |                                                             |                                |                                                    |                                                                                 |
|-----------------------|-----------------------|-------------------------------------------------------------|--------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------|
| Examiner Initials*    | Cite No. <sup>1</sup> | Document Number<br>Number Kind Code <sup>2</sup> (if known) | Publication Date<br>MM-DD-YYYY | Name of Patentee or<br>Applicant of Cited Document | Pages, Columns, Lines, Where<br>Relevant Passages or Relevant<br>Figures Appear |
|                       | 1                     | 5,440,723                                                   | 08-08-1995                     | Arnold et al.                                      |                                                                                 |
|                       | 2                     | 5,796,942                                                   | 08-18-1998                     | Esbensen                                           |                                                                                 |
|                       | 3                     | 5,909,493                                                   | 06-01-1999                     | Motoyama                                           |                                                                                 |
|                       | 4                     | 6,026,442                                                   | 02-15-2000                     | Lewis et al.                                       |                                                                                 |
|                       | 5                     | 6,088,804                                                   | 07-11-2000                     | Hill et al.                                        |                                                                                 |
|                       | 6                     | 6,119,236                                                   | 09-12-2000                     | Shipley                                            |                                                                                 |
|                       | 7                     | 6,125,390                                                   | 09-26-2000                     | Touboul                                            |                                                                                 |
|                       | 8                     | 6,182,226                                                   | 01-30-2001                     | Reid et al.                                        |                                                                                 |
|                       | 9                     | 6,205,551                                                   | 03-20-2001                     | Grosse                                             |                                                                                 |
|                       | 10                    | 6,298,445                                                   | 10-02-2001                     | Shostack et al.                                    |                                                                                 |
|                       | 11                    | 6,363,489                                                   | 03-26-2002                     | Comay et al.                                       |                                                                                 |
|                       | 12                    | 6,519,703                                                   | 02-11-2003                     | Joyce                                              |                                                                                 |
|                       | 13                    | 6,681,331                                                   | 01-20-2004                     | Munson et al.                                      |                                                                                 |
|                       | 14                    | 6,704,874                                                   | 03-09-2004                     | Porras et al.                                      |                                                                                 |

| FOREIGN PATENT DOCUMENTS |                       |                           |                     |                                   |                                |                                                    |                                                                                 |                |
|--------------------------|-----------------------|---------------------------|---------------------|-----------------------------------|--------------------------------|----------------------------------------------------|---------------------------------------------------------------------------------|----------------|
| Examiner Initials*       | Cite No. <sup>1</sup> | Foreign Patent Document   |                     |                                   | Publication Date<br>MM-DD-YYYY | Name of Patentee or<br>Applicant of Cited Document | Pages, Columns, Lines,<br>Where Relevant Passages<br>or Relevant Figures Appear | T <sup>6</sup> |
|                          |                       | Country Code <sup>3</sup> | Number <sup>4</sup> | Kind Code <sup>5</sup> (if known) |                                |                                                    |                                                                                 |                |
|                          |                       |                           |                     |                                   |                                |                                                    |                                                                                 |                |
|                          |                       |                           |                     |                                   |                                |                                                    |                                                                                 |                |

|                    |                               |                 |            |
|--------------------|-------------------------------|-----------------|------------|
| Examiner Signature | /Jenise Jackson/ (06/11/2009) | Date Considered | 06/11/2009 |
|--------------------|-------------------------------|-----------------|------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Kind Codes of U.S. Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language translation is attached.

61042835 V1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /JJ/

|                                                                                                                                        |   |    |   |                          |                   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--------------------------|-------------------|
| Substitute for form 1449B/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br>(Use as many sheets as necessary) |   |    |   | <b>Complete if Known</b> |                   |
|                                                                                                                                        |   |    |   | Application Number       | 11/551,606        |
|                                                                                                                                        |   |    |   | Filing Date              | November 21, 2006 |
|                                                                                                                                        |   |    |   | First Named Inventor     | Schneier, Bruce   |
|                                                                                                                                        |   |    |   | Art Unit                 | 2131              |
|                                                                                                                                        |   |    |   | Examiner Name            | Unassigned        |
| Sheet                                                                                                                                  | 2 | of | 3 | Attorney Docket Number   | 022133-000520US   |

| NON PATENT LITERATURE DOCUMENTS |                       |                                                                                                                                                                                                                                                                                           |                          |
|---------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Examiner Initials *             | Cite No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                           | T <sup>2</sup>           |
|                                 | 15                    | "FAQ: Network Intrusion Detection Systems," Version 0.3, Jan. 1, 1998, <a href="http://www.robertgraham.com/pubs/network-intrusion-detection.txt">http://www.robertgraham.com/pubs/network-intrusion-detection.txt</a> , downloaded Oct. 19, 2001, pp. 1-29.                              | <input type="checkbox"/> |
|                                 | 16                    | "Latest Network Management Products," (Product Information) <i>Communication News</i> , Jun. 2000, 2 pages total.                                                                                                                                                                         | <input type="checkbox"/> |
|                                 | 17                    | "Managed Security Services: Are They Right For You?" <i>ENT</i> , Nov. 22, 2000, 4 pages total.                                                                                                                                                                                           | <input type="checkbox"/> |
|                                 | 18                    | "Security Monitoring Services," <i>Information Week</i> , No. 792, June 26, 2000, p. 244.                                                                                                                                                                                                 | <input type="checkbox"/> |
|                                 | 19                    | BALASUBRAMANIAN, J. S. et al., "An Architecture for Intrusion Detection Using Autonomous Agents," Center for Education and Research in Information Assurance and Security, CERIAS Technical Report May 1995, Jun. 11, 1998, pp. 1-19.                                                     | <input type="checkbox"/> |
|                                 | 20                    | BLACHARSKI, "Outsourcing Firewall Management – Managed Firewall Services Prevent Security Burnouts – Firewall Management Requires 24-Hour Vigilance. If You Can't Pull Round-the-Clock Guard Duty, Outsourcing May Be for You," <i>Network Magazine</i> , Vol. 60, Aug. 1, 2000, 6 pages. | <input type="checkbox"/> |
|                                 | 21                    | Citation details: "Automated Information System--(AIS) Alarm System," W. Hunteman, <a href="http://citeseer.nj.nec.com/context/1642652/0">http://citeseer.nj.nec.com/context/1642652/0</a> , downloaded Oct. 19, 2001, 1 page.                                                            | <input type="checkbox"/> |
|                                 | 22                    | COMPUTEL WHITE PAPERS, "Managed Security Monitoring," 2001, pp. 1-4.                                                                                                                                                                                                                      | <input type="checkbox"/> |
|                                 | 23                    | ESSEX, "E-Sleuths Make Net Safe for E-Commerce; RIPTech Stakes Its Claim in the Growing Market for Remotely Managed Security," <i>Computerworld</i> , Vol. 80, No. 1, Jun. 12, 2000, 2 pages.                                                                                             | <input type="checkbox"/> |
|                                 | 24                    | FRATTO, "RFP: Managed Firewall Services," <i>Network Computing</i> , Vol. 9, No. 20, p.68, Nov. 1, 1998, 12 pages total.                                                                                                                                                                  | <input type="checkbox"/> |
|                                 | 25                    | HUNTEMAN, W., "Automated Information System--(AIS) Alarm System," University of California, Los Alamos National Laboratory, In Proceedings of the 20th National Information Systems Security Conference, National Institute of Standards and Technology, Oct. 1997, pp. 1-12.             | <input type="checkbox"/> |

|                    |                               |                 |            |
|--------------------|-------------------------------|-----------------|------------|
| Examiner Signature | /Jenise Jackson/ (06/11/2009) | Date Considered | 06/11/2009 |
|--------------------|-------------------------------|-----------------|------------|

\* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

|                                                                                                                                        |   |    |   |                          |                   |
|----------------------------------------------------------------------------------------------------------------------------------------|---|----|---|--------------------------|-------------------|
| Substitute for form 1449B/PTO<br><br><b>INFORMATION DISCLOSURE<br/>STATEMENT BY APPLICANT</b><br><br>(Use as many sheets as necessary) |   |    |   | <b>Complete if Known</b> |                   |
|                                                                                                                                        |   |    |   | Application Number       | 11/551,606        |
|                                                                                                                                        |   |    |   | Filing Date              | November 21, 2006 |
|                                                                                                                                        |   |    |   | First Named Inventor     | Schneier, Bruce   |
|                                                                                                                                        |   |    |   | Art Unit                 | 2131              |
|                                                                                                                                        |   |    |   | Examiner Name            | Unassigned        |
| Sheet                                                                                                                                  | 3 | of | 3 | Attorney Docket Number   | 022133-000520US   |

| NON-PATENT LITERATURE DOCUMENTS |                       |                                                                                                                                                                                                                                                                                                                                                                                          |                          |
|---------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Examiner Initials *             | Cite No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.                                                                                                                          | T <sup>2</sup>           |
|                                 | 26                    | M2 PRESSWIRE, "GTE Internetworking: GTE Internetworking Offers New Version of Its Site Patrol Managed Security Services," Sep. 3, 1999, pp. 1-3.                                                                                                                                                                                                                                         | <input type="checkbox"/> |
|                                 | 27                    | M2 PRESSWIRE, "ISS: ISS Acquires Netrex Secure Solutions," Aug. 31, 1999, 1 page.                                                                                                                                                                                                                                                                                                        | <input type="checkbox"/> |
|                                 | 28                    | MESSMER, "Security Needs Spawn Services Managed Detection Services Growing in Popularity," <i>Network World</i> , April 3, 2000, 1 page                                                                                                                                                                                                                                                  | <input type="checkbox"/> |
|                                 | 29                    | NEUMANN, P. G. et al., "Experience with Emerald to Date," Computer Science Laboratory, SRI International, 1st USENIX Workshop on Intrusion Detection and Networking Monitoring, Santa Clara, California, Apr. 11-12, 1999, pp. 73-80, <a href="http://www.csl.sri.com/users/neumann/det99.html">http://www.csl.sri.com/users/neumann/det99.html</a> , downloaded Oct. 19, 2001, pp. 1-9. | <input type="checkbox"/> |
|                                 | 30                    | PORRAS, P. A. et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Computer Science Laboratory, SRI International, 20th NISSC --Oct. 9, 1997 pp. 1-22 (version with legible text but no figures), pp. 1-13 (version with figures but illegible text)                                                                                                   | <input type="checkbox"/> |
|                                 | 31                    | REDSIREN, "Managed Solutions," downloaded from Internet << <a href="http://www.redsiren.com">http://www.redsiren.com</a> >>, p. 1-3 (Publication Date Unknown).                                                                                                                                                                                                                          | <input type="checkbox"/> |
|                                 | 32                    | RKON TECHNOLOGIES, downloaded from Internet << <a href="http://www.rkontechnologies.com">http://www.rkontechnologies.com</a> >> (Publication Date Unknown)                                                                                                                                                                                                                               | <input type="checkbox"/> |
|                                 | 33                    | SAVAGE, "Locking the Doors -- Denial of Services Attacks and Viruses Prime the Market For Security Solutions and Services," <i>Computer Reseller News</i> , Vol. 72, Sep. 25, 2000, 2 pages total.                                                                                                                                                                                       | <input type="checkbox"/> |
|                                 | 34                    | VPNTRUST: CONSULTING, "VPNTrust Services: Consulting" 1999, Technica Corporation, pp. 1-3.                                                                                                                                                                                                                                                                                               | <input type="checkbox"/> |

|                    |                               |                 |            |
|--------------------|-------------------------------|-----------------|------------|
| Examiner Signature | /Jenise Jackson/ (06/11/2009) | Date Considered | 06/11/2009 |
|--------------------|-------------------------------|-----------------|------------|

<sup>1</sup> EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>2</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached.

| Set | Items    | Description                                                                                                                                                                    |
|-----|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S1  | 2746445  | (PROBE? OR SENTRY OR HONEYPOT OR SCANNER? OR SENSOR?)                                                                                                                          |
| S2  | 12023516 | (MONITOR? OR DETECT? OR DETECTION OR INTRUD? OR INTRUSION -<br>OR RESPONSE OR ALERT? OR INCIDENT? OR ATTACK? OR ANALY?S OR A-<br>NALYZE OR FILTER)                             |
| S3  | 1259464  | (TROJAN()HORSE OR VIRUS OR FOOTPRINT? OR VULNERABIL? OR AT-<br>TACK(2N)SIGNATURE OR INTRUD? OR INTRUSION)                                                                      |
| S4  | 102042   | (NETWORK) (10N) (SECURITY OR INTELLIGEN?()DATABASE? ? OR MAN-<br>AGED() SECURITY)                                                                                              |
| S5  | 130681   | S4 OR (CONTROL(2N)CENTER OR SECURE(2N)OPERATIONS(2N)CENTER<br>OR CENTRAL(2N)FACILITY OR REMOTE(2N)CONSOLE OR SECURITY(2N)AN-<br>ALYST OR SECURITY(2N)ENGINEER OR ADMINSTRATOR) |
| S6  | 3301     | S1 AND S2 AND S3 AND S4                                                                                                                                                        |
| S7  | 71       | (SECURITY(2N)MONITORING) (5N) (NETWORK) AND S6                                                                                                                                 |
| ?   |          |                                                                                                                                                                                |

SYSTEM:OS - DIALOG OneSearch

File 2:INSPEC 1898-2009/May W5  
(c) 2009 The IET

File 6:NTIS 1964-2009/Jun W2  
(c) 2009 NTIS, Intl Cpyrght All Rights Res

File 8:Ei Compendex(R) 1884-2009/May W5  
(c) 2009 Elsevier Eng. Info. Inc.

File 34:SciSearch(R) Cited Ref Sci 1990-2009/May W5  
(c) 2009 The Thomson Corp

File 35:Dissertation Abs Online 1861-2009/May  
(c) 2009 ProQuest Info&Learning

File 56:Computer and Information Systems Abstracts 1966-2009/Jun  
(c) 2009 CSA.

File 60:ANTE: Abstracts in New Tech & Engineer 1966-2009/Jun  
(c) 2009 CSA.

File 65:Inside Conferences 1993-2009/Jun 11  
(c) 2009 BLDSC all rts. reserv.

File 92:IHS Intl.Stds.& Specs. 1999/Nov  
(c) 1999 Information Handling Services

\*File 92: This file is closed.

File 95:TEME-Technology & Management 1989-2009/May W3  
(c) 2009 FIZ TECHNIK

File 99:Wilson Appl. Sci & Tech Abs 1983-2009/May  
(c) 2009 The HW Wilson Co.

File 103:Energy SciTec 1974-2009/May B2  
(c) 2009 Contains copyrighted material

\*File 103: For access restrictions see Help Restrict.

File 144:Pascal 1973-2009/Jun W1  
(c) 2009 INIST/CNRS

File 239:Mathsci 1940-2009/May  
(c) 2009 American Mathematical Society

File 275:Gale Group Computer DB(TM) 1983-2009/May 14  
(c) 2009 Gale/Cengage

File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec  
(c) 2006 The Thomson Corp

File 647:UBM Computer Fulltext 1988-2009/Jun W1  
(c) 2009 UBM, LLC

File 674:Computer News Fulltext 1989-2006/Sep W1  
(c) 2006 IDG Communications

\*File 674: File 674 is closed (no longer updates).

File 696:DIALOG Telecom. Newsletters 1995-2009/Jun 10  
(c) 2009 Dialog

|                                   |                                       |                                                               |             |
|-----------------------------------|---------------------------------------|---------------------------------------------------------------|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/551,606 | Applicant(s)/Patent Under<br>Reexamination<br>SCHNEIER ET AL. |             |
|                                   | Examiner<br>JENISE E. JACKSON         | Art Unit<br>2439                                              | Page 1 of 1 |

**U.S. PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name              | Classification |
|---|---|--------------------------------------------------|-----------------|-------------------|----------------|
| * | A | US-5,970,149                                     | 10-1999         | Johnson, R. Brent | 714/46         |
|   | B | US-                                              |                 |                   |                |
|   | C | US-                                              |                 |                   |                |
|   | D | US-                                              |                 |                   |                |
|   | E | US-                                              |                 |                   |                |
|   | F | US-                                              |                 |                   |                |
|   | G | US-                                              |                 |                   |                |
|   | H | US-                                              |                 |                   |                |
|   | I | US-                                              |                 |                   |                |
|   | J | US-                                              |                 |                   |                |
|   | K | US-                                              |                 |                   |                |
|   | L | US-                                              |                 |                   |                |
|   | M | US-                                              |                 |                   |                |

**FOREIGN PATENT DOCUMENTS**

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--------------------------------------------------|-----------------|---------|------|----------------|
|   | N |                                                  |                 |         |      |                |
|   | O |                                                  |                 |         |      |                |
|   | P |                                                  |                 |         |      |                |
|   | Q |                                                  |                 |         |      |                |
|   | R |                                                  |                 |         |      |                |
|   | S |                                                  |                 |         |      |                |
|   | T |                                                  |                 |         |      |                |

**NON-PATENT DOCUMENTS**

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|-------------------------------------------------------------------------------------------|
|   | U |                                                                                           |
|   | V |                                                                                           |
|   | W |                                                                                           |
|   | X |                                                                                           |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier

Application No.: 11/551,606

Filed: October 20, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK  
INTRUSION MONITORING,  
DETECTION AND RESPONSE

Customer No.: 20350

Confirmation No. 1662

Examiner: Jenise E. Jackson

Technology Center/Art Unit: 2439

AMENDMENT

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

In response to the Office Action mailed June 18, 2009, please enter the following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 6 of this paper.

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings of claims in the application:

**Listing of Claims:**

1. - 44. (Canceled).

45. (Previously presented) A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:

- a) a sensor coupled to collect status data from at least one monitored component of the network;
- b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
- c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
- d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
- e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

46. (Previously presented) The system of claim 45, wherein the identifying step includes performing a multi-stage analysis of the status data.

47. (Previously presented) The system of claim 46, wherein the multi-stage analysis includes performing a discrimination analysis on the status data.

48. (Previously presented) The system of claim 47, wherein the discrimination analysis includes positive filtering.

49. (Previously presented) The system of claim 47, wherein the discrimination analysis includes negative filtering.

50. (Previously presented) The system of claim 46, wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe.

51. (Previously presented) The system of claim 45, wherein the identifying step includes aggregating and synthesizing the status data at the probe.

52. (Previously presented) The system of claim 51, wherein the identifying step includes cross-correlating data across the monitored components.

53. (Previously presented) The system of claim 51, wherein the identifying step includes analyzing the frequency of occurrence of the events.

54. (Previously presented) The system of claim 45, further comprising after the step (c), a secure operations center coupled to perform further computer-based analysis and to receive data from the probe.

55. (Previously presented) The system of claim 54, wherein the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

56. (Previously presented) The system of claim 54, wherein the identifying step includes cross-correlating data across the monitored components.

57. (Previously presented) The system of claim 54, wherein the identifying step includes analyzing the frequency of occurrence of the events.

58. (Previously presented) The system of claim 54, wherein the computer-based analysis includes cross-probe correlation.

59. (Previously presented) The system of claim 45, further comprising instantaneously self-tuning the probe based on previously collected status data.

60. (Previously presented) The system of claim 45, wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

61. (Previously presented) The system of claim 45, wherein the receiving feedback step occurs in substantially real time.

62. (Currently amended) A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:  
creating an event record for information received about an identified potentially security-related event occurring on the network;  
correlating the event record with customer information and a symptom record;  
using the correlated symptom record to link the event record to problem resolution information;  
consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket; and  
providing the problem ticket to a security analyst console for analysis.

63. (Previously presented) The method of claim 62, further comprising:  
correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and  
linking the event record to an open problem ticket associated with the pre-existing event record.

64. (Currently amended) The method of claim 62, wherein the problem resolution assistance information links the symptom to a diagnosis.

65. (Currently amended) The method of claim 62, wherein the problem resolution assistance information links the symptom to a technology.

66. (Currently amended) The method of claim 62, further comprising:  
correlating the event record with a vulnerability; and  
using the correlated vulnerability to link the event record to problem resolution assistance information.

67. (Currently amended) The method of claim 66, wherein the problem resolution assistance information links the vulnerability to a diagnosis.

68. (Currently amended) The method of claim 66, wherein the problem resolution assistance information links the vulnerability to a technology.

69. (Previously presented) The method of claim 62, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by filtering.

70. (Currently amended) The method of claim 62, further comprising:  
updating the problem resolution assistance information after the potentially security-related event is resolved.

**REMARKS/ARGUMENTS**

Claims 45-70 were pending in this application. In this amendment, no claims are cancelled or added and claims 62, 64-68 and 70 are amended. After entry of this amendment, claims 45-70 will remain pending. Applicant submits that the amended claims are supported by the specification as originally filed and therefore introduces no new matter.

In the Office Action, the Examiner rejected claims 45-61 under 35 USC §101, asserting obviousness-type nonstatutory double patenting with respect to claims in issued U.S. Patent No. 7,159,237. Without taking a position on whether such a rejection is appropriate, Applicant submits herewith a Terminal Disclaimer in accordance with 37 CFR §1.321(c). Since this overcomes the rejection of claims 45-61, those claims are allowable. It is noted that each of the claims are otherwise allowable under §101, since they are directed to statutory subject matter at least because claims 45-61 are directed to a system for operating a probe as part of a security monitoring system for a computer network and while claims 62-70 are directed to a method of operating a secure operations center as part of a security monitoring system for a customer computer network claims, they each meet the machine-or-transformation test set forth in In Re Bilski, 545 F.3d 943 (Fed. Cir. 2008)(en banc), cert. granted, \_\_\_ U.S. \_\_\_, 129 S.Ct. 2735 (2009).

In the Office Action, the Examiner also rejected claims 62-68 and 70 under 35 USC §102(b) as being anticipated by U.S. Patent No. 5,970,149 to Johnson (hereinafter "Johnson"). Applicant notes with appreciation the indication of allowability of claim 69 if rewritten in independent form, but in view of the explanation below as to the allowability of the rest of the rejected claims, Applicant declines to rewrite claim 69 in independent form.

Claim 62 is allowable over Johnson, as Johnson fails to disclose or suggest each element of the claim 62. For example, Johnson does not disclose or suggest the using step of claim 62 or the consolidating step of claim 62. In order to further clarify claim 62, "problem resolution information" is amended to read "problem resolution assistance information". While Johnson's system does provide problem details to a field engineer or remote support person, the teachings of Johnson do not appear to include the provision of problem resolution assistance

information. Instead, it appears that the field engineers are expected to solve the problem on their own or use other tools to find additional information. In any case, the claimed “consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a problem ticket” is not disclosed or suggested.

The Examiner cited to Johnson, col. 4, lines 9-20 and 39-40 as teaching the claimed consolidating. It is apparent that Johnson’s system provides for the creation of trouble tickets, but there is nothing to indicate that such trouble tickets are anything more than indicators of the occurrence of alerts, events or problems, much less something that would consolidate an event record, correlated customer information and symptom record, and linked problem resolution assistance information, as is claimed. Therefore, the Examiner’s mere assertion that the claimed element is taught therein cannot be supported and Applicant’s respectfully request withdrawal of the rejection of claim 62. Additionally, it does not appear that other portions of Johnson make up for this, which is understandable as the focus of Johnson appears to be how to solve the problem of providing a field engineer with a password to access a secure customer site in response to an alert, event or problem with that secure customer site. This is well illustrated by Fig. 5B of Johnson, where there are many steps, but the most relevant one on the page is simply labeled “Solve Problem” 172 and the accompanying text provides little in the way of detail as to what steps are used to provide details to the field engineer to solve the problem. While this may be reasonable in an environment wherein simply flagging a problem to a field engineer is sufficient to allow for solving the problem, claim 62 includes other claimed elements.

Claims 63-68 and 70 are allowable at least because they depend from allowable claim 62 and therefore their rejection should be withdrawn. Additionally, it should be noted that claim 63 recites an additional step of correlating an event record with a pre-existing event record and Johnson does not show that, despite the Examiner’s citation to Johnson, col. 5, lines 25-45. Likewise, Johnson does not appear to disclose or suggest the linking of symptom to diagnosis of claim 64, but instead appears to leave the diagnosis to the field engineer. Similar arguments apply to claims 65-68.

As for claim 70, which recites an updating step, there does not appear to be any disclosure or suggestion in Johnson beyond just the field engineer reporting that the problem is solved. In fact, it appears that one approach in Johnson is that the field engineer makes a telephone call to the dispatch control center to inform personnel there that a problem was solved. It is not apparent that such personnel would have a mechanism to update any problem resolution assistance information in response to the call. However, consistent with the focus of Johnson, it does describe the response of cancelling the field engineer's password on the customer's secure site once the dispatch control center is aware that the problem has been solved.

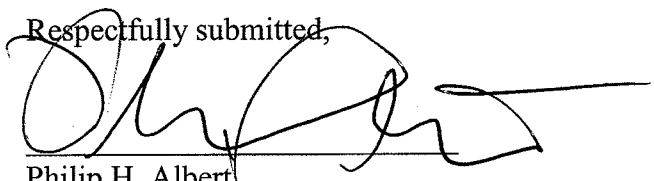
**CONCLUSION**

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Date: December 18, 2009

Respectfully submitted,

  
Philip H. Albert  
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400 Fax: 415-576-0300  
PHA:psc  
62338093 v1

## Electronic Patent Application Fee Transmittal

| <b>Application Number:</b>                     | 11551606                                                                           |          |        |                      |
|------------------------------------------------|------------------------------------------------------------------------------------|----------|--------|----------------------|
| <b>Filing Date:</b>                            | 20-Oct-2006                                                                        |          |        |                      |
| <b>Title of Invention:</b>                     | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |          |        |                      |
| <b>First Named Inventor/Applicant Name:</b>    | Bruce Schneier                                                                     |          |        |                      |
| <b>Filer:</b>                                  | Philip H. Albert/Paula Cunningham                                                  |          |        |                      |
| <b>Attorney Docket Number:</b>                 |                                                                                    |          |        |                      |
| Filed as Large Entity                          |                                                                                    |          |        |                      |
| <b>Utility under 35 USC 111(a) Filing Fees</b> |                                                                                    |          |        |                      |
| Description                                    | Fee Code                                                                           | Quantity | Amount | Sub-Total in USD(\$) |
| <b>Basic Filing:</b>                           |                                                                                    |          |        |                      |
| <b>Pages:</b>                                  |                                                                                    |          |        |                      |
| <b>Claims:</b>                                 |                                                                                    |          |        |                      |
| <b>Miscellaneous-Filing:</b>                   |                                                                                    |          |        |                      |
| <b>Petition:</b>                               |                                                                                    |          |        |                      |
| <b>Patent-Appeals-and-Interference:</b>        |                                                                                    |          |        |                      |
| <b>Post-Allowance-and-Post-Issuance:</b>       |                                                                                    |          |        |                      |
| <b>Extension-of-Time:</b>                      |                                                                                    |          |        |                      |
| Extension - 3 months with \$0 paid             | 1253                                                                               | 1        | 1110   | 1110                 |

| Description          | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|----------------------|----------|----------|--------|----------------------|
| Miscellaneous:       |          |          |        |                      |
| Statutory disclaimer | 1814     | 1        | 140    | 140                  |
| Total in USD (\$)    |          |          |        | 1250                 |

## Electronic Acknowledgement Receipt

|                                             |                                                                                                   |
|---------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 6673607                                                                                           |
| <b>Application Number:</b>                  | 11551606                                                                                          |
| <b>International Application Number:</b>    |                                                                                                   |
| <b>Confirmation Number:</b>                 | 1662                                                                                              |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response                |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                                    |
| <b>Correspondence Address:</b>              | COUNTERPANE INTERNET SECURITY, INC.<br>-<br>3031 TISCH WAY<br>-<br>SAN JOSE CA 95128<br>US -<br>- |
| <b>Filer:</b>                               | Philip H. Albert/Paula Cunningham                                                                 |
| <b>Filer Authorized By:</b>                 | Philip H. Albert                                                                                  |
| <b>Attorney Docket Number:</b>              |                                                                                                   |
| <b>Receipt Date:</b>                        | 18-DEC-2009                                                                                       |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                                       |
| <b>Time Stamp:</b>                          | 18:52:34                                                                                          |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)                                                                       |

### Payment information:

|                                          |                 |
|------------------------------------------|-----------------|
| Submitted with Payment                   | yes             |
| Payment Type                             | Deposit Account |
| Payment was successfully received in RAM | \$ 1250         |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                            |                                                     |                                                    |                         |                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|-----------------------------------------------------|----------------------------------------------------|-------------------------|-------------------------|
| RAM confirmation Number                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 5263                                                       |                                                     |                                                    |                         |                         |
| Deposit Account                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 201430                                                     |                                                     |                                                    |                         |                         |
| Authorized User                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                            |                                                     |                                                    |                         |                         |
| <p>The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)</p> <p>Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)</p> |                                                            |                                                     |                                                    |                         |                         |
| <b>File Listing:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                            |                                                     |                                                    |                         |                         |
| <b>Document Number</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <b>Document Description</b>                                | <b>File Name</b>                                    | <b>File Size(Bytes)/ Message Digest</b>            | <b>Multi Part /.zip</b> | <b>Pages (if appl.)</b> |
| 1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Power of Attorney                                          | Power_of_Attorney_022133-000520US.pdf               | 95145<br>e0fa5004695c402939003aea1c6f2b633fd459ba  | no                      | 1                       |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                            |                                                     |                                                    |                         |                         |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                            |                                                     |                                                    |                         |                         |
| 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Assignee showing of ownership per 37 CFR 3.73(b).          | Statement_Under_37CFR373b_022133-000520US.pdf       | 62541<br>45c5f7ff00809502591523a1d26b0a5754666c4   | no                      | 1                       |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                            |                                                     |                                                    |                         |                         |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                            |                                                     |                                                    |                         |                         |
| 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Extension of Time                                          | Petition_for_Extension_of_Tim e_022133-000520US.PDF | 58604<br>397c11251e5f00072e7e39af6d0e26fc495742af  | no                      | 1                       |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                            |                                                     |                                                    |                         |                         |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                            |                                                     |                                                    |                         |                         |
| 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Terminal Disclaimer Filed                                  | Terminal_Disclaimer_022133_000520US.PDF             | 73388<br>fe70de2125624e58ef58b3eb7b0b953e9f111025  | no                      | 1                       |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                            |                                                     |                                                    |                         |                         |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                            |                                                     |                                                    |                         |                         |
| 5                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                            | Amendment_June182009_OA_022133-000520US.PDF         | 400693<br>3a1f571c365f15d65424226f3f0514c4bc2ab88c | yes                     | 8                       |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Multipart Description/PDF files in .zip description</b> |                                                     |                                                    |                         |                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Document Description</b>                                |                                                     | <b>Start</b>                                       | <b>End</b>              |                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Amendment/Req. Reconsideration-After Non-Final Reject      |                                                     | 1                                                  | 1                       |                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Claims                                                     |                                                     | 2                                                  | 5                       |                         |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Applicant Arguments/Remarks Made in an Amendment           |                                                     | 6                                                  | 8                       |                         |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                         |              |                                          |    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|--------------|------------------------------------------|----|---|
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                         |              |                                          |    |   |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |              |                                          |    |   |
| 6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Fee Worksheet (PTO-875) | fee-info.pdf | 31971                                    | no | 2 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                         |              | d91a4655cbe06cb9aff0eeb80071d8d7683d4cda |    |   |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                         |              |                                          |    |   |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                         |              |                                          |    |   |
| Total Files Size (in bytes):                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                         |              | 722342                                   |    |   |
| <p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b><br/> <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b><br/> <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b><br/> <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p> |                         |              |                                          |    |   |

|                                                                                                                                                   |                             |                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---------------------------------------------------------------------------------------------|
| <b>POWER OF ATTORNEY<br/>OR<br/>REVOCATION OF POWER OF ATTORNEY<br/>WITH A NEW POWER OF ATTORNEY<br/>AND<br/>CHANGE OF CORRESPONDENCE ADDRESS</b> | <b>Application Number</b>   | 11/551,606                                                                                  |
|                                                                                                                                                   | <b>Filing Date</b>          | October 20, 2006                                                                            |
|                                                                                                                                                   | <b>First Named Inventor</b> | Schneier, Bruce                                                                             |
|                                                                                                                                                   | <b>Title</b>                | METHOD AND SYSTEM FOR<br>DYNAMIC NETWORK INTRUSION<br>MONITORING, DETECTION AND<br>RESPONSE |
|                                                                                                                                                   | <b>Art Unit</b>             | 2439                                                                                        |
|                                                                                                                                                   | <b>Examiner Name</b>        | Jenise E. Jackson                                                                           |
|                                                                                                                                                   | <b>Attorney Docket</b>      | 022133-000520US                                                                             |

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

**OR**

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

**20350**

**OR**

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

| Practitioner(s) Name | Registration Number |
|----------------------|---------------------|
|                      |                     |
|                      |                     |
|                      |                     |
|                      |                     |

I further authorize any of the above-identified practitioners to execute a Statement Under 37 CFR 3.73(b) on my/our behalf to certify the chain of title and establish my/our ownership in the application identified above.

Please recognize or change the correspondence address for the above-identified application to:

☒ The address associated with the above-mentioned Customer Number:

**OR**

☐ The address associated with Customer Number:

**OR**

|                                                  |  |       |  |     |  |
|--------------------------------------------------|--|-------|--|-----|--|
| <input type="checkbox"/> Firm or Individual Name |  |       |  |     |  |
| Address                                          |  |       |  |     |  |
| City                                             |  | State |  | Zip |  |
| Country                                          |  |       |  |     |  |
| Telephone                                        |  | Email |  |     |  |

I am the:

☐ Applicant/Inventor.

**OR**

☒ Assignee of record of the entire interest. See 37 CFR 3.71.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96 submitted herewith or filed on \_\_\_\_\_).

**SIGNATURE of Applicant or Assignee of Record**

|                   |                                                                                     |           |                  |
|-------------------|-------------------------------------------------------------------------------------|-----------|------------------|
| Signature         |  | Date      | December 7, 2009 |
| Name              | Jamie Newell                                                                        | Telephone | 888-710-8175     |
| Title and Company | Secretary BT Counterpane Internet Security, Inc.                                    |           |                  |

**NOTE:** Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below\*.

☒ \*Total of ONE forms are submitted.

**STATEMENT UNDER 37 CFR 3.73(b)**Applicant/Patent Owner: Bruce Schneier, et al.Application No./Patent No.: 11/551,606 Filed/Issue Date: October 20, 2006Titled: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE

BT Counterpane Internet Security, Inc., a corporation  
 (Name of Assignee) (Type of Assignee: corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in  
 (The extent (by percentage) of its ownership interest is \_\_\_\_\_ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

**OR**

- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Bruce Schneier, et al To: Counterpane Internet Security, Inc.

The document was recorded in the United States Patent and Trademark Office at  
 Reel 011845, Frame 0122, or for which a copy thereof is attached.

2. From: Counterpane Internet Security, Inc. To: BT Counterpane Internet Security, Inc.

The document was recorded in the United States Patent and Trademark Office at  
 Reel 023657, Frame 0530, or for which a copy thereof is attached.

3. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
 Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet (s).

- ☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

December 7, 2009



Signature

Date

Jamie Newell

Printed or Typed Name

Secretary

Title

|                                                                                                                                                                       |  |                                             |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------------------------------|--|
| <b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b><br><br><b>FY 2009</b><br><i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i> |  | Docket Number (Optional)<br>022133-000520US |  |
| Application Number 11/551,606                                                                                                                                         |  | Filed October 20, 2006                      |  |
| For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE                                                                                |  |                                             |  |
| Art Unit 2439                                                                                                                                                         |  | Examiner Jenise E. Jackson                  |  |

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

|                                                                      | <u>Fee</u> | <u>Small Entity Fee</u> |          |
|----------------------------------------------------------------------|------------|-------------------------|----------|
| <input type="checkbox"/> One month (37 CFR 1.17(a)(1))               | \$130      | \$65                    | \$ _____ |
| <input type="checkbox"/> Two months (37 CFR 1.17(a)(2))              | \$490      | \$245                   | \$ _____ |
| <input checked="" type="checkbox"/> Three months (37 CFR 1.17(a)(3)) | \$1110     | \$555                   | \$ 1110  |
| <input type="checkbox"/> Four months (37 CFR 1.17(a)(4))             | \$1730     | \$865                   | \$ _____ |
| <input type="checkbox"/> Five months (37 CFR 1.17(a)(5))             | \$2350     | \$1175                  | \$ _____ |

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 20-1430.

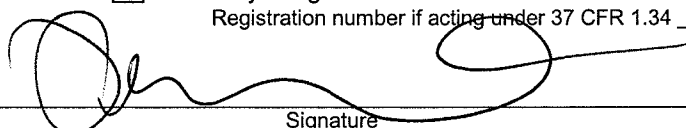
**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

I am the ☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration Number 35,819

☐ attorney or agent under 37 CFR 1.34.  
Registration number if acting under 37 CFR 1.34 \_\_\_\_\_

  
\_\_\_\_\_  
Signature

12/18/2009  
\_\_\_\_\_  
Date

Philip H. Albert, Reg. No. 35,819  
\_\_\_\_\_  
Typed or printed name

(650) 326-2400  
\_\_\_\_\_  
Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☒ Total of ONE forms are submitted.

**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING  
REJECTION OVER A "PRIOR" PATENT**

Docket Number (Optional)  
022133-000520US

In re Application of: Bruce Schneier

Application No.: 11/551,606

Filed: October 20, 2006

For: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE

The owner\*, Counterpane Internet Security, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application, which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,159,237 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

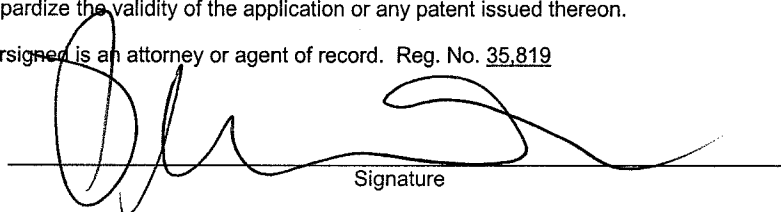
expires for failure to pay a maintenance fee;  
is held unenforceable;  
is found invalid by a court of competent jurisdiction;  
is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;  
has all claims canceled by a reexamination certificate;  
is reissued; or  
is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☒ The undersigned is an attorney or agent of record. Reg. No. 35,819



Signature

12/18/09  
Date

Philip H. Albert  
Typed or printed name

(650) 326-2400  
Telephone Number

- ☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).  
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| <b>PATENT APPLICATION FEE DETERMINATION RECORD</b><br>Substitute for Form PTO-875                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                               |                                  |                                    |               | Application or Docket Number<br><b>11/551,606</b> |                     | Filing Date<br><b>10/20/2006</b> |                     | <input type="checkbox"/> To be Mailed |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------------|---------------|---------------------------------------------------|---------------------|----------------------------------|---------------------|---------------------------------------|---|
| <b>APPLICATION AS FILED – PART I</b>                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                  | (Column 2)                         |               | SMALL ENTITY <input type="checkbox"/>             |                     | OR                               |                     | OTHER THAN SMALL ENTITY               |   |
| FOR                                                                                                                                                                                                                                                                                                                                                                                                                                  | NUMBER FILED                                                                                                                                                                                                                  | NUMBER EXTRA                     | RATE (\$)                          | FEE (\$)      | RATE (\$)                                         | FEE (\$)            |                                  |                     |                                       |   |
| <input type="checkbox"/> BASIC FEE<br>(37 CFR 1.16(a), (b), or (c))                                                                                                                                                                                                                                                                                                                                                                  | N/A                                                                                                                                                                                                                           | N/A                              | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> SEARCH FEE<br>(37 CFR 1.16(k), (l), or (m))                                                                                                                                                                                                                                                                                                                                                                 | N/A                                                                                                                                                                                                                           | N/A                              | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> EXAMINATION FEE<br>(37 CFR 1.16(o), (p), or (q))                                                                                                                                                                                                                                                                                                                                                            | N/A                                                                                                                                                                                                                           | N/A                              | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |   |
| TOTAL CLAIMS<br>(37 CFR 1.16(i))                                                                                                                                                                                                                                                                                                                                                                                                     | minus 20 =                                                                                                                                                                                                                    | *                                | X \$                               | =             | OR                                                | X \$                | =                                |                     |                                       |   |
| INDEPENDENT CLAIMS<br>(37 CFR 1.16(h))                                                                                                                                                                                                                                                                                                                                                                                               | minus 3 =                                                                                                                                                                                                                     | *                                | X \$                               | =             |                                                   | X \$                | =                                |                     |                                       |   |
| <input type="checkbox"/> APPLICATION SIZE FEE<br>(37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                    | If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s). |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| * If the difference in column 1 is less than zero, enter "0" in column 2.                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                               |                                  | TOTAL                              |               |                                                   | TOTAL               |                                  |                     |                                       |   |
| <b>APPLICATION AS AMENDED – PART II</b>                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                  | (Column 2)                         |               | (Column 3)                                        |                     | SMALL ENTITY                     |                     | OR OTHER THAN SMALL ENTITY            |   |
| AMENDMENT                                                                                                                                                                                                                                                                                                                                                                                                                            | 12/18/2009                                                                                                                                                                                                                    | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$)                                         | ADDITIONAL FEE (\$) | RATE (\$)                        | ADDITIONAL FEE (\$) |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Total (37 CFR 1.16(i))                                                                                                                                                                                                        | * 26                             | Minus                              | ** 26         | = 0                                               | X \$                | =                                | OR                  | X \$52=                               | 0 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Independent (37 CFR 1.16(h))                                                                                                                                                                                                  | * 2                              | Minus                              | *** 3         | = 0                                               | X \$                | =                                | OR                  | X \$220=                              | 0 |
| <input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     | OR                               |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                               |                                  |                                    |               | TOTAL ADD'L FEE                                   |                     | OR                               | TOTAL ADD'L FEE     | 0                                     |   |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                  | (Column 2)                         |               | (Column 3)                                        |                     | SMALL ENTITY                     |                     | OR OTHER THAN SMALL ENTITY            |   |
| AMENDMENT                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                               | CLAIMS REMAINING AFTER AMENDMENT | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$)                                         | ADDITIONAL FEE (\$) | RATE (\$)                        | ADDITIONAL FEE (\$) |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Total (37 CFR 1.16(i))                                                                                                                                                                                                        | *                                | Minus                              | **            | =                                                 | X \$                | =                                | OR                  | X \$                                  | = |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Independent (37 CFR 1.16(h))                                                                                                                                                                                                  | *                                | Minus                              | ***           | =                                                 | X \$                | =                                | OR                  | X \$                                  | = |
| <input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     | OR                               |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                               |                                  |                                    |               | TOTAL ADD'L FEE                                   |                     | OR                               | TOTAL ADD'L FEE     |                                       |   |
| <p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p> |                                                                                                                                                                                                                               |                                  |                                    |               |                                                   |                     |                                  |                     |                                       |   |

Legal Instrument Examiner:  
/ROZENIA HARMON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

|                                                                                                                |                                              |                                                                   |  |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------|--|
| <b>Application Number</b><br> | <b>Application/Control No.</b><br>11/551,606 | <b>Applicant(s)/Patent under Reexamination</b><br>SCHNEIER ET AL. |  |
| <b>Document Code - DISQ</b>                                                                                    |                                              | <b>Internal Document – DO NOT MAIL</b>                            |  |

|                                |                                                       |                                                 |
|--------------------------------|-------------------------------------------------------|-------------------------------------------------|
| <b>TERMINAL<br/>DISCLAIMER</b> | <input type="checkbox"/> APPROVED                     | <input checked="" type="checkbox"/> DISAPPROVED |
| Date Filed : 12/18/09          | This patent is subject<br>to a Terminal<br>Disclaimer |                                                 |

|                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved/Disapproved by:</b>                                                                                                  |
| ANDRE ROBINSON<br><br>OWNER INCORRECTLY IDENTIFIED. ACCORDING TO ASSIGNMENT, OWNER IS BT<br>COUNTERPANE INTERNET SECUIRITY, INC. |



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        |                        |

20350  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

**CONFIRMATION NO. 1662**  
**POA ACCEPTANCE LETTER**



Date Mailed: 01/29/2010

## NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/18/2009.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/rharmon/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        |                        |

COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

**CONFIRMATION NO. 1662**  
**POWER OF ATTORNEY NOTICE**



\*OC000000039912106\*

Date Mailed: 01/29/2010

**NOTICE REGARDING CHANGE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 12/18/2009.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/rharmon/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

## \*BIBDATASHEET\*

CONFIRMATION NO. 1662

Bib Data Sheet

|                                                                                                                                                                                                                                                               |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <b>SERIAL NUMBER</b><br>11/551,606                                                                                                                                                                                                                            | <b>FILING OR 371(c)<br/>DATE</b><br>10/20/2006<br><b>RULE</b>                                                     | <b>CLASS</b><br>726               | <b>GROUP ART UNIT</b><br>2439                                                                                                                                                                                                                                                      | <b>ATTORNEY<br/>DOCKET NO.</b> |
| <b>APPLICANTS</b><br>Bruce Schneier, Minneapolis, MN;<br>Andrew H. Gross, San Jose, CA;<br>Jonathan D. Callas, Mountain View, CA;                                                                                                                             |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| <b>** CONTINUING DATA *****</b><br>This application is a CON of 09/766,343 01/19/2001 PAT 7,159,237<br>which claims benefit of 60/190,326 03/16/2000                                                                                                          |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| <b>** FOREIGN APPLICATIONS *****</b>                                                                                                                                                                                                                          |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| <b>IF REQUIRED, FOREIGN FILING LICENSE GRANTED</b><br>** 11/20/2006                                                                                                                                                                                           |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no<br>35 USC 119 (a-d) conditions <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after<br>met Allowance<br>Verified and<br>Acknowledged |                                                                                                                   | <b>STATE OR<br/>COUNTRY</b><br>MN | <b>SHEETS<br/>DRAWING</b><br>9                                                                                                                                                                                                                                                     | <b>TOTAL<br/>CLAIMS</b><br>26  |
| <b>INDEPENDENT<br/>CLAIMS</b><br>2                                                                                                                                                                                                                            |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| <b>ADDRESS</b><br>20350                                                                                                                                                                                                                                       |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| <b>TITLE</b><br>Method and System for Dynamic Network Intrusion Monitoring, Detection and Response                                                                                                                                                            |                                                                                                                   |                                   |                                                                                                                                                                                                                                                                                    |                                |
| <b>FILING FEE<br/>RECEIVED</b><br>1430                                                                                                                                                                                                                        | FEES: Authority has been given in Paper<br>No. _____ to charge/credit DEPOSIT ACCOUNT<br>No. _____ for following: |                                   | <input type="checkbox"/> All Fees<br><input type="checkbox"/> 1.16 Fees ( Filing )<br><input type="checkbox"/> 1.17 Fees ( Processing Ext. of<br>time )<br><input type="checkbox"/> 1.18 Fees ( Issue )<br><input type="checkbox"/> Other _____<br><input type="checkbox"/> Credit |                                |

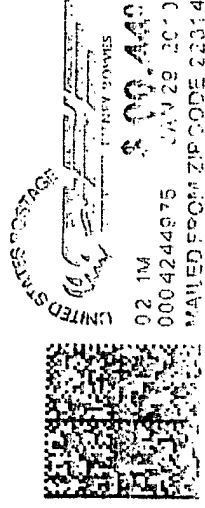
Jeti

1C2800

Organization Bldg./Room  
UNITED STATES PATENT AND TRADEMARK OFFICE  
P.O. Box 1450  
Alexandria, VA 22313-1450  
If Undeliverable Return In Ten Days

Official Business  
Penalty For Private Use, \$300

AN EQUAL OPPORTUNITY EMPLOYER



NIXIE 951 50 1 00 02/02/10  
RETURN TO SENDER  
NOT DELIVERABLE AS ADDRESSED  
UNABLE TO FORWARD  
BC: 2231314F036 \*0517-14427-29-09  
9512412541  
2231301450



*IPW*

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        |                        |

COUNTERPANE INTERNET SECURITY, INC.  
3031 TISCH WAY  
SAN JOSE, CA 95128

**CONFIRMATION NO. 1662**  
**POWER OF ATTORNEY NOTICE**



Date Mailed: 01/29/2010

**NOTICE REGARDING CHANGE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 12/18/2009.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/rharmon/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 11/551,606      | 10/20/2006  | Bruce Schneier       |                     | 1662             |

20350 7590 04/27/2010  
TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

|          |
|----------|
| EXAMINER |
|----------|

JACKSON, JENISE E

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2439

|           |               |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

04/27/2010

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

|                              |                                      |                                        |  |
|------------------------------|--------------------------------------|----------------------------------------|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>11/551,606 | <b>Applicant(s)</b><br>SCHNEIER ET AL. |  |
|                              | <b>Examiner</b><br>JENISE E. JACKSON | <b>Art Unit</b><br>2439                |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 1/29/10.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 45-70 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 62-68 and 70 is/are rejected.
- 7) ☒ Claim(s) 69 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |                                                                                     |                                                                   |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)         | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)         | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____                                                         | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION*****Double Patenting***

1. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

2. Claims 45-61 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-17 of U.S. Patent No. 7,159,237. Although the conflicting claims are not identical, they are not patentably distinct from each other because of the following rationale below:

3. Claim 45 of application 11/551606 discloses a system, and Claim 1 of Patent 7,159,237 discloses a method. It would have been obvious to include the system of application 11/551606 in Patent 7,159,237 that claims a method; the system performs certain steps/methods in order to perform security monitoring. Claim 45 of application 11/551606 discloses a sensor coupled to collect status data, and Claim 1 of Patent 7,159,237 discloses collecting status data. It would have been obvious to include a sensor of 11/551606 of application, in Patent 7159,237, in order

Art Unit: 2439

to have a device that can collect the status data of at least one monitored component of the network.

4. Claims 46-61 of application 11/551606 recite same limitations as claims 2-17 of Patent No. 7,159,237 respectively.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 62-68, 70 are rejected under 35 U.S.C. 102(b) as being anticipated by Johnson(5,970, 149)

7. As per claim 62, Johnson discloses a method of operating a secure operations center(i.e. secure dispatch control center)(see fig. 1 sheet 1) as part of a security monitoring system for a customer computer network(i.e. secure customer site, see fig. 1 sheet 1)(see col. 2, lines 46-61), comprising: creating an event record for information received about an identified potentially security-related event occurring on the network(see col. 2, lines 60-63, col. 3, lines 65-66, col. 4, lines 1-3); correlating the event record with customer information and a symptom record; using the correlated symptom record to link the event record to problem resolution assistant information(see col. 2, lines 32-36, col. 5, lines 25-45); consolidating the event record, correlated customer information and symptom record, and linked problem resolution information into a problem ticket; and providing the problem ticket to a security analyst console for analysis(see col. 4, lines 9-20, col. 4, lines 39-40).

Art Unit: 2439

8. As per claim 63, Johnson discloses correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and linking the event record to an open problem ticket associated with the pre-existing event record(see col. 5, lines 25-45).

9. As per claim 64, Johnson discloses wherein the problem resolution assistant information links the symptom to a diagnosis (col. 2, lines 32-36).

10. As per claim 65, Johnson discloses wherein the problem resolution assistant information links the symptom to a technology(see col. 4, lines 65-67, col. 4, lines 1-5).

11. As per claim 66, Johnson discloses correlating the event record with vulnerability; and using the correlated vulnerability to link the event record to problem resolution assistant information (see col. 2, lines 53-63).

12. As per claim 67, Johnson discloses wherein the problem resolution assistant information links the vulnerability to a diagnosis (see col. 2, lines 32-36).

13. As per claim 68, Johnson discloses wherein the problem resolution assistant information links the vulnerability to a technology(see col. 4, lines 65-67, col. 4, lines 1-5).

14. As per claim 70, Johnson discloses updating the problem resolution assistant information after the potentially security-related event is resolved(see col. 5, lines 39-55).

***Claim Objections***

15. Claim 69 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Response to Applicant***

16. A non-final action was mailed on 6/18/09 in which claims 45-68, and 70 were rejected. Claims 45-61 were only rejected based on double patenting. The Applicant responded on 12/18/09, in which the Applicant amended claims 62, 64-68, and 70. The terminal disclaimer was not approved because the Assignee is incorrect, the Assignee should be BT Counterpane Security. Correction is required in order to overcome double patenting rejection. Once the Terminal Disclaimer is corrected with the correct Assignee and approved, claims 45-61 will be allowed. In order to reduce prosecution, the Applicant is urged to include the limitations of claim 69 into independent claim 62.

17. The Applicant states that Johnson does not disclose problem resolution assistance information. The Examiner disagrees with the Applicant. Johnson discloses upon being alerted of a problem, a support person will be contacted to solve the problem(see col. 2, lines 33-36), thus a support person being able to solve problems on the customers network is problem resolution assistance. Johnson also discloses the field engineer has access to the mainframe and will endeavor to solve the problem presented(see col. 5, lines 36-38). Johnson also discloses problems being resolved(see col. 5, line 33). Thus, the field engineer has the knowledge and information in order to assist the customer in solving problems in regards to the customer's mainframe(see col. 5, lines 33-39).

Art Unit: 2439

18. The Applicant states that Johnson does not disclose consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance into a problem ticket. The Examiner disagrees with the Applicant. Johnson discloses the mainframe system alerts, events or problems, the console will issue a warning or alert to a dispatch control center where a field engineer will solve problem(see col. 4, lines 9-10). Johnson discloses the customer information is the internet protocol address for the customer site(see col. 7, lines 33-35), also the symptom record is the diagnose, Johnson discloses upon the alert being generated, a support person will be contacted to diagnose(i.e. symptom) and solve(i.e. problem resolution assistance) the particular problem(see col. 2, lines 29-36). Johnson discloses that a dispatcher will monitor any alarm codes received from the mainframe and the dispatcher will create a trouble ticket for each incoming alarm(see col. 2, lines 60-63).
19. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Art Unit: 2439

20. The Applicant states that Johnson does not disclose or suggest the linking of a symptom to a diagnosis. The Examiner disagrees with the Applicant. Johnson discloses an alert is issued to the console of a problem on the mainframe(see col. 4, lines 9-10). Johnson discloses that the dispatch control center upon being alerted of a problem will contact a support person to diagnose and solve the problem(see col. 2, lines 34-36). Johnson discloses that the problem is resolved by a field engineer (see col. 5, lines 39-40). Thus, in order for Johnson to resolve the problem, there has to be symptom in order to diagnose and solve the problem of Johnson.

21. The Applicant discloses that Johnson does not disclose an updating step. The Examiner disagrees with the Applicant. Johnson discloses that once the problem has been resolved (see col. 5, lines 39-40), the dispatcher closes the problem in the problem tracking system, and the dispatcher closes the problem in the dispatch central processing database(see col. 5, lines 49-52), thus the closing of the problem is updating of the problem, because the problem has been resolved thus the state of the problem has changed. In order to reduce prosecution the Applicant is urged to file a proper terminal disclaimer and add the limitation of claim 69 to claim 45.

### ***Final Action***

**22. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2439

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 11/551,606

Page 9

Art Unit: 2439

April 22, 2010

/J. E. J./

Examiner, Art Unit 2439

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439

|                                   |                                       |  |                                                               |             |
|-----------------------------------|---------------------------------------|--|---------------------------------------------------------------|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/551,606 |  | Applicant(s)/Patent Under<br>Reexamination<br>SCHNEIER ET AL. |             |
|                                   | Examiner<br>JENISE E. JACKSON         |  | Art Unit<br>2439                                              | Page 1 of 1 |

#### U.S. PATENT DOCUMENTS

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name               | Classification |
|---|---|--------------------------------------------------|-----------------|--------------------|----------------|
| * | A | US-2007/0288925                                  | 12-2007         | Hughes et al.      | 718/100        |
| * | B | US-2003/0135592                                  | 07-2003         | Vetter et al.      | 709/220        |
| * | C | US-6,829,734                                     | 12-2004         | Kreulen et al.     | 714/46         |
| * | D | US-6,804,665                                     | 10-2004         | Kreulen et al.     | 1/1            |
| * | E | US-6,625,750                                     | 09-2003         | Duso et al.        | 714/11         |
| * | F | US-6,311,274                                     | 10-2001         | Day, Michael David | 726/22         |
| * | G | US-6,260,048                                     | 07-2001         | Carpenter et al.   | 1/1            |
|   | H | US-                                              |                 |                    |                |
|   | I | US-                                              |                 |                    |                |
|   | J | US-                                              |                 |                    |                |
|   | K | US-                                              |                 |                    |                |
|   | L | US-                                              |                 |                    |                |
|   | M | US-                                              |                 |                    |                |

#### FOREIGN PATENT DOCUMENTS

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--------------------------------------------------|-----------------|---------|------|----------------|
|   | N |                                                  |                 |         |      |                |
|   | O |                                                  |                 |         |      |                |
|   | P |                                                  |                 |         |      |                |
|   | Q |                                                  |                 |         |      |                |
|   | R |                                                  |                 |         |      |                |
|   | S |                                                  |                 |         |      |                |
|   | T |                                                  |                 |         |      |                |

#### NON-PATENT DOCUMENTS

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|-------------------------------------------------------------------------------------------|
|   | U |                                                                                           |
|   | V |                                                                                           |
|   | W |                                                                                           |
|   | X |                                                                                           |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

|                                                                                                                        |                                                |                                                                       |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b><i>Index of Claims</i></b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                                        | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

|   |                 |   |                   |   |                     |   |                 |
|---|-----------------|---|-------------------|---|---------------------|---|-----------------|
| ✓ | <b>Rejected</b> | - | <b>Cancelled</b>  | N | <b>Non-Elected</b>  | A | <b>Appeal</b>   |
| = | <b>Allowed</b>  | ÷ | <b>Restricted</b> | I | <b>Interference</b> | O | <b>Objected</b> |

| <input type="checkbox"/> <b>Claims renumbered in the same order as presented by applicant</b> |          | <input type="checkbox"/> <b>CPA</b> |            | <input type="checkbox"/> <b>T.D.</b> |  | <input type="checkbox"/> <b>R.1.47</b> |  |  |  |
|-----------------------------------------------------------------------------------------------|----------|-------------------------------------|------------|--------------------------------------|--|----------------------------------------|--|--|--|
| CLAIM                                                                                         |          | DATE                                |            |                                      |  |                                        |  |  |  |
| Final                                                                                         | Original | 06/11/2009                          | 04/08/2010 | 04/22/2010                           |  |                                        |  |  |  |
|                                                                                               | 45       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 46       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 47       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 48       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 49       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 50       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 51       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 52       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 53       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 54       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 55       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 56       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 57       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 58       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 59       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 60       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 61       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 62       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 63       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 64       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 65       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 66       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 67       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 68       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |
|                                                                                               | 69       | O                                   | O          | O                                    |  |                                        |  |  |  |
|                                                                                               | 70       | ✓                                   | ✓          | ✓                                    |  |                                        |  |  |  |

|                                                                                                              |                                                |                                                                       |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b>Search Notes</b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                              | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

| SEARCHED |          |         |          |
|----------|----------|---------|----------|
| Class    | Subclass | Date    | Examiner |
| 726      | 3        | 4/22/10 | JJ       |
| 726      | 22-25    | 4/22/10 | JJ       |

| SEARCH NOTES                         |         |          |
|--------------------------------------|---------|----------|
| Search Notes                         | Date    | Examiner |
| Updated West text search             | 4/22/10 | JJ       |
| Updated West class and text search   | 4/22/10 | JJ       |
| Updated Inventor and assignee search | 4/22/10 | JJ       |

| INTERFERENCE SEARCH |          |      |          |
|---------------------|----------|------|----------|
| Class               | Subclass | Date | Examiner |
|                     |          |      |          |

|  |  |
|--|--|
|  |  |
|--|--|

# WEST Search History for Application 11551606

Creation Date: 2010042217:02

(NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) ) and (probe or sentry or scanner? or sensor? or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(sensor or filter\$5 or probe or sentry or black near box)near(collect\$5 or gather\$5)near(data or information or alert\$5 or event\$2) and ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(transmit\$8 or send\$8 or transfer\$8 or forward\$8)near(information or data or alert\$2 or event\$2 or footprint\$2)near(dispatch\$5 or engineer or analyst or admin\$8 or support near person or help near desk\$4)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009  
((sensor or filter\$5 or probe or sentry or black near box)near(collect\$5 or gather\$5)near(data or information or alert\$5 or event\$2) and (monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and ((transmit\$8 or send\$8 or transfer\$8 or forward\$8)near(information or data or alert\$2 or event\$2 or footprint\$2)near(dispatch\$5 or engineer or analyst or admin\$8 or support near person or help near desk\$4) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(filter\$5 or separate)near(data or information or alert\$5 or event\$5 or footprint\$2)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(post near filter\$5 near residue)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(keeping\$5 or sav\$5)near(residue or left near over)near(alert\$2 or data or information or event\$2 or footprint\$2)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(receiv\$5 or obtain\$5)near(feedback or results)near(probe or sensor? or sentry or black near box)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

((receiv\$5 or obtain\$5)near(feedback or results)near(probe or sensor? or sentry or black near box) ) and ((filter\$5 or separate)near(data or information or alert\$5 or event\$5 or footprint\$2) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(dynamically or real-time)near(modif\$8 or updat\$8 or chang\$8)near(probe or sentry or sensor? or black near box)near(feedback or result\$2)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/22.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/24.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/25.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/23.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/2.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/3.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/6.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/15.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/208.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/209.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/223.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/224.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/225.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/226.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/227.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/228.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/229.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

Bruce near Schneier.in. and (secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(Andrew near Gross.in.) and (secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(Jonathan near Callas).in. and (secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(Counterpane.as. and secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

((ticket) and (analyst or help near desk) and network ) and (intrusion)PGPB, USPT, EPAB,

JPAB, DWPI, TDBD OR YES 06-11-2009  
 ((ticket) and (analyst or help near desk) ) and networkPGPB, USPT, EPAB, JPAB, DWPI,  
 TDBD OR YES 06-11-2009  
 ((incident near log) ) and (analyst or help near desk)PGPB, USPT, EPAB, JPAB, DWPI,  
 TDBD OR YES 06-11-2009  
 (problem near ticket\$2) and (help near desk or analyst)PGPB, USPT, EPAB, JPAB, DWPI,  
 TDBD OR YES 06-11-2009  
 726/3.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

## Prior Art Searches

| Query                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | DB                                 | Op. | Plur. | Thes. | Date       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-----|-------|-------|------------|
| (monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 04-09-2010 |
| (creat? or compos? or conceiv? or construct? or generat? or mak? or produc? or form?)near(event or alert? or alarm? or incident or problem)with(record or directory or file or note or report? or list or log)                                                                                                                                                                                                                                                                                                                                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 04-09-2010 |
| (correlat? or correspond? or coordinat? or connect? or associat? or combin? or integrat? or organiz? or pool?)near(event or alert? or alarm? or incident or problem)with(record or directory or file or note or report? or list or log)near(customer near data or customer near information and symptom)                                                                                                                                                                                                                                      | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 04-09-2010 |
| (analyst or engineer or help near desk or admin or manager or boss or operator)near(creat? or generat?)near(ticket)                                                                                                                                                                                                                                                                                                                                                                                                                           | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 04-09-2010 |
| (resolution or assistance)with(data or information)near(symptom or diagnosis) and (analyst or engineer or help near desk or admin or manager or boss or operator)                                                                                                                                                                                                                                                                                                                                                                             | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR  | YES   |       | 04-09-2010 |

|                                                                                                                                                                                                          |                                                   |    |     |  |            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
| <b>((solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator)</b>                                        | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>((solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator) ) and (creat? or generat?)with(ticket)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>((solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator) ) and ticket</b>                           | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>726/22.ccls.</b>                                                                                                                                                                                      | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>726/24.ccls.</b>                                                                                                                                                                                      | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>726/25.ccls.</b>                                                                                                                                                                                      | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>726/23.ccls.</b>                                                                                                                                                                                      | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| <b>(Counterpane.as. and secure near operations near center)</b>                                                                                                                                          | PGPB,<br>USPT,<br>EPAB,<br>JPAB,                  | OR | YES |  | 04-09-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                   |    |     |  |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | DWPI,<br>TDBD                                     |    |     |  |            |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) ) and (analyst or engineer or help near desk or admin or manager or boss or operator)                                                                                   | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) ) and (resolution or assistance)with(data or information)near(symptom or diagnosis) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) ) and (resolution or assistance)with(data or information)                           | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) ) and (resolution or assistance)with(data or information)                           | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                    |    |     |  |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) and (resolution or assistance)with(data or information) ) and ticket                                                                                                                                                                                                                                                                         |                                    |    |     |  |            |
| (customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier)                                                                                                                                                                                                   | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| ((customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier) ) and (help near desk)                                                                                                                                                                           | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| ((customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier) and (help near desk) ) and (symptom)                                                                                                                                                             | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| ((customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier) and (help near desk) and (symptom) ) and (incident\$2 or problem\$2 or event\$2 or intrus\$5 or intrud\$5)                                                                                       | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| (consolidat? or combin? or build? near up or connect? or develop? or incorporat? or join? or mix? or unif?)near(event\$2 or record? or alert? or problem\$2 or intrus\$5 or intrud? or alarm\$5 or attack? or vulnerabilit\$6 or error or incident)near(customer near information or customer near name or name or id or identifier or work near number or address or phone near number or workstation near id or computer near id or building near number or office near location)near(symptom or indication or problem\$2) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| (correlat? or consolidat? or combin? or build? near up or connect? or develop? or incorporat? or join? or mix? or unif?)near(event\$2 or record? or alert? or problem\$2                                                                                                                                                                                                                                                                                                                                                     | PGPB, USPT, EPAB,                  | OR | YES |  | 04-22-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                   |    |     |  |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
| <p>or intrus\$5 or intrud? or alarm\$5 or attack? or<br/> vulnerabilit\$6 or error or incident)near(customer near<br/> information or customer near name or name or id or<br/> identifier or work near number or address or phone near<br/> number or workstation near id or computer near id or<br/> building near number or office near<br/> location)near(symptom or indication or<br/> problem\$2)near(ticket)</p> | JPAB,<br>DWPI,<br>TDBD                            |    |     |  |            |
| <p>(troubl?)with(ticket)near(help near desk or operator or<br/> analyst or admin or engineer)</p>                                                                                                                                                                                                                                                                                                                      | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-22-2010 |

AMENDMENT UNDER 37 CFR 1.116  
EXPEDITED PROCEDURE –  
EXAMINING GROUP 2439

---

PATENT

Attorney Docket No.: 022133-000520US

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier et al.

Application No.: 11/551,606

Filed: October 20, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Customer No.: 20350

Confirmation No. 1662

Examiner: Jenise E. Jackson

Technology Center/Art Unit: 2439

AMENDMENT UNDER 37 CFR 1.116  
EXPEDITED PROCEDURE EXAMINING  
GROUP 2439

---

Mail Stop AF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

In response to the Final Office Action mailed April 27, 2010 in the above-referenced application, please enter the following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 6 of this paper.

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1.-44. (Canceled).

45. (Previously presented) A system for operating a probe as part of a security monitoring system for a computer network, the system comprising:

- a) a sensor coupled to collect status data from at least one monitored component of the network;
- b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
- c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
- d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and
- e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

46. (Previously presented ) The system of claim 45, wherein the identifying step includes performing a multi-stage analysis of the status data.

47. (Previously presented) The system of claim 46, wherein the multi-stage analysis includes performing a discrimination analysis on the status data.

48. (Previously presented) The system of claim 47, wherein the discrimination analysis includes positive filtering.

49. (Previously presented) The system of claim 47, wherein the discrimination analysis includes negative filtering.

50. (Previously presented) The system of claim 46, wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe.

51. (Previously presented) The system of claim 45, wherein the identifying step includes aggregating and synthesizing the status data at the probe.

52. (Previously presented) The system of claim 51, wherein the identifying step includes cross-correlating data across the monitored components.

53. (Previously presented) The system of claim 51, wherein the identifying step includes analyzing the frequency of occurrence of the events.

54. (Previously presented) The system of claim 45, further comprising after the step (c), a secure operations center coupled to perform further computer-based analysis and to receive data from the probe.

55. (Previously presented) The system of claim 54, wherein the computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

56. (Previously presented) The system of claim 54, wherein the identifying step includes cross-correlating data across the monitored components.

57. (Previously presented) The system of claim 54, wherein the identifying step includes analyzing the frequency of occurrence of the events.

58. (Previously presented) The system of claim 54, wherein the computer-based analysis includes cross-probe correlation.

59. (Previously presented ) The system of claim 45, further comprising instantaneously self-tuning the probe based on previously collected status data.

60. (Previously presented) The system of claim 45, wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

61. (Previously presented) The system of claim 45, wherein the receiving feedback step occurs in substantially real time.

62. (Currently amended) A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:

creating an event record for information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering;

correlating the event record with customer information and a symptom record;

using the correlated symptom record to link the event record to problem resolution information;

consolidating the event record, correlated customer information and symptom record, and

linked problem resolution assistance information into a problem ticket; and

providing the problem ticket to a security analyst console for analysis.

63. (Previously presented ) The method of claim 62, further comprising:

correlating the event record with a pre-existing event record stored on an event database within the secure operations center; and

linking the event record to an open problem ticket associated with the pre-existing event record.

64. (Previously presented) The method of claim 62, wherein the problem resolution assistance information links the symptom to a diagnosis.

65. (Previously presented) The method of claim 62, wherein the problem resolution assistance information links the symptom to a technology.

66. (Previously presented) The method of claim 62, further comprising:  
correlating the event record with a vulnerability; and  
using the correlated vulnerability to link the event record to problem resolution assistance information.

67. (Previously presented ) The method of claim 66, wherein the problem resolution assistance information links the vulnerability to a diagnosis.

68. (Previously presented) The method of claim 66, wherein the problem resolution assistance information links the vulnerability to a technology.

69. (Canceled)

70. (Previously presented) The method of claim 62, further comprising:  
updating the problem resolution assistance information after the potentially security-related event is resolved.

### **REMARKS/ARGUMENTS**

Claims 45-70 were pending in this application. In this amendment, applicants have canceled allowable claim 69 and amended claim 62 to incorporate subject matter from canceled claim 69. The amendment is fully supported by the specification as originally filed and therefore no new matter had been added. Following this amendment, claims 45-68 and 70 will remain pending.

In the Office Action, the Examiner rejected claims 45-61 asserting nonstatutory obviousness-type double patenting over claims 1-17 of U.S. Patent No. 7,159,237 to Schneier et al. (hereinafter "Schneier"). The Examiner also rejected claims 62-68, 70 under 35 USC §102(b) asserting anticipation by U.S. Patent No. 5,970, 149 to Johnson (hereinafter "Johnson"). Claim 69 was objected to as being dependent on a rejected base claim, but the Examiner indicated that it would be allowable if rewritten in independent form to include all the limitations of the base claim and any intervening claims. Applicants note with appreciation the indication of allowable subject matter in claim 69.

Without taking a position on whether the nonstatutory obviousness-type double patenting rejection is appropriate, Applicants submit herewith a Terminal Disclaimer in accordance with 37 CFR §1.321(c) to obviate the nonstatutory obviousness-type double patenting rejection. Applicants respectfully request, therefore, that the rejection of claims 45-61 be withdrawn.

#### **The 35 USC §102(b) Rejection**

Claims 62-68 and 70 were rejected under 35 USC §102(b) using Johnson. Although Applicants traverse this rejection, in order to advance prosecution, applicants have amended independent claim 62 to include the allowable subject matter from previously pending claim 69. Applicants submit that claim 62 is therefore allowable over the prior art of record. Dependent claims 63-68 and 70, which include all the features of independent claim 62, are allowable for at least the same reason. Applicants respectfully request, therefore, that the §102(b) rejection be withdrawn.

Appl. No. 11/551,606  
Amdt. dated August 27, 2010  
Amendment under 37 CFR 1.116 Expedited Procedure  
Examining Group 2439

PATENT

**CONCLUSION**

In view of the foregoing, Applicants submit that claims 45-68 and 70 are in condition for allowance and an action to that end is respectfully requested. Further, the Commissioner is hereby authorized to charge any additional fees or credit any overpayment in connection with this paper to Deposit Account No. 20-1430.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

/Brian E. Mack/

Date: August 27, 2010

Brian E. Mack  
Reg. No. 57,189

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, Eighth Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400 Fax: 415-576-0300  
BEM/bem/ka  
62668863 v1

|                                                                                                                                                                   |  |                                             |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------------------------------|--|
| <b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b><br><b>FY 2009</b><br><i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i> |  | Docket Number (Optional)<br>022133-000520US |  |
| Application Number 11/551,606                                                                                                                                     |  | Filed October 20, 2006                      |  |
| For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE                                                                            |  |                                             |  |
| Art Unit 2439                                                                                                                                                     |  | Examiner Jenise E. Jackson                  |  |

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

|                                                                   | <u>Fee</u> | <u>Small Entity Fee</u> |        |
|-------------------------------------------------------------------|------------|-------------------------|--------|
| <input checked="" type="checkbox"/> One month (37 CFR 1.17(a)(1)) | \$130      | \$65                    | \$ 130 |
| <input type="checkbox"/> Two months (37 CFR 1.17(a)(2))           | \$490      | \$245                   | \$     |
| <input type="checkbox"/> Three months (37 CFR 1.17(a)(3))         | \$1110     | \$555                   | \$     |
| <input type="checkbox"/> Four months (37 CFR 1.17(a)(4))          | \$1730     | \$865                   | \$     |
| <input type="checkbox"/> Five months (37 CFR 1.17(a)(5))          | \$2350     | \$1175                  | \$     |

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 20-1430.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

I am the ☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration Number 57,189

☐ attorney or agent under 37 CFR 1.34.  
Registration number if acting under 37 CFR 1.34 \_\_\_\_\_

\_\_\_\_\_  
/Brian E. Mack/  
Signature

\_\_\_\_\_  
Brian E. Mack, Reg. No. 57,189  
Typed or printed name

\_\_\_\_\_  
August 27, 2010  
Date

\_\_\_\_\_  
650-326-2400  
Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☒ Total of 1 forms are submitted.

**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING  
REJECTION OVER A "PRIOR" PATENT**

Docket Number (Optional)  
022133-000520US

In re Application of: Bruce Schneier et al.

Application No.: 11/551,606

Filed: October 20, 2006

For: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE

The owner\*, BT Counterpane Internet Security, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application, which would extend beyond the expiration date of the full statutory term **prior patent** No. 7,159,237 as the term of said prior patent is defined in 35 U.S.C. 154 and 173, and as the term of said **prior patent** is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the **prior patent** are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 and 173 of the **prior patent**, "as the term of said **prior patent** is presently shortened by any terminal disclaimer," in the event that said **prior patent** later:

expires for failure to pay a maintenance fee;  
 is held unenforceable;  
 is found invalid by a court of competent jurisdiction;  
 is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;  
 has all claims canceled by a reexamination certificate;  
 is reissued; or  
 is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2 below, if appropriate.

1. ☐ For submissions on behalf of a business/organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the business/organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☒ The undersigned is an attorney or agent of record. Reg. No. 57,189

\_\_\_\_\_  
/Brian E. Mack/  
Signature

\_\_\_\_\_  
August 27, 2010  
Date

\_\_\_\_\_  
Brian E. Mack  
Typed or printed name

\_\_\_\_\_  
(650) 326-2400  
Telephone Number

- ☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

\*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).  
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

## Electronic Patent Application Fee Transmittal

|                                                |                                                                                    |                 |               |                             |
|------------------------------------------------|------------------------------------------------------------------------------------|-----------------|---------------|-----------------------------|
| <b>Application Number:</b>                     | 11551606                                                                           |                 |               |                             |
| <b>Filing Date:</b>                            | 20-Oct-2006                                                                        |                 |               |                             |
| <b>Title of Invention:</b>                     | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |                 |               |                             |
| <b>First Named Inventor/Applicant Name:</b>    | Bruce Schneier                                                                     |                 |               |                             |
| <b>Filer:</b>                                  | Brian Edward Mack/Kristina Alvarez                                                 |                 |               |                             |
| <b>Attorney Docket Number:</b>                 |                                                                                    |                 |               |                             |
| Filed as Large Entity                          |                                                                                    |                 |               |                             |
| <b>Utility under 35 USC 111(a) Filing Fees</b> |                                                                                    |                 |               |                             |
| <b>Description</b>                             | <b>Fee Code</b>                                                                    | <b>Quantity</b> | <b>Amount</b> | <b>Sub-Total in USD(\$)</b> |
| <b>Basic Filing:</b>                           |                                                                                    |                 |               |                             |
| <b>Pages:</b>                                  |                                                                                    |                 |               |                             |
| <b>Claims:</b>                                 |                                                                                    |                 |               |                             |
| <b>Miscellaneous-Filing:</b>                   |                                                                                    |                 |               |                             |
| <b>Petition:</b>                               |                                                                                    |                 |               |                             |
| <b>Patent-Appeals-and-Interference:</b>        |                                                                                    |                 |               |                             |
| <b>Post-Allowance-and-Post-Issuance:</b>       |                                                                                    |                 |               |                             |
| <b>Extension-of-Time:</b>                      |                                                                                    |                 |               |                             |
| Extension - 1 month with \$0 paid              | 1251                                                                               | 1               | 130           | 130                         |

| Description          | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|----------------------|----------|----------|--------|----------------------|
| Miscellaneous:       |          |          |        |                      |
| Statutory disclaimer | 1814     | 1        | 140    | 140                  |
| Total in USD (\$)    |          |          |        | 270                  |

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 8311852                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | Method and System for Dynamic Network Intrusion Monitoring, Detection and Response |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Brian Edward Mack                                                                  |
| <b>Filer Authorized By:</b>                 |                                                                                    |
| <b>Attorney Docket Number:</b>              |                                                                                    |
| <b>Receipt Date:</b>                        | 27-AUG-2010                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 18:10:37                                                                           |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)                                                        |

### Payment information:

|                                          |                 |
|------------------------------------------|-----------------|
| Submitted with Payment                   | yes             |
| Payment Type                             | Deposit Account |
| Payment was successfully received in RAM | \$ 270          |
| RAM confirmation Number                  | 4215            |
| Deposit Account                          | 201430          |
| Authorized User                          |                 |

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

## File Listing:

| Document Number              | Document Description                                | File Name       | File Size(Bytes)/<br>Message Digest      | Multi Part /.zip | Pages (if appl.) |
|------------------------------|-----------------------------------------------------|-----------------|------------------------------------------|------------------|------------------|
| 1                            |                                                     | AmendmentAF.pdf | 88875                                    | yes              | 7                |
|                              |                                                     |                 | c50d2aa8b3caefd34745dad358ba2f4301fb9f4  |                  |                  |
|                              | Multipart Description/PDF files in .zip description |                 |                                          |                  |                  |
|                              | Document Description                                | Start           | End                                      |                  |                  |
|                              | Amendment After Final                               | 1               | 1                                        |                  |                  |
|                              | Claims                                              | 2               | 5                                        |                  |                  |
|                              | Applicant Arguments/Remarks Made in an Amendment    | 6               | 7                                        |                  |                  |
| Warnings:                    |                                                     |                 |                                          |                  |                  |
| Information:                 |                                                     |                 |                                          |                  |                  |
| 2                            | Extension of Time                                   | ExtTme.pdf      | 72288                                    | no               | 1                |
|                              |                                                     |                 | e910e8347c474389941ad191ffff018d9dcf8af5 |                  |                  |
| Warnings:                    |                                                     |                 |                                          |                  |                  |
| Information:                 |                                                     |                 |                                          |                  |                  |
| 3                            | Terminal Disclaimer Filed                           | TermDis.pdf     | 61022                                    | no               | 1                |
|                              |                                                     |                 | 68fe089d8b2b2eb6e4e7805de2289525dc5d0abc |                  |                  |
| Warnings:                    |                                                     |                 |                                          |                  |                  |
| Information:                 |                                                     |                 |                                          |                  |                  |
| 4                            | Fee Worksheet (PTO-875)                             | fee-info.pdf    | 31850                                    | no               | 2                |
|                              |                                                     |                 | b53f9c835ff3377265ef22ddceb5a32e915255b5 |                  |                  |
| Warnings:                    |                                                     |                 |                                          |                  |                  |
| Information:                 |                                                     |                 |                                          |                  |                  |
| Total Files Size (in bytes): |                                                     |                 | 254035                                   |                  |                  |

**This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.**

**New Applications Under 35 U.S.C. 111**

**If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.**

**National Stage of an International Application under 35 U.S.C. 371**

**If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.**

**New International Application Filed with the USPTO as a Receiving Office**

**If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

| <b>PATENT APPLICATION FEE DETERMINATION RECORD</b><br>Substitute for Form PTO-875                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                               |                                    |                                    |               | Application or Docket Number<br><b>11/551,606</b> |                     | Filing Date<br><b>10/20/2006</b> |                     | <input type="checkbox"/> To be Mailed |   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|------------------------------------|---------------|---------------------------------------------------|---------------------|----------------------------------|---------------------|---------------------------------------|---|
| <b>APPLICATION AS FILED – PART I</b>                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                               |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                    | (Column 2)                         |               | SMALL ENTITY <input type="checkbox"/>             |                     | OR                               |                     | OTHER THAN SMALL ENTITY               |   |
| FOR                                                                                                                                                                                                                                                                                                                                                                                                                                  | NUMBER FILED                                                                                                                                                                                                                  | NUMBER EXTRA                       | RATE (\$)                          | FEE (\$)      | RATE (\$)                                         | FEE (\$)            |                                  |                     |                                       |   |
| <input type="checkbox"/> BASIC FEE<br>(37 CFR 1.16(a), (b), or (c))                                                                                                                                                                                                                                                                                                                                                                  | N/A                                                                                                                                                                                                                           | N/A                                | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> SEARCH FEE<br>(37 CFR 1.16(k), (l), or (m))                                                                                                                                                                                                                                                                                                                                                                 | N/A                                                                                                                                                                                                                           | N/A                                | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> EXAMINATION FEE<br>(37 CFR 1.16(o), (p), or (q))                                                                                                                                                                                                                                                                                                                                                            | N/A                                                                                                                                                                                                                           | N/A                                | N/A                                |               | N/A                                               |                     |                                  |                     |                                       |   |
| TOTAL CLAIMS<br>(37 CFR 1.16(i))                                                                                                                                                                                                                                                                                                                                                                                                     | minus 20 =                                                                                                                                                                                                                    | *                                  | X \$                               | =             | OR                                                | X \$                | =                                |                     |                                       |   |
| INDEPENDENT CLAIMS<br>(37 CFR 1.16(h))                                                                                                                                                                                                                                                                                                                                                                                               | minus 3 =                                                                                                                                                                                                                     | *                                  | X \$                               | =             |                                                   | X \$                | =                                |                     |                                       |   |
| <input type="checkbox"/> APPLICATION SIZE FEE<br>(37 CFR 1.16(s))                                                                                                                                                                                                                                                                                                                                                                    | If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s). |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| <input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| * If the difference in column 1 is less than zero, enter "0" in column 2.                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                               |                                    | TOTAL                              |               |                                                   | TOTAL               |                                  |                     |                                       |   |
| <b>APPLICATION AS AMENDED – PART II</b>                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                               |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
| (Column 1)                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                               |                                    | (Column 2)                         |               | (Column 3)                                        |                     | SMALL ENTITY                     |                     | OR OTHER THAN SMALL ENTITY            |   |
| <b>AMENDMENT</b>                                                                                                                                                                                                                                                                                                                                                                                                                     | <b>08/27/2010</b>                                                                                                                                                                                                             | CLAIMS REMAINING AFTER AMENDMENT   | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA | RATE (\$)                                         | ADDITIONAL FEE (\$) | RATE (\$)                        | ADDITIONAL FEE (\$) |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Total (37 CFR 1.16(i))                                                                                                                                                                                                        | * 25                               | Minus                              | ** 26         | = 0                                               | X \$ =              | OR                               | X \$52=             | 0                                     |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Independent (37 CFR 1.16(h))                                                                                                                                                                                                  | * 2                                | Minus                              | *** 3         | = 0                                               | X \$ =              | OR                               | X \$220=            | 0                                     |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | <input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))                                                                                                                                                                |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))                                                                                                                                      |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                               |                                    |                                    |               |                                                   | TOTAL ADD'L FEE     |                                  | OR                  | TOTAL ADD'L FEE                       | 0 |
| <b>AMENDMENT</b>                                                                                                                                                                                                                                                                                                                                                                                                                     | CLAIMS REMAINING AFTER AMENDMENT                                                                                                                                                                                              | HIGHEST NUMBER PREVIOUSLY PAID FOR | PRESENT EXTRA                      | RATE (\$)     | ADDITIONAL FEE (\$)                               | RATE (\$)           | ADDITIONAL FEE (\$)              |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Total (37 CFR 1.16(i))                                                                                                                                                                                                        | *                                  | Minus                              | **            | =                                                 | X \$ =              | OR                               | X \$ =              |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | Independent (37 CFR 1.16(h))                                                                                                                                                                                                  | *                                  | Minus                              | ***           | =                                                 | X \$ =              | OR                               | X \$ =              |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | <input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))                                                                                                                                                                |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      | <input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))                                                                                                                                      |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |
|                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                               |                                    |                                    |               |                                                   | TOTAL ADD'L FEE     |                                  | OR                  | TOTAL ADD'L FEE                       |   |
| <p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p> |                                                                                                                                                                                                                               |                                    |                                    |               |                                                   |                     |                                  |                     |                                       |   |

Legal Instrument Examiner:  
/SHERRY A. DAVIS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

|                                                                                                                |                                              |                                                                   |  |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------|--|
| <b>Application Number</b><br> | <b>Application/Control No.</b><br>11/551,606 | <b>Applicant(s)/Patent under Reexamination</b><br>SCHNEIER ET AL. |  |
| <b>Document Code - DISQ</b>                                                                                    |                                              | <b>Internal Document – DO NOT MAIL</b>                            |  |

|                                |                                                       |                                                 |
|--------------------------------|-------------------------------------------------------|-------------------------------------------------|
| <b>TERMINAL<br/>DISCLAIMER</b> | <input type="checkbox"/> APPROVED                     | <input checked="" type="checkbox"/> DISAPPROVED |
| Date Filed : 8/27/10           | This patent is subject<br>to a Terminal<br>Disclaimer |                                                 |

|                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved/Disapproved by:</b>                                                                                                                                                                                                                                                                                                                                                                             |
| ANDRE ROBINSON<br><br><input checked="" type="checkbox"/> The person who signed the terminal disclaimer:<br><input type="checkbox"/> has failed to state his/her capacity to sign for the business entity. (See FP 14.28)<br><input type="checkbox"/> is not recognized as an officer of the assignee. (See FP 14.29)<br><input checked="" type="checkbox"/> does not have power of attorney. (FP 14.29.01) |

|                                                                                                                |                                              |                                                                   |  |
|----------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------|--|
| <b>Application Number</b><br> | <b>Application/Control No.</b><br>11/551,606 | <b>Applicant(s)/Patent under Reexamination</b><br>SCHNEIER ET AL. |  |
| <b>Document Code - DISQ</b>                                                                                    |                                              | <b>Internal Document – DO NOT MAIL</b>                            |  |

|                                |                                                       |                                             |
|--------------------------------|-------------------------------------------------------|---------------------------------------------|
| <b>TERMINAL<br/>DISCLAIMER</b> | <input checked="" type="checkbox"/> <b>APPROVED</b>   | <input type="checkbox"/> <b>DISAPPROVED</b> |
| Date Filed : 8/27/10           | This patent is subject<br>to a Terminal<br>Disclaimer |                                             |

|                                 |
|---------------------------------|
| <b>Approved/Disapproved by:</b> |
| ANDRE ROBINSON                  |



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

## NOTICE OF ALLOWANCE AND FEE(S) DUE

20350 7590 10/28/2010

TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

EXAMINER

JACKSON, JENISE E

ART UNIT

PAPER NUMBER

2439

DATE MAILED: 10/28/2010

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

11/551,606

10/20/2006

Bruce Schneier

022133-000520US

1662

TITLE OF INVENTION: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE

| APPLN. TYPE    | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE   |
|----------------|--------------|---------------|---------------------|----------------------|------------------|------------|
| nonprovisional | NO           | \$1510        | \$300               | \$0                  | \$1810           | 01/28/2011 |

**THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.**

**THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.**

### HOW TO REPLY TO THIS NOTICE:

#### I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

**IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.**

# **PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

20350 7590 10/28/2010

**TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834**

## **Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

|                    |
|--------------------|
| (Depositor's name) |
| (Signature)        |
| (Date)             |

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

11/551,606 10/20/2006 Bruce Schneier 022133-000520US 1662

**TITLE OF INVENTION: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE**

| APPLN. TYPE | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE |
|-------------|--------------|---------------|---------------------|----------------------|------------------|----------|
|-------------|--------------|---------------|---------------------|----------------------|------------------|----------|

nonprovisional NO \$1510 \$300 \$0 \$1810 01/28/2011

| EXAMINER | ART UNIT | CLASS-SUBCLASS |
|----------|----------|----------------|
|----------|----------|----------------|

JACKSON, JENISE E 2439 726-003000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 \_\_\_\_\_
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 \_\_\_\_\_
- 3 \_\_\_\_\_

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s); (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.                                                                                               | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---------------------------------------------------------------------------------------------------------------|-------------|----------------------|---------------------|------------------|
| 11/551,606                                                                                                    | 10/20/2006  | Bruce Schneier       | 022133-000520US     | 1662             |
| 20350                                                                                                         | 7590        | 10/28/2010           | EXAMINER            |                  |
| TOWNSEND AND TOWNSEND AND CREW, LLP<br>TWO EMBARCADERO CENTER<br>EIGHTH FLOOR<br>SAN FRANCISCO, CA 94111-3834 |             |                      | JACKSON, JENISE E   |                  |
|                                                                                                               |             |                      | ART UNIT            | PAPER NUMBER     |
|                                                                                                               |             |                      | 2439                |                  |
| DATE MAILED: 10/28/2010                                                                                       |             |                      |                     |                  |

## Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 392 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 392 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

|                               |                        |                     |  |
|-------------------------------|------------------------|---------------------|--|
| <b>Notice of Allowability</b> | <b>Application No.</b> | <b>Applicant(s)</b> |  |
|                               | 11/551,606             | SCHNEIER ET AL.     |  |
|                               | <b>Examiner</b>        | <b>Art Unit</b>     |  |
|                               | JENISE E. JACKSON      | 2439                |  |

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 8/27/10.
2. ☒ The allowed claim(s) is/are 45-68 and 70.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some\*    c) ☐ None    of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
- \* Certified copies not received: \_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)</p> <p>3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br/>Paper No./Mail Date ____</p> <p>4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material</p> | <p>5. <input type="checkbox"/> Notice of Informal Patent Application</p> <p>6. <input type="checkbox"/> Interview Summary (PTO-413),<br/>Paper No./Mail Date ____.</p> <p>7. <input type="checkbox"/> Examiner's Amendment/Comment</p> <p>8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance</p> <p>9. <input type="checkbox"/> Other ____.</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

/Michael J Simitoski/  
Primary Examiner, Art Unit 2439

***Reasons for Allowance***

1. The following is an examiner's statement of reasons for allowance: listed below:

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

2. ***Status of Claims:*** Application 11/551606 is a continuation of 09/766343 which is now Patent 7159237. Application 11/551606 is allowed for the same reasons as Application 09/766343. A Terminal Disclaimer was filed on 8/27/10.

3. Claims 45-68, and 70 are allowed.

4. The prior art of Non-patent literature, by Essex. Essex teaches a company that outsources intrusion detection, RipTech. RipTech puts its own experts at one end of a secure Internet link, ready to ply their skills and experience to analyze suspicious data generated by security services. The data goes through four main eSentry modules, each of which represents a major step in the security management process. Real-time monitoring and management collects the information, while an event-processing engine looks for signs of hackers and viruses. An event-tracking module wades through the data to flag potential trouble spots, and a secure portal lets RipTech analysts post alerts or take emergency action. Thus, Essex teaches that all data is filtered, and those with signs of suspicion or maliciousness are looked into further. Essex does not teach or suggest, wherein the post-filtering residue is data neither discarded nor selected by filtering.

5. Porras et al. discloses a network that monitors for intrusion detections. The networks of Porras that are being monitored by using sensors that monitors various host and network activity,

Art Unit: 2439

and each sensor generate a stream of alerts. These alerts are triggered by potentially suspicious events or possible malicious intrusions. The alert manager includes a receive-input logic module. The receive-input logic of the alert manager subscribes, i.e., establishes a transport connection, to receive each of the alert streams produced by the sensors. The alert streams contain raw, i.e., unprocessed alerts. The monitors may format their respective alerts streams in a variety of formats; For Example, XML-based standard format. Once the alerts are in a common format, they are sent to the alert processing engine. The formatted alerts are passed thorough user-specified filters and alerts not matching criteria of the user-specified filters are discarded. The filtered alerts are then prioritized and rated or scored based upon potential impact of the attack. Porras fails to disclose or suggest the claim limitation, wherein the post-filtering residue is data neither discarded nor selected by filtering. Porras discloses that if the filter does not match the criteria the data is discarded.

6. Hill et al. discloses a network security system includes a plurality of security agents. The security agents are configured to detect occurrences of security events. Data about security events is collected by security agents and transmitted via links. Hill et al. security system responds to a plurality of training signatures, each of the training signatures representing one of a plurality of simulated attacks. Each of the simulated attacks of Hill is given a score/attack severity as to how certain attacks would affect the network or harm the network more than others. These scores or mapped and plotted on a two dimensional array. Hill does not disclose or suggest the claim limitation, wherein the post-filtering residue is data neither discarded nor selected by filtering. Hill does not disclose any type of filtering of data or attacks. Hill et al.

Art Unit: 2439

system is merely a system that simulates attacks to determine how these attacks will affect or have the potential to affect the network.

7. Shipley discloses an intelligent network security device residing within a computer network. The device will examine data packets to recognize suspicious patterns of behavior. The device will be connected to control a firewall such that unauthorized or disruptive outside users will be blocked from accessing the network. Shipley discloses that data in the Ethernet packet is compared to attack signatures. Shipley fails to disclose or suggest, wherein the post-filtering residue is data neither discarded nor selected by filtering. Shipley discloses that certain patterns are given a certain weight. Shipley is silent on any post-filtering residue.

8. A negative filtering system, which discards uninteresting information, and then a positive filtering system, which selects interesting information and forwards it to an admin. Lastly, prior art does not disclose or suggest data neither discarded by negative or positive is the residue that is sent for further analysis. In Networking and Security, all data is filtered by intrusion detection, firewall, gateway, proxy, sensor, probe, or sentry, or some other type of device. The device monitors the network for possible attacks, if an attack occurs the data is transmitted for further analysis or it is attacked upon. All other data is usually blocked or discarded if not a possible attack or one that is occurring on the network. Therefore, for the reason listed above, claims 45-68, and 70 are allowable.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JENISE E. JACKSON whose telephone number is (571)272-

Art Unit: 2439

3791. The examiner can normally be reached on Increased Flex time, but generally in the office M-Fri(8-4:30)..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

September 7, 2010

/J. E. J./

Examiner, Art Unit 2439

/Michael J Simitoski/

Primary Examiner, Art Unit 2439

|                                   |                                       |  |                                                               |             |
|-----------------------------------|---------------------------------------|--|---------------------------------------------------------------|-------------|
| <b>Notice of References Cited</b> | Application/Control No.<br>11/551,606 |  | Applicant(s)/Patent Under<br>Reexamination<br>SCHNEIER ET AL. |             |
|                                   | Examiner<br>JENISE E. JACKSON         |  | Art Unit<br>2439                                              | Page 1 of 1 |

#### U.S. PATENT DOCUMENTS

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Name               | Classification |
|---|---|--------------------------------------------------|-----------------|--------------------|----------------|
| * | A | US-2007/0288925                                  | 12-2007         | Hughes et al.      | 718/100        |
| * | B | US-2003/0135592                                  | 07-2003         | Vetter et al.      | 709/220        |
| * | C | US-6,829,734                                     | 12-2004         | Kreulen et al.     | 714/46         |
| * | D | US-6,804,665                                     | 10-2004         | Kreulen et al.     | 1/1            |
| * | E | US-6,625,750                                     | 09-2003         | Duso et al.        | 714/11         |
| * | F | US-6,311,274                                     | 10-2001         | Day, Michael David | 726/22         |
| * | G | US-6,260,048                                     | 07-2001         | Carpenter et al.   | 1/1            |
|   | H | US-                                              |                 |                    |                |
|   | I | US-                                              |                 |                    |                |
|   | J | US-                                              |                 |                    |                |
|   | K | US-                                              |                 |                    |                |
|   | L | US-                                              |                 |                    |                |
|   | M | US-                                              |                 |                    |                |

#### FOREIGN PATENT DOCUMENTS

| * |   | Document Number<br>Country Code-Number-Kind Code | Date<br>MM-YYYY | Country | Name | Classification |
|---|---|--------------------------------------------------|-----------------|---------|------|----------------|
|   | N |                                                  |                 |         |      |                |
|   | O |                                                  |                 |         |      |                |
|   | P |                                                  |                 |         |      |                |
|   | Q |                                                  |                 |         |      |                |
|   | R |                                                  |                 |         |      |                |
|   | S |                                                  |                 |         |      |                |
|   | T |                                                  |                 |         |      |                |

#### NON-PATENT DOCUMENTS

| * |   | Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages) |
|---|---|-------------------------------------------------------------------------------------------|
|   | U | Essex, E-Sleuths Make Net Safe for E-Commerce, June 12, 2000, Computerworld, 80(1).       |
|   | V |                                                                                           |
|   | W |                                                                                           |
|   | X |                                                                                           |

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Untitled

SYSTEM OS - DIALOG OneSearch

- File 2: INSPEC 1898-2010/ Aug W5  
(c) 2010 The IET
- File 6: NTIS 1964-2010/ Aug W5  
(c) 2010 NTIS, Intl Copyright All Rights Res
- File 8: Ei Compendex(R) 1884-2010/ Aug W5  
(c) 2010 Elsevier Eng. Info. Inc.
- File 34: Sci Search(R) Cited Ref Sci 1990-2010/ Aug W5  
(c) 2010 The Thomson Corp
- File 35: Dissertation Abs Online 1861-2010/ Aug  
(c) 2010 ProQuest Info&Learning
- File 56: Computer and Information Systems Abstracts 1966-2010/ Jun  
(c) 2010 CSA.
- File 60: ANTE: Abstracts in New Tech & Engineer 1966-2010/ Jul  
(c) 2010 CSA.
- File 65: Inside Conferences 1993-2010/ Sep 07  
(c) 2010 BLDSC all rts. reserv.
- File 92: IHS Intl. Stds. & Specs. 1999/ Nov  
(c) 1999 Information Handling Services
- \* File 92: This file is closed.
- File 95: TEMA- Technology & Management 1989-2010/ Aug W5  
(c) 2010 FIZ TECHNIK
- File 99: Wilson Appl. Sci & Tech Abs 1983-2010/ Jun  
(c) 2010 The H.W. Wilson Co.
- File 103: Energy Sci Tec 1974-2010/ Jul B2  
(c) 2010 Contains copyrighted material
- \* File 103: For access restrictions see Help Restrict.
- File 144: Pascal 1973-2010/ Aug W5  
(c) 2010 INIST/CNRS
- File 275: Gale Group Computer DB(TM) 1983-2010/ Jul 26  
(c) 2010 Gale/Cengage
- File 434: Sci Search(R) Cited Ref Sci 1974-1989/ Dec  
(c) 2006 The Thomson Corp
- File 647: UBM Computer Fulltext 1988-2010/ Aug W5  
(c) 2010 UBM LLC
- File 674: Computer News Fulltext 1989-2006/ Sep W5  
(c) 2006 IDG Communications
- \* File 674: File 674 is closed (no longer updates).
- File 696: DIALOG Telecom Newsletters 1995-2010/ Sep 04  
(c) 2010 Dialog

|                                                                                                                        |                                                |                                                                       |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b><i>Index of Claims</i></b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                                        | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

|   |                 |   |                   |   |                     |   |                 |
|---|-----------------|---|-------------------|---|---------------------|---|-----------------|
| ✓ | <b>Rejected</b> | - | <b>Cancelled</b>  | N | <b>Non-Elected</b>  | A | <b>Appeal</b>   |
| = | <b>Allowed</b>  | ÷ | <b>Restricted</b> | I | <b>Interference</b> | O | <b>Objected</b> |

| <input type="checkbox"/> Claims renumbered in the same order as presented by applicant |          |            |            |            |            | <input type="checkbox"/> CPA |  | <input checked="" type="checkbox"/> T.D. |  | <input type="checkbox"/> R.1.47 |  |
|----------------------------------------------------------------------------------------|----------|------------|------------|------------|------------|------------------------------|--|------------------------------------------|--|---------------------------------|--|
| CLAIM                                                                                  |          | DATE       |            |            |            |                              |  |                                          |  |                                 |  |
| Final                                                                                  | Original | 06/11/2009 | 04/08/2010 | 04/22/2010 | 09/07/2010 |                              |  |                                          |  |                                 |  |
| 1                                                                                      | 45       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 2                                                                                      | 46       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 3                                                                                      | 47       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 4                                                                                      | 48       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 5                                                                                      | 49       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 6                                                                                      | 50       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 7                                                                                      | 51       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 8                                                                                      | 52       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 9                                                                                      | 53       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 10                                                                                     | 54       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 11                                                                                     | 55       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 12                                                                                     | 56       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 13                                                                                     | 57       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 14                                                                                     | 58       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 15                                                                                     | 59       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 16                                                                                     | 60       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 17                                                                                     | 61       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 18                                                                                     | 62       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 19                                                                                     | 63       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 20                                                                                     | 64       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 21                                                                                     | 65       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 22                                                                                     | 66       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 23                                                                                     | 67       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
| 24                                                                                     | 68       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |
|                                                                                        | 69       | O          | O          | O          | -          |                              |  |                                          |  |                                 |  |
| 25                                                                                     | 70       | ✓          | ✓          | ✓          | =          |                              |  |                                          |  |                                 |  |

|                                                                                                                            |                                                |                                                                       |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b><i>Issue Classification</i></b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                                            | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

[illegible][illegible]

|                                                         |  |            |  |                       |                   |
|---------------------------------------------------------|--|------------|--|-----------------------|-------------------|
| /JENISE E JACKSON/<br>Examiner.Art Unit 2439            |  | 9/7/10     |  | Total Claims Allowed: |                   |
| (Assistant Examiner)                                    |  | (Date)     |  | 25                    |                   |
| /MICHAEL J SIMITOSKI/<br>Primary Examiner.Art Unit 2439 |  | 09/23/2010 |  | O.G. Print Claim(s)   | O.G. Print Figure |
| (Primary Examiner)                                      |  | (Date)     |  | 1                     | 2                 |

|                                                                                                              |                                                |                                                                       |
|--------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------------------------------------|
| <b>Search Notes</b><br><br> | <b>Application/Control No.</b><br><br>11551606 | <b>Applicant(s)/Patent Under Reexamination</b><br><br>SCHNEIER ET AL. |
|                                                                                                              | <b>Examiner</b><br><br>JENISE E JACKSON        | <b>Art Unit</b><br><br>2439                                           |

| SEARCHED |          |        |          |
|----------|----------|--------|----------|
| Class    | Subclass | Date   | Examiner |
| 726      | 3        | 9/7/10 | JJ       |
| 726      | 22-25    | 9/7/10 | JJ       |

| SEARCH NOTES                         |        |          |
|--------------------------------------|--------|----------|
| Search Notes                         | Date   | Examiner |
| Updated West text search             | 9/7/10 | JJ       |
| Updated West class and text search   | 9/7/10 | JJ       |
| Updated Inventor and assignee search | 9/7/10 | JJ       |
| Non-patent literature search         | 9/7/10 |          |

| INTERFERENCE SEARCH |                                |        |          |
|---------------------|--------------------------------|--------|----------|
| Class               | Subclass                       | Date   | Examiner |
|                     | West Interference search .CLM. | 9/7/10 | JJ       |

|  |  |
|--|--|
|  |  |
|--|--|

## WEST Search History for Application 11551606

Creation Date: 2010090716:09

(NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) ) and (probe or sentry or scanner? or sensor? or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(sensor or filter\$5 or probe or sentry or black near box)near(collect\$5 or gather\$5)near(data or information or alert\$5 or event\$2) and ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(transmit\$8 or send\$8 or transfer\$8 or forward\$8)near(information or data or alert\$2 or event\$2 or footprint\$2)near(dispatch\$5 or engineer or analyst or admin\$8 or support near person or help near desk\$4)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009  
((sensor or filter\$5 or probe or sentry or black near box)near(collect\$5 or gather\$5)near(data or information or alert\$5 or event\$2) and (monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and (NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and ((transmit\$8 or send\$8 or transfer\$8 or forward\$8)near(information or data or alert\$2 or event\$2 or footprint\$2)near(dispatch\$5 or engineer or analyst or admin\$8 or support near person or help near desk\$4) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(filter\$5 or separate)near(data or information or alert\$5 or event\$5 or footprint\$2)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(post near filter\$5 near residue)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(keeping\$5 or sav\$5)near(residue or left near over)near(alert\$2 or data or information or event\$2 or footprint\$2)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(receiv\$5 or obtain\$5)near(feedback or results)near(probe or sensor? or sentry or black near box)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

((receiv\$5 or obtain\$5)near(feedback or results)near(probe or sensor? or sentry or black near box) ) and ((filter\$5 or separate)near(data or information or alert\$5 or event\$5 or footprint\$2) )PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(dynamically or real-time)near(modif\$8 or updat\$8 or chang\$8)near(probe or sentry or sensor? or black near box)near(feedback or result\$2)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/22.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/24.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/25.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/23.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/2.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/3.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/6.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

726/15.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/208.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/209.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/223.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/224.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/225.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/226.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/227.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/228.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

709/229.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

Bruce near Schneier.in. and (secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(Andrew near Gross.in.) and (secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(Jonathan near Callas).in. and (secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

(Counterpane.as. and secure near operations near center)PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

((ticket) and (analyst or help near desk) and network ) and (intrusion)PGPB, USPT, EPAB,

JPAB, DWPI, TDBD OR YES 06-11-2009  
 ((ticket) and (analyst or help near desk) ) and networkPGPB, USPT, EPAB, JPAB, DWPI,  
 TDBD OR YES 06-11-2009  
 ((incident near log) ) and (analyst or help near desk)PGPB, USPT, EPAB, JPAB, DWPI,  
 TDBD OR YES 06-11-2009  
 (problem near ticket\$2) and (help near desk or analyst)PGPB, USPT, EPAB, JPAB, DWPI,  
 TDBD OR YES 06-11-2009  
 726/3.ccls.PGPB, USPT, EPAB, JPAB, DWPI, TDBD OR YES 06-11-2009

## Interference Searches

| Query                                                                                                                                                                                                                             | DB               | Op. | Plur. | Thes. | Date       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-----|-------|-------|------------|
| 726/22.ccls. and (secure near operation \$ 2 near center and creat ? near event near record and security near event and filter ? near residue and residue near discard ? and correlat ? near record and problem near ticket).CLM. | PGPB, USPT, UPAD | OR  | YES   |       | 09-07-2010 |
| 726/23.ccls. and (secure near operation \$ 2 near center and creat ? near event near record and security near event and filter ? near residue and residue near discard ? and correlat ? near record and problem near ticket).CLM. | PGPB, USPT, UPAD | OR  | YES   |       | 09-07-2010 |
| 726/24.ccls. and (secure near operation \$ 2 near center and creat ? near event near record and security near event and filter ? near residue and residue near discard ? and correlat ? near record and problem near ticket).CLM. | PGPB, USPT, UPAD | OR  | YES   |       | 09-07-2010 |
| 726/25.ccls. and (secure near operation \$ 2 near center and creat ? near event near record and security near event and filter ? near residue and residue near discard ? and correlat ? near record and problem near ticket).CLM. | PGPB, USPT, UPAD | OR  | YES   |       | 09-07-2010 |
| 726/3.ccls. and (secure near operation \$ 2 near center and creat ? near event near record and security near event and filter ? near residue and residue near discard ? and correlat ? near record and problem near ticket).CLM.  | PGPB, USPT, UPAD | OR  | YES   |       | 09-07-2010 |

## Prior Art Searches

| Query                                                                                                                                                             | DB                | Op. | Plur. | Thes. | Date       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----|-------|-------|------------|
| (monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or | PGPB, USPT, EPAB, | OR  | YES   |       | 04-09-2010 |

|                                                                                                                                                                                                                                                                                                                                                                             |                                    |    |     |  |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) | JPAB, DWPI, TDBD                   |    |     |  |            |
| (creat? or compos? or conceiv? or construct? or generat? or mak? or produc? or form?)near(event or alert? or alarm? or incident or problem)with(record or directory or file or note or report? or list or log)                                                                                                                                                              | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| (correlat? or correspond? or coordinat? or connect? or associat? or combin? or integrat? or organiz? or pool?)near(event or alert? or alarm? or incident or problem)with(record or directory or file or note or report? or list or log)near(customer near data or customer near information and symptom)                                                                    | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| (analyst or engineer or help near desk or admin or manager or boss or operator)near(creat? or generat?)near(ticket)                                                                                                                                                                                                                                                         | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| (resolution or assistance)with(data or information)near(symptom or diagnosis) and (analyst or engineer or help near desk or admin or manager or boss or operator)                                                                                                                                                                                                           | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| (solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator)                                                                                                                                                                                                                   | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| ((solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator) ) and (creat? or generat?)with(ticket)                                                                                                                                                                           | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| ((solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator) ) and ticket                                                                                                                                                                                                     | PGPB, USPT, EPAB,                  | OR | YES |  | 04-09-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                   |    |     |  |            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | JPAB,<br>DWPI,<br>TDBD                            |    |     |  |            |
| 726/22.ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| 726/24.ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| 726/25.ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| 726/23.ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| (Counterpane.as. and secure near operations near center)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 04-09-2010 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                   | OR | YES |  | 04-09-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |    |     |  |            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) ) and (resolution or assistance)with(data or information)near(symptom or diagnosis) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD |    |     |  |            |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) ) and (resolution or assistance)with(data or information)                           | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot) ) and (analyst or engineer or help near desk or admin or manager or boss or operator) and (resolution or assistance)with(data or information) ) and ticket                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-09-2010 |
| (customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier)                                                                                                                                                                                                                                                                                                                                                                                             | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| ((customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | PGPB, USPT, EPAB,                  | OR | YES |  | 04-22-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                    |    |     |  |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier) ) and (help near desk)                                                                                                                                                                                                                                                                                                                                                                 | JPAB, DWPI, TDBD                   |    |     |  |            |
| ((customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier) and (help near desk) ) and (symptom)                                                                                                                                                                                      | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| ((customer near information or customer near data or employee near name or employee near number or office near number or building near name or building near number or office near number or office near location or work near phone near number or workstation near id or computer near id or workstation near identifier) and (help near desk) and (symptom) ) and (incident\$2 or problem\$2 or event\$2 or intrus\$5 or intrud\$5)                                                                                                                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| (consolidat? or combin? or build? near up or connect? or develop? or incorporat? or join? or mix? or unif?)near(event\$2 or record? or alert? or problem\$2 or intrus\$5 or intrud? or alarm\$5 or attack? or vulnerabilit\$6 or error or incident)near(customer near information or customer near name or name or id or identifier or work near number or address or phone near number or workstation near id or computer near id or building near number or office near location)near(symptom or indication or problem\$2)                          | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| (correlat? or consolidat? or combin? or build? near up or connect? or develop? or incorporat? or join? or mix? or unif?)near(event\$2 or record? or alert? or problem\$2 or intrus\$5 or intrud? or alarm\$5 or attack? or vulnerabilit\$6 or error or incident)near(customer near information or customer near name or name or id or identifier or work near number or address or phone near number or workstation near id or computer near id or building near number or office near location)near(symptom or indication or problem\$2)near(ticket) | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |
| (troubl?)with(ticket)near(help near desk or operator or analyst or admin or engineer)                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 04-22-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                    |    |     |  |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| <b>(filter? or separat?)near(event\$2 or alert\$2 or alarm\$2 or incident\$2 or problem\$2 or attack near signature\$2 or vulnerab? or intrusion\$2 or virus or trojan near horse or malware or residue or left near over near data)</b>                                                                                                                                                                                                                                                                                        | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| <b>(analyz? or examin? or determin? or evaluat? or figur? or inspect? or investigat? or audit? or verif? or review? or check? or filter?)near(residue or residual or extra or excess)near(information or data or event\$2 or alert\$2 or alarm\$2 or incident\$2 or problem\$2)</b>                                                                                                                                                                                                                                             | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| <b>((analyz? or examin? or determin? or evaluat? or figur? or inspect? or investigat? or audit? or verif? or review? or check? or filter?)near(residue or residual or extra or excess)near(information or data or event\$2 or alert\$2 or alarm\$2 or incident\$2 or problem\$2) ) and ((filter? or separat?)near(event\$2 or alert\$2 or alarm\$2 or incident\$2 or problem\$2 or attack near signature\$2 or vulnerab? or intrusion\$2 or virus or trojan near horse or malware or residue or left near over near data) )</b> | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| <b>(creat? or compos? or conceiv? or construct? or generat? or mak? or produc? or form?)near(event or alert? or alarm? or incident or problem)with(record or directory or file or note or report? or list or log)</b>                                                                                                                                                                                                                                                                                                           | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| <b>(correlat? or correspond? or coordinat? or connect? or associat? or combin? or integrat? or organiz? or pool?)near(event or alert? or alarm? or incident or problem)with(record or directory or file or note or report? or list or log)near(customer near data or customer near information and symptom)</b>                                                                                                                                                                                                                 | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| <b>(analyst or engineer or help near desk or admin or manager or boss or operator)near(creat? or generat?)near(ticket)</b>                                                                                                                                                                                                                                                                                                                                                                                                      | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| <b>(resolution or assistance)with(data or information)near(symptom or diagnosis) and (analyst or engineer or help near desk or admin or manager or boss or operator)</b>                                                                                                                                                                                                                                                                                                                                                        | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                    | OR | YES |  | 09-07-2010 |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                    |    |     |  |            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|----|-----|--|------------|
| ((solv? or resolv? or fix?)near(problem or error or alert? or incident)near(analyst or engineer or help near desk or admin or manager or boss or operator) ) and (creat? or generat?)with(ticket)                                                                                                                                                                                                                                                                                                                                                             | PGPB, USPT, EPAB, JPAB, DWPI, TDBD |    |     |  |            |
| (726/22).ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| (726/24).ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| (726/25).ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| (726/23).ccls.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| (Counterpane.as. and secure near operations near center)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |
| ((monitor? or detect? or intrud? or intrusion or response or alert? or incident? or attack? or vulnerability or analysis or analy\$6 or malicious or harmful\$5 or suspicious)near(data or information or signature\$2 or footprint\$2 or virus\$6 or trojan near horse) and ((NSOC or SOC or secure near operation? near center or master near system or security near subsystem? or sub near program or control near center or operation\$2 near center or central near facility) and (probe or sentry or scanner? or sensor? or honeypot)) and (analyst or | PGPB, USPT, EPAB, JPAB, DWPI, TDBD | OR | YES |  | 09-07-2010 |

|                                                                                                                                                 |                                                   |    |     |  |            |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
| <b>engineer or help near desk or admin or manager or boss or operator) and (resolution or assistance)with(data or information) ) and ticket</b> |                                                   |    |     |  |            |
| <b>726/2.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>                | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>726/3.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>                | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>726/6.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>                | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>726/15.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>               | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/208.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>              | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/209.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>              | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/223.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b>              | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |

|                                                                                                                                    |                                                   |    |     |  |            |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
| <b>709/224.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/225.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/226.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/227.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/228.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>709/229.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>Bruce near Schneier.in. and (secure near operations near center)</b>                                                            | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>(Andrew near Gross.in.) and (secure near operations near center)</b>                                                            | PGPB,<br>USPT,<br>EPAB,<br>JPAB,                  | OR | YES |  | 09-07-2010 |

|                                                                                                                                    |                                                   |    |     |  |            |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----|-----|--|------------|
|                                                                                                                                    | DWPI,<br>TDBD                                     |    |     |  |            |
| <b>(Jonathan near Callas).in. and (secure near operations near center)</b>                                                         | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>726/3.ccls.</b>                                                                                                                 | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>713/154.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |
| <b>713/165.ccls.and (security near subsystem or black near box or sensor or sensors or probe or sentry or scanner or honeypot)</b> | PGPB,<br>USPT,<br>EPAB,<br>JPAB,<br>DWPI,<br>TDBD | OR | YES |  | 09-07-2010 |

Please enter /JEJ/  
9/10/10

AMENDMENT UNDER 37 CFR 1.116  
EXPEDITED PROCEDURE –  
EXAMINING GROUP 2439

---

PATENT  
Attorney Docket No.: 022133-000520US

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Bruce Schneier et al.

Application No.: 11/551,606

Filed: October 20, 2006

For: METHOD AND SYSTEM FOR  
DYNAMIC NETWORK INTRUSION  
MONITORING, DETECTION AND  
RESPONSE

Customer No.: 20350

Confirmation No. 1662

Examiner: Jenise E. Jackson

Technology Center/Art Unit: 2439

AMENDMENT UNDER 37 CFR 1.116  
EXPEDITED PROCEDURE EXAMINING  
GROUP 2439

---

Mail Stop AF  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Commissioner:

In response to the Final Office Action mailed April 27, 2010 in the above-referenced application, please enter the following amendments and remarks:

**Amendments to the Claims** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks/Arguments** begin on page 6 of this paper.



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

## BIB DATA SHEET

CONFIRMATION NO. 1662

|                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                   |                                                          |                                                                                                                                                                                                                                                                           |                                                   |                               |                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------|------------------------------------|
| <b>SERIAL NUMBER</b><br>11/551,606                                                                                                                                                                                                                                                                                                                                                                          | <b>FILING or 371(c)<br/>DATE</b><br>10/20/2006<br><b>RULE</b>                                                     | <b>CLASS</b><br>726                                      | <b>GROUP ART UNIT</b><br>2439                                                                                                                                                                                                                                             | <b>ATTORNEY DOCKET<br/>NO.</b><br>022133-000520US |                               |                                    |
| <b>APPLICANTS</b><br>Bruce Schneier, Minneapolis, MN;<br>Andrew H. Gross, San Jose, CA;<br>Jonathan D. Callas, Mountain View, CA;<br>** <b>CONTINUING DATA</b> *****<br>This application is a CON of 09/766,343 01/19/2001 PAT 7,159,237<br>which claims benefit of 60/190,326 03/16/2000<br>** <b>FOREIGN APPLICATIONS</b> *****<br>** <b>IF REQUIRED, FOREIGN FILING LICENSE GRANTED</b> **<br>11/20/2006 |                                                                                                                   |                                                          |                                                                                                                                                                                                                                                                           |                                                   |                               |                                    |
| Foreign Priority claimed <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>35 USC 119(a-d) conditions met <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No<br>Verified and Acknowledged <u>/JENISE E JACKSON/</u><br>Examiner's Signature                                                                                                                           |                                                                                                                   | <input type="checkbox"/> Met after Allowance<br>Initials | <b>STATE OR<br/>COUNTRY</b><br>MN                                                                                                                                                                                                                                         | <b>SHEETS<br/>DRAWINGS</b><br>9                   | <b>TOTAL<br/>CLAIMS</b><br>26 | <b>INDEPENDENT<br/>CLAIMS</b><br>2 |
| <b>ADDRESS</b><br>TOWNSEND AND TOWNSEND AND CREW, LLP<br>TWO EMBARCADERO CENTER<br>EIGHTH FLOOR<br>SAN FRANCISCO, CA 94111-3834<br>UNITED STATES                                                                                                                                                                                                                                                            |                                                                                                                   |                                                          |                                                                                                                                                                                                                                                                           |                                                   |                               |                                    |
| <b>TITLE</b><br>METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE                                                                                                                                                                                                                                                                                                          |                                                                                                                   |                                                          |                                                                                                                                                                                                                                                                           |                                                   |                               |                                    |
| <b>FILING FEE<br/>RECEIVED</b><br>1430                                                                                                                                                                                                                                                                                                                                                                      | FEES: Authority has been given in Paper<br>No. _____ to charge/credit DEPOSIT ACCOUNT<br>No. _____ for following: |                                                          | <input type="checkbox"/> All Fees<br><input type="checkbox"/> 1.16 Fees (Filing)<br><input type="checkbox"/> 1.17 Fees (Processing Ext. of time)<br><input type="checkbox"/> 1.18 Fees (Issue)<br><input type="checkbox"/> Other _____<br><input type="checkbox"/> Credit |                                                   |                               |                                    |

# **PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

20350 7590 10/28/2010  
**TOWNSEND AND TOWNSEND AND CREW, LLP**  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

## **Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

|                    |
|--------------------|
| (Depositor's name) |
| (Signature)        |
| (Date)             |

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

11/551,606 10/20/2006 Bruce Schneier 022133-000520US 1662

TITLE OF INVENTION: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE

| APPLN. TYPE | SMALL ENTITY | ISSUE FEE DUE | PUBLICATION FEE DUE | PREV. PAID ISSUE FEE | TOTAL FEE(S) DUE | DATE DUE |
|-------------|--------------|---------------|---------------------|----------------------|------------------|----------|
|-------------|--------------|---------------|---------------------|----------------------|------------------|----------|

nonprovisional NO \$1510 \$300 \$0 \$1810 01/28/2011

| EXAMINER | ART UNIT | CLASS-SUBCLASS |
|----------|----------|----------------|
|----------|----------|----------------|

JACKSON, JENISE E 2439 726-003000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

Kilpatrick Townsend

1. & Stockton LLP

2. \_\_\_\_\_

3. \_\_\_\_\_

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

BT COUNTERPANE INTERNET SECURITY, INC.

MOUNTAIN VIEW, CALIFORNIA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☒ Advance Order - # of Copies 1

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 20-1430 (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature /Brian E. Mack/  
Typed or printed name Brian E. Mack

Date January 14, 2011  
Registration No. 57,189

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Electronic Patent Application Fee Transmittal

|                                                |                                                                                    |                 |               |                             |
|------------------------------------------------|------------------------------------------------------------------------------------|-----------------|---------------|-----------------------------|
| <b>Application Number:</b>                     | 11551606                                                                           |                 |               |                             |
| <b>Filing Date:</b>                            | 20-Oct-2006                                                                        |                 |               |                             |
| <b>Title of Invention:</b>                     | METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE |                 |               |                             |
| <b>First Named Inventor/Applicant Name:</b>    | Bruce Schneier                                                                     |                 |               |                             |
| <b>Filer:</b>                                  | Brian Edward Mack/Cynthia McKinley                                                 |                 |               |                             |
| <b>Attorney Docket Number:</b>                 | 022133-000520US                                                                    |                 |               |                             |
| Filed as Large Entity                          |                                                                                    |                 |               |                             |
| <b>Utility under 35 USC 111(a) Filing Fees</b> |                                                                                    |                 |               |                             |
| <b>Description</b>                             | <b>Fee Code</b>                                                                    | <b>Quantity</b> | <b>Amount</b> | <b>Sub-Total in USD(\$)</b> |
| <b>Basic Filing:</b>                           |                                                                                    |                 |               |                             |
| <b>Pages:</b>                                  |                                                                                    |                 |               |                             |
| <b>Claims:</b>                                 |                                                                                    |                 |               |                             |
| <b>Miscellaneous-Filing:</b>                   |                                                                                    |                 |               |                             |
| <b>Petition:</b>                               |                                                                                    |                 |               |                             |
| <b>Patent-Appeals-and-Interference:</b>        |                                                                                    |                 |               |                             |
| <b>Post-Allowance-and-Post-Issuance:</b>       |                                                                                    |                 |               |                             |
| Utility Appl issue fee                         | 1501                                                                               | 1               | 1510          | 1510                        |
| Publ. Fee- early, voluntary, or normal         | 1504                                                                               | 1               | 300           | 300                         |

| Description                       | Fee Code | Quantity | Amount | Sub-Total in USD(\$) |
|-----------------------------------|----------|----------|--------|----------------------|
| Extension-of-Time:                |          |          |        |                      |
| Miscellaneous:                    |          |          |        |                      |
| Printed copy of patent - no color | 8001     | 1        | 3      | 3                    |
| Total in USD (\$)                 |          |          |        | 1813                 |

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 9236310                                                                            |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Brian Edward Mack                                                                  |
| <b>Filer Authorized By:</b>                 |                                                                                    |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 14-JAN-2011                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 16:11:24                                                                           |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)                                                        |

### Payment information:

|                                          |                 |
|------------------------------------------|-----------------|
| Submitted with Payment                   | yes             |
| Payment Type                             | Deposit Account |
| Payment was successfully received in RAM | \$ 1813         |
| RAM confirmation Number                  | 3241            |
| Deposit Account                          | 201430          |
| Authorized User                          |                 |

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

## File Listing:

| Document Number | Document Description        | File Name                    | File Size(Bytes)/ Message Digest             | Multi Part /.zip | Pages (if appl.) |
|-----------------|-----------------------------|------------------------------|----------------------------------------------|------------------|------------------|
| 1               | Issue Fee Payment (PTO-85B) | 022133_000520US_IssueFee.pdf | 133870                                       | no               | 1                |
|                 |                             |                              | 439367f78a35f6aad9c3ac21ec0c18cda8dc<br>ef39 |                  |                  |

### Warnings:

### Information:

|   |                         |              |                                             |    |   |
|---|-------------------------|--------------|---------------------------------------------|----|---|
| 2 | Fee Worksheet (PTO-875) | fee-info.pdf | 33830                                       | no | 2 |
|   |                         |              | 06ffbdcc27bff761d9e955cdbc3e06f9e95<br>6989 |    |   |

### Warnings:

### Information:

|                              |  |  |        |
|------------------------------|--|--|--------|
| Total Files Size (in bytes): |  |  | 167700 |
|------------------------------|--|--|--------|

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

#### New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

#### National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

#### New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

| APPLICATION NO. | ISSUE DATE | PATENT NO. | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|------------|------------|---------------------|------------------|
| 11/551,606      | 02/22/2011 | 7895641    | 022133-000520US     | 1662             |

20350 7590 02/02/2011  
KILPATRICK TOWNSEND & STOCKTON LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

## ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

### **Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)** (application filed on or after May 29, 2000)

The Patent Term Adjustment is 873 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Bruce Schneier, Minneapolis, MN;  
Andrew H. Gross, San Jose, CA;  
Jonathan D. Callas, Mountain View, CA;

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

|                                                                                                                                                            |                        |                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-------------------------------------------------------|
| <b>PATENT - POWER OF ATTORNEY<br/>OR<br/>REVOCATION OF POWER OF ATTORNEY<br/>WITH A NEW POWER OF ATTORNEY<br/>AND<br/>CHANGE OF CORRESPONDENCE ADDRESS</b> | Patent Number          | 7,895,641                                             |
|                                                                                                                                                            | Issue Date             | October 20, 2006                                      |
|                                                                                                                                                            | First Named Inventor   | Brusa SCHNEIER                                        |
|                                                                                                                                                            | Title                  | METHOD AND SYSTEM FOR<br>DYNAMIC NETWORK INTRUSION... |
|                                                                                                                                                            | Attorney Docket Number | RYM-36-1                                              |

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

23117

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

| Practitioner(s) Name | Registration Number |
|----------------------|---------------------|
|                      |                     |
|                      |                     |
|                      |                     |
|                      |                     |

Please recognize or change the correspondence address for the above-identified patent to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number:

OR

☐ Firm or  
Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the:

☐ Inventor, having ownership of the patent.

OR

☒ Patent owner.

Statement under 37 CFR 3.73(b) (Form PTO/SB/95) submitted herewith or filed on \_\_\_\_\_

SIGNATURE of Inventor or Patent Owner

Signature

Name

Title and Company

Date

Telephone

NOTE: Signatures of all the inventors or patent owners of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☐ \*Total of \_\_\_\_\_ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## Electronic Acknowledgement Receipt

|                                             |                                                                                    |
|---------------------------------------------|------------------------------------------------------------------------------------|
| <b>EFS ID:</b>                              | 24793217                                                                           |
| <b>Application Number:</b>                  | 11551606                                                                           |
| <b>International Application Number:</b>    |                                                                                    |
| <b>Confirmation Number:</b>                 | 1662                                                                               |
| <b>Title of Invention:</b>                  | METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE |
| <b>First Named Inventor/Applicant Name:</b> | Bruce Schneier                                                                     |
| <b>Customer Number:</b>                     | 20350                                                                              |
| <b>Filer:</b>                               | Raymond Y. Mah/Deborah White                                                       |
| <b>Filer Authorized By:</b>                 | Raymond Y. Mah                                                                     |
| <b>Attorney Docket Number:</b>              | 022133-000520US                                                                    |
| <b>Receipt Date:</b>                        | 02-FEB-2016                                                                        |
| <b>Filing Date:</b>                         | 20-OCT-2006                                                                        |
| <b>Time Stamp:</b>                          | 13:14:08                                                                           |
| <b>Application Type:</b>                    | Utility under 35 USC 111(a)                                                        |

### Payment information:

|                        |    |
|------------------------|----|
| Submitted with Payment | no |
|------------------------|----|

### File Listing:

| Document Number | Document Description | File Name                       | File Size(Bytes)/<br>Message Digest                 | Multi Part /.zip | Pages (if appl.) |
|-----------------|----------------------|---------------------------------|-----------------------------------------------------|------------------|------------------|
| 1               |                      | POA_ChangeofAddress_7895641.pdf | 2869629<br>e0905ef3452871d49db11257f85e4196348c448b | yes              | 2                |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                            |              |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|--------------|------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>Multipart Description/PDF files in .zip description</b> |              |            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>Document Description</b>                                | <b>Start</b> | <b>End</b> |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Assignee showing of ownership per 37 CFR 3.73              | 1            | 1          |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Power of Attorney                                          | 2            | 2          |
| <b>Warnings:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                            |              |            |
| <b>Information:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                            |              |            |
| <b>Total Files Size (in bytes):</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                            | 2869629      |            |
| <p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b><br/> <b>If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</b></p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b><br/> <b>If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</b></p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b><br/> <b>If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</b></p> |                                                            |              |            |

**STATEMENT UNDER 37 CFR 3.73(b)**Applicant/Patent Owner: BT AMERICAS INC.Application No./Patent No.: 7,895,641Filed/Issue Date: October 20, 2006Titled: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE

BT AMERICAS INC. , a CORPORATION

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;
2. ☐ an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is \_\_\_\_\_ %); or
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)
- the patent application/patent identified above, by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 023657, Frame 0530, or for which a copy therefore is attached.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at

Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

2. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at

Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

3. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at

Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature

JAMIE ABUELL

Printed or Typed Name

Date

1/21/15  
SECRETARY

Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | 022133-000520US        |

**CONFIRMATION NO. 1662**

**POWER OF ATTORNEY NOTICE**



\*OC000000080528821\*

20350  
KILPATRICK TOWNSEND & STOCKTON LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

Date Mailed: 02/12/2016

**NOTICE REGARDING CHANGE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 02/02/2016.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/khoang/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NUMBER | FILING OR 371(C) DATE | FIRST NAMED APPLICANT | ATTY. DOCKET NO./TITLE |
|--------------------|-----------------------|-----------------------|------------------------|
| 11/551,606         | 10/20/2006            | Bruce Schneier        | RYM-38-1               |

23117  
NIXON & VANDERHYE, PC  
901 NORTH GLEBE ROAD, 11TH FLOOR  
ARLINGTON, VA 22203

**CONFIRMATION NO. 1662**  
**POA ACCEPTANCE LETTER**



Date Mailed: 02/12/2016

**NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 02/02/2016.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/khoang/

AO 120 (Rev. 08/10)

|                                                                                                                                               |                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>TO: Mail Stop 8</b><br><b>Director of the U.S. Patent and Trademark Office</b><br><b>P.O. Box 1450</b><br><b>Alexandria, VA 22313-1450</b> | <b>REPORT ON THE</b><br><b>FILING OR DETERMINATION OF AN</b><br><b>ACTION REGARDING A PATENT OR</b><br><b>TRADEMARK</b> |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been  
filed in the U.S. District Court District of Delaware on the following

☐ Trademarks or ☒ Patents. ( ☐ the patent action involves 35 U.S.C. § 292.):

|                                                                      |                                |                                             |
|----------------------------------------------------------------------|--------------------------------|---------------------------------------------|
| DOCKET NO.                                                           | DATE FILED                     | U.S. DISTRICT COURT<br>District of Delaware |
| PLAINTIFF<br>BRITISH TELECOMMUNICATIONS PLC and<br>BT AMERICAS, INC. |                                | DEFENDANT<br>FORTINET, INC.                 |
| PATENT OR<br>TRADEMARK NO.                                           | DATE OF PATENT<br>OR TRADEMARK | HOLDER OF PATENT OR TRADEMARK               |
| 1 US 7,159,237 B2                                                    | 1/2/2007                       | BT AMERICAS, INC.                           |
| 2 US 7,895,641 B2                                                    | 2/22/2011                      | BT AMERICAS, INC.                           |
| 3 US 7,370,358 B2                                                    | 5/6/2008                       | BRITISH TELECOMMUNICATIONS PLC              |
| 4 US 7,693,971 B2                                                    | 4/6/2010                       | BRITISH TELECOMMUNICATIONS PLC              |
| 5 US 7,774,845 B2                                                    | 8/10/2010                      | BRITISH TELECOMMUNICATIONS PLC              |

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

|                            |                                                                                                                                                               |                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| DATE INCLUDED              | INCLUDED BY<br><input type="checkbox"/> Amendment <input type="checkbox"/> Answer <input type="checkbox"/> Cross Bill <input type="checkbox"/> Other Pleading |                               |
| PATENT OR<br>TRADEMARK NO. | DATE OF PATENT<br>OR TRADEMARK                                                                                                                                | HOLDER OF PATENT OR TRADEMARK |
| 1                          |                                                                                                                                                               |                               |
| 2                          |                                                                                                                                                               |                               |
| 3                          |                                                                                                                                                               |                               |
| 4                          |                                                                                                                                                               |                               |
| 5                          |                                                                                                                                                               |                               |

In the above—entitled case, the following decision has been rendered or judgement issued:

|                    |
|--------------------|
| DECISION/JUDGEMENT |
|--------------------|

|       |                   |      |
|-------|-------------------|------|
| CLERK | (BY) DEPUTY CLERK | DATE |
|-------|-------------------|------|

Copy 1—Upon initiation of action, mail this copy to Director    Copy 3—Upon termination of action, mail this copy to Director  
Copy 2—Upon filing document adding patent(s), mail this copy to Director    Copy 4—Case file copy