01/022/01

JC539 U.S. PTO 09/766343 01/19/01

JC878 U.S. PTO 09/766343 01/19/01

PTO/SB/05 (11-00)
Approved for use through 10/31/2002 OMB 0651-0032
U S Patent and Trademark Office, U S. DEPARTMENT OF COMMERCE

Please type a plus sign (+) inside this box → +

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

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	028490-0007
First Inventor	B. Schneier et al.
Title	Method and System for Dynamic Network Intrusion Monitoring, Detection and Response
Express Mail Label No.	EK 447 202 148 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. [ ] Applicant claims small entity status. See 37 CFR 1.27.
3. [X] Specification [Total Pages 58] *(preferred arrangement set forth below)*
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. [X] Drawing(s) *(35 U.S.C. 113)* [Total Sheets 9]
5. Oath or Declaration [Total Pages 4]
   a. [X] ~~Newly executed (original or copy)~~ unexecuted
   b. [ ] Copy from a prior application (37 CFR 1.63 (d)) *(for continuation/divisional with Box 18 completed)*
      i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b)
6. [ ] Application Data Sheet. See 37 CFR 1.76
7. [ ] CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] paper
   c. [ ] Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. [ ] Assignment Papers (cover sheet & document(s))
10. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [X] Power of Attorney unexecuted
11. [ ] English Translation Document *(if applicable)*
12. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
13. [ ] Preliminary Amendment
14. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Request and Certification under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. [ ] Other: .....

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No _____/_____

Prior application information Examiner _____ *Group Art Unit* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

[ ] *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or [X] *Correspondence address below*

Name	Robert B. Beyers, Ph.D.				
Address	Skadden, Arps, Slate, Meagher & Flom LLP 525 University Avenue				
City	Palo Alto	State	CA	Zip Code	94301
Country	U.S.A.	Telephone	650 470-4500	Fax	470-4570

Name (Print/Type)	Robert B. Beyers, Ph.D.	Registration No. (Attorney/Agent)	46,552
Signature	Robert B. Beyers	Date	Jan. 19, 2001

Burden Hour Statement: This form is estimated to take 0 2 hours to complete. Time will vary depending upon the needs of the individual case Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231

PAN EX1002
Palo Alto Networks v. BT Americas
IPR2023-00888

PTO/SB/17 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U S Patent and Trademark Office, U S. DEPARTMENT OF COMMERCE
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.

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 1,142.00

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	B. Schneier et al.
Examiner Name	
Group Art Unit	
Attorney Docket No.	028490-0007

jc670 U.S. PTO 09/766343 01/19/01

METHOD OF PAYMENT

1. [XX] The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:
   Deposit Account Number: 19-2385
   Deposit Account Name: Skadden, Arps et al.
   [X] Charge Any Additional Fee Required Under 37 CFR 1 16 and 1.17
   [ ] Applicant claims small entity status. See 37 CFR 1 27
2. [X] **Payment Enclosed:**
   [X] Check [ ] Credit card [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 710

2. EXTRA CLAIM FEES

		Extra Claims		Fee from below		Fee Paid
Total Claims	44	-20** =	24	X 18	=	432
Independent Claims	3	- 3** =	0	X 80	=	0
Multiple Dependent					=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 432

**or number previously paid, if greater, For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1 17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1 129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1 129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	
Other fee (specify)					

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Robert B. Beyers, Ph.D.	Registration No. (Attorney/Agent)	46,552	Telephone	650 470-4500
Signature	Robert Beyers			Date	Jan. 19, 2001

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.

Burden Hour Statement. This form is estimated to take 0 2 hours to complete Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U S Patent and Trademark Office, Washington, DC 20231 DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO Assistant Commissioner for Patents, Washington, DC 20231

Our Ref. No.: 028490-0007

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

Inventors:

Bruce Schneier
Andrew H. Gross
Jonathan D. Callas

Prepared by:
Joseph Yang, Ph.D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
(650) 470-4500

I hereby certify that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" under 37 CFR § 1.10 (Label No. EK 447 202 148 US) in an envelope addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231, on January 19, 2001.

Jan Steele

(Signature)

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

FIELD OF THE INVENTION

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

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.

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.

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.

SUMMARY OF THE INVENTION

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).

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.

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.

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 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.

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

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.

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 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.

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 SOCs 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 SOCs can be used to provide redundancy and additional capacity for increased traffic or failure of one of the SOCs.

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.

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.

F. The "SOCRATES" Problem and Expertise Management System: In an exemplary embodiment, security analysts at a SOC work in concert with the "SOCRATES"[1] 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 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 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 FIGURES AND APPENDICES

FIG. 1 is an overview of the system architecture of an exemplary embodiment of the present invention.

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

---

1 "SOCRATES" is an acronym standing for Secure Operations Center Responsive Analyst Technical Expertise System.

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

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.

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

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

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 exemplary embodiment of the present invention.

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.

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

Appendix A provides specific details pertaining to an exemplary system for the transfer of information between customer networks and gateway systems (the "Pipes Protocol").

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

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

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.

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.

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") 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 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.

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 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 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**.

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.

In a preferred embodiment, Pipes **3000** provides an encrypted, secure 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.

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 ("PKI") 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.

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.

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.

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

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

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.

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.

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).

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.) 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**.)

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.

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.

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.

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 **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 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 are examples of data discrimination analyses, other types of which are well-known to those skilled in the art.

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 (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 **2060** can also monitor a "heartbeat" passing between probe/sentry system **2000** and gateway system **4000**.

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.

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 authenticated, can view such pages using any browser.

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 a "fix" might be sufficient to stop a transient attack, such as someone repeatedly trying to log in to the customer's network.

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.

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 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**.

FIG. 4 is a system overview of an exemplary embodiment of a "SOCRATES" problem and expertise management system. The SOCRATES system is a consolidated 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;
- access and authority management;

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

In an exemplary implementation, processing of gateway messages by SOCRATES **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**.

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**.

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.

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.

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.)

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.

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.

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.

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;
- generating a report for the problem; and
- incrementing or decrementing the priority of the problem.

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.

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.

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).

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 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**).

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 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 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 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 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 problem and whether the customer is now in an "all clear" state. If yes, in step **880**, the ticket can be closed.

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.

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 the 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.

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**.

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.

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.

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.

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.

Modifications, Enhancements and Alternate Embodiments

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.

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.

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

Exhibit 1002 - Page 29 of 30

CLAIMS

What is claimed is:

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

    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.

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

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

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

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

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

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

8. The method of claim 1, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

9. The method of claim 8, wherein said identifying step includes cross-correlating data across said monitored components.

10. The method of claim 8, wherein said identifying step includes analyzing the frequency of occurrence of said events.

11. The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.

12. The method of claim 11, wherein said computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

13. The method of claim 11, wherein said identifying step includes cross-correlating data across said monitored components.

14. The method of claim 11, wherein said identifying step includes analyzing the frequency of occurrence of said events.

15. The method of claim 11, wherein said computer-based analysis includes cross-probe correlation.

16. The method of claim 1, further comprising instantaneously self-tuning said probe based on previously collected status data.

17. The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

18. The method of claim 1, wherein said receiving feedback step occurs in substantially real time.

19. A computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by 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.

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

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

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

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

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

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

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

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

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

37. A security monitoring system for a computer network, comprising

a) a plurality of sensors for monitoring components of said network;

b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and

c) at least one probe, wherein said probe is configured to

(1) collect status data from at least one sensor monitoring at least one component of said network;

(2) identify potentially security-related events pertaining to said network by analyzing said status data;

(3) transmit information about said identified events to an analyst associated with said secure operations center;

(4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system in a manner customized to said network; and

(5) dynamically modify an analysis capability of said probe during operation thereof based on said received feedback in a manner customized to said network.

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

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

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

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

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

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

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

Attorney Docket No. 50277-0036

ABSTRACT

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.

FIG. 1 - Architectural Diagram

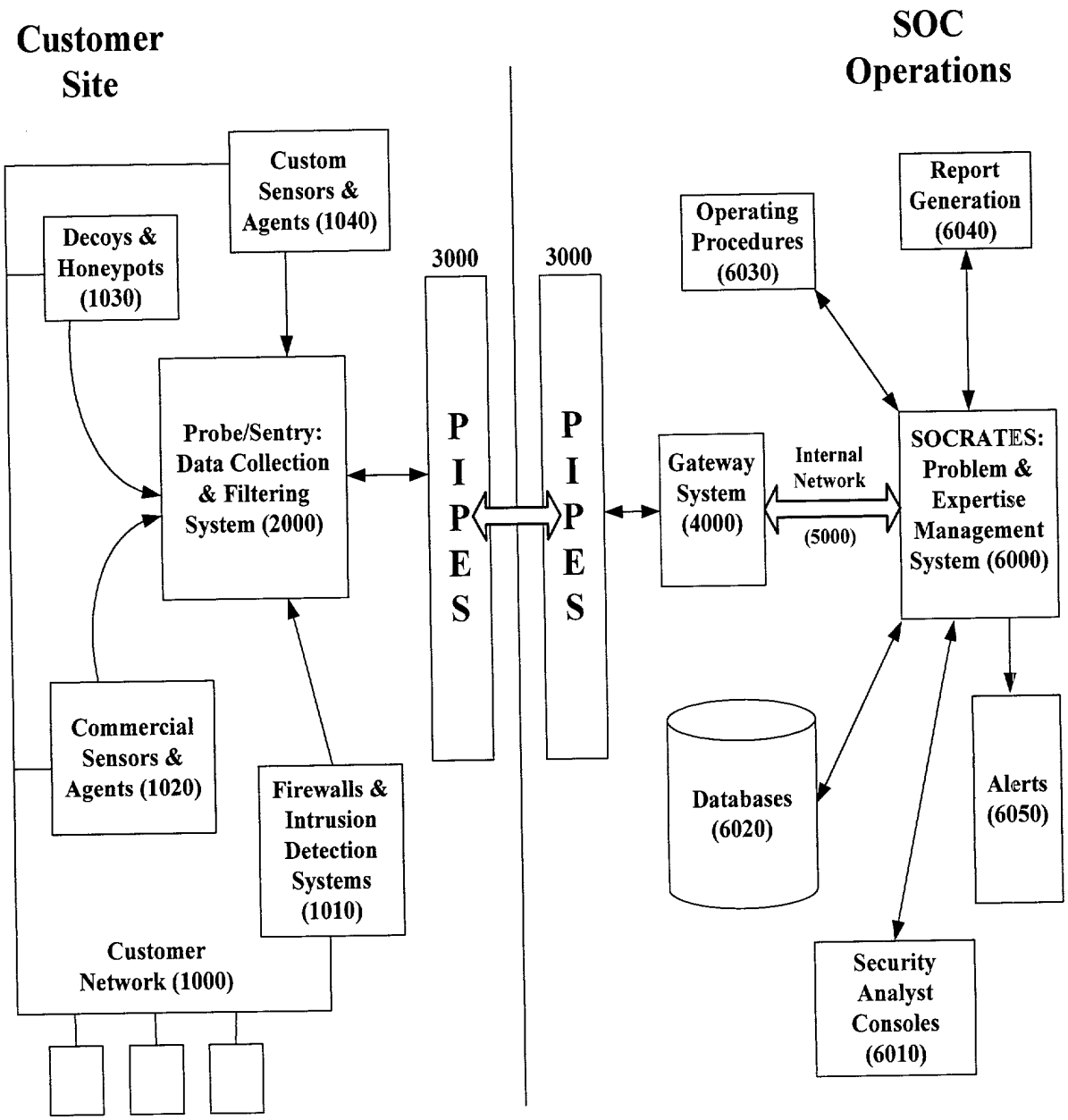


FIG. 2 - Probe/Sentry System Overview

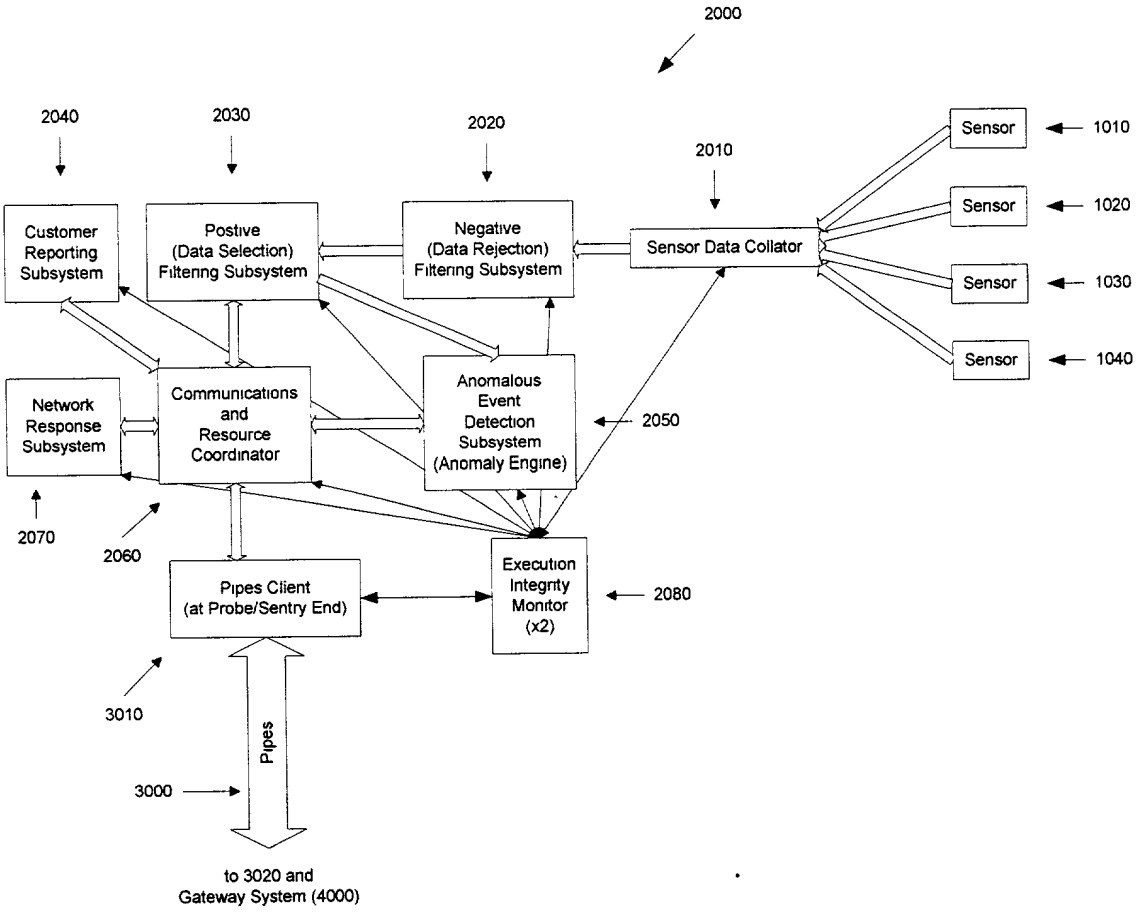


FIG. 3 - Gateway System Overview

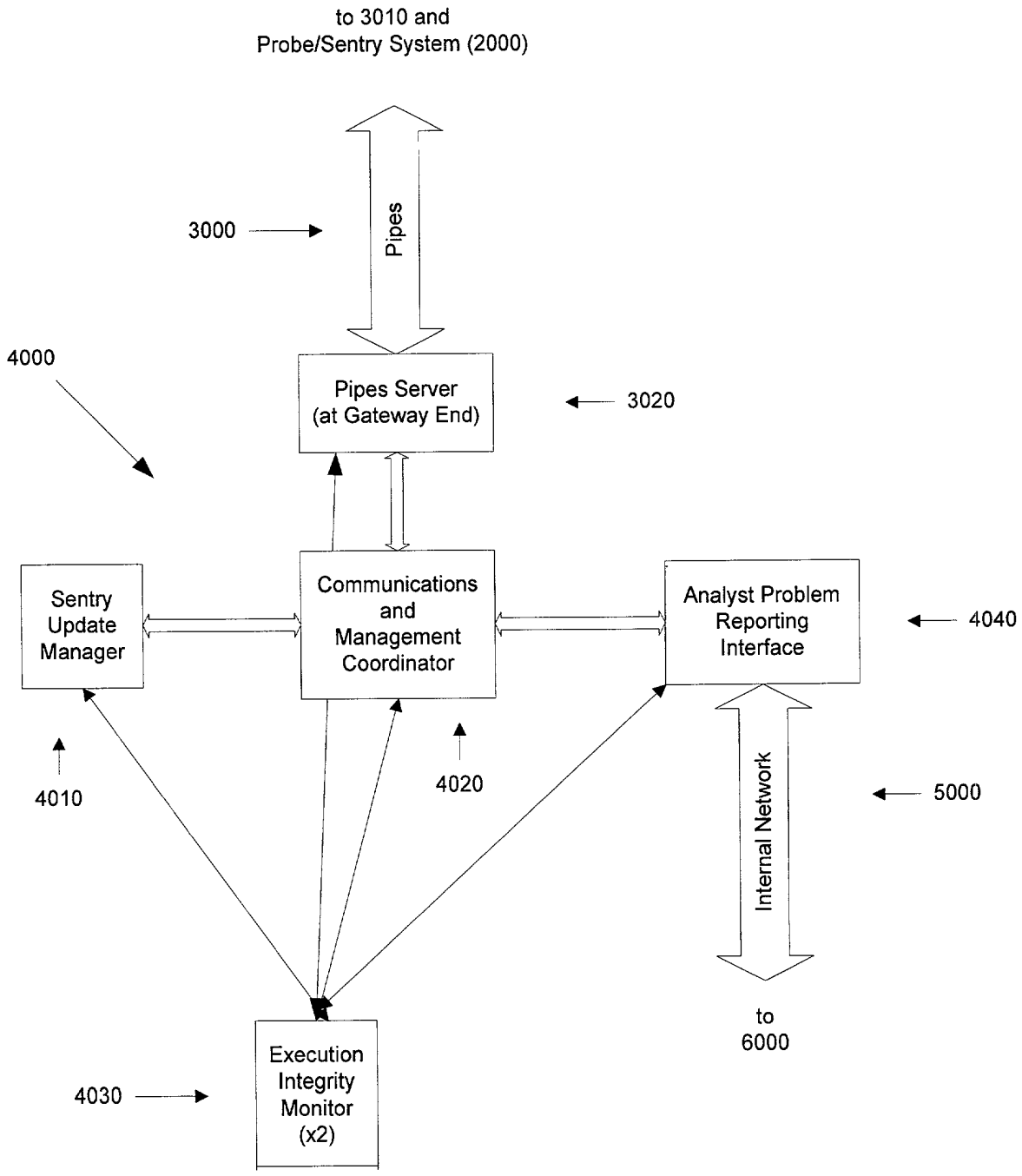


FIG. 4 - SOCRATES System Overview

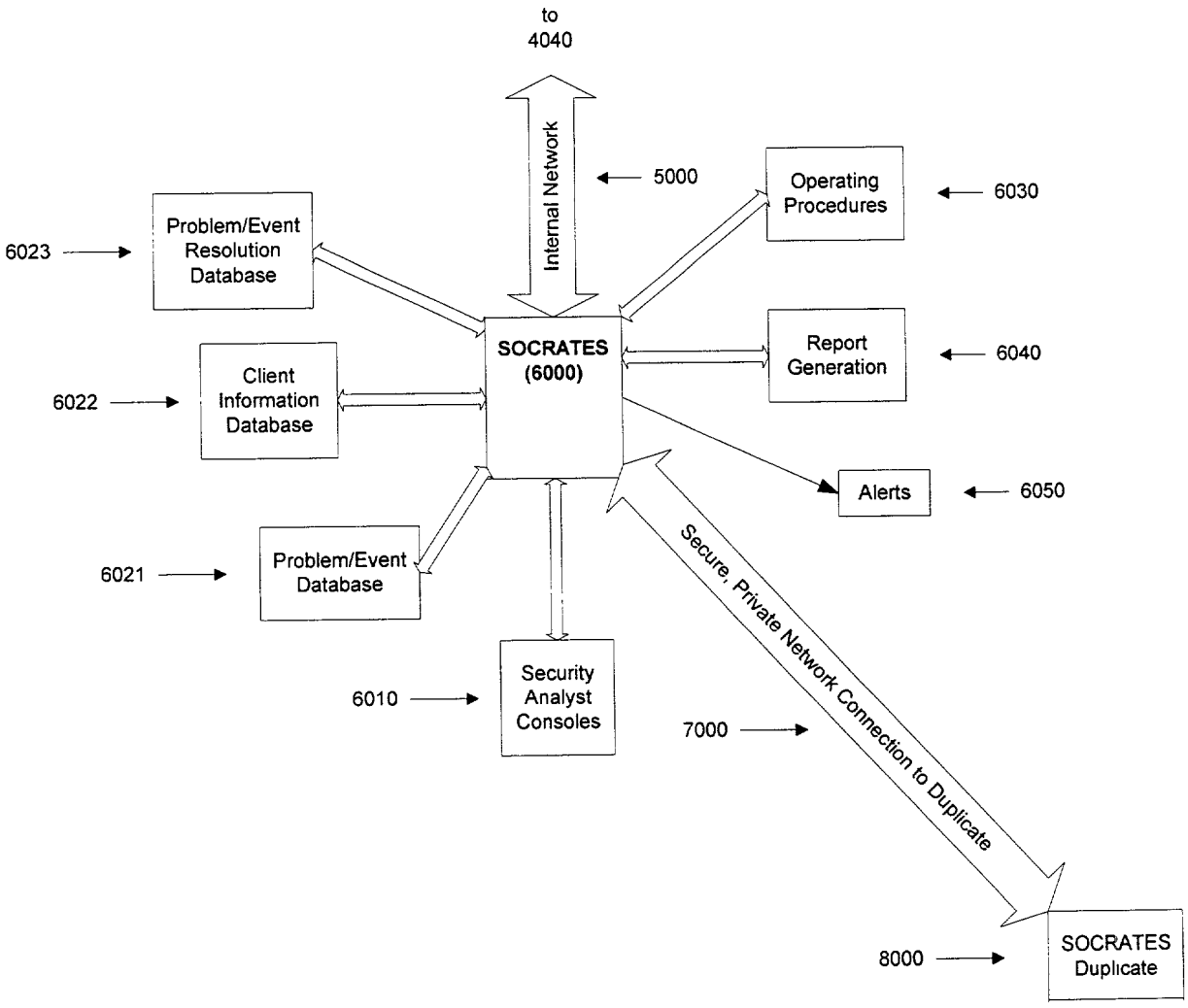


FIG. 5 - Incident Handling

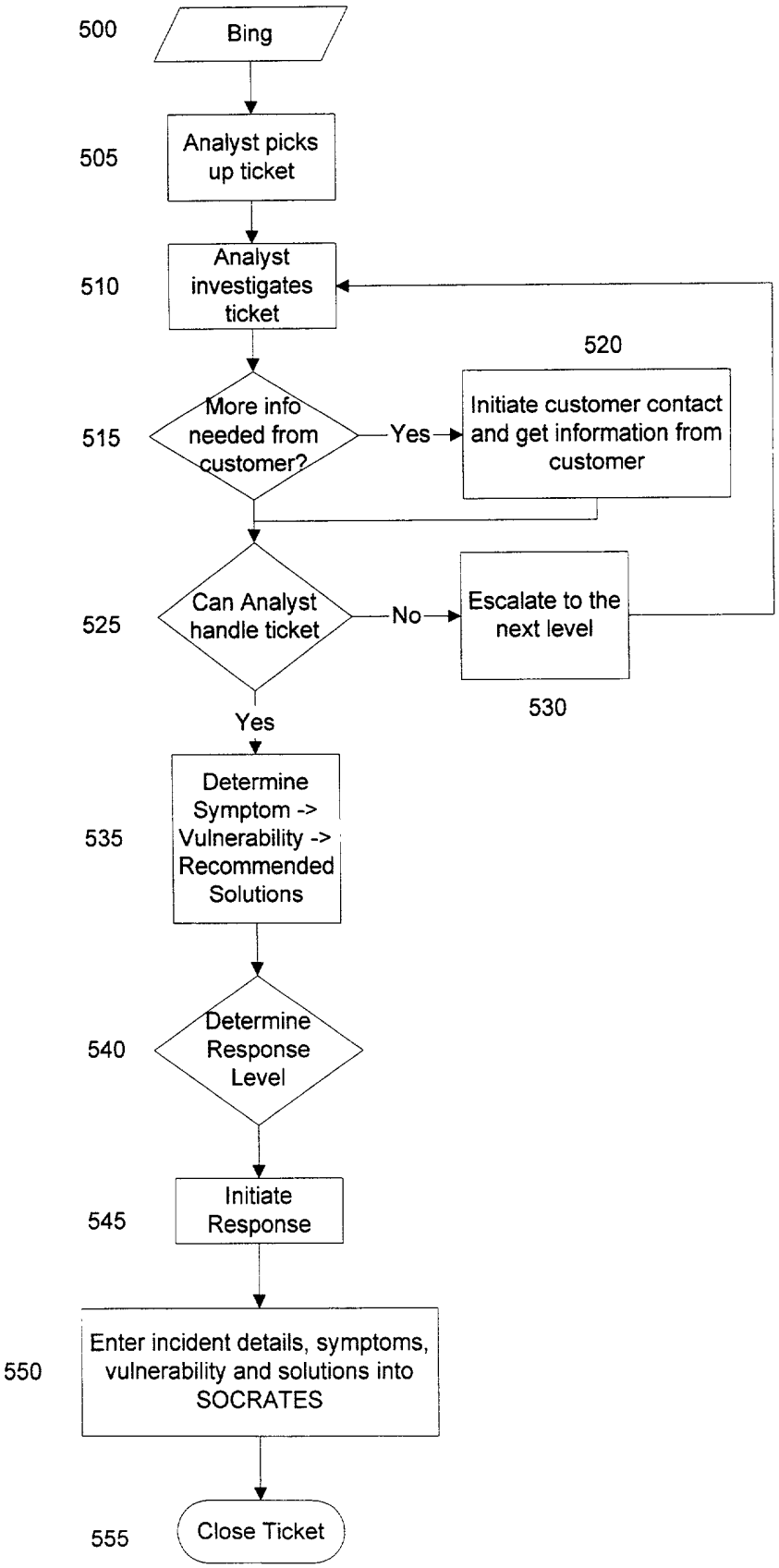
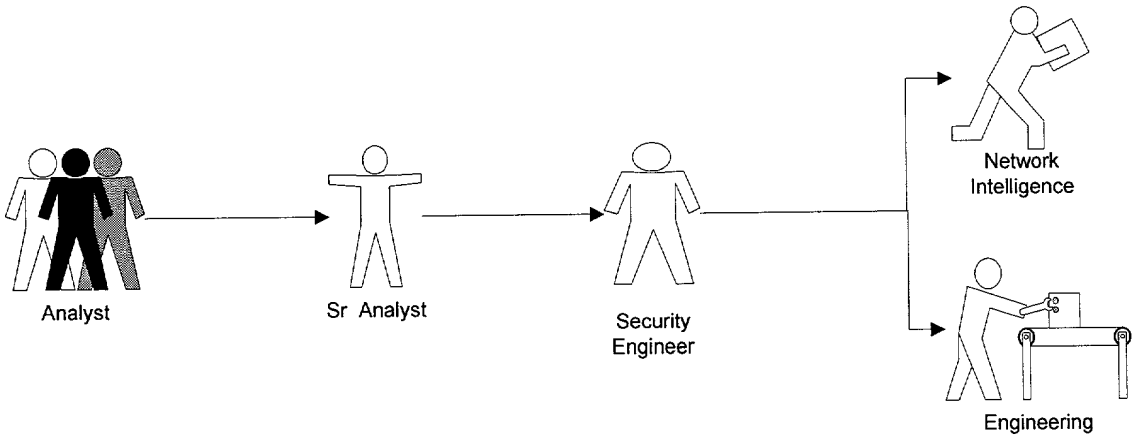
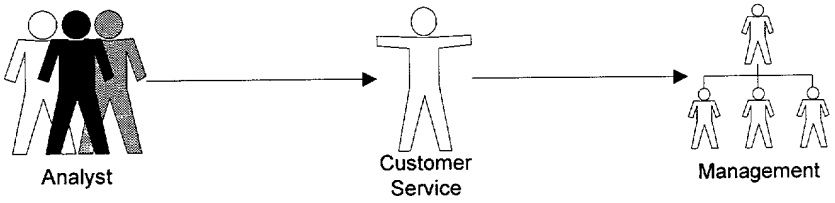


FIG. 6 - Escalation

Incident Escalation:



Customer Service Escalation:



Technical Support Escalation:

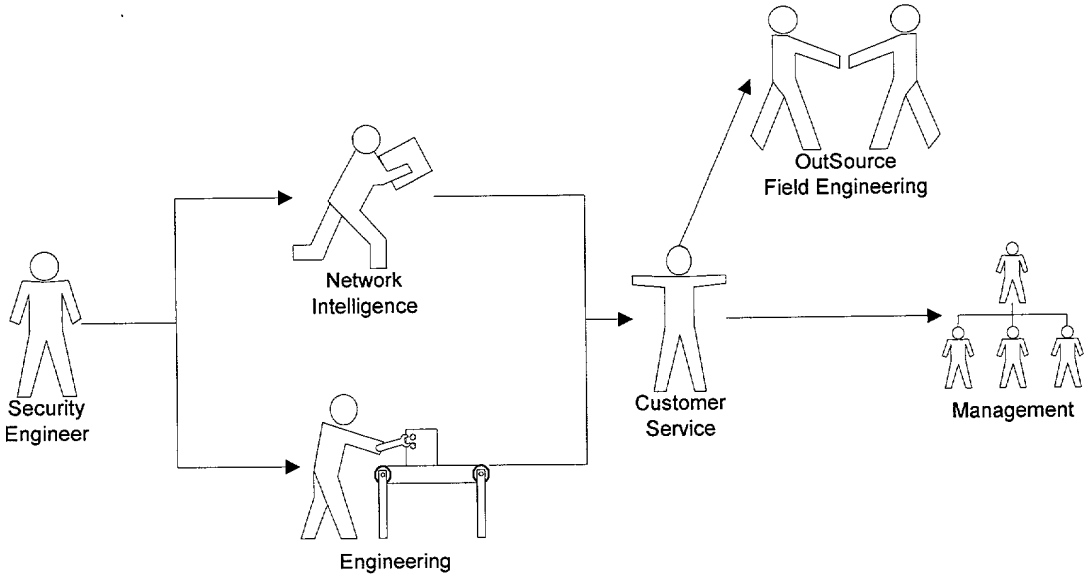


FIG. 7 - Call Handling Procedure (Existing Ticket)

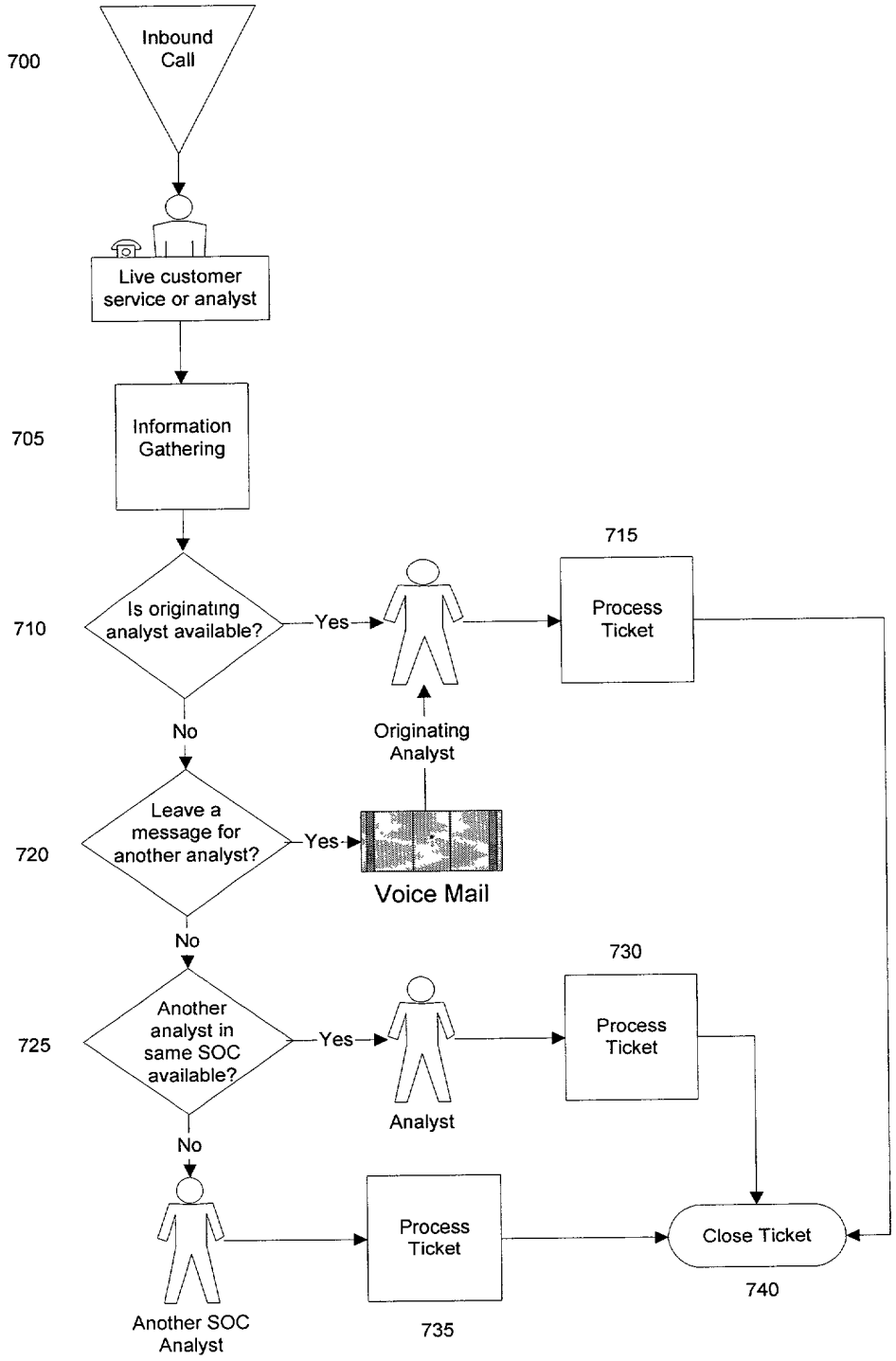


FIG. 8 - Call Handling Procedure (Customer Cold Call)

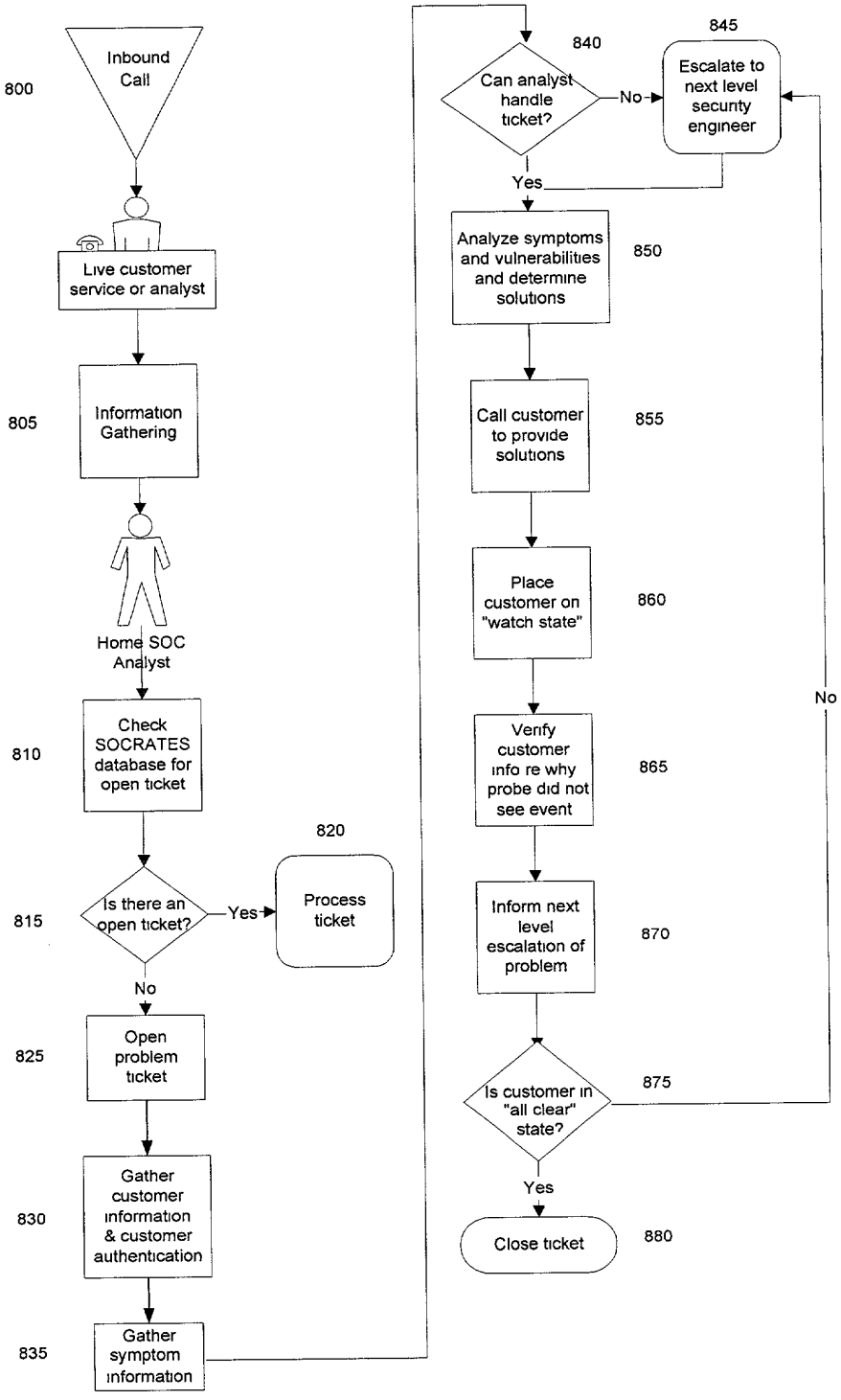
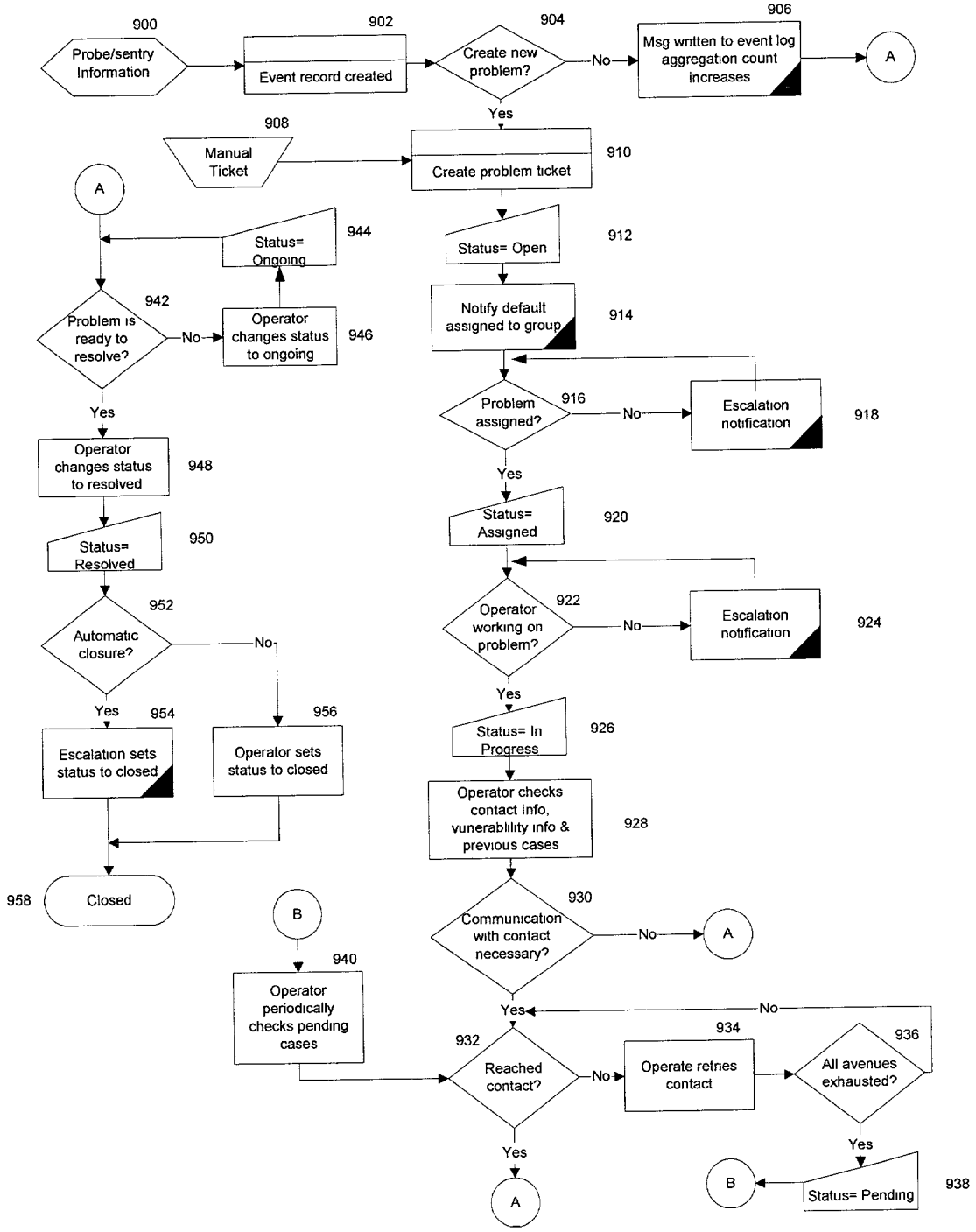


FIG. 9 - Problem Workflow



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 _____ as United States Application No. or PCT International Application Number _____

and was amended on _____

(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) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (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 **Bruce Schneier**
Sole or first inventor's signature Date
Residence **101 East Minnehaha Parkway, Minneapolis, MN 55419**
Citizenship **U.S.A.**
Post Office Address **same as above**

Full name of second inventor, if any **Andrew H. Gross**
Second inventor's signature Date
Residence **1055 Coleman Road, #2309, San Jose, CA 95123**
Citizenship **U.S.A.**
Post Office Address **same as above**

Full name of third inventor, if any **Jonathan D. Callas**
Third inventor's signature Date
Residence **1781 Wema Way, San Jose, CA 95124**
Citizenship **U.S.A.**
Post Office Address **same as above**

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

Doc Code: SB/59.0

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

"001f 0000 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

0052

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

0053

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.

0054

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 ContactA1-B10	Char 15, 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 For Unknown Victim For Known Victim 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, HardwareName	Char 15, Char 255	Pointer into Technology table representing the Hardware for this device.
ProductID, ProductName	Char 15, Char 255	Pointer into Technology table representing the Product for this device.
OSID, OSName	Char 15, 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, 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.

0062

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.

Oracle Exhibit 1045 - Page 0063

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, Reoccuring 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.
1st Symptom ID	Char 45	Pointer into the Symptom table to the most relevant Symptom.
1st Symptom Name	Char 65	Name of the above Symptom
Diagnoses with the above symptom	Table	A table of all Diagnoses that are linked to 1st 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.

0064

Room, Cage, Region, Site, Street Number, Street Name, Other Street Info, City, State, Country, Zip Code, Hardware, 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, published, updated, remote, local, Vulnerable, Not Vulnerable, Credit, Discussion, Exploit, Reference, Solution	Char	SecurityFocus.com defined information fields as described in http://www.securityfocus.
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 For Unknown Victim For Known Victim For Mission Critical Victim	Drop-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, Char 255	Pointer to the Symptom record.
Technology ID Technology Name	Char 15, 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, Char 128	Pointer to Company table indicating the vendor of this Technology.
Product Number, Description, Supplier Name, Manufacturer 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. 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, Vulnerability Name	Char 30, Char 255	Pointer to the Vulnerability record.
Technology ID, Technology Name	Char 15, Char 255	Pointer to the Technology record.
Relationship	Drop-Down List	Possible values: Confirmed Unrelated, "Low" Relationship, "Medium" Relationship, "High" Relationship, Confirmed Relationship.

DRAFT SECURE SOCKETS LAYER

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:DTDisplayPersonRecord	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, SOC:INOSName, 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:TOGenerateToolNameFrom Cat	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 FindSecurityFocusVulnerabilty 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:PRSetSentryEventProble mID	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

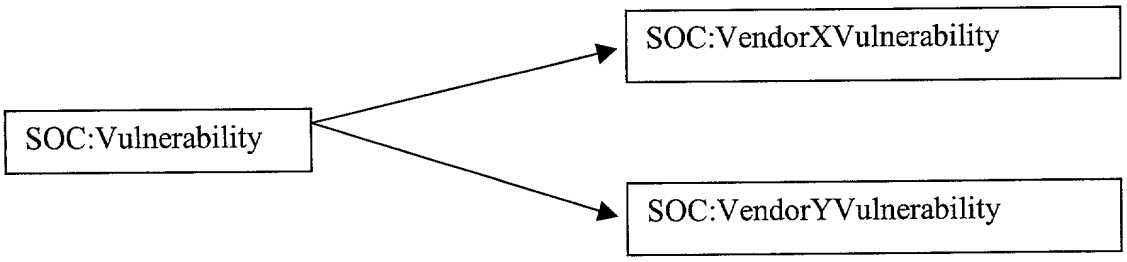
Name	Description
SOC:Category1	A list of categories describing this level of a specific Technology.
SOC:Category2	A list of categories describing this level of a specific Technology.
SOC:Category3	A list of categories describing this level of a specific Technology.
SOC:Category4	A list of categories 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

Subclass	ISSUE CLASSIFICATION
Class	

PATENT NUMBER

U.S. UTILITY Patent Application

O.I.P.E.	PATENT DATE
SCANNED K&W Q.A.	

APPLICATION NO.	CONT/PRIOR	CLASS	SUBCLASS	ART UNIT	EXAMINER
09/766343	D	713	200	2131	Hayes Jackson

APPLICANTS

Bruce Schneier
Andrew Gross
Jonathan Callas

BEST AVAILABLE COPY

TITLE

Mehtod and system for dynamic network intrusion monitoring detection and response

ISSUING CLASSIFICATION

ORIGINAL		CROSS REFERENCE(S)	
CLASS	SUBCLASS	CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)
INTERNATIONAL CLASSIFICATION			

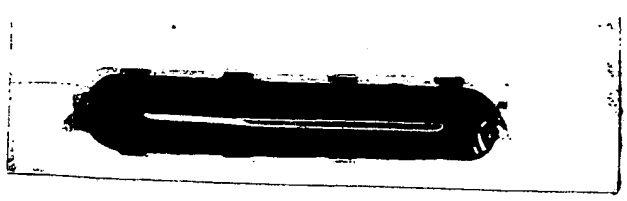
☐ Continued on Issue Slip Inside File Jacket

☐ TERMINAL DISCLAIMER	DRAWINGS			CLAIMS ALLOWED	
	Sheets Drwg.	Figs. Drwg.	Print Fig.	Total Claims	Print Claim for O.G.
☐ The term of this patent subsequent to _____ (date) has been disclaimed.				NOTICE OF ALLOWANCE MAILED	
	(Assistant Examiner)		(Date)		
☐ The term of this patent shall not extend beyond the expiration date of U.S Patent No. _____				ISSUE FEE	
	(Primary Examiner)		(Date)	Amount Due	Date Paid
☐ The terminal ____months of this patent have been disclaimed.				ISSUE BATCH NUMBER	
	(Legal Instruments Examiner)		(Date)		

WARNING:
The information disclosed herein may be restricted. Unauthorized disclosure may be prohibited by the United States Code Title 35, Sections 122, 181 and 368. Possession outside the U.S. Patent & Trademark Office is restricted to authorized employees and contractors only.

Form PTO-436A
(Rev. 6/99)

FILED WITH: ☐ DISK (CRF) ☐ FICHE ☐ CD-ROM
(Attached in pocket on right inside flap)



BEST AVAILABLE COPY

SEARCHED

Class	Sub.	Date	Exmr.
713	200	3/8/04	SS
1	201		
709	208		
	220		
	223		
	224		
	225		
	229		

INTERFERENCE SEARCHED

Class	Sub.	Date	Exmr.

SEARCH NOTES
(INCLUDING SEARCH STRATEGY)

	Date	Exmr.
Examiner Searched	3/8/04	SS
Proquest		
Dialog		
East		
hot bot		
Lycos		
Waybach Machine		
Related Application PCT US02/17602	done 7/19/03	
done by SS		

ISSUE SLIP STAPLE AREA (for additional cross references)

POSITION	INITIALS	ID NO.	DATE
FEE DETERMINATION			
O.I.P.E. CLASSIFIER	PMR	32	2/27
FORMALITY REVIEW	SG	1077	4/25/01
RESPONSE FORMALITY REVIEW		1691	6-12-01

INDEX OF CLAIMS

✔	Rejected	N	Non-elected
=	Allowed	I	Interference
—	(Through numeral)... Canceled	A	Appeal
÷	Restricted	O	Objected

Claim		Date
Final	Original	
	1	3/15/04
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

If more than 150 claims or 10 actions staple additional sheet here

BEST AVAILABLE COPY

01/022/01

A

JC639 U.S. PTO 01/19/01

JC878 U.S. PTO 09/766343 01/19/01

Please type a plus sign (+) inside this box → +

PTO/SB/05 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	028490-0007
First Inventor	B. Schneier et al.
Title	Method and System for Dynamic Network Intrusion Monitoring, Detection and Response
Express Mail Label No.	EK 447 202 148 US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [X] Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. [ ] Applicant claims small entity status. See 37 CFR 1.27.
3. [X] Specification [*Total Pages* 58] *(preferred arrangement set forth below)*
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. [X] Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 9]
5. Oath or Declaration [*Total Pages* 4]
   a. [X] ~~Newly executed (original or copy)~~ unexecuted
   b. [ ] Copy from a prior application (37 CFR 1.63 (d)) *(for continuation/divisional with Box 18 completed)*
      i. [ ] DELETION OF INVENTOR(S)
      Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [ ] Application Data Sheet. See 37 CFR 1.76

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

7. [ ] CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] paper
   c. [ ] Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. [ ] Assignment Papers (cover sheet & document(s))
10. [ ] 37 CFR 3.73(b) Statement *(when there is an assignee)* [X] Power of Attorney unexecuted
11. [ ] English Translation Document *(if applicable)*
12. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
13. [ ] Preliminary Amendment
14. [X] Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. [ ] Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. [ ] Request and Certification under 35 U.S.C. 122 (b)(2)(B)(i). Applicant must attach form PTO/SB/35 or its equivalent.
17. [ ] Other: .....

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No.: _____/_____

Prior application information: Examiner _____ Group Art Unit: _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

19. CORRESPONDENCE ADDRESS

[ ] *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* or [X] *Correspondence address below*

Name	Robert B. Beyers, Ph.D.				
Address	Skadden, Arps, Slate, Meagher & Flom LLP				
	525 University Avenue				
City	Palo Alto	*State*	CA	*Zip Code*	94301
Country	U.S.A.	*Telephone*	650 470-4500	*Fax*	470-4570

Name (Print/Type)	Robert B. Beyers, Ph.D.	*Registration No.(Attorney/Agent)*	46,552
Signature	Robert B. Beyers	*Date*	Jan. 19, 2001

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

PTO/SB/17 (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

FEE TRANSMITTAL for FY 2001

Patent fees are subject to annual revision.

TOTAL AMOUNT OF PAYMENT ($) 1,142.00

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	B. Schneier et al.
Examiner Name	
Group Art Unit	
Attorney Docket No.	028490-0007

jc676 U.S. PTO 09/766343 01/19/01

METHOD OF PAYMENT

1. [XX] The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:
   Deposit Account Number: 19-2385
   Deposit Account Name: Skadden, Arps et al.
   [X] Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17
   [ ] Applicant claims small entity status. See 37 CFR 1.27
2. [X] **Payment Enclosed:** [X] Check [ ] Credit card [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	710	201	355	Utility filing fee	710
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 710

2. EXTRA CLAIM FEES

		Extra Claims	Fee from below	Fee Paid
Total Claims	44	-20** = 24	X 18	= 432
Independent Claims	3	- 3** = 0	X 80	= 0
Multiple Dependent				= 0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 432

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for *ex parte* reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Processing fee under 37 CFR 1.17(q)	
126	180	126	180	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

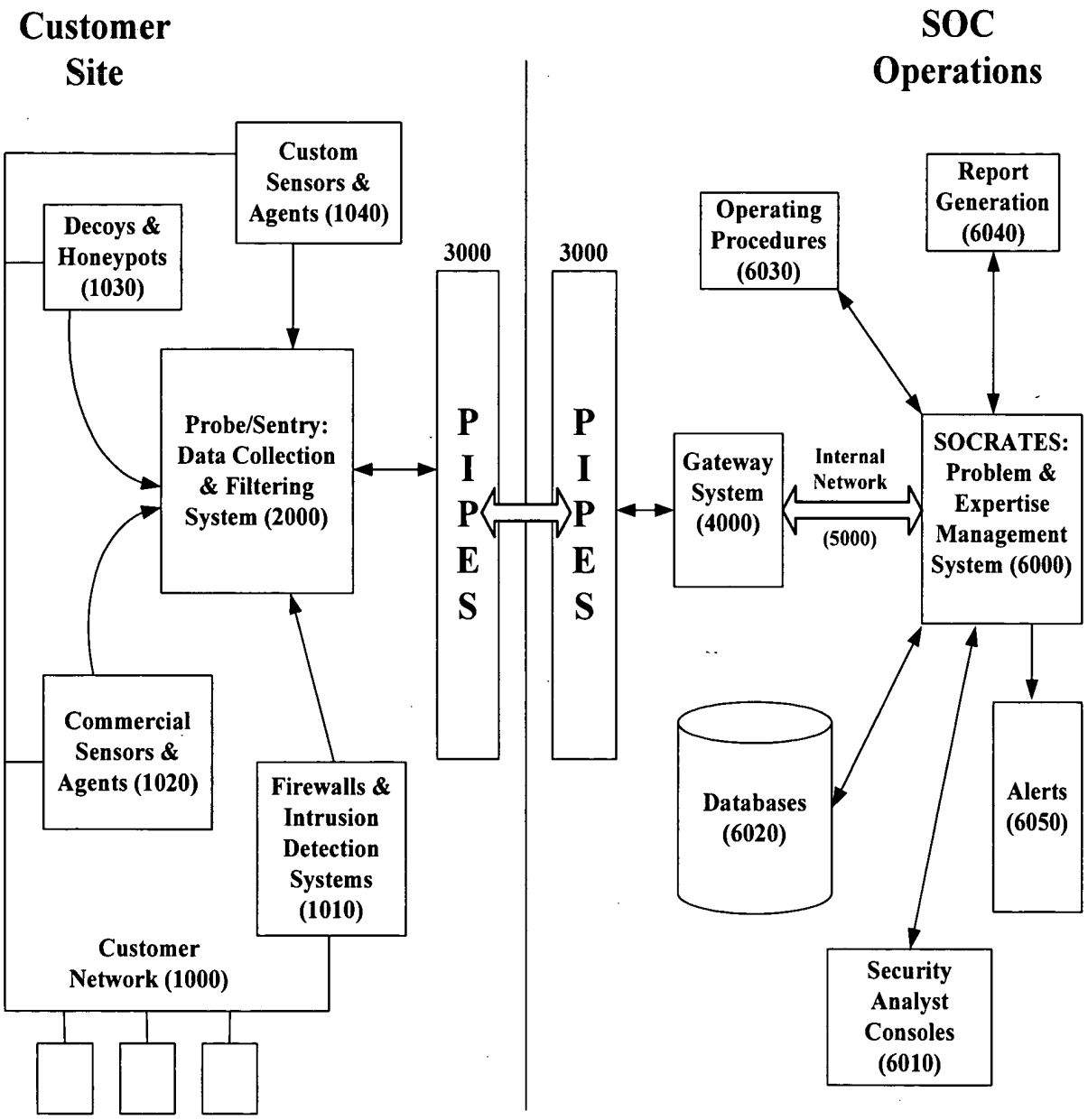
SUBTOTAL (3) ($) 0

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Robert B. Beyers, Ph.D.	Registration No. (Attorney/Agent)	46,552	Telephone	650 470-4500
Signature	Robert Beyers			Date	Jan. 19, 2001

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.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

FIG. 1 - Architectural Diagram



Fortinet Exhibit 1003

FIG. 2 - Probe/Sentry System Overview

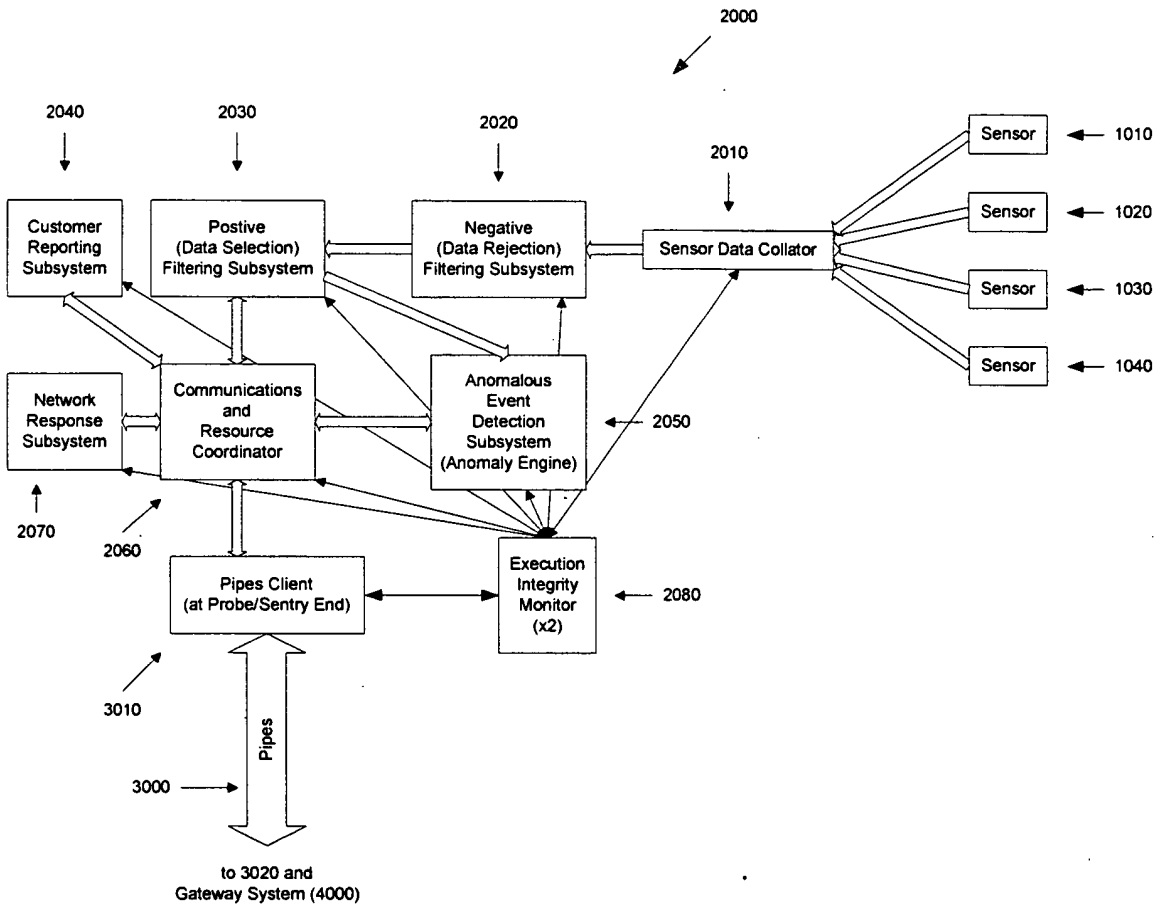


Exhibit 2005, Page 9 of 9

FIG. 3 - Gateway System Overview

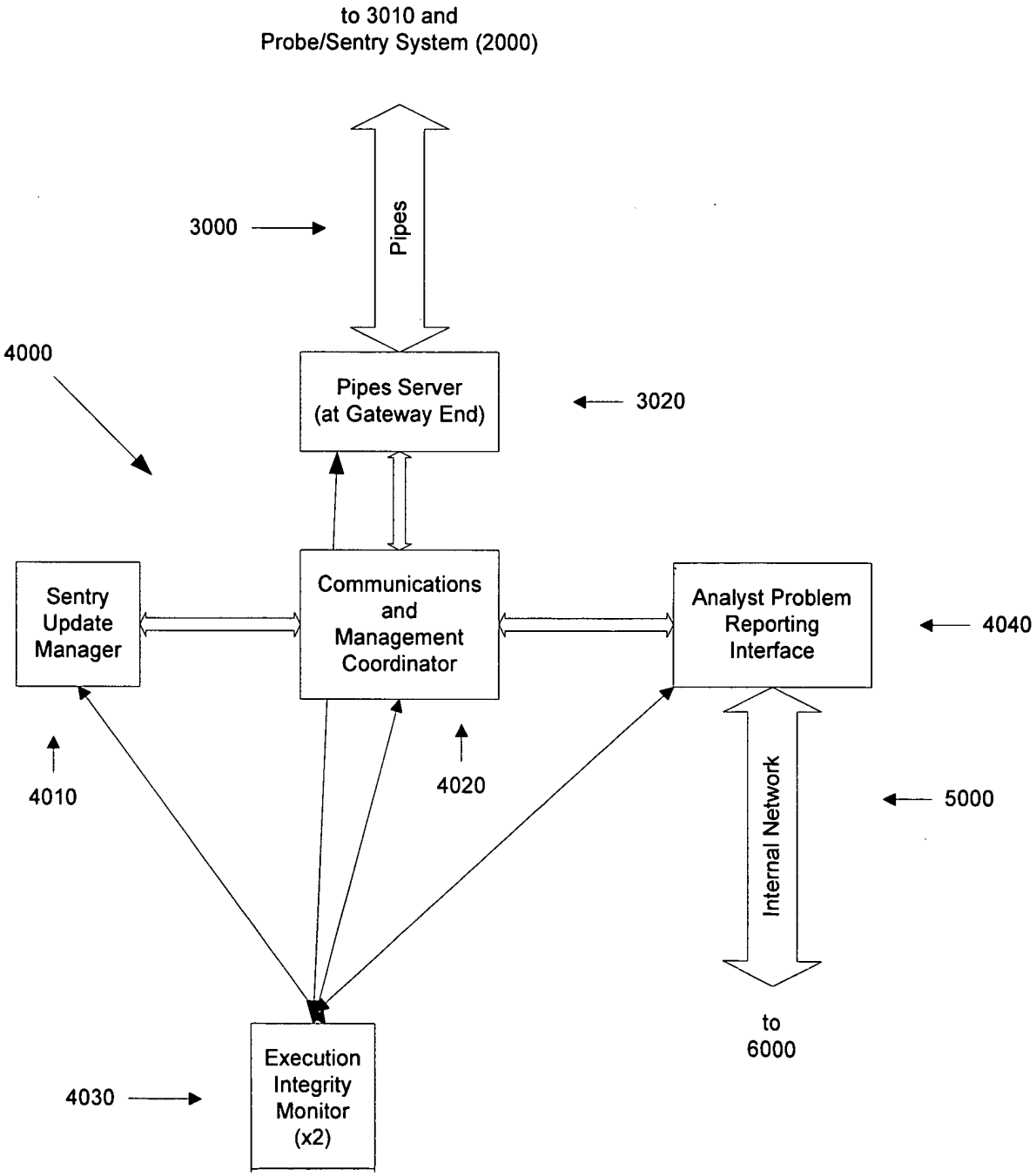
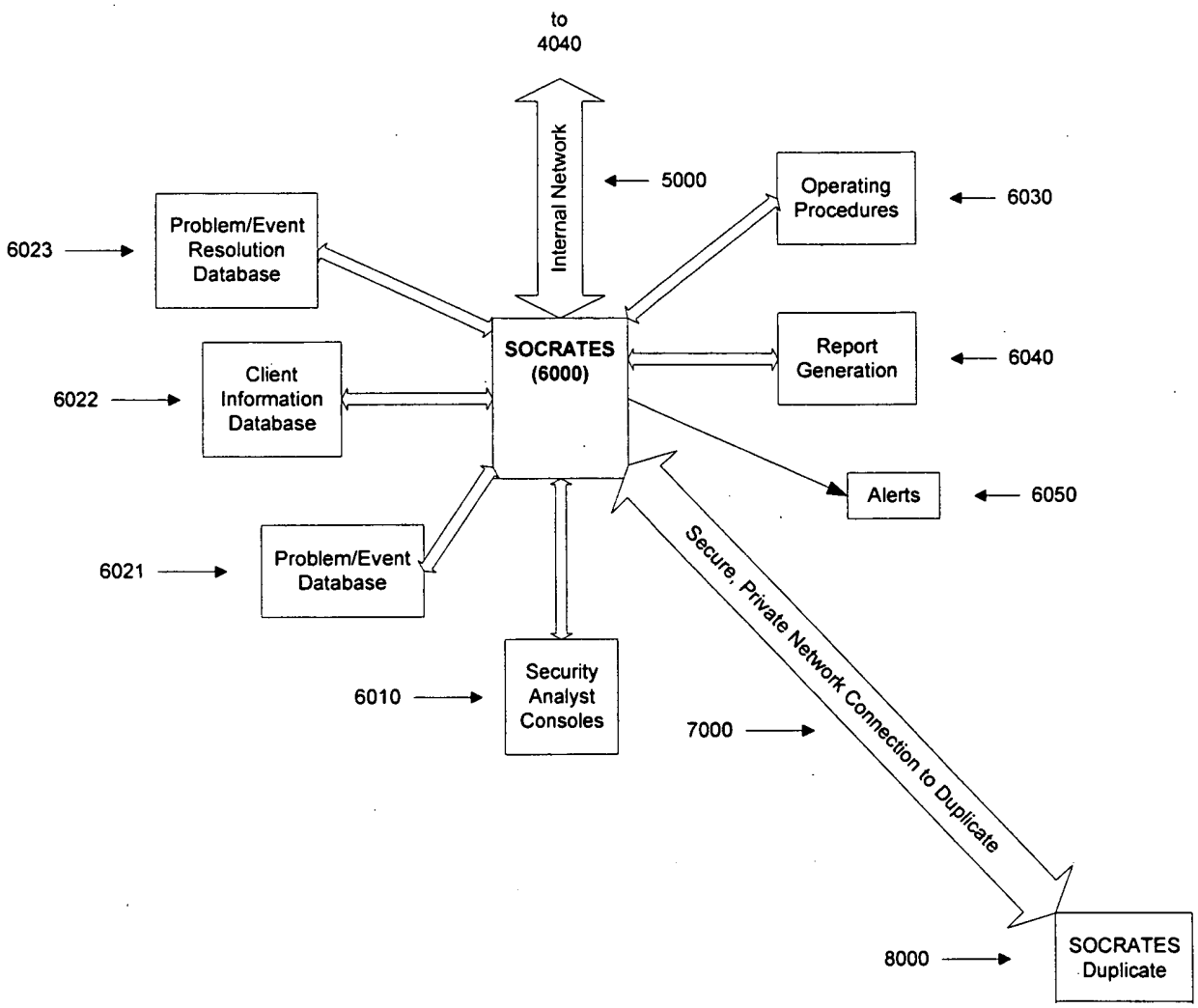
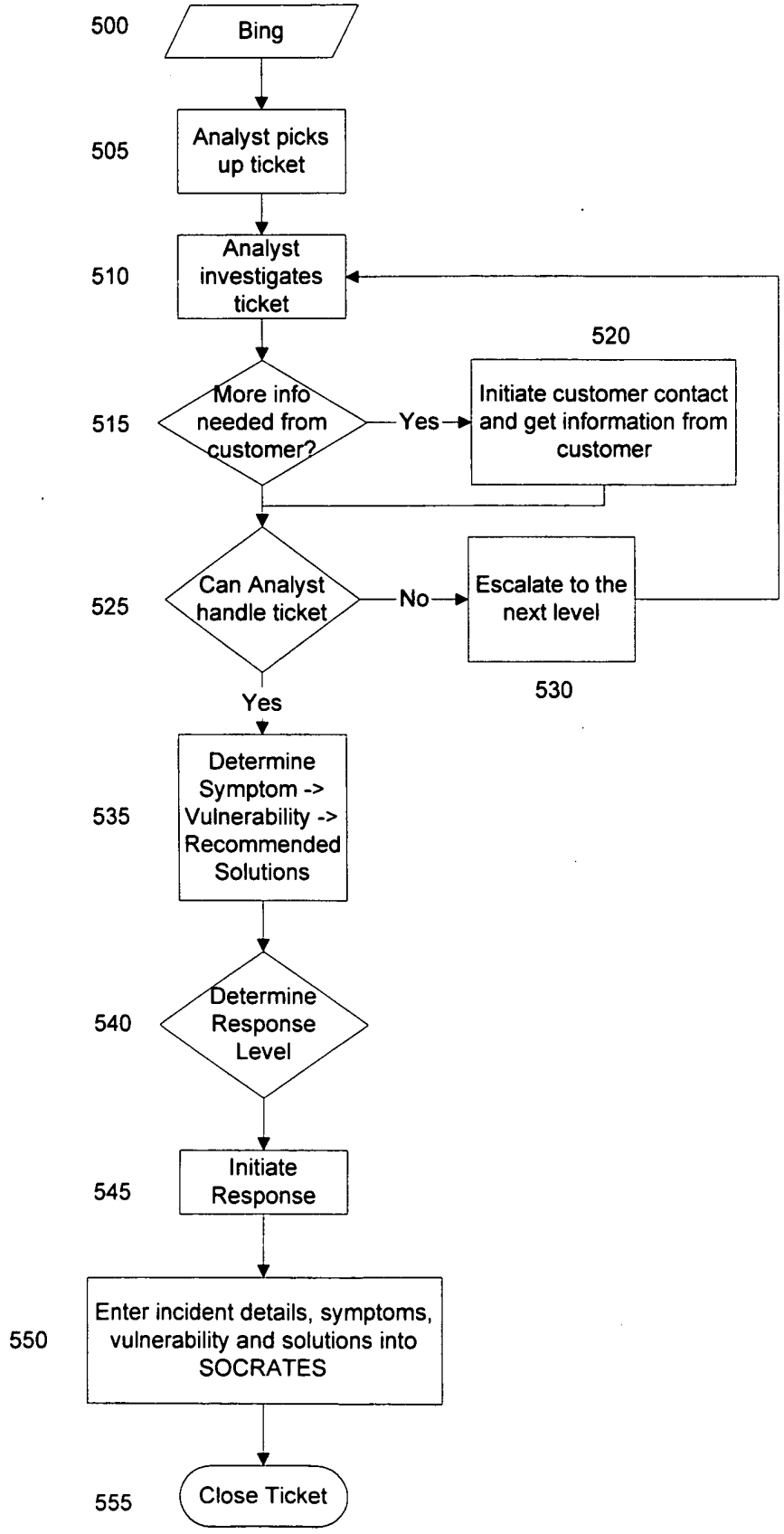


FIG. 4 - SOCRATES System Overview



1056T4.6465.60

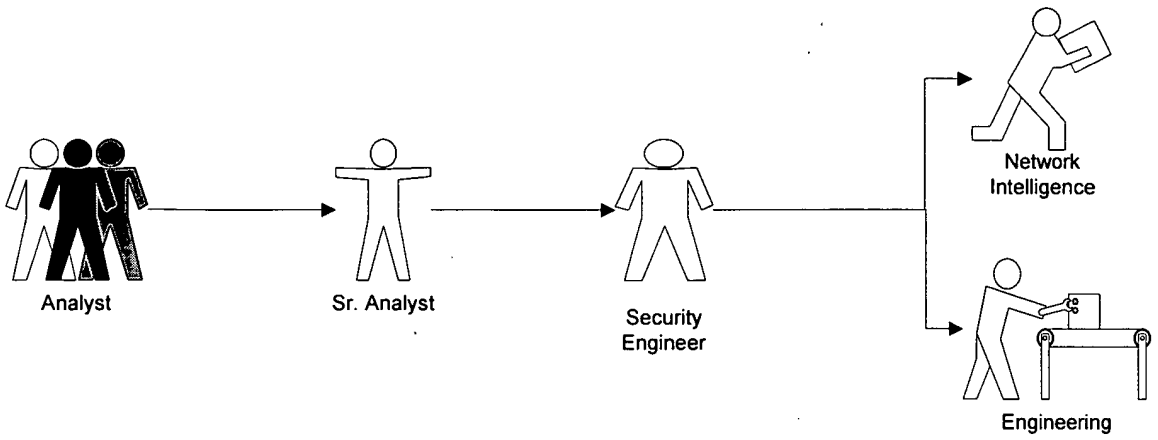
FIG. 5 - Incident Handling



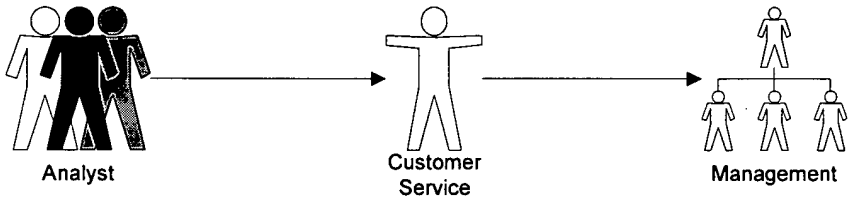
Confidential

FIG. 6 - Escalation

Incident Escalation:



Customer Service Escalation:



Technical Support Escalation:

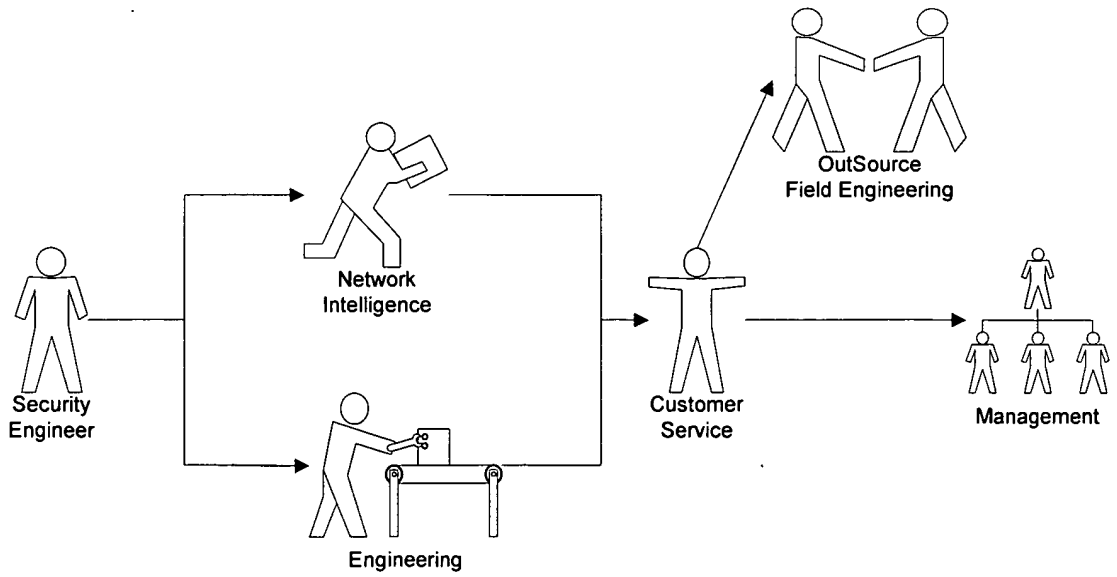


FIG. 7 - Call Handling Procedure (Existing Ticket)

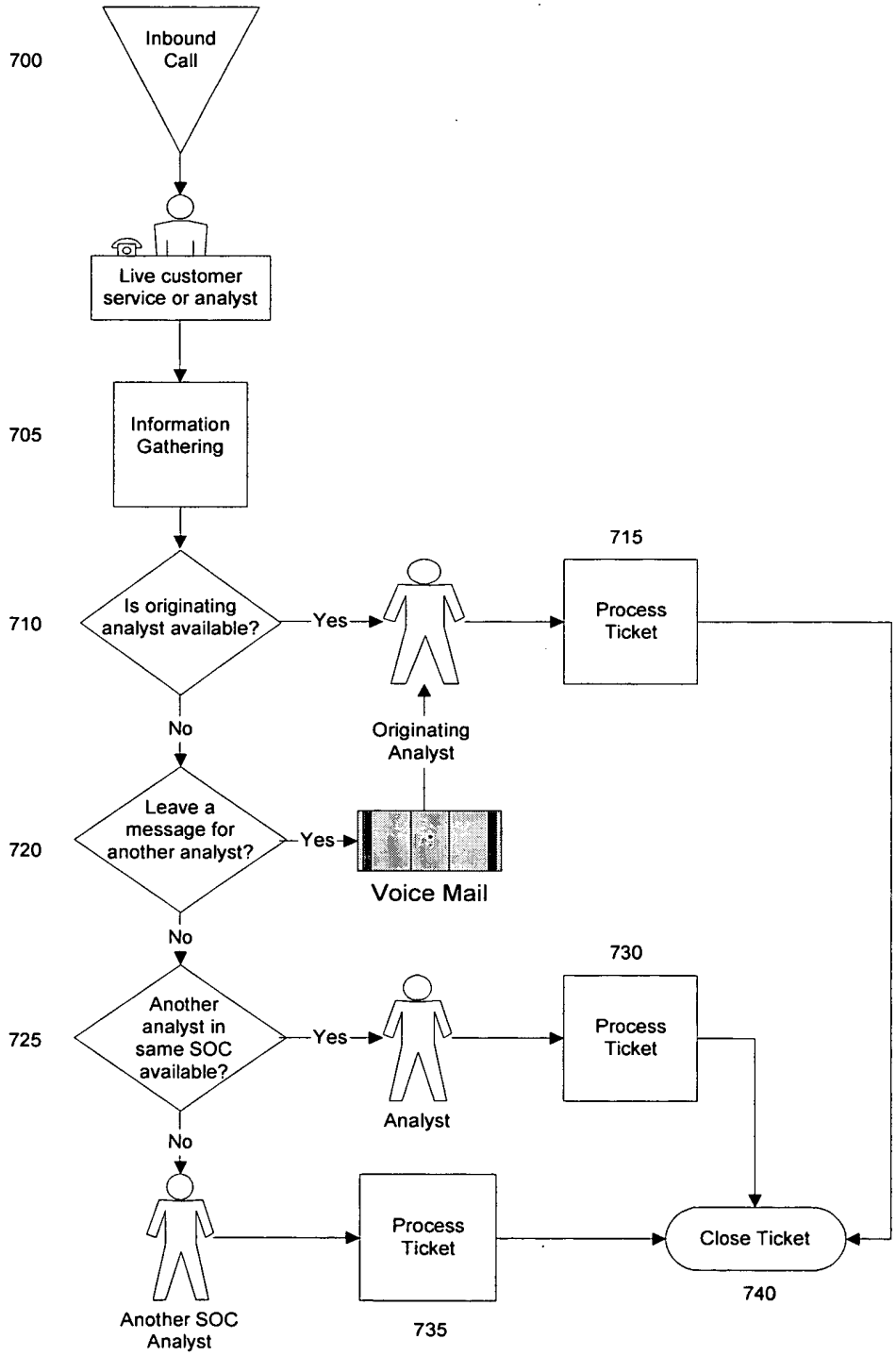
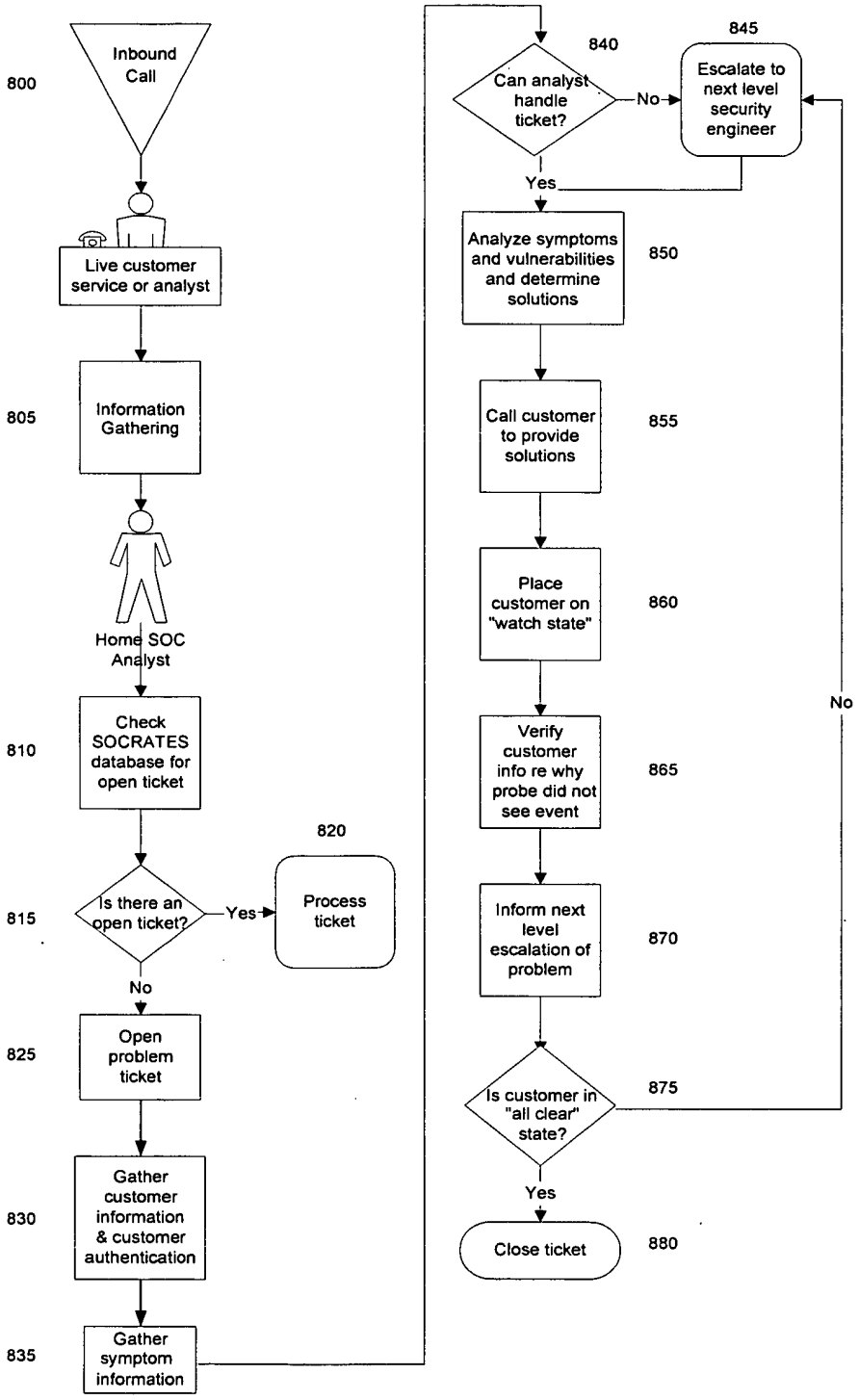
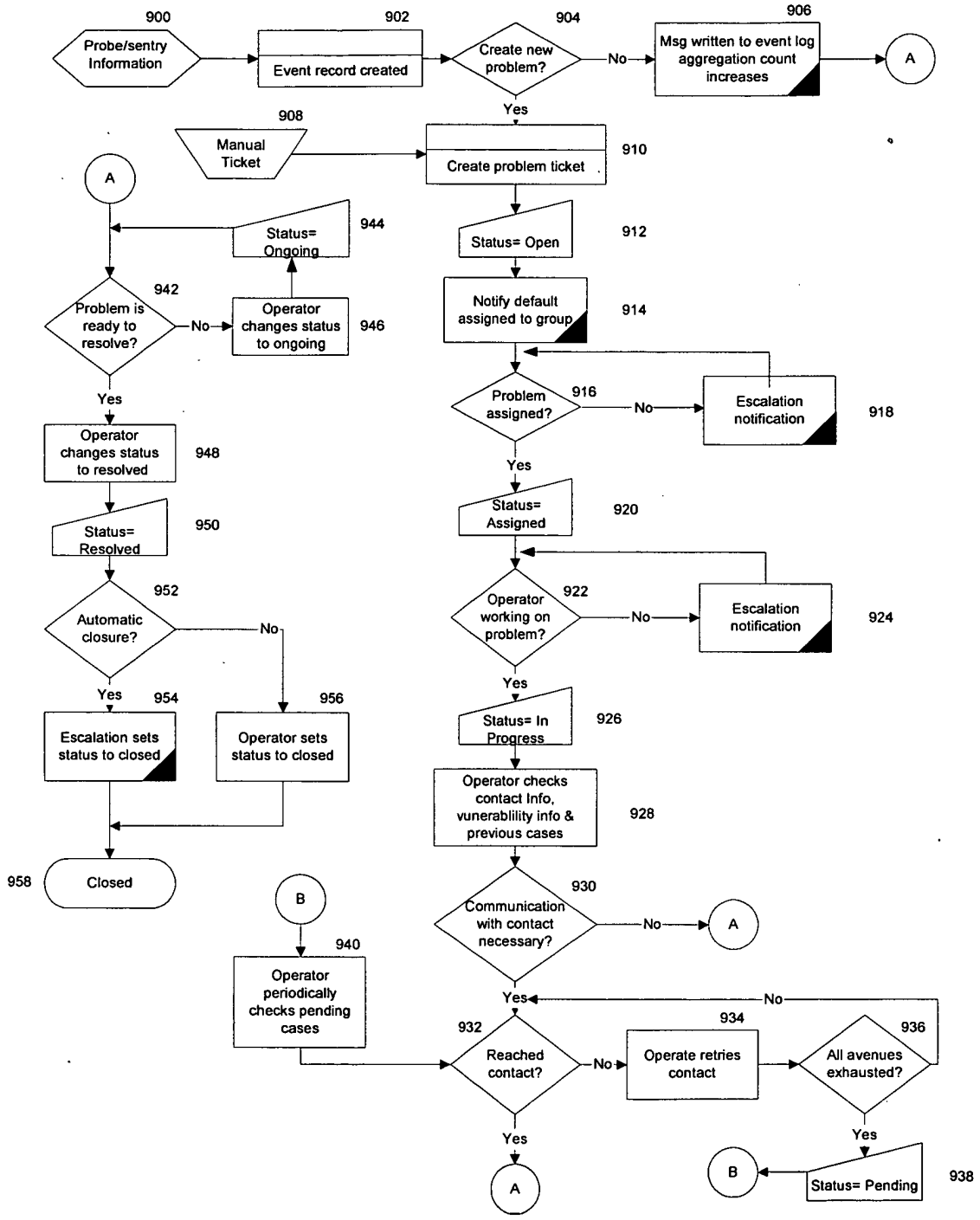


FIG. 8 - Call Handling Procedure (Customer Cold Call)



Patent Application Publication Sep. 25, 2003 Sheet 8 of 9 US 2003/0182420 A1

FIG. 9 - Problem Workflow



Our Ref. No.: 028490-0007

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

Inventors:

Bruce Schneier
Andrew H. Gross
Jonathan D. Callas

Prepared by:
Joseph Yang, Ph.D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
(650) 470-4500

I hereby certify that this correspondence is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" under 37 CFR § 1.10 (Label No. EK 447 202 148 US) in an envelope addressed to: Assistant Commissioner for Patents, Box Patent Application, Washington, D.C. 20231, on January 19, 2001.

Jan Steele

(Signature)

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

FIELD OF THE INVENTION

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

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.

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.

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.

SUMMARY OF THE INVENTION

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).

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.

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.

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 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.

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

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.

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 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.

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 SOCs 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 SOCs can be used to provide redundancy and additional capacity for increased traffic or failure of one of the SOCs.

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.

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.

F. The "SOCRATES" Problem and Expertise Management System: In an exemplary embodiment, security analysts at a SOC work in concert with the "SOCRATES"[1] 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 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 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.

Express Mail No. EV 339 054 405 US

BRIEF DESCRIPTION OF THE FIGURES AND APPENDICES

FIG. 1 is an overview of the system architecture of an exemplary embodiment of the present invention.

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

---

[1] "SOCRATES" is an acronym standing for Secure Operations Center Responsive Analyst Technical Expertise System.

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

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.

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

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

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 exemplary embodiment of the present invention.

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.

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

Appendix A provides specific details pertaining to an exemplary system for the transfer of information between customer networks and gateway systems (the "Pipes Protocol").

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

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

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.

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.

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") 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 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.

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 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 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**.

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.

In a preferred embodiment, Pipes **3000** provides an encrypted, secure 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.

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 ("PKI") 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.

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.

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.

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

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

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.

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.

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).

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.) 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**.)

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.

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.

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.

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 **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 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 are examples of data discrimination analyses, other types of which are well-known to those skilled in the art.

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 (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 **2060** can also monitor a "heartbeat" passing between probe/sentry system **2000** and gateway system **4000**.

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.

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 authenticated, can view such pages using any browser.

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 a "fix" might be sufficient to stop a transient attack, such as someone repeatedly trying to log in to the customer's network.

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.

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 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**.

FIG. 4 is a system overview of an exemplary embodiment of a "SOCRATES" problem and expertise management system. The SOCRATES system is a consolidated 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;
- access and authority management;

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

In an exemplary implementation, processing of gateway messages by SOCRATES **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**.

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**.

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.

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.

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.)

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.

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.

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.

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;
- generating a report for the problem; and
- incrementing or decrementing the priority of the problem.

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.

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.

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).

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 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**).

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 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 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 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 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 problem and whether the customer is now in an "all clear" state. If yes, in step **880**, the ticket can be closed.

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.

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 the 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.

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**.

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.

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.

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.

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.

Modifications, Enhancements and Alternate Embodiments

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.

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.

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

FOSTER: 5469760

CLAIMS

What is claimed is:

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

    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.

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

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

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

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

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

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

8. The method of claim 1, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

9. The method of claim 8, wherein said identifying step includes cross-correlating data across said monitored components.

10. The method of claim 8, wherein said identifying step includes analyzing the frequency of occurrence of said events.

11. The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.

12. The method of claim 11, wherein said computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

13. The method of claim 11, wherein said identifying step includes cross-correlating data across said monitored components.

14. The method of claim 11, wherein said identifying step includes analyzing the frequency of occurrence of said events.

15. The method of claim 11, wherein said computer-based analysis includes cross-probe correlation.

16. The method of claim 1, further comprising instantaneously self-tuning said probe based on previously collected status data.

17. The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

18. The method of claim 1, wherein said receiving feedback step occurs in substantially real time.

19. A computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by 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.

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

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

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

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

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

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

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

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

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

37. A security monitoring system for a computer network, comprising

a) a plurality of sensors for monitoring components of said network;

b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and

c) at least one probe, wherein said probe is configured to

(1) collect status data from at least one sensor monitoring at least one component of said network;

(2) identify potentially security-related events pertaining to said network by analyzing said status data;

(3) transmit information about said identified events to an analyst associated with said secure operations center;

(4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system in a manner customized to said network; and

(5) dynamically modify an analysis capability of said probe during operation thereof based on said received feedback in a manner customized to said network.

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

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

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

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

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

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

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

Date: 03/05/2004

ABSTRACT

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.

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 _____ as United States Application No. or PCT International Application Number _____

and was amended on _____

(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) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (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.

PTO/SB/01 (6-95)

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 **Bruce Schneier**
Sole or first inventor's signature Date
Residence **101 East Minnehaha Parkway, Minneapolis, MN 55419**
Citizenship **U.S.A.**
Post Office Address **same as above**

Full name of second inventor, if any **Andrew H. Gross**
Second inventor's signature Date
Residence **1055 Coleman Road, #2309, San Jose, CA 95123**
Citizenship **U.S.A.**
Post Office Address **same as above**

Full name of third inventor, if any **Jonathan D. Callas**
Third inventor's signature Date
Residence **1781 Wema Way, San Jose, CA 95124**
Citizenship **U.S.A.**
Post Office Address **same as above**

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

Page 4 of 5

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. 7642

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/766,343	01/19/2001 RULE	713	2131	028490-0007

APPLICANTS

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

**** CONTINUING DATA ***************************

This appln claims benefit of 60/190,326 03/16/2000

**** FOREIGN APPLICATIONS *********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
** 04/25/2001

		STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed	☐ yes ☐ no	MN	9	44	3
35 USC 119 (a-d) conditions met	☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged	Examiner's Signature Initials				

#10

ADDRESS
20350

TITLE
Method and system for dynamic network intrusion monitoring, detection and response

FILING FEE RECEIVED	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit
1272		

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 7642

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/766,343	01/19/2001 RULE	713	2131	028490-0007

APPLICANTS

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

**** CONTINUING DATA ***************************

THIS APPLN CLAIMS BENEFIT OF 60/190,326 03/16/2000

**** FOREIGN APPLICATIONS ********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 04/25/2001

		STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed	☐ yes ☐ no	MN	9	44	3
35 USC 119 (a-d) conditions met	☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged	Examiner's Signature Initials				

ADDRESS

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto ,CA 94301

TITLE

Mehtod and system for dynamic network intrusion monitoring detection and response

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1272	No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

0[illegible]/25/2001 SDENBOB1 00000062 09766343

01 FC:101 710.00 OP
02 FC:103 432.00 OP

PTO-1556
(5/87)

*U.S. GPO: 2000-468-987/39595

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2000

Application or Docket Number

CLAIMS AS FILED - PART I

	(Column 1)		(Column 2)
TOTAL CLAIMS	44		
FOR	NUMBER FILED		NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	44 minus 20=	*	24
INDEPENDENT CLAIMS	3 minus 3 =	*	0
MULTIPLE DEPENDENT CLAIM PRESENT			☐

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

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	355.00	OR	BASIC FEE	710.00
X$ 9=		OR	X$18=	432.00
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL		OR	TOTAL	142.00

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. 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.

CLAIMS ONLY

SERIAL NO.	FILING DATE
09766343	

APPLICANT(S)

CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
1	1					
2		1				
3		1				
4		1				
5		1				
6		1				
7		1				
8		1				
9		1				
10		1				
11		1				
12		1				
13		1				
14		1				
15		1				
16		1				
17		1				
18		1				
19	1					
20		1				
21		1				
22		1				
23		1				
24		1				
25		1				
26		1				
27		1				
28		1				
29		1				
30		1				
31		1				
32		1				
33		1				
34		1				
35		1				
36		1				
37	1					
38		1				
39		1				
40		1				
41		1				
42		1				
43		1				
44		1				
45						
46						
47						
48						
49						
50						
TOTAL IND.	3					
TOTAL DEP.	41					
TOTAL CLAIMS	44					

	*		*		*	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						
TOTAL IND.						
TOTAL DEP.						
TOTAL CLAIMS						

*MAY BE USED FOR ADDITIONAL CLAIMS OR ADMENDMENTS

FORM PTO-2022 (1-98)

U.S.DEPARTMENT OF COMMERCE
Patent and Trademark Office

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

"001f 0000 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.

Exhibit 1005 - 36 of 59

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

0135

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.

HE 3975.D54 no.96-2350

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

0137

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.

0139

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 ContactA1-B10	Char 15, 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 For Unknown Victim For Known Victim 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, HardwareName	Char 15, Char 255	Pointer into Technology table representing the Hardware for this device.
ProductID, ProductName	Char 15, Char 255	Pointer into Technology table representing the Product for this device.
OSID, OSName	Char 15, 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, 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.

EXHIBIT 1036

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.

Page 3 of 3 - 3/5/2004

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.

Page 45 of 69

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, Reoccuring 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.
1st Symptom ID	Char 45	Pointer into the Symptom table to the most relevant Symptom.
1st Symptom Name	Char 65	Name of the above Symptom
Diagnoses with the above symptom	Table	A table of all Diagnoses that are linked to 1st 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.

Exhibit 1029, page 0146 of 0146

Room, Cage, Region, Site, Street Number, Street Name, Other Street Info, City, State, Country, Zip Code, Hardware, 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, published, updated, remote, local, Vulnerable, Not Vulnerable, Credit, Discussion, Exploit, Reference, Solution	Char	SecurityFocus.com defined information fields as described in http://www.securityfocus.
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 For Unknown Victim For Known Victim For Mission Critical Victim	Drop-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, Char 255	Pointer to the Symptom record.
Technology ID Technology Name	Char 15, 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, Char 128	Pointer to Company table indicating the vendor of this Technology.
Product Number, Description, Supplier Name, Manufacturer Name	Char	Recent information regarding how this Technology was purchased.

0148

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. 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, Vulnerability Name	Char 30, Char 255	Pointer to the Vulnerability record.
Technology ID, Technology Name	Char 15, Char 255	Pointer to the Technology record.
Relationship	Drop-Down 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:DTDisplayPersonRecord	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, SOC:INOSName, 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.

4,054,359

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:TOGenerateToolNameFrom Cat	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 FindSecurityFocusVulnerabilty 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:PRSetSentryEventProble mID	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

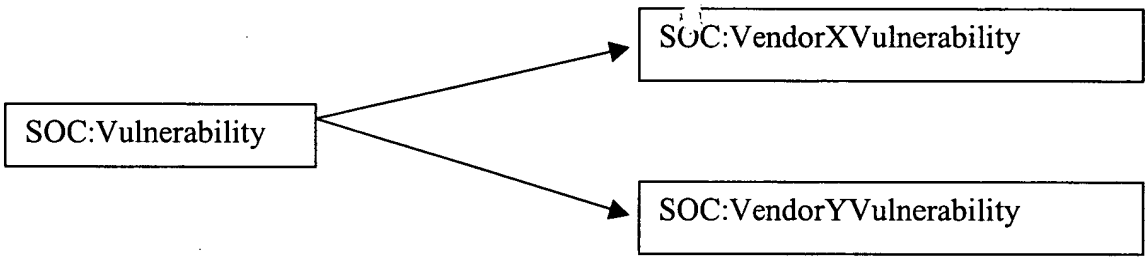
Name	Description
SOC:Category1	A list of categories describing this level of a specific Technology.
SOC:Category2	A list of categories describing this level of a specific Technology.
SOC:Category3	A list of categories describing this level of a specific Technology.
SOC:Category4	A list of categories 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

EXHIBIT 5

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
09/766,343	01/19/2001	Bruce Schneier	028490-0007

CONFIRMATION NO. 7642

FORMALITIES LETTER

OC000000006011475

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, CA 94301

Date Mailed: 04/26/2001

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

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 oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is $ 130.**

A copy of this notice MUST be returned with the reply.

Customer Service Center
Initial Patent Examination Division (703) 308-1202
PART 3 - OFFICE COPY

OIPE
MAY 24 2001
PATENT & TRADEMARK OFFICE

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) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (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 **Bruce Schmeier**
Sole or first inventor's signature Date 2/21/01
Residence **101 East Minnehaha Parkway, Minneapolis, MN 55419**
Citizenship **U.S.A.**
Post Office Address **same as above**

Full name of second inventor, if any **Andrew H. Gross**
Second inventor's signature Date 23Feb01
Residence **1055 Coleman Road, #2309, San Jose, CA 95123**
Citizenship **U.S.A.**
Post Office Address **same as above**

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

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

OIPE JC16 MAY 24 2001 PATENT & TRADEMARK OFFICE

05-29-01

Sector 4

Response To Notice To File Missing Parts Of Application Filing Date Granted (PTO-1533)(Large Entity)	Docket No. 028490-0007

Application Of: **B. Schneier et al.**

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

Invention:

Method for Dynamic Network Intrusion Monitoring, Detection and Response

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

This is a response to the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533) mailed on

April 26, 2001
Date

Enclosed herewith for filing are the following:

- ☒ A copy of the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533). **(REQUIRED)**
- ☐ An oath or declaration in compliance with 37 CFR 1.63, including residence information and identifying the application by the above Application Number and Filing Date.
- ☒ A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date.
- ☐ An oath or declaration in compliance with 37 CFR 1.63 listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date.
- ☐ A verified English translation of the non-English language application papers as originally filed. It is requested that this translation be used as the copy for examination purposes in the United States Patent and Trademark Office.
- ☐ Other (list):

OIPE JC185 MAY 24 2001 PATENT & TRADEMARK OFFICE

Response To Notice To File Missing Parts Of Application Filing Date Granted (PTO-1533)(Large Entity)	Docket No. 028490-0007

In Re Application Of: **B. Schneier et al.**

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

Invention:

Method for Dynamic Network Intrusion Monitoring, Detection and Response

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

☒ Completion of application fees as calculated below:

☐ Utility application filing fee	
☐ Design application filing fee	
☐ Total number of independent claims = _____	
☐ Total number of claims = _____	
☐ Multiple dependent claims	
☒ Surcharge for late payment of filing fee and/or late filing of original declaration or oath	**$130.00**
☐ Petition and fee for filing by other than all the inventors or a person not the invention	
☐ Fee for processing an application filed with a non-English language specification	
☐ Fee for processing and retention of application	
Total completion of application fees	**$130.00**

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the above-identified Notice to File Missing Parts of Application. The requested extension is as follows (check time period desired). If an additional time extension is required, please consider this a petition therefor.

☐ One month ☐ Two months ☐ Three months ☐ Four months ☐ Five months

from: _____ *Date* until: _____ *Date*

Total time extension fees _____

Total fees due **$130.00**

OIPE JC186 MAY 24 2001 PATENT & TRADEMARK OFFICE

Response To Notice To File Missing Parts Of Application Filing Date Granted (PTO-1533) (Large Entity)	Docket No. 028490-0007

In Re Application Of: **B. Schneier et al.**

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

Invention:

Method for Dynamic Network Intrusion Monitoring, Detection and Response

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

The fee of **$130** is to be paid as follows:

☒ A check in the amount of the fee is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. **19-2385**
A duplicate copy of this sheet is enclosed.

☒ If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No. **19-2385**
A duplicate copy of this sheet is enclosed.

Robert B Beyers
Signature

Dated: **May 24, 2001**

Robert B. Beyers
Registration No. 46,552
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570

I certify that this document and fee is being deposited on with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

[See attached Certificate of Mailing]

Typed or Printed Name of Person Mailing Correspondence

cc:

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

OIPE
MAY 24 2001
PATENT & TRADEMARK OFFICE

Invention:

Method for Dynamic Network Intrusion Monitoring, Detection and Response

I hereby certify that this **Response to Notice to File Missing Parts of Application and all enclosures**
(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 Assistant Commissioner for Patents, Washington, D.C. 20231 on

May 24, 2001
(Date)

Jan Steele
(Typed or Printed Name of Person Mailing Correspondence)

Jan Steele
(Signature of Person Mailing Correspondence)

EL 728 500 059 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

Copyright 1995 Legalsoft

OIPE
MAY 24 2001
PATENT & TRADEMARK OFFICE

#3

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
09/766,343	01/19/2001	Bruce Schneier	028490-0007

CONFIRMATION NO. 7642

FORMALITIES LETTER

OC000000006011475

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, CA 94301

Date Mailed: 04/26/2001

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

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 oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is $ 130.**

A copy of this notice MUST be returned with the reply.

Customer Service Center
Initial Patent Examination Division (703) 308-1202
PART 2 - COPY TO BE RETURNED WITH RESPONSE

05/31/2001 BNGUYEN1 00000078 09766343

01 FC:105 130.00 OP

OIPE
JUN 22 2001
PATENT & TRADEMARK OFFICE

9P2131
#7

In the United States Patent and Trademark Office

028490-0007

Inventors:	Bruce Schneier et al.
Serial No:	09/766,343
Filing Date:	January 19, 2001
Examiner:	Not yet assigned
Group Art Unit:	2131
Invention:	Method and System for Dynamic Network Intrusion Monitoring Detection and Response

RECEIVED
JUN 26 2001
Technology Center 2100

CERTIFICATE OF MAILING
BY FIRST CLASS MAIL UNDER 37 CFR § 1.8

Date of Deposit: June 18, 2001

I hereby certify that this paper is being deposited with the United States Postal Service as First Class Mail under 37 CFR § 1.8 on the date indicated above and is addressed to the Commissioner for Patents, Washington, D.C. 20231

Type or Print Name of Person Mailing: Bridget Cougar

Bridget Cougar
Signature of Person Mailing

REVOCATION AND SUBSTITUTION OF NEW POWER OF ATTORNEY

Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

The undersigned hereby revokes all prior Powers of Attorney and appoints as its attorneys:

Ronald S. Laurie	Reg. No. 25,431
Joseph Yang, Ph.D.	Reg. No. 41,387
Frederick D. Kim, Ph.D.	Reg. No. 38,513
Stacey J. Farmer, Ph.D.	Reg. No. 42,526
Robert B. Beyers, Ph.D.	Reg. No. 46,552
Constance F. Ramos, Ph.D.	Reg. No. 47,883
Daniel J. Lin	Reg. No. 47,750

of the firm of Skadden, Arps, Slate, Meagher & Flom LLP to prosecute the above-identified application for Letters Patent, and to transact all business in the U.S. Patent and Trademark Office connected therewith.

OIPE
JUN 22 2001
PATENT & TRADEMARK OFFICE

Please address all correspondence to the following address:

RECEIVED
JUN 26 2001
Technology Center 2100

Joseph Yang, Ph.D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570

The undersigned (whose title is supplied below) is empowered to act on behalf of the Assignee in the above-referenced application.

Date: June 15, 2001

Thomas E. Rowley
Chief Executive Officer
Counterpane Internet Security, Inc.

2131 #6 BT 10-31-01

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. 028490-0007

In Re Application Of: **B. Schneier et al.**

PTO/SB/08A (10-01)
AUG 27 2001
PATENT & TRADEMARK OFFICE

Serial No.	Filing Date	Examiner	Group Art Unit
09/766,343	January 19, 2001	unknown	2131

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

RECEIVED
AUG 29 2001
Technology Center 2100

Address to:
Assistant Commissioner for Patents
Washington, D.C. 20231

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application; within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; or before the mailing date of a first Office Action on the merits, whichever event occurs last.

37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after three months of the filing of a national application, or the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; or after the mailing date of a first Office Action on the merits, whichever occurred last but before the mailing date of either:

   1. a Final Action under 37 CFR 1.113, or
   2. a Notice of Allowance under 37 CFR 1.311,

   whichever occurs first.

Also submitted herewith is:

☐ a certification as specified in 37 CFR 1.97(e);

OR

☐ the fee set forth in 37 CFR 1.17(p) for submission of an Information Disclosure Statement under 37 CFR 1.97(c).

Copyright 1996 Legalsoft

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. 028490-0007

In Re Application Of: **B. Schneier et al.**

PATENT & TRADEMARK OFFICE AUG 27 2001 LEGAL

Serial No.	Filing Date	Examiner	Group Art Unit
09/766,343	January 19, 2001	unknown	2131

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

RECEIVED
AUG 29 2001
Technology Center 2100

Payment of Fee
(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

☐ A check in the amount of is attached.

☒ The Assistant Commissioner is hereby authorized to charge and credit Deposit Account No. **19-2385** as described below. A duplicate copy of this sheet is enclosed.

- ☐ Charge the amount of
- ☒ Credit any overpayment.
- ☒ Charge any additional fee required.

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (Fax. No.) on (Date)

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited on **August 22, 2001** with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

Bridget Cougar

Typed or Printed Name of Person Mailing Correspondence

***This certificate may only be used if paying by deposit account.**

Signature

Dated: **August 22, 2001**

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

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

cc:

Copyright 1996 Legalsoft

OIPE JC67
AUG 27 2001
PATENT & TRADEMARK OFFICE

Receipt

Practitioner's Docket No. 028490-0007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: B. Schneier et al.

Application No.:	09/766,343	Group No.:	2131
Filed:	January 19, 2001	Examiner:	unknown

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

Assistant Commissioner for Patents
Office of Initial Patent Examination
Customer Service Center
Washington, DC 20231

REQUEST FOR CORRECTED FILING RECEIPT

1. Attached is a copy of the official filing receipt received from the PTO in the above application for which issuance of a corrected filing receipt is respectfully requested.

NOTE: The PTO will not correct the filing receipt until the application is complete (in other words, the applicant files a response to the notice to file missing parts).

2. There is an error with respect to the following data, which is:

X incorrectly entered

and/or

omitted.

		Error in	Correct data
1.	☐	Applicant's name	1.
2.	☐	Applicant's address	2.
3.	X	Title	3. Method and system for dynamic network intrusion monitoring, detection and response
4.	☐	Filing Date	4.
5.	☐	Application Number	5.
6.	☐	Foreign/PCT Application Re:	6.
7.	☐	Other	7.

3. The corrections are not due to any error by applicant, and no fee is due.

Date: August 22, 2001

Signature of Practitioner

Joseph Yang, Ph.D.
Registration No. 41,387

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

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. § 1.8a)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

X deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the Assistant Commissioner for Patents, Office of Initial Patent Examination, Customer Service Center, Washington, DC 20231.

Date: August 22, 2001

FACSIMILE

☐ transmitted by facsimile to the Patent and Trademark Office.

Signature

Bridget Cougar

(type or print name of person certifying)

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	DRAWINGS	TOT CLAIMS	IND CLAIMS
09/766,343	01/19/2001	2131	1272	028490-0007	9	44	3

CONFIRMATION NO. 7642

UPDATED FILING RECEIPT

OC000000006175431

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, CA 94301

OIPE
AUG 27 2001
PATENT & TRADEMARK OFFICE
TC 2100

Date Mailed: 06/13/2001

Receipt is acknowledged of this nonprovisional 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 write to the Office of Initial Patent Examination's Customer Service Center. 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, San Jose, CA;

Domestic Priority data as claimed by applicant

THIS APPLN CLAIMS BENEFIT OF 60/190,326 03/16/2000

Foreign Applications

If Required, Foreign Filing License Granted 04/25/2001

Projected Publication Date: 07/25/2002

Non-Publication Request: No

Early Publication Request: No

SASM&F
JUN 18 2001
RECEIVED
DOCKETED
6-20-01 jes

Title Method

~~Mehtod~~ and system for dynamic network intrusion monitoring detection and response

Preliminary Class

713

Data entry by : LULU, TARIQUA **Team :** OIPE **Date:** 06/13/2001

[redacted]

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 Office of Export Administration, Department of Commerce (15 CFR 370.10 (j)); 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).

PLEASE NOTE the following information about the Filing Receipt:

- The articles such as "**a**," "**an**" and "**the**" are not included as the first words in the title of an application. They are considered to be unnecessary to the understanding of the title.
- The words "**new**," "**improved**," "**improvements in**" or "**relating to**" are not included as first words in the title of an application because a patent application, by nature, is a new idea or improvement.
- The title may be truncated if it consists of more than 500 characters (letters and spaces combined).
- The docket number allows a maximum of 25 characters.
- If your application was submitted under 37 CFR 1.10, your filing date should be the "date in" found on the Express Mail label. If there is a discrepancy, you should submit a request for a corrected Filing Receipt along with a copy of the Express Mail label showing the "date in."
- The title is recorded in sentence case.

Any corrections that may need to be done to your Filing Receipt should be directed to:

Assistant Commissioner for Patents
Office of Initial Patent Examination
Customer Service Center
Washington, DC 20231

#9

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. 028490-0007

In Re Application: **B. Schneier et al.**

Serial No.	Filing Date	Examiner	Group Art Unit
09/766,343	January 19, 2001	unknown	2131

METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION RESPONSE

Payment of Fee

(Only complete if Applicant elects to pay the fee set forth in 37 CFR 1.17(p))

☐ A check in the amount of is attached.

☒ The Assistant Commissioner is hereby authorized to charge and credit Deposit Account No. **19-2385** as described below. A duplicate copy of this sheet is enclosed.

- ☐ Charge the amount of
- ☐ Credit any overpayment.
- ☒ Charge any additional fee required.

Certificate of Transmission by Facsimile*

I certify that this document and authorization to charge deposit account is being facsimile transmitted to the United States Patent and Trademark Office (F

_____
(Date)

Signature

Typed or Printed Name of Person Signing Certificate

Certificate of Mailing by First Class Mail

I certify that this document and fee is being deposited with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Certificate

***This certificate may only be used if paying by deposit account.**

Robert B Beyers
Signature

Dated: **December 4, 2001**

Robert B. Beyers, Ph.D.
Registration No. 46,552
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, California 94301
Telephone: (650) 470-4500
Facsimile: (650) 470-4570

cc:

Received
DEC 0 5 2001
Technology Center 2100

#9

TRANSMITTAL OF INFORMATION DISCLOSURE STATEMENT (Under 37 CFR 1.97(b) or 1.97(c))	Docket No. 028490-0007

In Re Application Of: **B. Schneier et al.**

Serial No.	Filing Date	Examiner	Group Art Unit
09/766,343	January 19, 2001	unknown	2131

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

Address to:
Assistant Commissioner for Patents
Washington, D.C. 20231

37 CFR 1.97(b)

1. ☒ The Information Disclosure Statement submitted herewith is being filed within three months of the filing of a national application other than a continued prosecution application under 37 CFR 1.53(d); within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 in an international application; before the mailing of a first Office Action on the merits, or before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

37 CFR 1.97(c)

2. ☐ The Information Disclosure Statement submitted herewith is being filed after the period specified in 37 CFR 1.97(b), provided that the Information Disclosure Statement is filed before the mailing date of a Final Action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an Action that otherwise closes prosecution in the application, and is accompanied by one of:

   ☐ the statement specified in 37 CFR 1.97(e);

   OR

   ☐ the fee set forth in 37 CFR 1.17(p).

Received
DEC 0 5 2001
Technology Center 2100

#8

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
09/766,343	01/19/2001	Bruce Schneier	028490-0007

CONFIRMATION NO. 7642

OC000000007243384

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, CA 94301

Date Mailed: 12/31/2001

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/22/2001.

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.

Brenda Harrison

BRENDA V HARRISON
2100 7033059632

OFFICE COPY

#7

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

APPLICATION NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
09/766,343	01/19/2001	Bruce Schneier	028490-0007

CONFIRMATION NO. 7642

OC000000007243383

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, CA 94301

Date Mailed: 12/31/2001

NOTICE REGARDING POWER OF ATTORNEY

This is in response to the Power of Attorney filed 06/22/2001.

- 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).

Brenda Harrison

BRENDA V HARRISON
2100 7033059632

OFFICE COPY

PTO JC109
FEB 0 9 2004
TRADEMARK OFFICE

2/31

PTO/SB/21 (08-03) #10

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

		Application Number	09/766,343
		Filing Date	January 19, 2001
		First Named Inventor	Schneier, Bruce
		Art Unit	2131
		Examiner Name	Unassigned
Total Number of Pages in This Submission	3	Attorney Docket Number	022133-000510US

ENCLOSURES ***(Check all that apply)***

☐ Fee Transmittal Form	☐ Drawing(s)	☐ After Allowance Communication to Group
☐ Fee Attached	☐ Licensing-related Papers	☐ Appeal Communication to Board of Appeals and Interferences
☐ Amendment/Reply	☐ Petition	☐ Appeal Communication to Group (**Appeal Notice, Brief, Reply Brief**)
☐ After Final	☐ Petition to Convert to a Provisional Application	☐ Proprietary Information
☐ Affidavits/declaration(s)	☒ Power of Attorney, Revocation Change of Correspondence Address	☐ Status Letter
☐ Extension of Time Request	☐ Terminal Disclaimer	☒ Other Enclosure(s) *(please identify below)*:
☐ Express Abandonment Request	☐ Request for Refund	Return Postcard
☐ Information Disclosure Statement	☐ CD, Number of CD(s)	Statement Under 3.73 (b)
☐ Certified Copy of Priority Document(s)		
☐ Response to Missing Parts/ Incomplete Application		
☐ Response to Missing Parts under 37 CFR 1.52 or 1.53		

Remarks	The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

RECEIVED
FEB 12 2004
Technology Center 2100

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual	Townsend and Townsend and Crew LLP Philip H. Albert Reg. No. 35,819
Signature	
Date	2/5/04

FEB 13 2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Landon Clark		
Signature	Landon Clark	Date	2-6-04

60128618 v1

FEB 0 9 2004
TRADEMARK OFFICE
TC109

#10

PTO/SB/82 (09-03)

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

RECEIVED
FEB 1 2 2004
Technology Center 2100

☐ 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 Harms		
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.

60124613 v1

OIPE JC109
FEB 0 9 2004
PATENT & TRAD

PTO/SB/96 (08-03)

Attorney Docket No. 022133-000510US

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Bruce Schneier, et. al.

Application No./Patent No.: 09/766,343 Filed/Issue Date: January 19, 2001

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

Counterpane 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 number

Christopher Huems
Typed or printed name

Signature

Acting CFO
Title

RECEIVED
FEB 12 2004
Technology Center 2100

60118965 v1

#11

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
09/766,343	01/19/2001	Bruce Schneier	028490-0007

CONFIRMATION NO. 7642

OC000000011932598

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

Date Mailed: 02/19/2004

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/09/2004.

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.

Brenda Harrison

BRENDA V HARRISON
2100 (703) 305-9632

OFFICE COPY

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
09/766,343	01/19/2001	Bruce Schneier	028490-0007

CONFIRMATION NO. 7642

OC000000011932562

Robert B. Beyers, Ph. D.
Skadden, Arps, Slate, Meagher & Flom LLP
525 University Avenue
Palo Alto, CA 94301

Date Mailed: 02/19/2004

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/09/2004.

- 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).

Brenda Harrison

BRENDA V HARRISON
2100 (703) 305-9632

OFFICE COPY

	Type	L #	Hits	Search Text	DBs	Time Stamp
1	BRS	L32	121107	probe or sentry or honeypot	USPAT	2004/03/18 14:55
2	BRS	L33	21509	intrusion or misuse	USPAT	2004/03/18 14:55
3	BRS	L34	1110	L32 and L33	USPAT	2004/03/18 14:55
4	BRS	L35	114762	(secure near2 operations near2 center) or (network near2 operations near2 center) or (soc) or (security near2 center)	USPAT	2004/03/18 14:56
5	BRS	L36	82	L34 and L35	USPAT	2004/03/18 14:56
6	BRS	L37	0	managed near2 security near2 monitoring	USPAT	2004/03/18 14:57

	Comments	Error Definition	Errors
1			0
2			0
3			0
4			0
5			0
6			0

File 2:INSPEC 1969-2004/Feb W5
(c) 2004 Institution of Electrical Engineers
*File 2: Alert feature enhanced for multiple files, duplicates removal, customized scheduling. See HELP ALERT.
File 6:NTIS 1964-2004/Mar W1
(c) 2004 NTIS, Intl Cpyrght All Rights Res
File 8:Ei Compendex(R) 1970-2004/Feb W5
(c) 2004 Elsevier English Info. Inc.
File 34:SciSearch(R) Cited Ref Sci 1990-2004/Mar W1
(c) 2004 Inst for Sci Info
File 35:Dissertation Abs Online 1861-2004/Feb
(c) 2004 ProQuest Info&Learning
File 65:Inside Conferences 1993-2004/Mar W1
(c) 2004 BLDSC all rts. reserv.
File 92:IHS Intl.Stds.& Specs. 1999/Nov
(c) 1999 Information Handling Services
*File 92: This file is closed (no updates)
File 94:JICST-EPlus 1985-2004/Feb W5
(c)2004 Japan Science and Tech Corp(JST)
File 95:TEME-Technology & Management 1989-2004/Feb W4
(c) 2004 FIZ TECHNIK
File 99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
(c) 2004 The HW Wilson Co.
File 103:Energy SciTec 1974-2004/Feb B2
(c) 2004 Contains copyrighted material
*File 103: For access restrictions see Help Restrict.
File 144:Pascal 1973-2004/Feb W5
(c) 2004 INIST/CNRS
File 202:Info. Sci. & Tech. Absolute 1966-2004/Feb 27
(c) 2004 EBSCO Publishing
File 233:Internet & Personal Comp. Absolute 1981-2003/Sep
(c) 2003 EBSCO Pub.
File 239:Mathsci 1940-2004/Apr
(c) 2004 American Mathematical Society
File 275:Gale Group Computer DB(TM) 1983-2004/Mar 11
(c) 2004 The Gale Group
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 647:CMP Computer Fulltext 1988-2004/Feb W5
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Feb W5
(c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Mar 10
(c) 2004 The Dialog Corp.

Set	Items	Description
S1	0	(SECURE ADJ OPERATIONS ADJ CENTER)
S2	142965	(SOC)
S3	37	(SECURE)(2N)(OPERATIONS)(2N)(CENTER)
S4	3085	(NOC)
S5	146047	S2 OR S3 OR S4
S6	115	MANAGED(2N)SECURITY(2N)MONITOR?
S7	2	S5 AND S6
S8	496	OUTSOURCING(2N)SECURITY
S9	13	S6 AND S8
S10	12	OUTSOURCING(2N)INTRUSION
S11	1	S6 AND PROBE
S12	531527	(PROBE OR SENTRY OR HONEYPOT OR (BLACK)(2N)(BOX))
S13	0	S6(S)S12
S14	5	S6 AND S12

?

```
Set     Items   Description
S1     517991   (PROBE OR SENTRY)
S2       1493   (NEGATIVE OR POSITIVE)(2N)(FILTER?)
S3         33   S1 AND S2
S4          4   S3 AND MONITOR?
S5       5719   S1(S)FILTER?
S6         24   S5 AND INTRUSION
?
```

Build a firewall. (protecting Internet servers from ***intrusion***)
(includes related articles on safe network services, network security policy, top security threats)(State of the Art)(Tutorial)
Bryan, John
Byte, v20, n4, p91(5)
April, 1995
DOCUMENT TYPE: Tutorial ISSN: 0360-5280 LANGUAGE: ENGLISH
RECORD TYPE: CITATION

ABSTRACT: A guide to establishing a 'firewall' to protect an Internet-connected LAN from intruders is presented. Firewalls are barriers placed between a network and the outside world to prevent unwanted ***intrusion*** . A firewall may take the form of a router-based **filter**, a host computer gateway or a separate isolation network for very sensitive data; costs range from $100,000 for a turnkey solution to freeware available on the Internet. ***Filtering*** routers are the simplest firewall approach; programmable routers control traffic at the IP level and can be used to **filter** out packets from unauthorized sites, but some major Internet services are not well handled by packet ***filters*** . A host-based firewall has a 'bastion' or ***sentry*** system designed as a defense point and tightly controlled with regular audits. Such a host requires specialized software gateways and service proxies. An isolation network is a subnetwork that sits between the Internet and internal networks and is configured so that both can access it but so that traffic across is blocked. A variety of commercial firewall products are available.

DESCRIPTORS: Internet; Data Security Issue; Technology Tutorial; Computer networks
FILE SEGMENT: CD File 275
?

www.securityfocus.com/infocus/1231 - November 3, 2000 - 33 KB

5. Security Accreditation, Management and Monitoring - Getting the...
Security Accreditation, Management and **Monitoring** - Getting the Balance Right! Peter J Fisch **Security** Manager, Government Communications Headquarters, Cheltenham, UK Tel: +44-124 ... and **security** has been struck, and where **security** is. properly **managed** and monitored thr the ...
csrc.nist.gov/nissc/1998/proceedings/paperE1.pdf - October 28, 1998 - 27 KB

6. CCA: Internet Monitoring & Security
Free Web site hosting - Freeservers.com CCA & Associates Co., Ltd.Â® Telemanagement Consu Solutions **SECURITY**, SOLUTIONS, SERVICES, SUPPORT, STRATEGY, SURVEILLANCE, SURVIV/ ... .
www.ccaassociates.8m.com/internetm.htm - January 21, 2000 - 20 KB

7. Security UI References
... Usability of Computer **Security**: A Bibliography ... the usability of computer **security** that cc types ... term user-centered **security** to refer to **security** models, mechanisms, systems, ...
www.sims.berkeley.edu/~rachna/security_usability.html - August 9, 2000 - 60 KB

8. Real-Time Security Monitoring and Control of Power Systems
Consortium for Electric Reliability Technology Solutions Grid of the Future White Paper on Real- **Security Monitoring** and Control of Power Systems Transmission Reliability Program Office of that need to be **managed** in RTSMC. The volumes of data will increase notwithstanding ...
www.eren.doe.gov/der/transmission/pdfs/realtimecontrol.pdf - August 22, 2000 - 103 KB

9. improving the security of your unix system
... April 1990 IMPROVING THE **SECURITY** OF YOUR UNIX SYSTEM ... 1 INTRODUCTION 1 1.1 U **Security** ... 29 3 **MONITORING SECURITY**..... .... 31 3.1 Account **Securi**
www.alw.nih.gov/Security/Docs/unix-security.html - October 11, 1994 - 160 KB

10. Managed Care and Children with Special Health Care Needs: Strategies...
Managed Care and Children with Special Health Care Needs: Strategies for **Monitoring** the Qu North Carolina Division of Maternal and Child Health Renee Schwalberg, Vivian Gabor, and Ian .
www.hsrnet.com/pdf/nc-rpt.pdf - December 22, 2000 - 164 KB

« **Previous** | **Next** »

Search for "**managed security monitoring**" using: Lycos, Google, Ask Jeeves

Portions powered by Inktomi

Advertise | Help | Text-only Skin | Submit Site | HotBot International | Visit Canada travel.Sympatico.ca | Yellow Pages
© Copyright 2003, Lycos, Inc. All Rights Reserved. | **Privacy Policy** | Terms & Conditions | **HotBot Your Site**

h h b c e ge ec g c e chb



automated intrusion response Homepage | Advanced Search

Search using: HotBot Lycos Google Ask Jeeves

CUSTOM WEB FILTERS Tools | HotBot Skins | !

Date: **Before January 2001** [Edit this Search]

SPONSORED LINKS (filters not applied)

- **Intrusion** detection tool
  Event Correlation Server solution. Download ECS for free!
  download.eventgnosis.com

- Autoresponder Software
  No Monthly Fee, Simple To Install, Unlimited Responders, No Adverts.
  www.Autoresponder-Software.biz

WEB RESULTS (Showing Results 1 - 10 of 2,614)

1. A Methodology for Using Intelligent Agents to provide Automated...
... This paper proposes a new methodology for adaptive, **automated intrusion response** (IR) the role of software ...
www.ai.usma.edu/Marin/Wshop/Abstracts/TP1_1.pdf - May 9, 2000 - 19 KB

2. Carver 2000 An Intrusion Response Taxonomy and its Role IAÂ...
An **Intrusion Response** Taxonomy and its Role in Automatic **Intrusion Response** and Udo W proposes an **intrusion response** taxonomy and discusses the role of such a taxonomy in an ai
www.ai.usma.edu/workshop/2000/Abstracts/TP1_4.pdf - May 9, 2000 - 10 KB

3. Infrastructure for Intrusion Detection and Response
Infrastructure for **Intrusion** Detection and **Response** Boeing Phantom Works NAI Labs, Netwo **Automated response** to intrusions has become a major issue in defending critical systems. ...
www.nai.com/common/media/nai/pdf/DISCEX-IDR-Infrastructure.pdf - June 28, 2000 - 239 KB

4. Security Agility in Response to Intrusion Detection
Security Agility in **Response** to **Intrusion** Detection Cooperative frameworks for **intrusion** de **response** exemplify a key area of todayâ€™s computer research: automating defenses against cooperative frameworks for **intrusion** detection and. **response**, seeks to develop **automated** capable of ...
www.acsac.org/2000/papers/43.pdf - September 21, 2000 - 147 KB

5. Toward Cost-Sensitive Modeling for Intrusion Detection and Response
Toward Cost-Sensitive Modeling for **Intrusion** Detection and **Response** Computer Science Dep North Carolina State University Raleigh, NC 27695 wenke@csc.ncsu.edu - Wei Fan, Matthew Mi
www1.cs.columbia.edu/~ezk/research/acm_ccs - November 9, 2000 - 5 KB

6. A Distributed Autonomous Agent Network Intrusion Detection and...
A Distributed Autonomous-Agent Network-**Intrusion** Detection and **Response** System 11440 Ct., Suite 290 San Diego, CA 92127 Neil C. Rowe Naval Postgraduate School Monterey, CA 939 are few **automated** methods to perform this recognition. ...

www.cs.nps.navy.mil/people/faculty/rowe/barruspap.html - April 13, 1998 - 30 KB

7. Distributed Object Computation Testbed (DOCT)
... for supporting **intrusion response**, sometimes referred to as **intrusion** ... applications to e **intrusion response**, specifically in the ... of the **intrusion response** process. This paper ...
www.sdsc.edu/DOCT/Publications/e3-3/e3-3.html - December 15, 1997 - 33 KB

8. Toward Cost-Sensitive Modeling for **Intrusion** Detection and **Response**
Toward Cost-Sensitive Modeling for **Intrusion** Detection and Computer Science Department Nc State University Raleigh, NC 27695 Wei Fan, Matthew Miller, Sal Stolfo, and Erez Zadok ... ... d due to successful intrusions, and the cost of manual and **automated response** to intrusions. ..
www.cs.columbia.edu/~ezk/research/acm_ccs/acm_ccs.pdf - November 9, 2000 - 137 KB

9. Cyber-defense offers automatic **response** to **intrusion**
... the exchange of **intrusion** and **response** information, due to ... â€œThere are currently no mechanisms for the ...
www.afrl.af.mil/news/winter00/roundups/cyber-defense-roundups.pdf - May 12, 2000 - 11 KB

10. MimeStar.com **Intrusion** Detection
Menu Options AutoDetect Flash Menu Imagemap News: 5 JUL 2000 - **Intrusion**.com Acquires I Inc. View Release Â· Text Only MimeStar, Inc. is a developer of advanced network monitoring a
www.mimestar.com/ - July 5, 2000 - 11 KB

« **Previous** | **Next** »

Search for "**automated intrusion response**" using: Lycos, Google, Ask Jeeves

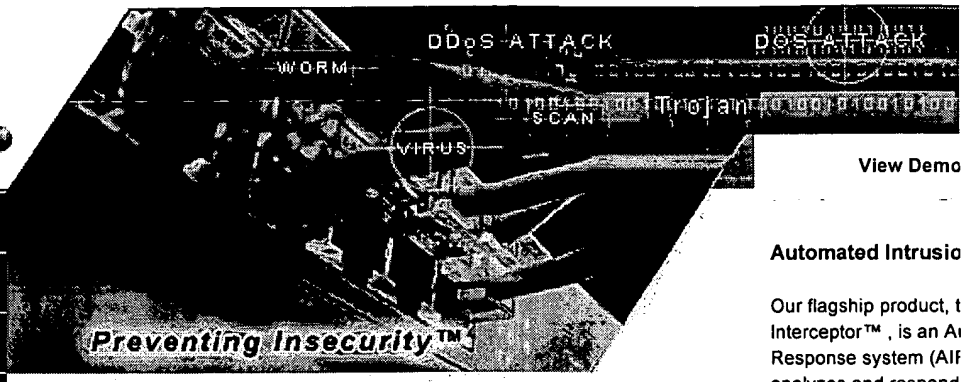


Portions powered by Inktomi

Advertise | Help | Text-only Skin | Submit Site | HotBot International | Visit Canada travel.Sympatico.ca | Yellow Pages
© Copyright 2003, Lycos, Inc. All Rights Reserved. | **Privacy Policy** | Terms & Conditions | **HotBot Your Site**

INTRUSION DETECTION AND PREVENTION MAST

REFLEX SECURITY



PRODUCTS
SERVICES
MARKET
COMPANY
PARTNERS

As businesses connect to the Internet, they open up the front door of their networks to the world. Opening these corporate networks to mobile employees, remote offices, home offices, customers and other entities in the value chain introduces new security risks and further exposure.

Reflex Security is a next-generation Intrusion Detection & Prevention software company. Our mission is to help enterprises detect and prevent malicious external and internal attacks to their computer systems efficiently and in a cost-effective manner.

Recent Press Release

Reflex Security Announces Version 4.0 of its Interceptor™ Intrusion Prevention Solution

View press releases

View Demo

Automated Intrusio

Our flagship product, t
Interceptor™ , is an A
Response system (AIF
analyzes and respond
external network secu
without the need for h
(find out more)

Deployment Solutic

Economical for smalle
remote offices of distri

Reflex Intercepto

For environments up t
mbit/second all with ur

Reflex Intercepto

Ideal for large organiz
network environments

Reflex Intercepto

Dedicated server prote

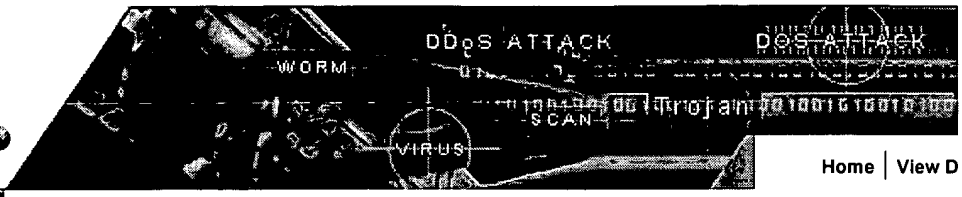
Reflex Intercepto

Core management en
operator GUI

Interceptor Mana

Reflex Security, Inc. • 5730 Glenridge Dr., Suite 10 • Atlanta, GA 30328 • 888.872.7555

INTRUSION DETECTION AND PREVENTION MAST



PRODUCTS
SERVICES
MARKET

Market assessment
Value Proposition

COMPANY
PARTNERS

Market Assessment

On the one hand, the Internet enables companies to partake in cost-efficient, automated commerce. On the other hand, the Internet provides a medium for malicious forces to attack, penetrate, and thereby exploit, in order to gain notoriety, to achieve financial gain or just to perpetrate general mischief. Viruses, worms, Trojan attacks and hybrid threats propagate, spread and wreak havoc on corporate networks, and by doing so, debilitate business.

Gone are the days when passwords and anti-virus software represent a comprehensive security strategy. A typical enterprise requires protection at physical access points, Internet gateways, networks, client machines, as well as, at application servers.

Legal, social and regulatory trends are raising the bar for corporate IT security.

- **IT Security threats on mission-critical corporate networks continue to increase in numbers, in severity and in sophistication.** Blended threats, such as NIMDA and Code Red, cause billions of dollars in damages by exploiting flaws in well-known software programs. The sophistication of attacks continues to increase, while the level of expertise required to perform an attack continues to decline due to the proliferation of automated tools that benefit the attacker.
- **Vulnerabilities are appearing at an ever-increasing rate, while the time companies have to protect against newly discovered vulnerabilities continues to diminish.** The number of vulnerabilities reported to the CERT Coordination Center mushroomed from 171 in 1995 to 3,222 in the first 9 months of 2002 alone.
- **As corporations have invested in security products for their networks, the level of threat activity and potential liability increases. How can this be?** The answer is that the first-generation of network security devices -- firewalls and intrusion detection systems in particular -- can no longer cope with the new generation of threats. These first-generation security technologies generate volumes of data to be

The security dil

- Th
  co
  ov
  in
  wo
- Th
  ina
  in
  se
  inc
- Att
  mc
  an
  dy
- Fir
  se
  pr
  co
  ex

analyzed by humans who have less and less time to analyze and act on that data in a timely manner.

- **Intrusion Detection and Prevention technologies are increasingly regarded as an essential component of any enterprise IT security strategy.**
  Intrusion Detection and Prevention solutions address security threats beyond the reach of perimeter protection technologies such as firewall and anti-virus solutions. Survey data indicates that 80% of security technology is focused on keeping outsiders out -- although 80% of the most serious attacks occur from within. This problem is made worse as not only employees but clients, trading partners, as well as, temporary employees are given network access and are thereby in a position to wreak havoc should they seek to do harm.

Reflex Security, Inc. • 5730 Glenridge Dr., Suite 10 • Atlanta, GA 30328 • 888.872.7555

Copyright © 2004, Reflex Security,



Intrusion Detection, Honeypots and Incident Handling Resources

DNSSEC.NET	BIND9.NET	BGP4.AS	HONEYPOTS.NET	WARDRIVE.NET	FORENSICS.NL	PCVIRUS.ORG	SE
Securing the Domain Name System with DNSSEC	DNS, BIND, DHCP, LDAP Resource Directory	Border Gateway Protocol and Advanced Routing	Intrusion Detection, Honeypots & Incident Response	Wireless LAN (802.11) Security and Wardriving	Computer Forensics and Cybercrime Resources	Computer Viruses, Anti-Virus and Protection	

Tipping Point - Multi Gig
Evaluation Units 866-301-2880 x211 High-Speed asic technology

Intrusion Prevent/Detect
McAfee's multi-tier network and host based prevention/detection.

Network Intrusion
Network security made simple Request a free vulnerability scan

Network Intrusion
Protect your company i IPS/IDS Only $499, Fre

Intrusion Detection

Intrusion Detection Links Library
Intrusion Detection Software
Intrusion Detection Mgt. Suites
Intrusion Detection Books
Intrusion Detection Mailinglists
Intrusion Detection Courses
Integrity Management Software
Managed IDS Services

Honeypots, Honeynets

Honeypot Links Library
Honeypot & Deception Software
Honeypot & Honeynet Projects
Honeypot & Deception Books
Honeypot Mailinglists
Honeypot Courses

Incident Handling

Incident Handling Links Library
Incident Handling Mailinglists
Incident Handling Courses
Incident Handling Books

Home - About - Contact

Always handy:
Internet Protocols List
Sans Top 20 Vulnerabilities
Port Numbers List
Protocol Encapsulation Chart (PDF)
The RFC Archive NEW!
Top 75 Security Tools



Intrusion Detection Software (IDS Software)

AccessGuard
by Access Security Advisors
AccessGuard is a fully automated intrusion prevention service, that instantly protects your IT infrastructure from known and unknown attacks by hackers, worms, server based 'Denial of Service' and other Internet risks.

ActiveScout
by ForeScout Technologies
ActiveScout's patented Active Response technology provides intelligence to dynamically protect the perimeter against threats. This adaptive capability enables the accurate assessment of attackers in real, allowing blocking to be automatic.

AirDefense Guard
by AirDefense, Inc.
AirDefense Guard is an 802.11a/b/g wireless LAN intrusion detection and security solution that identifies security risks and attacks, provides real-time nework audits and monitors the health of the wireless LAN.

Attack Mitigator IPS
by Top Layer Networks
Top Layer's Attack Mitigator IPS is a family of high performance, ASIC-based intrusion prevention solutions with precision blocking and control against the most prevalent cyber attacks. Hybrid attacks such as HTTP worms, DoS/DDoS attacks, protocol and traffic anomalies, IP spoofing, SYN flood attacks, and more, are accurately detected, and stopped in real-time.

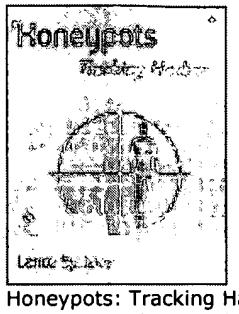
Autonomous Agents for Intrusion Detection (AAFID)
by CERIAS/Purdue University
The Autonomous Agents for Intrusion Detection Group is composed of a number of students and faculty within the CERIAS at Purdue University who are interested in

ipAngel
by Lucid Security
Lucid Security's ipANGEL, coupled with Check Point FireWall-1, provides complete protection against all network and application attacks. ipANGEL marks a departure from the traditional thinking of what an intrusion prevention product should do. It detects and shields vulnerable applications without duplicating the capabilities of the firewall.

KFSensor
by Keyfocus
KFSensor is a honeypot based Intrusion Detection System (IDS). It acts as a honeypot to attract and detect hackers by simulating vulnerable system services and trojans. The system is highly configurable and features detailed logging, analysis of attack and security alerts. This approach complements other forms of security and adds another defense against the growing security threat faced by all organizations.

LANGuard Security Event Log Monitor
by GFI Software
GFI LANguard S.E.L.M. monitors the security event logs of all your Windows NT/2000/XP servers and workstations and alerts you to possible intrusions/attacks in real time, giving you peace of mind.

Manhunt
by Symantec
Symantec ManHunt provides high-speed, network intrusion detection, real-time analysis and correlation, and proactive prevention and response to protect enterprise networks against internal and external intrusions and denial-of-service attacks. The ability to detect unknown threats, using protocol anomaly detection, helps eliminates network exposure and the vulnerability inherent in traditional signature-based IDS products. Symantec ManHunt traffic rate monitoring capability



Honeypots: Tracking Hackers
With this book you will gain an understanding of honeypot concepts and architecture, as well as the skills to deploy the best honeypot solutions for your environment.

You will arm yourself with the expertise to track attackers and learn about them on your own. Security professionals, researchers, law enforcement agents, and members of the intelligence and military communities will find this book indispensable.

studying novel distributed methods of Intrusion Detection.

BenIDS ⇨🗋

by Theron Toomey
BENIDS is a pcap-based Network Intrusion Detection System for Linux. It uses its own XML rule file format which allows arbitrary, complex boolean matching conditions. It generates IDMEFv0.3 alert messages, and also supports fragment and TCP stream reassembly.
Note: This is experimental/educational software in a pre-alpha development phase. It is not yet suitable for general consumption/use.

Blink ⇨🗋

by eEYE Digital Security
Blink combines the protection of a firewall, intrusion detection and prevention system, policy enforcer, and vulnerability assessment engine in one complete product. Smart protocol analysis and application monitoring engines allow Blink to proactively protect against unknown attacks. Fully customizable signature databases, firewall rulesets, and policies allow the machine to be properly locked-down and secured against intruders or misuse.

Border Guard ⇨🗋

by StillSecure / Latis Networks
Border Guard products reduce the risk and liability from cyber attacks. Employing our exclusive Dynamic Attack Detection, Dynamic Attack Qualification, and Dynamic Attack Response technologies, Border Guard identifies and terminates attacks before they damage your network.

Bro ⇨🗋

by Lawrence Berkeley National Laboratory
Bro is an intrusion detection system that works by passively watching traffic seen on a network link. Bro runs the events produced by the event engine through a policy script. Bro scripts are made up of event handlers that specify what to do whenever a given event occurs. Event handlers can maintain and update global state information, write arbitrary information to disk files, generate new events, call functions (either user-defined or predefined), generate alerts that produce syslog messages, and invoke arbitrary shell commands. These latter might terminate a running connection or talk to your border router to install an ACL prohibiting traffic from a particular host, for example. Bro uses libpcap, and assumes that you've already installed it. If not, you can get it from www.tcpdump.org. Furthermore, Bro needs flex, and it needs bison or byacc.

Captus IPS 4000 Series ⇨🗋

by Captus Networks
The Captus IPS 4000 series prevents network attacks - including DDoS attacks, port scans, and exploits from unknown worms - as well as unsanctioned traffic, such as file-swapping. At the same time, it optimizes the performance allows for detection of stealth scans and denial-of-service attacks that can cripple even the most sophisticated networks.

McAfee IntruShield ⇨🗋

by Network Associates
McAfee IntruShield network security products are built upon the industry's first architecture for real-time detection and prevention of network intrusions against enterprise and government networks. The innovative IntruShield architecture integrates patented signature, anomaly and Denial of Service (DoS) analysis techniques, enabling accurate and intelligent attack detection and prevention at multi-gigabit speeds.

Minesweeper IDS ⇨🗋

by BarbedWire Technologies
Minesweeper IDS offers a comprehensive security feature set into a centralized secure SSL based management console making network security management simple, secure and efficient.

NetBait ⇨🗋

by NetBait Inc.
NetBait acts as an additional layer of defense, diverting intruders from your real systems and directing them to controlled computing environments, or pseudo-networks. NetBait creates these environments by projecting a diversionary picture of your network. This picture consists of your real network nodes surrounded by multiples of "fake" NetBait Nodes or "targets", each of which may be configured to present any combination of operating systems, services, and applications.

NETSTAT ⇨🗋

by University of California
The STAT project provides a framework that supports the development and the control of scenario-based sensors. By using STAT, it is possible to create a set of sensors that will operate in different domains and environments, e.g., network-based sensors, host-based sensors, and application-based sensors. In addition, STAT provides an infrastructure to communicate securely with the deployed sensors so that it is possible to collect the results of scenario-based analysis and control sensors' configuration from a central location. Centralized management systems can be composed hierarchically to achieve scalability and extended control over large sets of sensors.

Next Generation Intrusion Detection Expert System (NIDES) ⇨🗋

by SRI
NIDES is a comprehensive intrusion-detection system that performs real-time monitoring of user activity on multiple target systems connected via Ethernet. NIDES runs on its own workstation (the NIDES host) and analyzes audit data collected from various interconnected systems, searching for activity that may indicate unusual and/or malicious

and management of valid traffic, including surges in customer traffic. When the network is optimally managed, security is automatic.

Chkrootkit ⇨🗋
by several authors
chkrootkit is a tool to locally check for signs of a rootkit.

Cisco Secure IDS (CSIDS) ⇨🗋
by Cisco Systems
The Cisco Intrusion Detection System is designed to efficiently protect your data and information infrastructure.

Data Sentinel ⇨🗋
by Ionx
Data Sentinel is a highly advanced host based intrusion detection system (HIDS) that empowers you with the ability to maintain the integrity of business critical data, and detect unauthorised access by hackers or viruses.

Dragon Intrusion Defense ⇨🗋
by Enterasys Networks
Designed specifically to meet the unique security requirements of the enterprise environment, Enterasys Dragon Intrusion Defense System offers comprehensive features that bring improved security to the enterprise. Only Dragon, with its unique network-based detection and active response capabilities, modular host intrusion detection components, server management, and event management provides a reliable solution for detecting and responding to the broad array of attacks present in today's constantly changing security landscape.

DShield ⇨🗋
by Euclidian Consulting
DShield provides a platform for users of firewalls to share intrusion information. DShield is a free and open service.

Emerald ⇨🗋
by SRI
EMERALD represents state-of-the art in research and development of systems and components for anomaly and misuse detection in computer systems and networks.

Entercept IDS ⇨🗋
by Network Associates
Entercept's award-winning, intrusion prevention solutions provides enterprise-class security that is manageable, more cost-effective than detection and monitoring and effectively defends the critical assets of your business from malicious attacks like buffer overflows and worm including Code Red, Nimda and the recent SQL Slammer.

eTrust Intrusion Detection ⇨🗋
by Computer Associates
eTrust Intrusion Detection is a complete session security solution that incorporates three key security capabilities into one package - comprehensive network protection, network session monitoring and Internet user behavior.

NFR Network IDS ⇨🗋
by NFR Security
With NFR Security's intelligent intrusion management system, you'll not only detect and deter network attacks, you also integrate with popular firewall providers to prevent future attacks. Here are twelve reasons a leading business journal refers to NFR as "the Holy Grail" of intrusion management.

nPatrol ⇨🗋
by nSecure
nPatrol is an adaptive Intrusion Detection System designed not only to protect the systems from known vulnerabilities, but also from new modes of attack. It helps in addressing the business risks and coping with rapid ongoing changes within an organization.

PowerSecure ⇨🗋
by Mazu Networks, Inc.
PowerSecure solutions 'learn' the behaviors of the environments in which they are deployed by profiling and characterizing all aspects of these networks and the traffic that courses through them. They capture information on every network connection over time in order to dynamically profile 'normal' traffic flow. PowerSecure solutions then compare real-time traffic data against the profile to detect anomalous network traffic, which has a high likelihood of being malicious activity.

Prelude IDS ⇨🗋
by Yoann Vandoorselaere et al.
Prelude is a full featured Intrusion Detection System distributed under the GPL License. Prelude is developed primarily under GNU/Linux, but also supports the *BSD, as well as any POSIX compliant platform. It has been designed from the ground up to be optimized for distributed environments, completely modular, robust, and fast. Prelude takes benefits from the combination of traces of malicious activity from differents sensors (snort, honeyd, nessus vulnerability scan, hogwash, samhain, grsecurity, systems logs, and others) in order to better qualify the attack and in the end to perform automatic correlation between the various traces. Prelude is commited to provide an IDS that offer the ability to unify the currently available tools into one, powerful application.

Proventia Enterprise Protection ⇨🗋
by Internet Security Systems (ISS)
Range of IDS Appliances. Proventia products deliver protection at the gateway, network, server and desktop, and are all centrally managed by ISS' SiteProtector™ centralized management system. Each enterprise has unique security needs, so Proventia's flexibility provides complete, unified protection for every environment. Using Proventia's complete, unified protection capability is ideal for a remote office lacking dedicated security personnel. To strengthen network protection against hybrid worms,

content blocking. eTrust Intrusion Detection defends against network attacks and helps enforce corporate security policies.

Exposé ⇨🗋
by Intrusec Inc.
Intrusec's Exposé is a new class of network security software, a network change detection system, that provides continuous monitoring of your network for the appearance of new systems and services, and changes to existing ones. It installs on a single PC and proactively monitors up to several thousand devices on the network for changes to the state of any of the devices on it or the network itself.

FireProof ⇨🗋
by Radware Ltd.
FireProof guarantees the full availability, redundancy and highest operation of FireWalls, Virtual Private Networks and Intrusion Detection Tools, while extending real-time Intrusion Prevention and DoS Protection to prevent malicious signature attacks and debilitating network service denials.

Firestorm NIDS ⇨🗋
by Gianni Tedesco
Firestorm is an extremely high performance network intrusion detection system (NIDS). At the moment it is just a sensor but plans are to include real support for analysis, reporting, remote console and on-the-fly sensor configuration. It is fully pluggable and hence extremely flexible.

G-Server ⇨🗋
by Gilian Technologies Inc.
Gilian's G-Server is the first and only appliance designed to keep fraudulent information and corrupted transactions from ever being published on your Web site. Guaranteed. Based on revolutionary ExitControl technology, the G-Server scrutinizes, in real-time, every object leaving the Web server, assuring all content - static or dynamic - as well as all Web applications are authentic and unaltered. Any misrepresented data is seamlessly replaced with authentic, original content. As a result, even if hackers get in, you can be certain your Web audience will only see what you intend them to see. No downtime and no need to post "Site Unavailable" messages. All attacks are neutralized leaving your reputation, liability and credibility safe and sound.

Host IDS ⇨🗋
by Symantec
Symantec Host IDS is a scalable intrusion detection and prevention solution for critical servers. It provides enterprises with a sophisticated combination of host intrusion protection technology with advanced management capabilities. Symantec Host IDS is part of an overall security strategy that provides enterprises a holistic view of enterprise security. Symantec Host IDS provides real-time monitoring, detection, and prevention of security breaches, delivering Proventia's intrusion prevention capabilities can be utilized to augment an existing firewall. For areas of the network that require the highest level of monitoring, Proventia's intrusion detection function will support security forensics and remediation.

PureSecure ⇨🗋
by DeMarc Security
Demarc PureSecure is a one of a kind, Total Intrusion Detection System (TIDS), which provides an unsurpassed level of comprehensive security. For the first time you will be able to reliably prevent, detect, and deter internal and external threats to your organization's valuable assets with complete confidence, 24 hours a day. Advanced cross platform compatible technology means PureSecure can be deployed and scaled in a wide variety of network infrastructures.

RealSecure ⇨🗋
by Internet Security Systems (ISS)
The RealSecure Network Sensor provides broad-based detection, prevention and response for attacks and misuse that originate from across a network.

Secuplat Host IDS ⇨🗋
by Inzen
Secuplat HIDS is a server-based intrusion detection system. It adopts misuse detection to detect illegal access attempts that firewall or network-based intrusion detection systems cannot. It provides detailed information on individual hosts in internal computer networks and provides effective response procedures in order to enhance the stability of a server.

Secureplat Network IDS ⇨🗋
by Inzen
Secuplat NIDS is a network-based intrusion detection system. It provides an overall strategy to enhance enterprise-wide security by offering blueprints, as well as detailed information to deal with potential attack attempts over the Internet or other networks. Secuplat NIDS detects intrusions over the network and responds without decreasing network speed.

Sentarus CounterSleuth ⇨🗋
by Silicon Defense
Sentarus CounterSleuth is a military-grade intelligent network intrusion detection (INID) system that goes far beyond traditional defenses to proactively profile network attackers by employing behavior-based, real-time analysis of suspicious traffic patterns. Unlike most network intrusion detection (NID) systems that only protect against invasion of known threats, Silicon Defense's INID technology detects 'ground zero' attacks, that is, as yet unseen threats. CounterSleuth catches the most dangerous top 5 percent of dedicated internal and external attackers, allowing companies to protect against network-based threats.

Shadow IDS ⇨🗋

automated policy enforcement and incident response for servers, applications, and data. As a complement to firewalls and other access controls, it enables administrators to develop proactive policies to stop hackers or authorized users with malicious intent from misusing systems.

Hogwash ⇨

by Jason Larsen
Hogwash is an intrusion detection system (IDS)/packet scrubber. It can detect attacks on your network, and if you want, filter them out.

IDSA ⇨

by Marc Welz
The idsa project tries to help programmers add a simple form of security awareness to their applications. Idsa does this by providing an integrated reference monitor, logger and IDS which is accessible to applications through a simple API. Applications can use this infrastructure to delegate access control and intruder detection to idsa.

IDS Balancer ⇨

by Top Layer Networks
The Top Layer IDS Balancer family of products are the only balancers optimized specifically for overcoming IDS performance issues. The IDS Balancer maximizes the effectiveness, availability, and performance of your IDS solution, and addresses specific deployment issues these devices face in several environments. The IDS Balancer is a dedicated security appliance that provides simultaneous monitoring of multiple network segments at a full range of network speeds up to multi-Gigabit configurations.

iForce Intrusion Detection Appliance ⇨

by Sun and Symantec
iForce Intrusion Detection Appliance powered by Sun and Symantec is a comprehensive, pre-configured security solution that offers "out-of-the-box" experience, ease of use, and simplified daily operations to help lower TCO (Total Cost of Ownership). The Sun LX50 server, running the enterprise-class Solaris OS x86, the powerful, two-way server for compute-intensive environments, coupled with Symantec ManHunt security software enables enterprise-wide multi-source event collection. The solution provides a highly effective and coordinated approach to managing intrusion detection security. Symantec ManHunt, a network-based intrusion detection system, protects vital information infrastructures with enterprise-wide high-speed gigabit detection, real-time threat analysis, and policy-based responses to guard against intrusions and attacks. The iForce IDS Appliance gathers intelligence from across the enterprise to quickly identify and respond to both known and unknown (or zero-day) attacks.

iForce Intrusion Management

by the CIDER Project
SHADOW is an Intrusion Detection system developed on inexpensive PC hardware running Open Source, public domain, or freely available software.

Shoki IDS ⇨

by Stephen P. Berry
Shoki is a free, open source network intrusion detection system for conducting traffic analysis. The fundamental design goals of shoki are: 1) Simplicity: The components of shoki are designed to be as straightforward (and therefore as easy to understand) as possible. 2) Modularity: The functionalities provided by the various components of shoki are intended to be as decoupled from each other as practically possible. Major features include: Signature matching using libpcap-style filter expressions, Support for searches using POSIX extended regular expressions, Optional support for searches using Perl-compatible regular expressions, Dynamic rule-based signature generation, Correlation of data from multiple sources.

Siren ⇨

by Penta Security
Siren is an Intrusion Detection System capable of detecting and responding to technical attacks. As a hybrid type IDS, Siren incorporates both misuse detection as well as anomaly detection for maximum protection.

Snort IDS ⇨

by Marty Roesch
Snort is an open source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.

Snort-Wireless ⇨

by Andrew Lockhart
The Snort-Wireless project is an attempt to make a scalable (and free!) 802.11 intrusion detection system that is easily integratable into an IDS infrastructure. It is completely backwards compatible with Snort 2.0.x and adds several additional features. Currently it allows for 802.11 specific detection rules through the new "wifi" rule protocol, as well as rogue AP, AdHoc network, and Netstumbler detection. Many more new features are planned for future releases. Bascially, Snort-Wireless intends to eventually be the opensource answer to AirDefense.

Sourcefire IMS ⇨

by Sourcefire Inc.
Sourcefire Intrusion Management System (IMS) is the industry's first fully integrated security monitoring infrastructure for identifying and protecting against network threats. Unlike current intrusion detection systems, Sourcefire offers a comprehensive system that gives one visibility, flexibility,

Appliance ⇨🗋
by Sun and Sourcefire
iForce Intrusion Management Appliance, Powered by Sun and Sourcefire is the industry's leading complete intrusion detection system - delivering all of the capabilities needed to proactively defend against intruders. Unlike current intrusion detection systems, Sourcefire offers a comprehensive system that gives one granular flexibility, scalability, and complete data management. iForce Intrusion Management Appliance, Powered by Sun and Sourcefire offers the industry's best protection and allows users to customize every aspect of the system to suit their specific environment and security needs.

iForce Intrusion Prevention Appliance (Sleuth9) ⇨🗋
by Sun and DeepNines
Sleuth9 is a new, proactive, intelligent, intrusion prevention and anti-virus solution specifically designed to stop complex, blended threats. Sleuth9 sits in front of the router and evaluates all network traffic at the packet level, both ingress and egress, to determine what is valid and what is malicious. Sleuth9 detects and automatically prevents cyber attacks from entering or leaving a network by forming a new perimeter of defense against DoS, DDoS, port scans, Trojan horses, self-propagating attacks, worms and viruses, as well as other attacks launched from infected internal or external computers.

Intruder Alert ⇨🗋
by Symantec
Symantec Intruder Alert is a host-based, real-time intrusion monitoring system that detects unauthorized activity and security breaches and responds automatically. If Intruder Alert detects a threat, it sounds an alarm or takes other countermeasures according to pre-established security policies in order to prevent information loss or theft.

Intrusion Alert ⇨🗋
by Unified Access
Intrusion Alert protects your organization by intelligently monitoring and responding to electronic fraud, espionage, theft and snooping by people within your network and hackers outside of your network. Intrusion Alert mitigates the risk of unwanted activity and intrusion on a computer network.

Intrusion Detection Appliance ⇨🗋
by Intrusion Inc.
Intrusion Inc.'s suite of security products helps businesses protect critical information assets by quickly detecting, analyzing and responding to network and host-based attacks. The company's products include intrusion detection, VPN/Firewall and vulnerability assessment systems and modular, scalable security platforms.

Intrusion and Detection Platform ⇨🗋
scalability, and complete data management. Sourcefire IMS offers the industry's best protection and allows users to customize every aspect of the system to suit their specific environment and security needs.

STAT Neutralizer ⇨🗋
by Harris Corp.
Far exceeding traditional network security methods, STAT Neutralizer provides real-time defense for your networked computers against malicious code (like Trojan horses and email viruses), hackers, intrusion attempts and even human error. Protection is based upon rules of behavior rather than signatures, which allows STAT Neutralizer to effectively shield your systems from new, unknown types of attacks as well as traditional ones.

StealthWatch ⇨🗋
by Lancope
StealthWatch identifies network misuse and abuse, service usage and IP behavior and allows security teams to track suspicious behavior and network misuse before it's too late. For more comprehensive protection, multiple StealthWatch appliances may be deployed at key points along the network, allowing teams to profile activity, detect security breaches and keep tabs on bandwidth usage and abuses.

Systrace ⇨🗋
by Niels Provos
Systrace enforces system call policies for applications by constraining the application's access to the system. The policy is generated interactively. Operations not covered by the policy raise an alarm, allowing an user to refine the currently configured policy.

Tamandua ⇨🗋
by Tamandua Labs
A free light-weight network intrusion detection system. Tamandua NID intends to get fast and reliable intrusion detection mechanism by analyzing the network contents on its powerful multi layering boolean technic (MLB) providing realiable logs and less false-positives. With MLB, you can not only detect an attempt, but making sure if this attempt has been successfully exploited.

Tivoli Access Manager for Operating Systems ⇨🗋
by IBM
Tivoli Access Manager for Operating Systems can help protect individual application and operating system resources, enforce security policies consistently across the enterprise with a single security model, prevent unauthorized access, monitor sensitive access and send alerts to a centralized event management console.

UnityOne Network Defense System ⇨🗋
by TippingPoint Technologies
UnityOne Network-Based Intrusion Prevention Appliances and Systems provide true intrusion

by Netscreen
The NetScreen Intrusion Detection and Prevention (NetScreen-IDP) system effectively identifies and stops attacks on your network, minimizing the time and costs associated with intrusions. It compliments your firewall, providing the next layer of security by looking deep into the network traffic to accurately identify intrusions and stop the attacks from ever reaching their destination.

prevention. Based on breakthrough high-speed security processors, UnityOne stops cyber attacks in your network before such attacks can infect, damage or destroy core IT assets.

© 2002-2003 HONEYPOTS.NET. All rights reserved.
Page last modified on Tue 24 February 2004 11:57:13 CET
HONEYPOTS.NET - HONEYPOTS.ORG - INTRUSIONS.ORG
INTRUSION-DETECTION.NET - INTRUSION-DETECTION.ORG
INCIDENT-HANDLING.COM - INCIDENT-RESPONSE.COM

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.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

20350 7590 03/26/2004

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

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	12

DATE MAILED: 03/26/2004

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

Office Action Summary	Application No.	Applicant(s)	
	09/766,343	SCHNEIER ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- 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) 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 the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- 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 _____.

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) *1-44* 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) *1-44* is/are rejected.

7)☐ Claim(s) _____ 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) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. 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:

> (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.

2. Claims 1-44 are rejected under 35 U.S.C. 102(b) as being anticipated by Esbensen(5,796,942).

3. As per claims 1, 19, Esbensen discloses a method of operating a probe(i.e. remote surveillance agents, RSA) as part of a security monitoring system for a computer network(see col. 7, lines 19-23), collecting status data from at least one monitored component of the network(see col. 7, lines 23-27); identifying potentially security-related events pertaining to the network by analyzing the status data(see col. 7, lines 28-30); transmitting information about the identified events to an analyst associated with the security monitoring system(see col. 5, lines 22-28, col. 7, lines 30-34) ; receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system in a manner customized to the network(see col. 5, lines 56-59); and dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback in a manner customized to the network(see col. 5, lines 60-65).

4. As per claim 2, Esbensen discloses wherein the identifying step includes performing a multi-stage analysis of the status data(see col. 5, lines 14-21).

5. As per claim 3, Esbensen discloses wherein the multi-stage analysis includes performing a discrimination analysis on the status data(see col. 5, lines 14-21).

6. As per claim 4, Esbensen discloses wherein the discrimination analysis includes positive filtering(see col. 5, lines 1-13).

7. As per claim 5, Esbensen discloses wherein the discrimination analysis includes negative filtering(see col. 5, lines 1-13).

8. As per claims 6 and 24, Esbensen discloses post filtering residue(see col. 5, lines 1-13).

9. As per claim 7, Esbensen discloses wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe(see col. 7, lines 19-54).

10. As per claim 8, Esbensen discloses identifying step includes aggregating and synthesizing the status data at the probe(see col. 7, lines 19-34).

11. As per claim 9, Esbensen discloses wherein the identifying step includes cross-correlating data across the monitored components(see col. 7, lines 35-43).

12. As per claim 10, Esbensen discloses identifying step includes analyzing the frequency of occurrence of the events(see col. 5, lines 14-21).

13. As per claim 11, Esbensen discloses computer based analysis at a secure operations center configured to receive data from the probe(see col. 7, lines 19-43).

14. As per claim 12, Esbensen discloses computer-based analysis includes aggregating, synthesizing, presenting alerts on an ensemble basis(see col. 5, lines 14-28).

15. As per claim 13, it is rejected under the same basis as claim 9.

16. As per claim 14, it is rejected under the same basis as claim 10.

17. As per claim 15, Esbensen discloses computer-based analysis includes cross-probe correlation(see col. 7, lines 19-43).

18. As per claim 16, Esbensen discloses self-tuning the probe based on previously collected status data(see col. 5, lines 60-65).

19. As per claim 17, Esbensen discloses wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts(see col. 5, lines 14-59).

20. As per claim 18, Esbensen discloses wherein the receiving feedback step occurs in substantially real time(see col. 14-50).

21. As per claim 20, it is rejected under the same basis as claim 2.

22. As per claim 21, it is rejected under the same basis as claim 3.

23. As per claim 22, it is rejected under the same basis as claim 4.

24. As per claim 23, it is rejected under the same basis as claim 5.

25. As per claim 25, it is rejected under the same basis as claim 7.

26. As per claim 26, it is rejected under the same basis as claim 8.

27. As per claim 27, it is rejected under the same basis as claim 9.

28. As per claim 28, it is rejected under the same basis as claim 11.

29. As per claim 30, it is rejected under the same basis as claim 12.

30. As per claim 31, it is rejected under the same basis as claim 9.

31. As per claim 32, it is rejected under the same basis as claim 10.

32. As per claim 33, it is rejected under the same basis as claim 15.

33. As per claim 34, it is rejected under the same basis as claim 16.

34. As per claim 35, it is rejected under the same basis as claim 17.

35. As per claim 36, it is rejected under the same basis as claim 18.

36. As per claim 37, it is rejected under the same basis as claim 1, and further claim 37, is rejected for a plurality of sensors for monitoring components of the network, is inherent is intrusion detection, proof of this inherency is provided by Fratto, in which he teaches net ranger sensors that monitor the network.

37. As per claim 38, it is rejected under the same basis as claim 3.

38. As per claim 39, limitations have already been addressed(see claim 4).

39. As per claim 40, limitations have already been addressed(see claim 5).

40. As per claim 41, it is rejected under the same basis as claim 7.

41. As per claim 42, Esbensen discloses wherein the multi-stage analysis includes analysis at the probe and analysis at the secure operations center(see col. 7, lines 19-33).

37. As per claim 43, limitations have already been addressed(see claim 7).

38. As per claim 44, Esbensen discloses wherein the computer-based analysis is configured to correlate data from different probes(see col. 7, lines 19-43).

Cited Art, But Not Applied

39. Fratto, teaches a managed security service that monitors the customer's network, 24 hours 7 days a week. However, Fratto is silent on a probe, it is inherent is managed security service..

40. M2 Presswire, August and September article also teaches managed security service.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

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).

***

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control 09/766,343	Applicant(s)/Patent Under Reexamination SCHNEIER ET AL.	
	Examiner Jenise E Jackson	Art Unit 2131	Page 1 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,796,942	08-1998	Esbensen, Daniel	713/201
	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 Country Code-Number-Kind Code	Date 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	M2 Presswire, September 3, 1999, pg. 1-3. ✓
	V	VPNTrust: Consulting, 1999, pg. 1-3. ✓
	W	Fratto, November 1, 1998, vol. 9, iss. 20; pg. 68, pg. 1-12. ✓
	X	M2 Presswire, August 31, 1999, pg. 1. ✓

*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.

Notice of References Cited	Application/Control No. 09/766,343	Applicant(s)/Patent Under Reexamination SCHNEIER ET AL.	
	Examiner Jenise E Jackson	Art Unit 2131	Page 2 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	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 Country Code-Number-Kind Code	Date 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	http://www.redsiren.com, pg. 1-3. ✓
	V	http://www.rkontechnologies.com ✓
	W	Messmer, April 3, 2000, Network World ✓
	X	Communication News, June 2000. ✓

*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.

Notice of References Cited	Application/Control No. 09/766,343	Applicant(s)/Patent Under Reexamination SCHNEIER ET AL.	
	Examiner Jenise E Jackson	Art Unit 2131	Page 3 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	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 Country Code-Number-Kind Code	Date 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	Savage, Computer Reseller News, September 25, 2000. ✓
	V	Information Week, 2000, n 792, pg 244. ✓
	W	Essex, Computerworld, June 12, 2000. ✓
	X	Blacharski, Network Magazine, August 1, 2000. ✓

*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.

Notice of References Cited	Application/Control No. 09/766,343	Applicant(s)/Patent Under Reexamination SCHNEIER ET AL.	
	Examiner Jenise E Jackson	Art Unit 2131	Page 4 of 4

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A.	US-			
	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 Country Code-Number-Kind Code	Date 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	ENT, November 22, 2000. ✓
	V	Computel white papers, 2001, pg. 1-4. ✓
	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.

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Docket Number (Optional)	Application Number
028490-0001	09/766,343
Applicant(s) B. Schneier et al.	
Filing Date January 19, 2001	**Group Art Unit** 2131

PATENT & TRADEMARK OFFICE DATE AUG 27 2001 JC1687

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL	REF	DOCUMENT NUMBER		NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
		6,205,551 B1	3/20/01	Grosse			
		5,909,493	6/1/99	Motoyama			
		5,796,942	8/18/98	Esbensen			

RECEIVED
AUG 29 2001
Technology Center 2100

FOREIGN PATENT DOCUMENTS

	REF	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	Translation YES	Translation NO

OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*

EXAMINER	DATE CONSIDERED
	3/11/04

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

#9

INFORMATION DISCLOSURE CITATION

(Use several sheets if necessary)

Docket Number (Optional)	Application Number
028490-[redacted]	09/766,343 #9
Applicant(s)	
B. Schneier et al.	
Filing Date	**Group Art Unit**
Jan. 19, 2001	2131

*EXAMINER INITIAL		OTHER DOCUMENTS *(Including Author, Title, Date, Pertinent Pages, Etc.)*
		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 98/05, June 11, 1998, pp. 1-19.
		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, October 1997, pp. 1-12.
		Citation details: "Automated Information System - (AIS) Alarm System," W. Hunteman, http://citeseer.nj.nec.com/context/1642652/0, downloaded October 19, 2001, 1 p.
		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, 11-12 April 1999, pages 73-80, http://www.csl.sri.com/users/neumann/det99.html, downloaded October 19, 2001, pp. 1-9.
		Porras, P. A. et al., "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disburbances," Computer Science Laboratory, SRI International, 20th NISSC - October 9, 1997 pp. 1-22 (version with legible text but no figures) pp. 1-13 (version with figures but illegible text)
		"FAQ: Network Intrusion Detection Systems," Version 0.3, January 1, 1998, http://www.robertgraham.com/pubs/network-instrusion-detection.txt, downloaded October 19, 2001, pp. 1-29.

EXAMINER	DATE CONSIDERED
[signature]	3/11/04

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

OIPE JUL 29 2004 PATENT & TRADEMARK OFFICE

2131 #5
V 91

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

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

On 7-26-04

TOWNSEND and TOWNSEND and CREW LLP

By: [signature]

PATENT
Attorney Docket No.: 022133-000510US

RECEIVED
AUG 0 3 2004
Technology Center 2100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 7642
Bruce Schneier	Examiner: Jenise Jackson
Application No.: 09/766,343	Technology Center/Art Unit: 2131
Filed: January 19, 2001	AMENDMENT
For: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Customer No.: 20350	

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

Sir:

In response to the Office Action mailed March 26, 2004, 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 9 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. (Currently Amended) A method of operating a probe as part of a security monitoring system for a computer network, comprising:

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

b) analyzing status data to identify~~ing~~ potentially security-related events represented in the ~~pertaining to said network by analyzing said~~ 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) transmitting information about said identified events to an analyst system 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~~.

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

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

4. (Original) The method of claim 3, wherein the discrimination analysis includes positive filtering.

5. (Original) The method of claim 3, wherein the discrimination analysis includes negative filtering.

6. (Canceled)

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

8. (Original) The method of claim 1, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

9. (Original) The method of claim 8, wherein said identifying step includes cross-correlating data across said monitored components.

10. (Original) The method of claim 8, wherein said identifying step includes analyzing the frequency of occurrence of said events.

11. (Original) The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.

12. (Original) The method of claim 11, wherein said computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

13. (Original) The method of claim 11, wherein said identifying step includes cross-correlating data across said monitored components.

14. (Original) The method of claim 11, wherein said identifying step includes analyzing the frequency of occurrence of said events.

15. (Original) The method of claim 11, wherein said computer-based analysis includes cross-probe correlation.

16. (Original) The method of claim l, further comprising instantaneously self-tuning said probe based on previously collected status data.

17. (Original) The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

18. (Original) The method of claim 1, wherein said receiving feedback step occurs in substantially real time.

19. (Currently Amended) A computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of:

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

b) analyzing status data to identify~~ing~~ potentially security-related events represented in the ~~pertaining to said network by analyzing said~~ 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) transmitting information about said identified events to an analyst system 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. (Original) The computer-readable medium of claim 19, wherein said identifying step includes performing a multi-stage analysis of said status data.

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

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

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

24. (Canceled)

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

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

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

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

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

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

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

33. (Original) The computer-readable medium of claim 29, wherein said computer-based analysis includes cross-probe correlation.

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

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

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

37. (Currently Amended) A security monitoring system for a computer network, comprising

a) a plurality of sensors for monitoring components of said network;

b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and

c) at least one probe, wherein said probe is configured to

(1) collect status data from at least one sensor monitoring at least one component of said network;

(2) analyzing status data to identify potentially security-related events represented in the ~~pertaining to said network by analyzing said~~ 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;

(3) transmit information about said identified events to an analyst system associated with said secure operations center;

(4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system ~~in a manner customized to said network~~; and

(5) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback ~~in a manner customized to said network~~.

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

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

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

41. (Original) The security monitoring system of claim 37, wherein said probe and said secure operations center are configured to identify potentially security-related events by performing a multistage analysis of said status data.

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

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

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

REMARKS/ARGUMENTS

Claims 1-44 were pending. Claims 1, 19, and 37 have been amended; claims 6 and 24 have been canceled; and no claims are added. Thus, claims 1-5, 7-23, and 25-44 remain pending.

35 U.S.C. §102(b) Rejection, Esbensen.

In the Office Action, claims 1-44 were rejected under 35 USC §102(b) as being unpatentable over Esbensen (U.S. Patent Number 5,796,942). Reconsideration in view of the following remarks is respectfully requested.

I. Claim 1-5, 7-18

Esbensen fails to anticipate claim 1 because it fails to disclose or suggest each element of claim 1. For example, claim1 recites, among other elements, "analyzing 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." In the Office Action in paragraph 8, the Examiner asserts that Esbensen's reconstruction of session data (citing to column 5 lines 1-13 of Esbensen) anticipates the analysis of post-filtering residue in claim 1, formerly in claim 6.

In col. 5 lines 1-8, Esbensen discusses reconstructing session data that may be in separate record files into a single session window in order to "detect patterns that cross record files," and not as a filtering step. In col. 5 lines 9-13, Esbensen states "[t]he reconstructed session data is passed through a series of user-defined rules." "When . . . a session window contains the pattern, the alert is triggered." In this part of Esbensen, there is no mention of session data that does not contain a pattern specified by a rule, and particularly there is no mention of any analysis of such data. Thus, Esbensen does not teach of analyzing post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.

For at least the reasons stated above, Applicant submits that claim 1 is allowable over the cited references. As claim 1 is allowable, claims 2-5 and 7-18 dependent therefrom are also allowable for at least that reason.

II. Claim 19-23, 25-36

Claim 19 recites similar features as recited for claim 1, thus claim 19 and its dependent claims should be allowable for at least similar reasons as claim 1.

III. Claim 37-44

Claim 37 recites similar features as recited for claim 1, thus claim 37 and its dependent claims should be allowable for at least similar reasons as claim 1.

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 415-576-0200.

Respectfully submitted,

Brian N. Young
Reg. No. 48,602

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
Attachments
PHA:jtc
60217253 v1

OIPE
JUL 29 2004
PATENT & TRADEMARK OFFICE

PTO/SB/21 (04-04)

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/766,343
Filing Date	January 19, 2001
First Named Inventor	Schneier, Bruce
Art Unit	2131
Examiner Name	Jenise Jackson
Total Number of Pages in This Submission: 12	Attorney Docket Number: 022133-000510US

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☒ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☒ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):

Return Postcard

Remarks: The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

RECEIVED
AUG 0 3 2004
Technology Center 2100

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Townsend and Townsend and Crew LLP Brian N. Young Reg. No. 48,602
Signature	
Date	July 26, 2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	D. Bullock		
Signature		Date	July 26, 2004

60269363 v1

OIPE
JUL 2 9 2004
PATENT & TRADEMARK OFFICE

PTO/SB/22 (08-03)

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 022133-000510US

In re Application of Bruce Schneier	
Application Number 09/766,343	Filed January 19, 2001
For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Art Unit 2131	Examiner Jenise 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 appropriate non-small-entity fee are as follows (check time period desired):

RECEIVED
AUG 0 3 2004
Technology Center 2100

- ☒ One month (37 CFR 1.17(a)(1)) $110
- ☐ Two months (37 CFR 1.17(a)(2)) $
- ☐ Three months (37 CFR 1.17(a)(3)) $
- ☐ Four months (37 CFR 1.17(a)(4)) $
- ☐ Five months (37 CFR 1.17(a)(5)) $

☒ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee amount shown above is reduced by one-half, and the resulting fee is: $ 55 .

☐ 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.

I have enclosed a duplicate copy of this sheet.

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 48,602

☐ attorney or agent under 37 CFR 1.34(a).

Registration number if acting under 37 CFR 1.34(a). _____ .

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.

July 26, 2004
Date

Signature

Brian N. Young, Reg. No. 48,602
Typed or printed name

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.

60269366 v1

07/30/2004 WASFAW1 00000034 201430 09766343

01 FC:2251 55.00 DA

OIPE
JUL 2 9 2004
PATENT & TRADEMARK OFFICE

PTO/SB/22 (08-03)

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 022133-000510US

In re Application of Bruce Schneier	
Application Number 09/766,343	Filed January 19, 2001
For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Art Unit 2131	Examiner Jenise 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 appropriate non-small-entity fee are as follows (check time period desired):

RECEIVED
AUG 0 3 2004
Technology Center 2100

- ☒ One month (37 CFR 1.17(a)(1)) $110
- ☐ Two months (37 CFR 1.17(a)(2)) $
- ☐ Three months (37 CFR 1.17(a)(3)) $
- ☐ Four months (37 CFR 1.17(a)(4)) $
- ☐ Five months (37 CFR 1.17(a)(5)) $

☒ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee amount shown above is reduced by one-half, and the resulting fee is: $ 55 .

☐ 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.

I have enclosed a duplicate copy of this sheet.

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 48,602

☐ attorney or agent under 37 CFR 1.34(a).

Registration number if acting under 37 CFR 1.34(a). _____ .

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.

July 26, 2004
Date

Signature

Brian N. Young, Reg. No. 48,602
Typed or printed name

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.

60269366 v1

07/30/2004 WASFAW1 00000034 201430 09766343

01 FC:2251 55.00 DA

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2000

Application or Docket Number: 9.766343

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	44	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	44 minus 20=	* 24
INDEPENDENT CLAIMS	3 minus 3 =	* 0
MULTIPLE DEPENDENT CLAIM PRESENT		☐

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

SMALL ENTITY TYPE ☐			OR	OTHER THAN SMALL ENTITY	
RATE	FEE			RATE	FEE
BASIC FEE	355.00		OR	BASIC FEE	710.00
X$ 9=			OR	X$18=	432.00
X40=			OR	X80=	
+135=			OR	+270=	
TOTAL			OR	TOTAL	1142.00

7/29/04

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 42	Minus	** 44	=
Independent	* 3	Minus	*** 3	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY			OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE			RATE	ADDITIONAL FEE
X$ 9=			OR	X$18=	
X40=			OR	X80=	
+135=			OR	+270=	
TOTAL ADDIT. FEE			OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. 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.

Refine Search

Search Results -

Terms	Documents
L27 and admin	41

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L28

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Thursday, January 06, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; PLUR=YES; OP=OR		
L28	L27 and admin	41	L28
L27	L26 and intrusion adj detection	334	L27
L26	filtering(2n)residue	461237	L26
L25	L23 and filtering	277	L25
L24	L23 and filtering(2n)residue	308142	L24
L23	713/201.ccls.	1485	L23
L22	713/201.ccls. and filtering(2n)reside and intrusion adj detection	43897	L22
L21	713/201.ccls. and filtering(2n)residue	308142	L21
L20	L19 and alert	109	L20
L19	L17 and intrusion adj detection	333	L19
L18	L17 and intrusion	1950	L18
L17	filtering(2n)residue and network	235296	L17
L16	713/201.ccls. and honeypot	2	L16
L15	713/201.ccls. and sentry	6	L15

L14	L13 and network	70	L14
L13	audit adj logs and filter?	70	L13
L12	L11 and intrusion	109	L12
L11	L10 and filter?	4718	L11
L10	probe and network	18692	L10
L9	L8 and filter?	41	L9
L8	sentry and network	184	L8
L7	L6 and anomaly	15	L7
L6	sentry	763	L6
L5	L4 and residue	2	L5
L4	L3 and anomaly	45	L4
L3	L2 and detect?	543	L3
L2	filter? and intrusion	1835	L2
L1	anomaly adj engine and network	5	L1

END OF SEARCH HISTORY

WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Thursday, January 06, 2005

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=OR	
☐	L28	L27 and admin	41
☐	L27	L26 and intrusion adj detection	334
☐	L26	filtering(2n)residue	461237
☐	L25	L23 and filtering	277
☐	L24	L23 and filtering(2n)residue	308142
☐	L23	713/201.ccls.	1485
☐	L22	713/201.ccls. and filtering(2n)reside and intrusion adj detection	43897
☐	L21	713/201.ccls. and filtering(2n)residue	308142
☐	L20	L19 and alert	109
☐	L19	L17 and intrusion adj detection	333
☐	L18	L17 and intrusion	1950
☐	L17	filtering(2n)residue and network	235296
☐	L16	713/201.ccls. and honeypot	2
☐	L15	713/201.ccls. and sentry	6
☐	L14	L13 and network	70
☐	L13	audit adj logs and filter?	70
☐	L12	L11 and intrusion	109
☐	L11	L10 and filter?	4718
☐	L10	probe and network	18692
☐	L9	L8 and filter?	41
☐	L8	sentry and network	184
☐	L7	L6 and anomaly	15
☐	L6	sentry	763
☐	L5	L4 and residue	2
☐	L4	L3 and anomaly	45
☐	L3	L2 and detect?	543
☐	L2	filter? and intrusion	1835
☐	L1	anomaly adj engine and network	5

END OF SEARCH HISTORY



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.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

20350 7590 01/13/2005

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

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/13/2005

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

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)	
	09/766,343	SCHNEIER ET AL.	
	Examin r	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the c ver sheet with the corresp ndence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) 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 the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- 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 _____.

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) 1-44 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) 1-44 is/are rejected.

7)☐ Claim(s) _____ 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) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Final Action

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-44 are rejected under 35 U.S.C. 103(a) as being obvious over Esbensen(5,796,942) in view of Porras(6,704,874).

3. As per claims 1, 19, Esbensen discloses a method of operating a probe(i.e. remote surveillance agents, RSA) as part of a security monitoring system for a computer network(see col. 7, lines 19-23), collecting status data from at least one monitored component of the network(see col. 7, lines 23-27); identifying potentially security-related events pertaining to the network by analyzing the status data(see col. 7, lines 28-30); transmitting information about the identified events to an analyst associated with the security monitoring system(see col. 5, lines 22-28, col. 7, lines 30-34) ; receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system in a manner customized to the network(see col. 5, lines 56-59); and dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback in a manner customized to the network(see col. 5, lines 60-65). Esbensen does not disclose wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded or selected by filtering. Porras et al. discloses wherein the analysis

includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded or selected by filtering (see col. 3, lines 61-67, col. 4, lines 1-32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include post filtering reside that is data neither discarded or selected by filtering of Porras, because the motivation is that the data that is left, that has not been filtered, which is the raw data of Porras can be analyzed further.

4. As per claim 2, Esbensen discloses wherein the identifying step includes performing a multi-stage analysis of the status data(see col. 5, lines 14-21).

5. As per claim 3, Esbensen discloses wherein the multi-stage analysis includes performing a discrimination analysis on the status data(see col. 5, lines 14-21).

6. As per claim 4, Esbensen discloses wherein the discrimination analysis includes positive filtering(see col. 5, lines 1-13).

7. As per claim 5, Esbensen discloses wherein the discrimination analysis includes negative filtering(see col. 5, lines 1-13).

8. As per claims 6 and 24, Esbensen discloses post-filtering residue(see col. 5, lines 1-13).

9. As per claim 7, Esbensen discloses wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe(see col. 7, lines 19-54).

10. As per claim 8, Esbensen discloses identifying step includes aggregating and synthesizing the status data at the probe(see col. 7, lines 19-34).

11. As per claim 9, Esbensen discloses wherein the identifying step includes cross-correlating data across the monitored components(see col. 7, lines 35-43).

12. As per claim 10, Esbensen discloses identifying step includes analyzing the frequency of occurrence of the events(see col. 5, lines 14-21).

13. As per claim 11, Esbensen discloses computer based analysis at a secure operations center configured to receive data from the probe(see col. 7, lines 19-43).

14. As per claim 12, Esbensen discloses computer-based analysis includes aggregating, synthesizing, presenting alerts on an ensemble basis(see col. 5, lines 14-28).

15. As per claim 13, it is rejected under the same basis as claim 9.

16. As per claim 14, it is rejected under the same basis as claim 10.

17. As per claim 15, Esbensen discloses computer-based analysis includes cross-probe correlation(see col. 7, lines 19-43).

18. As per claim 16, Esbensen discloses self-tuning the probe based on previously collected status data(see col. 5, lines 60-65).

19. As per claim 17, Esbensen discloses wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts(see col. 5, lines 14-59).

20. As per claim 18, Esbensen discloses wherein the receiving feedback step occurs in substantially real time(see col. 14-50).

21. As per claim 20, it is rejected under the same basis as claim 2.

22. As per claim 21, it is rejected under the same basis as claim 3.

23. As per claim 22, it is rejected under the same basis as claim 4.

24. As per claim 23, it is rejected under the same basis as claim 5.

25. As per claim 25, it is rejected under the same basis as claim 7.

26. As per claim 26, it is rejected under the same basis as claim 8.

27. As per claim 27, it is rejected under the same basis as claim 9.

28. As per claim 28, it is rejected under the same basis as claim 11.

29. As per claim 30, it is rejected under the same basis as claim 12.

30. As per claim 31, it is rejected under the same basis as claim 9.

31. As per claim 32, it is rejected under the same basis as claim 10.

32. As per claim 33, it is rejected under the same basis as claim 15.

33. As per claim 34, it is rejected under the same basis as claim 16.

34. As per claim 35, it is rejected under the same basis as claim 17.

35. As per claim 36, it is rejected under the same basis as claim 18.

36. As per claim 37, it is rejected under the same basis as claim 1, and further claim 37, is rejected for a plurality of sensors for monitoring components of the network, is inherent is intrusion detection, proof of this inherency is provided by Fratto, in which he teaches net ranger sensors that monitor the network.

37. As per claim 38, it is rejected under the same basis as claim 3.

38. As per claim 39, limitations have already been addressed(see claim 4).

39. As per claim 40, limitations have already been addressed(see claim 5).

40. As per claim 41, it is rejected under the same basis as claim 7.

41. As per claim 42, Esbensen discloses wherein the multi-stage analysis includes analysis at the probe and analysis at the secure operations center(see col. 7, lines 19-33).

42. As per claim 43, limitations have already been addressed(see claim 7).

43. As per claim 44, Esbensen discloses wherein the computer-based analysis is configured to correlate data from different probes(see col. 7, lines 19-43).

Response to Amendment

44. The Applicant has stated that Esbensen does not disclose, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering reside is data neither discarded nor selected by filtering. The Examiner did not use Esbensen to reject new limitations. Porras has been applied to this limitation (see above for explanation). Thus, this rejection is Final, Necessitated by Amendment.

Final, Necessitated by Amendment

45. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). 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 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 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 (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

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).

Jenise Jackson

January 7, 2004

E. Moise

EMMANUEL MOISE
PRIMARY EXAMINER

Notice of References Cited	Application/Control No. 09/766,343	Applicant(s)/Patent Under Reexamination SCHNEIER ET AL.	
	Examiner Jenise E Jackson	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,704,874	03-2004	Porras et al.	713/201
	B	US-6,182,226	01-2001	Reid et al.	713/201
	C	US-6,681,331	01-2004	Munson et al.	713/201
	D	US-6,363,489	03-2002	Comay et al.	713/201
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date 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.

Index of Claims

Application No.	Applicant(s)	
09/766,343	SCHNEIER ET AL.	
Examiner	**Art Unit**	
Jenise E Jackson	2131	

√	Reject d	–	(Through numeral) Cancelled	N	Non-Elected	A	App al
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	11/6/05
	1	√
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	√
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

Search Notes	Application N .	Applicant(s)	
	09/766,343	SCHNEIER ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

SEARCHED			
Class	Subclass	Date	Examiner
713	200-201	12/29/04	DQ
709	223-224 229	↓	↓

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
West search Update	1/6/04	DQ

Atty Docket No. 022133-000510US

PTO FAX NO.: 1 703 872-9306

ATTENTION: Examiner Jenise Jackson Group Art Unit 2131

OFFICIAL COMMUNICATION

FOR THE PERSONAL ATTENTION OF

EXAMINER Jenise Jackson

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that the following documents in re Application of Bruce Schneier, Application No. 09/766,343, filed January 19, 2001 for METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE are being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Documents Attached

1. Amendment

Number of pages being transmitted, including this page: 14

Dated: 4/13/05 Lata Olivier

PLEASE CONFIRM RECEIPT OF THIS PAPER BY RETURN FACSIMILE AT (415) 576-0300

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834
Telephone: 415-576-0200
Fax: 415-576-0300
0303

60468095 v1

PAGE 1/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

#Received: 13 pages. CH

I hereby certify that this correspondence is being faxed to: 1 703 872-9306

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

On April 13, 2005

TOWNSEND and TOWNSEND and CREW LLP

By: _____
Lata Olivier

AMENDMENT UNDER 37 CFR 1.116
EXPEDITED PROCEDURE –
EXAMINING GROUP 2131

PATENT
Attorney Docket No.: 022133-000510US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Bruce Schneier

Application No.: 09/766,343

Filed: January 19, 2001

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

Customer No.: 20350

Confirmation No. 7642

Examiner: Jenise Jackson

Technology Center/Art Unit: 2131

AMENDMENT UNDER 37 CFR 1.116
EXPEDITED PROCEDURE EXAMINING
GROUP 2131

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

Sir:

In response to the Final Office Action mailed January 13, 2005 on 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 9 of this paper.

PAGE 2/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

Amendments to the Claims:

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

Listing of Claims:

1. (Previously Presented) A method of operating a probe as part of a security monitoring system for a computer network, comprising:

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

b) analyzing 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) transmitting information about said identified events to an analyst system associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

4. (Original) The method of claim 3, wherein the discrimination analysis includes positive filtering.

PAGE 3/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

5. (Original) The method of claim 3, wherein the discrimination analysis includes negative filtering.

6. (Canceled)

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

8. (Original) The method of claim 1, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

9. (Original) The method of claim 8, wherein said identifying step includes cross-correlating data across said monitored components.

10. (Original) The method of claim 8, wherein said identifying step includes analyzing the frequency of occurrence of said events.

11. (Original) The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.

12. (Original) The method of claim 11, wherein said computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

13. (Original) The method of claim 11, wherein said identifying step includes cross-correlating data across said monitored components.

14. (Original) The method of claim 11, wherein said identifying step includes analyzing the frequency of occurrence of said events.

PAGE 4/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

15. (Original) The method of claim 11, wherein said computer-based analysis includes cross-probe correlation.

16. (Original) The method of claim l, further comprising instantaneously self-tuning said probe based on previously collected status data.

17. (Original) The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

18. (Original) The method of claim 1, wherein said receiving feedback step occurs in substantially real time.

19. (Previously Presented) A computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of:

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

b) analyzing 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) transmitting information about said identified events to an analyst system associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

PAGE 5/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

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

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

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

24. (Canceled)

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

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

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

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

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

PAGE 6/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

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

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

33. (Original) The computer-readable medium of claim 29, wherein said computer-based analysis includes cross-probe correlation.

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

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

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

37. (Currently Amended) A security monitoring system for a computer network, comprising

a) a plurality of sensors for monitoring components of said network;

b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and

c) at least one probe, wherein said probe is configured to

(1) collect status data from at least one sensor monitoring at least one component of said network;

(2) **[analyzing]** **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;

PAGE 7/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

(3) transmit information about said identified events to an analyst system associated with said secure operations center;

(4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system; and

(5) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

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

41. (Original) The security monitoring system of claim 37, wherein said probe and said secure operations center are configured to identify potentially security-related events by performing a multistage analysis of said status data.

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

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

PAGE 8/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

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

PAGE 9/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

REMARKS/ARGUMENTS

Claims 1-5, 7-23, and 25-44 are pending. While the Examiner indicates that claims 1-44 are pending, applicant respectfully submits that claims 6 and 24 were cancelled in the Office Action mailed July 26, 2004.

Claim 37 has been amended to correct a typographical error.

Claims 1-44 were rejected under 35 U.S.C. §103(a), as being obvious over Esbensen (U.S. Patent No. 5,796,942) in view of Porras et al. (U.S. Patent No. 6,704,874). This rejection is respectfully traversed and reconsideration is respectfully requested.

In his rejection of claims 1 and 19, the Examiner admits that Esbensen does not disclose that the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering. However, the Examiner contends that Porras et al. discloses that 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. The Examiner relies on column 3, lines 61-67 and column 4, lines 1-32 of Porras et al. It is respectfully submitted that the Examiner is mistaken in his reliance upon Porras et al.

Porras et al. discloses a network-based alert management system 10 that includes a network 12; a network 14, and a network 16. Each of the networks 12-16 includes a number of computer systems collectively labeled 18, interconnected by an Ethernet cable 20. Each of the networks 12-16 includes security and fault monitoring systems generally labeled 22. Each security and fault monitoring system 22 is linked to an alert manager 24. The alert manager 24 is linked to one or more remote processing centers generally labeled 26. (See column 3, lines 16-25.)

Each of the security and fault monitoring systems 22 produces an alert stream in the form of security alerts, fault reports, and performance logs. The alert stream is sent to the alert manager 24 for collection, processing and distribution to the remote processing center 26. (See column 3, lines 34-38.)

PAGE 10/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

Sensors 22 monitor various host and/or network activity within the networks 12-16, and each sensor 22 generates a stream of alerts, triggered by potentially suspicious events, such as network packet data transfer commands, data transfer errors, network packet data transfer volume, and so forth. The alerts indicate a suspicion of possible malicious intrusion or other threat to operations within the networks 12-16. (See column 3, lines 54-61.)

The alert manager 24 includes a receive-input logic module 28. In an embodiment, the receive-input logic module 28 of the alert manager 24 subscribes, i.e., establishes a transport connection, to receive each of the alert streams produced by the sensors 22 through a secure electronic communication line (SSL) 30. The alert streams contain raw, i.e., unprocessed, alerts. (See column 3, lines 62 - column 4, line 1.) Thus, it is clear that the alerts have not been filtered since Porras et al. clearly disclose that the alerts are raw and unprocessed.

The receive-input logic 28 of the alert manager 24 is equipped with translation modules 32 to translate the original, raw alert streams from the monitors 22 into a common format for further processing, if the alerts do not arrive in the common format. (See column 4, lines 6-10.) In another embodiment, the monitors 22 include conversion software that translates a monitor's raw alert stream into the common format used by the alert manager 24. (See column 4, lines 11-14.) The conversion software may add data items of interest to the alert manager 24 by querying its network 12-16. (See column 4, lines 14-16.)

In another embodiment, a combination of monitors 22 having conversion software and the receive-input logic 28 preprocessing raw alerts in the alert management network 10 are present to accommodate a heterogeneous base of monitors 22 that an end-user desires to manage. (See column 4, lines 17-21.) The alert manager 24 includes an alert processing engine 34. Raw alerts received by the receive-input module 28 and formatted into the common format are sent to the alert processing engine 34. (See column 4, lines 22-26.)

Finally, with reference to Figure 2, an alert management process 50 residing in the alert processing engine 34 includes receiving formatted alerts from the receive-input logic 28. The formatted alerts are passed through user specified filters and alerts not matching criteria of the user-specified filters are discarded. (See column 4, lines 27-32.)

PAGE 11/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

Thus, it is apparent that Porras et al. do not disclose "analyzing 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." While Porras et al. disclose filtering formatted alerts and discarding alerts that do not match certain criteria of the user-specified filters, no mention is made of analyzing data that was not discarded and that was also not selected by the filtering process. Any analysis performed by Porras et al. is clearly done on alerts that were selected by the filtering process.

In contrast to both Porras et al. and Esbensen, claim 1 is directed to a method of operating a probe as part of a security monitoring system for a computer network, wherein the method comprises, among other things, "analyzing 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." Accordingly, since neither Esbensen nor Porras et al., either alone in combination, teach, disclose or even suggest a method as recited in claim 1, it is respectfully submitted that claim 1 is allowable.

Claims 2-5 and 7-18 depend, either directly or indirectly on claim 1, and therefore they are allowable for at least the reasons that claim 1 is allowable.

Claim 19 is directed to a computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of, among other things, "analyzing 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." As discussed above, neither Esbensen nor Porras et al., either alone or in combination, teach, disclose, or even suggest a computer-readable medium as recited in claim 19. Accordingly, it is respectfully submitted that claim 19 is allowable.

PAGE 12/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729308 * CSID:415 576 0300 * DURATION (mm-ss):04-36

Claims 20-23 and 25-36 depend, either directly or indirectly, on claim 19 and therefore, they are allowable for at least the reasons claim 19 is allowable.

Claim 37 is directed to a security monitoring system for a computer network, where the system comprises, among other things, "at least one probe, wherein the probe is configured 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." As discussed above, neither Esbensen nor Porras et al., either alone or in combination, teach, disclose or even suggest a system as recited in claim 37. Accordingly, it is respectfully submitted that claim 37 is allowable.

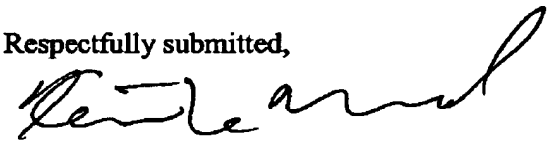
Claims 38-44 depend, either directly or indirectly, on claim 37 and therefore, they are allowable for at least the reasons claim 37 is allowable.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,



Kevin T. LeMond
Reg. No. 35,933

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
KTL:ldr
60467318 v1

PAGE 13/13 * RCVD AT 4/13/2005 6:01:30 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):04-36

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2000

Application or Docket Number: 9.766343

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	44	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	44 minus 20=	* 24
INDEPENDENT CLAIMS	3 minus 3 =	* 0
MULTIPLE DEPENDENT CLAIM PRESENT	☐	

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

SMALL ENTITY TYPE ☐			OR	OTHER THAN SMALL ENTITY	
RATE	FEE			RATE	FEE
BASIC FEE	355.00		OR	BASIC FEE	710.00
X$ 9=			OR	X$18=	432.00
X40=			OR	X80=	
+135=			OR	+270=	
TOTAL			OR	TOTAL	1142.00

7/29/04

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 42	Minus	** 44	=
Independent	* 3	Minus	*** 3	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM	☐			

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

4/13/05

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 42	Minus	** 44	= 0
Independent	* 3	Minus	*** 3	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM	☐			

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
~~X$ 9=~~		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	0

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM	☐			

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. 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.

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.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

20350 7590 04/28/2005

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

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/28/2005

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

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 09/766,343	**Applicant(s)** SCHNEIER ET AL.	
	Examiner Jenise E. Jackson	**Art Unit** 2131	

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

THE REPLY FILED _____ FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☐ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-5,7-23 and 25-44*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: The Applicant's remarks are not persuasive. The Applicant remarks that Porras does not disclose that the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering. The Examiner disagrees with the Applicant. Porras does disclose that the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering. Porras discloses that the end-user subscriber can define his or her own customized user-specified filters(see col. 4, lines 33-40). Porras discloses that the alert streams contain raw alerts(see col. 3, lines 66, col. 4, line 1). The Examiner asserts that data that is left, that has not been filtered, is the raw data of Porras that can be analyzed.

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 M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

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).

Jenise Jackson

April 21, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

RECEIVED
CENTRAL FAX CENTER
JUL 0 6 2005

I hereby certify that this correspondence is being faxed to: 1 703 872-9306

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

On July 6, 2005

TOWNSEND and TOWNSEND and CREW LLP

By: _____
Landon Clark

AMENDMENT UNDER 37 CFR 1.116
EXPEDITED PROCEDURE –
EXAMINING GROUP 2131

PATENT
Attorney Docket No.: 022133-000510US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 7642
Bruce Schneier	Examiner: Jenise Jackson
Application No.: 09/766,343	Technology Center/Art Unit: 2131
Filed: January 19, 2001	SECOND AMENDMENT UNDER 37 CFR 1.116 EXPEDITED PROCEDURE EXAMINING GROUP 2131
For: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Customer No.: 20350	

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

Sir:

In response to the Final Office Action mailed January 13, 2005 on the above-referenced application, the Advisory Action mailed April 28, 2005 and the telephone interview of July 6, 2005, 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 9 of this paper.

PAGE 3/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

RECEIVED
CENTRAL FAX CENTER
JUL 0 6 2005

Atty Docket No. 022133-000510US

PTO FAX NO.: 1-703-872-9306

ATTENTION: Examiner Jenise Jackson Group Art Unit 2131

OFFICIAL COMMUNICATION

FOR THE PERSONAL ATTENTION OF

EXAMINER Jenise Jackson

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that the following documents in re Application of Bruce Schneier, Application No. 09/766,343, filed January 19, 2001 for METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE are being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Documents Attached

1. Petition for Extension of Time Under 37 CFR 1.136(a) (3 months)
2. Amendment

Number of pages being transmitted, including this page: 15

Dated: July 6, 2005 _____
Landon Clark

PLEASE CONFIRM RECEIPT OF THIS PAPER BY RETURN FACSIMILE AT (415) 576-0300

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834
Telephone: 415-576-0200
Fax: 415-576-0300
KTL/llc

60531822 v1

Amendments to the Claims:

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

Listing of Claims:

1. (Previously Presented) A method of operating a probe as part of a security monitoring system for a computer network, comprising:

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

b) analyzing 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) transmitting information about said identified events to an analyst system associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

4. (Original) The method of claim 3, wherein the discrimination analysis includes positive filtering.

PAGE 4/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

5. (Original) The method of claim 3, wherein the discrimination analysis includes negative filtering.

6. (Canceled)

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

8. (Original) The method of claim 1, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

9. (Original) The method of claim 8, wherein said identifying step includes cross-correlating data across said monitored components.

10. (Original) The method of claim 8, wherein said identifying step includes analyzing the frequency of occurrence of said events.

11. (Original) The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.

12. (Original) The method of claim 11, wherein said computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

13. (Original) The method of claim 11, wherein said identifying step includes cross-correlating data across said monitored components.

14. (Original) The method of claim 11, wherein said identifying step includes analyzing the frequency of occurrence of said events.

PAGE 5/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

15. (Original) The method of claim 11, wherein said computer-based analysis includes cross-probe correlation.

16. (Original) The method of claim 1, further comprising instantaneously self-tuning said probe based on previously collected status data.

17. (Original) The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

18. (Original) The method of claim 1, wherein said receiving feedback step occurs in substantially real time.

19. (Previously Presented) A computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of:

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

b) analyzing 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) transmitting information about said identified events to an analyst system associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

PAGE 6/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

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

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

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

24. (Canceled)

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

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

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

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

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

PAGE 7/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

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

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

33. (Original) The computer-readable medium of claim 29, wherein said computer-based analysis includes cross-probe correlation.

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

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

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

37. (Currently Amended) A security monitoring system for a computer network, comprising

a) a plurality of sensors for monitoring components of said network;

b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and

c) at least one probe, wherein said probe is configured to

(1) collect status data from at least one sensor monitoring at least one component of said network;

(2) **[analyzing]** **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;

PAGE 8/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

(3) transmit information about said identified events to an analyst system associated with said secure operations center;

(4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system; and

(5) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

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

41. (Original) The security monitoring system of claim 37, wherein said probe and said secure operations center are configured to identify potentially security-related events by performing a multistage analysis of said status data.

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

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

PAGE 9/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

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

PAGE 10/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

REMARKS/ARGUMENTS

Claims 1-5, 7-23, and 25-44 are pending.

Applicant wishes to thank the Examiner for the courtesies extended during the telephone interview of July 6, 2005.

Claim 37 was amended in the Amendment filed April 13, 2005 to correct a typographical error. However, in the Advisory Action mailed April 28, 2005, the Examiner indicated that, for purposes of appeal, the amendment would not be entered. Thus, applicant is once again presenting the amendment for claim 37 to correct the same typographical error.

Claims 1-44 were rejected under 35 U.S.C. §103(a), as being obvious over Esbensen (U.S. Patent No. 5,796,942) in view of Porras et al. (U.S. Patent No. 6,704,874). This rejection is respectfully traversed and reconsideration is respectfully requested.

In her rejection of claims 1 and 19, the Examiner admits that Esbensen does not disclose that the analysis includes "filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering." However, the Examiner contends that Porras et al. discloses that 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. The Examiner relies on column 3, lines 61-67 and column 4, lines 1-32 of Porras et al. It is respectfully submitted that the Examiner is mistaken in her reliance upon Porras et al. Indeed, during the telephone interview of July 6, 2005, the Examiner failed to find where Porras et al. discloses or even suggests filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering.

As previously discussed, Porras et al. discloses a network-based alert management system 10 that includes a network 12, a network 14, and a network 16. Each of the networks 12-16 includes a number of computer systems collectively labeled 18, interconnected by an Ethernet cable 20. Each of the networks 12-16 includes security and fault monitoring systems generally labeled 22. Each security and fault monitoring system 22 is linked to an alert manager 24. The

PAGE 11/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

alert manager 24 is linked to one or more remote processing centers generally labeled 26. (See column 3, lines 16-25.)

Each of the security and fault monitoring systems 22 produces an alert stream in the form of security alerts, fault reports, and performance logs. The alert stream is sent to the alert manager 24 for collection, processing and distribution to the remote processing center 26. (See column 3, lines 34-38.)

Sensors 22 monitor various host and/or network activity within the networks 12-16, and each sensor 22 generates a stream of alerts, triggered by potentially suspicious events, such as network packet data transfer commands, data transfer errors, network packet data transfer volume, and so forth. The alerts indicate a suspicion of possible malicious intrusion or other threat to operations within the networks 12-16. (See column 3, lines 54-61.)

The alert manager 24 includes a receive-input logic module 28. In an embodiment, the receive-input logic module 28 of the alert manager 24 subscribes, i.e., establishes a transport connection, to receive each of the alert streams produced by the sensors 22 through a secure electronic communication line (SSL) 30. The alert streams contain raw, i.e., unprocessed, alerts. (See column 3, lines 62 - column 4, line 1.) Thus, it is clear that the alerts have not been filtered since Porras et al. clearly disclose that the alerts are raw and unprocessed.

The receive-input logic 28 of the alert manager 24 is equipped with translation modules 32 to translate the original, raw alert streams from the monitors 22 into a common format for further processing, if the alerts do not arrive in the common format. (See column 4, lines 6-10.) In another embodiment, the monitors 22 include conversion software that translates a monitor's raw alert stream into the common format used by the alert manager 24. (See column 4, lines 11-14.) The conversion software may add data items of interest to the alert manager 24 by querying its network 12-16. (See column 4, lines 14-16.)

In another embodiment, a combination of monitors 22 having conversion software and the receive-input logic 28 preprocessing raw alerts in the alert management network 10 are present to accommodate a heterogeneous base of monitors 22 that an end-user desires to manage. (See column 4, lines 17-21.) The alert manager 24 includes an alert processing engine 34. Raw

PAGE 12/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

alerts received by the receive-input module 28 and formatted into the common format are sent to the alert processing engine 34. (See column 4, lines 22-26.)

Finally, with reference to Figure 2, an alert management process 50 residing in the alert processing engine 34 includes receiving formatted alerts from the receive-input logic 28. The formatted alerts are passed through user specified filters and alerts not matching criteria of the user-specified filters are discarded. (See column 4, lines 27-32.)

Thus, it is apparent that Porras et al. do not disclose "analyzing 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." While Porras et al. disclose filtering formatted alerts and discarding alerts that do not match certain criteria of the user-specified filters, no mention is made of analyzing data that was not discarded and that was also not selected by the filtering process. Any analysis performed by Porras et al. is clearly done on alerts that were selected by the filtering process.

In contrast to both Porras et al. and Esbensen, claim 1 is directed to a method of operating a probe as part of a security monitoring system for a computer network, wherein the method comprises, among other things, "analyzing 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." Accordingly, since neither Esbensen nor Porras et al., either alone in combination, teach, disclose or even suggest a method as recited in claim 1, it is respectfully submitted that claim 1 is allowable.

Claims 2-5 and 7-18 depend, either directly or indirectly on claim 1, and therefore they are allowable for at least the reasons that claim 1 is allowable.

Claim 19 is directed to a computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of, among other things, "analyzing status data to identify potentially security-related events represented in the status data, wherein the analysis includes

PAGE 13/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering." As discussed above, neither Esbensen nor Porras et al., either alone or in combination, teach, disclose, or even suggest a computer-readable medium as recited in claim 19. Accordingly, it is respectfully submitted that claim 19 is allowable.

Claims 20-23 and 25-36 depend, either directly or indirectly, on claim 19 and therefore, they are allowable for at least the reasons claim 19 is allowable.

Claim 37 is directed to a security monitoring system for a computer network, where the system comprises, among other things, "at least one probe, wherein the probe is configured 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." As discussed above, neither Esbensen nor Porras et al., either alone or in combination, teach, disclose or even suggest a system as recited in claim 37. Accordingly, it is respectfully submitted that claim 37 is allowable.

Claims 38-44 depend, either directly or indirectly, on claim 37 and therefore, they are allowable for at least the reasons claim 37 is allowable.

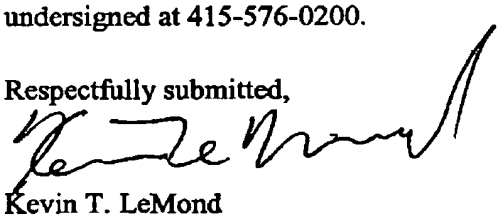
PAGE 14/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,



Kevin T. LeMond
Reg. No. 35,933

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
KTL:ldr
60531414 v1

PAGE 15/15 * RCVD AT 7/6/2005 7:32:27 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/3 * DNIS:8729306 * CSID:415 576 0300 * DURATION (mm-ss):05-24

RECEIVED
CENTRAL FAX CENTER
JUL 0 6 2005

PTO/SB/22 (12-04)

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) FY 2005 *(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)*	Docket Number (Optional) 022133-000510US
Application Number 09/766,343	Filed January 19, 2001
For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Art Unit 2131	Examiner Jenise 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):

	Fee	Small Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$120	$60	$
☐ Two months (37 CFR 1.17(a)(2))	$450	$225	$
☒ Three months (37 CFR 1.17(a)(3))	$1020	$510	$ 510
☐ Four months (37 CFR 1.17(a)(4))	$1590	$795	$
☐ Five months (37 CFR 1.17(a)(5))	$2160	$1080	$

☒ 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. I have enclosed a duplicate copy of this sheet.

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.

RECEIVED
OIPE/IAP
JUL 0 7 2005

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 35,933

☐ attorney or agent under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature — July 6, 2005 (Date)

Kevin T. LeMond, Reg. No. 35,933 (Typed or printed name) — 415-576-0200 (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 _____ forms are submitted.

60531815 v1

07/07/2005 SMINHSS1 00000050 201430 09766343
01 FC:2253 510.00 DA

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2000

Application or Docket Number: 9.766343

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	44	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	44 minus 20=	* 24
INDEPENDENT CLAIMS	3 minus 3 =	* 0
MULTIPLE DEPENDENT CLAIM PRESENT	☐	

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

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	355.00	OR	BASIC FEE	710.00
X$ 9=		OR	X$18=	432.00
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL		OR	TOTAL	1142.00

7/29/04

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 42	Minus	** 44	=
Independent	* 3	Minus	*** 3	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM	☐			

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

4/13/05

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 42	Minus	** 44	= 0
Independent	* 3	Minus	*** 3	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM	☐			

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X40=		OR	X80=	
+135=		OR	+270=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	0

7-6-05

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 42	Minus	** 44	= 0
Independent	* 3	Minus	*** 3	= 0
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM	☐			

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	0
X40=		OR	X80=	0
+135=		OR	+270=	0
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	0

* 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.

FORM PTO-875 (Rev. 8/00)

Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

BEST AVAILABLE COPY

RECEIVED
CENTRAL FAX CENTER
JUL 13 2005

Atty Docket No. 022133-000510US

PTO FAX NO.: 1 703 872-9306

ATTENTION: Examiner Jenise Jackson

Group Art Unit 2131

OFFICIAL COMMUNICATION

FOR THE PERSONAL ATTENTION OF

EXAMINER Jenise Jackson

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that the following documents in re Application of Bruce Schneier, Application No. 09/766,343, filed January 19, 2001 for METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE are being facsimile transmitted to the Patent and Trademark Office on the date shown below.

Documents Attached

1. Notice of Appeal (1 page submitted in duplicate)

Number of pages being transmitted, including this page: 3

Dated: 7/13/05

Lata Olivier

PLEASE CONFIRM RECEIPT OF THIS PAPER BY RETURN FACSIMILE AT (415) 576-0300

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834
Telephone: 415-576-0200
Fax: 415-576-0300
0303

60537141 v1

RECEIVED
CENTRAL FAX CENTER
JUL 13 2005

PTO/SB/31 (04-05)

NOTICE OF APPEAL FROM THE EXAMINER TO THE BOARD OF PATENT APPEALS AND INTERFERENCES	Docket Number (Optional) 022133-000510US

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]
on July 13, 2005
Signature _____
Typed or printed name Lata Olivier

In re Application of Bruce Schneier

Application Number 09/766,343	Filed January 19, 2001

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

Art Unit 2131	Examiner Jenise Jackson

Applicant hereby **appeals** to the Board of Patent Appeals and Interferences from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 500

☒ Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ 250

☐ 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. I have enclosed a duplicate copy of this sheet.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 20-1430. I have enclosed a duplicate copy of this sheet.

☒ A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) **was faxed with our Amendment of 7/13/05.**

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 35,933.

☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____

Signature
Kevin T. LeMond
Typed or printed name
415 576-0200
Telephone number
7/13/05
Date

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 2 forms are submitted.

07/14/2005 TL0111 00000054 201420 09766343
01 FC:2401 250.00 DA

60537110 v1

WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Friday, September 23, 2005

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=OR	
☐	L4	L3 and (alert? or alarm?)	195
☐	L3	L1 and L2	1494
☐	L2	L1 and (filter?)near3 (data or information or residue or packets)	1494
☐	L1	(sentry or honeypot or intrusion adj detect? or sensor or sensors)	421352

END OF SEARCH HISTORY

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.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

20350 7590 10/03/2005

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

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 10/03/2005

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

Office Action Summary	Application No.	Applicant(s)	
	09/766,343	SCHNEIER ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- 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 *13 July 2005*.

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) *1-44* 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) *1-44* is/are rejected.

7)☐ Claim(s) _____ 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) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Final Action

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-44 are rejected under 35 U.S.C. 103(a) as being obvious over Esbensen(5,796,942) in view of Porras(6,704,874).

3. As per claims 1, 19, Esbensen discloses a method of operating a probe(i.e. remote surveillance agents, RSA) as part of a security monitoring system for a computer network(see col. 7, lines 19-23), collecting status data from at least one monitored component of the network(see col. 7, lines 23-27); identifying potentially security-related events pertaining to the network by analyzing the status data(see col. 7, lines 28-30); transmitting information about the identified events to an analyst associated with the security monitoring system(see col. 5, lines 22-28, col. 7, lines 30-34) ; receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system in a manner customized to the network(see col. 5, lines 56-59); and dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback in a manner customized to the network(see col. 5, lines 60-65). Esbensen does not disclose wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded or selected by filtering. Porras et al. discloses wherein the analysis

includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded or selected by filtering (see col. 3, lines 61-67, col. 4, lines 1-32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include post filtering reside that is data neither discarded or selected by filtering of Porras, because the motivation is that the data that is left, that has not been filtered, which is the raw data of Porras can be analyzed further.

4. As per claim 2, Esbensen discloses wherein the identifying step includes performing a multi-stage analysis of the status data(see col. 5, lines 14-21).

5. As per claim 3, Esbensen discloses wherein the multi-stage analysis includes performing a discrimination analysis on the status data(see col. 5, lines 14-21).

6. As per claim 4, Esbensen discloses wherein the discrimination analysis includes positive filtering(see col. 5, lines 1-13).

7. As per claim 5, Esbensen discloses wherein the discrimination analysis includes negative filtering(see col. 5, lines 1-13).

8. As per claims 6 and 24, Esbensen discloses post-filtering residue(see col. 5, lines 1-13).

9. As per claim 7, Esbensen discloses wherein the multi-stage analysis includes analysis at the probe and analysis at a secure operations center configured to receive data from the probe(see col. 7, lines 19-54).

10. As per claim 8, Esbensen discloses identifying step includes aggregating and synthesizing the status data at the probe(see col. 7, lines 19-34).

11. As per claim 9, Esbensen discloses wherein the identifying step includes cross-correlating data across the monitored components(see col. 7, lines 35-43).

12. As per claim 10, Esbensen discloses identifying step includes analyzing the frequency of occurrence of the events(see col. 5, lines 14-21).

13. As per claim 11, Esbensen discloses computer based analysis at a secure operations center configured to receive data from the probe(see col. 7, lines 19-43).

14. As per claim 12, Esbensen discloses computer-based analysis includes aggregating, synthesizing, presenting alerts on an ensemble basis(see col. 5, lines 14-28).

15. As per claim 13, it is rejected under the same basis as claim 9.

16. As per claim 14, it is rejected under the same basis as claim 10.

17. As per claim 15, Esbensen discloses computer-based analysis includes cross-probe correlation(see col. 7, lines 19-43).

18. As per claim 16, Esbensen discloses self-tuning the probe based on previously collected status data(see col. 5, lines 60-65).

19. As per claim 17, Esbensen discloses wherein the dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts(see col. 5, lines 14-59).

20. As per claim 18, Esbensen discloses wherein the receiving feedback step occurs in substantially real time(see col. 14-50).

21. As per claim 20, it is rejected under the same basis as claim 2.

22. As per claim 21, it is rejected under the same basis as claim 3.

23. As per claim 22, it is rejected under the same basis as claim 4.

24. As per claim 23, it is rejected under the same basis as claim 5.

25. As per claim 25, it is rejected under the same basis as claim 7.

26. As per claim 26, it is rejected under the same basis as claim 8.

27. As per claim 27, it is rejected under the same basis as claim 9.

28. As per claim 28, it is rejected under the same basis as claim 11.

29. As per claim 30, it is rejected under the same basis as claim 12.

30. As per claim 31, it is rejected under the same basis as claim 9.

31. As per claim 32, it is rejected under the same basis as claim 10.

32. As per claim 33, it is rejected under the same basis as claim 15.

33. As per claim 34, it is rejected under the same basis as claim 16.

34. As per claim 35, it is rejected under the same basis as claim 17.

35. As per claim 36, it is rejected under the same basis as claim 18.

36. As per claim 37, it is rejected under the same basis as claim 1, and further claim 37, is rejected for a plurality of sensors for monitoring components of the network, is inherent is intrusion detection, proof of this inherency is provided by Fratto, in which he teaches net ranger sensors that monitor the network.

37. As per claim 38, it is rejected under the same basis as claim 3.

38. As per claim 39, limitations have already been addressed(see claim 4).

39. As per claim 40, limitations have already been addressed(see claim 5).

40. As per claim 41, it is rejected under the same basis as claim 7.

41. As per claim 42, Esbensen discloses wherein the multi-stage analysis includes analysis at the probe and analysis at the secure operations center(see col. 7, lines 19-33).

42. As per claim 43, limitations have already been addressed(see claim 7).

43. As per claim 44, Esbensen discloses wherein the computer-based analysis is configured to correlate data from different probes(see col. 7, lines 19-43).

Response to Amendment

44. The Applicant states that Porras does not disclose analyzing post filtering residue. Porras et al. discloses wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded or selected by filtering (see col. 3, lines 61-67, col. 4, lines 1-32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include post filtering reside that is data neither discarded or selected by filtering of Porras, because the motivation is that the data that is left, that has not been filtered, which is the raw data of Porras can be analyzed further.

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 M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Shiekh can be reached on (571) 272-3795. 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).

September 23, 2005

Primary Examiner
AU 2131
9/27/05

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
09/766,343	SCHNEIER ET AL.
Examiner	**Art Unit**
Jenise E. Jackson	2131

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	9/23/05
	1	✓
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	✓
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

Search Notes

Application/Control No.	Applicant(s)/Patent under Reexamination	
09/766,343	SCHNEIER ET AL.	
Examiner	**Art Unit**	
Jenise E. Jackson	2131	

SEARCHED

Class	Subclass	Date	Examiner
726	3, 13, 22-25	9/23/05	DJ
709	223-229	↓	

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)

	DATE	EXMR
West updated Search	9/23/05	DJ

OIPE IAP19
FEB 07 2006
PATENT & TRADEMARK OFFICE

PATENT
Attorney Docket No.: 022133-000510US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No. 7642
Bruce Schneier et al.	Examiner: Jenise E. Jackson
Application No.: 09/766,343	Technology Center/Art Unit: 2131
Filed: January 19, 2001	AMENDMENT
For: METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Customer No.: 20350	

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

Sir:

In response to the Office Action mailed October 3, 2005, 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 8 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. (previously presented) A method of operating a probe as part of a security monitoring system for a computer network, comprising:

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

b) analyzing 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) transmitting information about said identified events to an analyst system associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

4. (original) The method of claim 3, wherein the discrimination analysis includes positive filtering.

5. (original) The method of claim 3, wherein the discrimination analysis includes negative filtering.

6. (canceled)

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

8. (original) The method of claim 1, wherein said identifying step includes aggregating and synthesizing said status data at the probe.

9. (original) The method of claim 8, wherein said identifying step includes cross-correlating data across said monitored components.

10. (original) The method of claim 8, wherein said identifying step includes analyzing the frequency of occurrence of said events.

11. (original) The method of claim 1, further comprising after said step (c), performing further computer-based analysis at a secure operations center configured to receive data from said probe.

12. (original) The method of claim 11, wherein said computer-based analysis includes aggregating, synthesizing, and presenting alerts on an ensemble basis.

13. (original) The method of claim 11, wherein said identifying step includes cross-correlating data across said monitored components.

14. (original) The method of claim 11, wherein said identifying step includes analyzing the frequency of occurrence of said events.

15. (original) The method of claim 11, wherein said computer-based analysis includes cross-probe correlation.

16. (original) The method of claim l, further comprising instantaneously self-tuning said probe based on previously collected status data.

17. (original) The method of claim 1, wherein said dynamic modifying step includes consideration of non-real-time information from ongoing security research efforts.

18. (original) The method of claim 1, wherein said receiving feedback step occurs in substantially real time.

19. (previously presented) A computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of:

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

b) analyzing 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) transmitting information about said identified events to an analyst system associated with said security monitoring system;

d) receiving feedback at the probe based on empirically-derived information reflecting operation of said security monitoring system; and

e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

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

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

24. (canceled)

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

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

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

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

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

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

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

33. (original) The computer-readable medium of claim 29, wherein said computer-based analysis includes cross-probe correlation.

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

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

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

37. (previously presented) A security monitoring system for a computer network, comprising:

a) a plurality of sensors for monitoring components of said network;

b) at least one secure operations center configured to receive and analyze potentially security-related event data from at least one probe; and

c) at least one probe, wherein said probe is configured to

(1) collect status data from at least one sensor monitoring at least one component of said network;

(2) 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;

(3) transmit information about said identified events to an analyst system associated with said secure operations center;

(4) receive feedback based on empirically-derived information reflecting operation of said security monitoring system; and

(5) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

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

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

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

41. (original) The security monitoring system of claim 37, wherein said probe and said secure operations center are configured to identify potentially security-related events by performing a multistage analysis of said status data.

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

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

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

REMARKS/ARGUMENTS

Claims 1-5, 7-23, and 25-44 are pending. No claims are amended. In the Office Action, the Examiner asserted that claims 1-44 were pending and rejected those claims under 35 USC §103(a) as being obvious over Esbensen (US Patent No. 5,796,942) in view of Porras (US Patent No. 6,704,874). Claims 6 and 24 were cancelled in an early amendment, so their continued rejection is not appropriate. The rejection of the remaining claims is respectfully traversed and reconsideration is respectfully requested.

In the Office Action, the Examiner admits that Esbensen does not disclose analysis including "filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering" in the rejection of claim 1 (see ¶3 of the Office Action), but later rejects the no longer pending claim 6 asserting that Esbensen discloses post-filtering residue (see ¶8 of the Office Action citing to col. 5, lines 1-13 of Esbensen). Upon review of that citation, Applicant takes the position that Esbensen does not in fact disclose post-filtering residue at that citation and fails to disclose or suggest "filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering", but that it appears that the rejection of claims 6 and 24 is in the Office Action as an unintentionally carried over portion of a previous and no longer relevant Office Action.

In rejecting claims 1 and 19 (and in part, claim 37), the Examiner appears to be relying on a combination of Esbensen and Porras, with Porras allegedly teaching the claimed "filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering". Upon careful review of Porras, it does not appear that the reference discloses or suggests any sort of post-filtering residue, so that reference is not relevant to the patentability of the pending claims, each of which recites an element including post-filtering residue. The term "post-filtering residue" is clearly defined, in the claim language itself, as data that is neither discarded nor selected by filtering.

In detail, Porras describes how its alert processing engine 34 can format the stream of raw alerts into a common format and filter the alerts according to what a user wants to

see. Porras even contemplates different users filtering using different criteria. However, as to each user, the whole of the raw data is selected by the filter is discarded. See, Porras, col. 4, lines 27-32. There is no post-filtering residue, as the raw data is filtered into the selected data and the discarded data.

In citing Porras, the Examiner merely states:

> Porras et al. discloses wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data that is neither discarded nor selected by filtering (see col. 3, lines 61-67, col. 4, lines 1-32). It would have been obvious to one of ordinary skill in the art at the time of the invention to include post filtering reside [residue] that is data neither discarded or selected by filtering of Porras, because the motivation is that the data that is left, that has not been filtered, which is the raw data of Porras can be analyzed further. (emphasis added)

This is the entire argument presented. This argument was presented twice, with exact wording, once in the rejection of claims 1, 19 and once in a response to a prior argument by Applicant. The underlined portions are text taken from the Applicant's claims. Parsing the above paragraph, the Examiner's entire argument seems to be that 1) Porras discloses a claimed element at a particular citation and 2) it would have been obvious to include Porras' version of that claimed element because "that the data that is left, that has not been filtered, which is the raw data of Porras can be analyzed further".

As to the first point, Applicant submits that Porras does not in fact disclose or suggest any use of post-filtering residue at those citations and the Examiner has provided no explanation as to how this could be disclosed, beyond providing a citation to Porras and restating the words of the claims. Post-filtering residue is data that is neither discarded nor selected by filtering. Porras clearly discloses data that is selected by filtering, such as the outputs of user-specified filters. See, Porras, col. 4, lines 27-40. Porras discloses that data is discarded in the filtering process. See, Porras, col. 4, lines 27-32.

Claim 1 recites "an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering". Thus, to anticipate or render obvious claim 1, there at least needs to be some teaching, or suggestion, of three kinds of data: 1) data selected by filtering, 2) data discarded by filtering and 3) post-filtering residue that is neither of

the first two. Applicant submits that there is no suggestion in Porras of a third type of data that could be considered post-filtering residue. In the portions of Porras cited by the Examiner, the reference describes receiving raw alert streams and processing them to format or translate the raw alerts into a common form. There is nothing in the Examiner's statements to suggest otherwise.

As to the second point, the Examiner's statement is not well understood, and it is not clear whether the Examiner is asserting that Porras' raw data is the data that is left or that the portions of the raw data that are left after filtering form the claimed post-filtering residue. Applicant interpreted the statement as being an assertion that the raw data that is "left" (i.e., not passed through the filter) can be analyzed further and that the Examiner is asserting that such analysis is the claimed "analysis of post-filtering residue". In any case, it appears that Porras does not disclose or suggest post-filtering residue as claimed and since Esbensen also lacks that disclosure, the combination of Esbensen and Porras would also lack that disclosure, so the motivation to combine is irrelevant.

Accordingly, since neither Esbensen nor Porras et al., either alone in combination, teach, disclose or even suggest a method as recited in claim 1, Applicant submits that claim 1 is allowable. Claims 2-5 and 7-18 depend, either directly or indirectly on allowable claim 1, and therefore they are allowable for at least the reasons cited above.

Claim 19 is directed to a computer-readable medium whose contents cause a computer system to operate a probe as part of a security monitoring system for a computer network, by performing the steps of, among other things, "analyzing 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." For reasons similar to those presented above, Applicant submits that the references fail to disclose or suggest at least analysis of post-filtering residue and therefore that claim 19 is allowable.

Claims 20-23 and 25-36 depend, either directly or indirectly, on allowable claim 19 and therefore, they are allowable for at least the reasons cited above.

Claim 37 is directed to a security monitoring system for a computer network, where the system comprises, among other things, "at least one probe, wherein the probe is configured 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." For reasons similar to those presented above, Applicant submits that the references fail to disclose or suggest at least analysis of post-filtering residue and therefore that claim 37 is allowable.

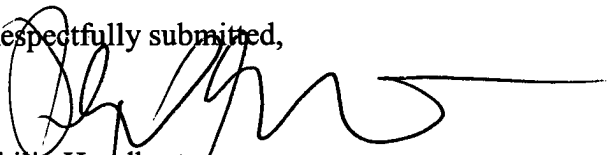
Claims 38-44 depend, either directly or indirectly, on allowable claim 37 and therefore, they are allowable for at least the reasons cited above.

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,



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:djb
60689276 v1

OIPE IAP19
FEB 07 2006
PATENT & TRADEMARK OFFICE

PTO/SB/22 (12-04)

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a) FY 2005 *(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)*	Docket Number (Optional) 022133-000510US
Application Number 09/766,343	Filed January 19, 2001
For METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE	
Art Unit 2131	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):

	Fee	Small Entity Fee	
☒ One month (37 CFR 1.17(a)(1))	$120	$60	$ 60
☐ Two months (37 CFR 1.17(a)(2))	$450	$225	$
☐ Three months (37 CFR 1.17(a)(3))	$1020	$510	$
☐ Four months (37 CFR 1.17(a)(4))	$1590	$795	$
☐ Five months (37 CFR 1.17(a)(5))	$2160	$1080	$

☒ 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**. I have enclosed a duplicate copy of this sheet.

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	February 3, 2006 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 2 forms are submitted.

60695936 v1

02/08/2006 YPOLITE1 00000009 201430 09766343

01 FC:2251 60.00 DA

2131
TEW

PTO/SB/21 (09-04)

OIPE
FEB 07 2006
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

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

ENCLOSURES (Check all that apply)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☒ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☒ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):
  Return Postcard

Remarks: The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Townsend and Townsend and Crew LLP		
Signature			
Printed name	Philip H. Albert		
Date	February 3, 2006	Reg. No.	35,819

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature			
Typed or printed name	Valerie Peterson	Date	February 3, 2006

v

PTO/SB/06 (08-03)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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: 09/766343

CLAIMS AS ~~FILED – PART I~~ Amended

2-7-06

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE	SMALL ENTITY FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY FEE
BASIC FEE (37 CFR 1.16(a))				$	OR		$
TOTAL CLAIMS (37 CFR 1.16(c))	42 minus ~~20~~ 44 =	* 0	X $ =	0	OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(b))	3 minus 3 =	* 0	X $ =	0	OR	X $ =	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(d))		0	+ $ =	0	OR	+ $ =	
			TOTAL	0	OR	TOTAL	

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

CLAIMS AS AMENDED – PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total (37 CFR 1.16(c))	*	Minus	**	=
Independent (37 CFR 1.16(b))	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))				

SMALL ENTITY RATE	SMALL ENTITY ADDITIONAL FEE	OR	OTHER THAN SMALL ENTITY RATE	OTHER THAN SMALL ENTITY ADDITIONAL FEE
X $ =		OR	X $ =	
X $ =		OR	X $ =	
+ $ =		OR	+ $ =	
TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total (37 CFR 1.16(c))	*	Minus	**	=
Independent (37 CFR 1.16(b))	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))				

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X $ =		OR	X $ =	
X $ =		OR	X $ =	
+ $ =		OR	+ $ =	
TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total (37 CFR 1.16(c))	*	Minus	**	=
Independent (37 CFR 1.16(b))	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))				

RATE	ADDITIONAL FEE	OR	RATE	ADDITIONAL FEE
X $ =		OR	X $ =	
X $ =		OR	X $ =	
+ $ =		OR	+ $ =	
TOTAL ADD'L FEE		OR	TOTAL ADD'L 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.

WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Thursday, April 27, 2006

Hide?	Set Name	Query	Hit Count
		DB=USPT; PLUR=YES; OP=OR	
☐	L6	L4 and (filter?)near5(data or information or packets)	343
☐	L5	(anomaly adj engine)	11
☐	L4	L1 and L3	42171
☐	L3	(probe or audit adj logs)	157817
☐	L2	(filter?)near5(residue) and network	25
☐	L1	(honeypot or sentry or intrud? or intrus? or sensor or hack? or crack?)	502178

END OF SEARCH HISTORY

```
SYSTEM:OS  - DIALOG OneSearch
  File   2:INSPEC 1898-2006/Apr W5
         (c) 2006 Institution of Electrical Engineers
  File   6:NTIS 1964-2006/Apr W5
         (c) 2006 NTIS, Intl Cpyrght All Rights Res
  File   8:Ei Compendex(R) 1970-2006/Apr W5
         (c) 2006 Elsevier Eng.  Info. Inc.
  File  34:SciSearch(R) Cited Ref Sci 1990-2006/Apr W5
         (c) 2006 Inst for Sci Info
  File  35:Dissertation Abs Online 1861-2006/Apr
         (c) 2006 ProQuest Info&Learning
  File  56:Computer and Information Systems Abstracts 1966-2006/Apr
         (c) 2006 CSA.
  File  60:ANTE: Abstracts in New Tech & Engineer 1966-2006/Apr
         (c) 2006 CSA.
  File  65:Inside Conferences 1993-2006/May 09
         (c) 2006 BLDSC all rts. reserv.
  File  92:IHS Intl.Stds.& Specs. 1999/Nov
         (c) 1999 Information Handling Services
  File  94:JICST-EPlus 1985-2006/Feb W1
         (c)2006 Japan Science and Tech Corp(JST)
  File  95:TEME-Technology & Management 1989-2006/May W1
         (c) 2006 FIZ TECHNIK
  File  99:Wilson Appl. Sci & Tech Abs 1983-2006/Apr
         (c) 2006 The HW Wilson Co.
  File 103:Energy SciTec 1974-2006/Apr B1
         (c) 2006 Contains copyrighted material
*File 103: For access restrictions see Help Restrict.
  File 144:Pascal 1973-2006/Apr W3
         (c) 2006 INIST/CNRS
  File 239:Mathsci 1940-2006/Jun
         (c) 2006 American Mathematical Society
  File 275:Gale Group Computer DB(TM) 1983-2006/May 08
         (c) 2006 The Gale Group
  File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
  File 647:CMP  Computer Fulltext 1988-2006/Jun W1
         (c) 2006 CMP Media, LLC
  File 674:Computer News Fulltext 1989-2006/Apr W5
         (c) 2006 IDG Communications
  File 696:DIALOG Telecom. Newsletters 1995-2006/May 09
         (c) 2006 Dialog

      Set  Items  Description
      ---  -----  -----------
? s (probe or sensor or sentry or manag?(2n)intrusion(2n)detect? or
intrus?(2n)detect? or firewall or gateway or proxy)
Processing
Processed  10 of  20 files ...
Completed processing all files
          609193  PROBE
          599117  SENSOR
            2453  SENTRY
         4152947  MANAG?
           65871  INTRUSION
         4110955  DETECT?
             949  MANAG?(2N)INTRUSION(2N)DETECT?
          109191  INTRUS?
         4110955  DETECT?
           17163  INTRUS?(2N)DETECT?
           27665  FIREWALL
           80973  GATEWAY
           34772  PROXY
```

```
      S1 1337499  (PROBE OR SENSOR OR SENTRY OR
                  MANAG?(2N)INTRUSION(2N)DETECT? OR INTRUS?(2N)DETECT? OR
                  FIREWALL OR GATEWAY OR PROXY)
? s (audit? or review? or check? or filter? or inspect? or exam? or
assess?)(5n)(data or information or packets or malicious or suspicious)
Processing
Processing
Processed  10 of  20 files ...
>>>File 95 processing for FILTER? stopped at FILTERTECHNOLOGIE
Processing
Processed  20 of  20 files ...
Completed processing all files
          287749  AUDIT?
         2939566  REVIEW?
          617031  CHECK?
         1138318  FILTER?
          846144  INSPECT?
         6784085  EXAM?
         2656133  ASSESS?
         9274905  DATA
         5133460  INFORMATION
           86890  PACKETS
           14897  MALICIOUS
           16724  SUSPICIOUS
      S2  538982  (AUDIT? OR REVIEW? OR CHECK? OR FILTER? OR INSPECT? OR
                  EXAM? OR ASSESS?)(5N)(DATA OR INFORMATION OR PACKETS OR
                  MALICIOUS OR SUSPICIOUS)
? s s1 and s2
         1337499  S1
          538982  S2
      S3   21696  S1 AND S2
? s s3 and (alarm or alert?)
           21696  S3
           75285  ALARM
           73366  ALERT?
      S4    1863  S3 AND (ALARM OR ALERT?)
? s s4 and (analyz? or review? or check? or inspect? or exam? or
assess?)(5n)(residue)
Processing
Processed  10 of  20 files ...
Completed processing all files
            1863  S4
         2636201  ANALYZ?
         2939566  REVIEW?
          617031  CHECK?
          846144  INSPECT?
         6784085  EXAM?
         2656133  ASSESS?
          225037  RESIDUE
            3821  (((((ANALYZ? OR REVIEW?) OR CHECK?) OR INSPECT?) OR
                  EXAM?) OR ASSESS?)(5N)RESIDUE
      S5       3  S4 AND (ANALYZ? OR REVIEW? OR CHECK? OR INSPECT? OR EXAM?
                  OR ASSESS?)(5N)(RESIDUE)
```

```
Set     Items   Description
S1    1337499   (PROBE OR SENSOR OR SENTRY OR MANAG?(2N)INTRUSION(2N)DETEC-
            T? OR INTRUS?(2N)DETECT? OR FIREWALL OR GATEWAY OR PROXY)
S2     538982   (AUDIT? OR REVIEW? OR CHECK? OR FILTER? OR INSPECT? OR EXA-
            M? OR ASSESS?)(5N)(DATA OR INFORMATION OR PACKETS OR MALICIOUS
             OR SUSPICIOUS)
S3      21696   S1 AND S2
S4       1863   S3 AND (ALARM OR ALERT?)
S5          3   S4 AND (ANALYZ? OR REVIEW? OR CHECK? OR INSPECT? OR EXAM? -
            OR ASSESS?)(5N)(RESIDUE)
?
```

```
Set     Items   Description
S1    4978308   DETECT? OR DISCOVER? OR SENSE? ? OR SENSING OR IDENTIFYING
            OR IDENTIFY OR INVESTGAT? OR MONITOR? OR WATCH?
S2     900583   INTRUSION OR MISUSE? OR INTERRUPT? OR IMPOSITION? OR DISTU-
            RB? OR INVASION? OR INCURSION OR MISTREAT? OR ABUS??? OR EXPL-
            OT? OR MALTREAT? OR MISHAND?
S3      74993   (EARLIER OR EARLY)(2N)(WARN? OR INDICAT? OR SIGNAL?) OR (S-
            USPICIOUS? OR WARY OR SKEPTICAL?)(2N)(BEHAVIOR? OR ACTION? OR
            CONDUCT)
S4    9074522   AUDIT? ? OR REVIEW? OR CHECK? OR INSPECT? OR EXAM? OR ASSE-
            SS?
S5    9886121   WEIGHT? OR VALUE? OR POINT? OR SCORE? OR RATES OR RATE
S6    2528256   ASSIGN? OR DESIGNATE? OR ALLOT? OR DELEGAT? OR APPOINT?
S7      40362   S1(5N)S2
S8      30293   S1(2N)S2
S9      32346   S5(2N)S6
S10      9785   S5(N)S6
S11         1   S8(S)S10(S)S4
S12         0   S8(S)S10(S)AUDIT? ?
S13         0   S10(S)SAUDIT? ?
S14        37   S10(S)AUDIT? ?
S15         2   S14(S)S2
S16     62110   INTRUSION?
S17    768327   DETECT?
S18     19620   S17(N)S16
S19        14   S18 AND S10
S20         1   S19 AND AUDIT? ?
S21         0   S14 AND PD<=19990304
S22        17   S15 OR S11 OR S19
S23         5   S22 AND PY<=1999
S24        35   S14 NOT S23
S25        27   S24 AND PY<=1999
S26        25   RD (unique items)
?show files
File  88:Gale Group Business A.R.T.S. 1976-2002/Jun 11
         (c) 2002 The Gale Group
File   9:Business & Industry(R) Jul/1994-2002/Jun 11
         (c) 2002 Resp. DB Svcs.
File 275:Gale Group Computer DB(TM) 1983-2002/Jun 11
         (c) 2002 The Gale Group
File 583:Gale Group Globalbase(TM) 1986-2002/Jun 12
         (c) 2002 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2002/Jun 12
         (c) 2002 The Gale group
File 621:Gale Group New Prod.Annou.(R) 1985-2002/Jun 11
         (c) 2002 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2002/Jun 11
         (c) 2002 The Gale Group
File  16:Gale Group PROMT(R) 1990-2002/Jun 11
         (c) 2002 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2002/Jun 12
         (c)2002 The Gale Group
?
```

23/3,K/1 (Item 1 from file: 88)
DIALOG(R)File 88:Gale Group Business A.R.T.S.
(c) 2002 The Gale Group. All rts. reserv.

02068440 SUPPLIER NUMBER: 06321829
Index of employers. (hospital profiles) (Nursing Opportunities supplement)
RN, v51, n1, pS6(377)
Jan, 1988
ISSN: 0033-7021 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 168102 LINE COUNT: 18943

... Care. Some of our specialty services include: MICU/SICU, Progressive Care, Hemodialysis, Pediatrics and Substance **Abuse** programs. Nurses play a vital role in our health care team. Unique scheduling plans such...

19880100

23/3,K/2 (Item 1 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

01989697
Fast Track Alarm (TM) from Telos Labs, Inc. provides local audible and visual warning at key areas in the event of a toxic gas leak.
News Release June 7, 1988 p. 1

Publication Year: **1988**

... of the detectors and the advanced analytical capability of the central monitoring system. As an **example** , Telos notes, if a leak is detected, the Fast Track Alarm alerts personnel and automatically signals the central **monitor** to **interrupt** its scan sequence and lock onto the **point designated** . Should an individual suspect a problem, smell something unusal, or simply want reassurance, the Fast...

23/3,K/3 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

07194893 SUPPLIER NUMBER: 15161314 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Catching intruders in a neural net. (neural networks)
Somers, James; Sanders, Ann; Skiffington, Barbara; Mogensen, Chip
Security Management, v38, n2, p68(4)
Feb, 1994
ISSN: 0145-9406 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2393 LINE COUNT: 00189

... potential of the neural network concept.
ASP is a computer processor that performs real-time **intrusion detection** . The processor can be installed with new or existing perimeter security systems. A common configuration...

...inputs to a particular node are equal. The knowledge in the network lies in the **weights assigned** to the connections between the nodes. During the network training process, it is the weights...by Acatel SEL, which is referenced at the end of this article.) A variety of **intrusion detection** sensors were used in the field tests, including monostatic microwave, bistatic microwave, fence-mounted fiber...

19940200

23/3,K/4 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

04109221 SUPPLIER NUMBER: 07764241 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Access to Utopia. (access control security)
Suneborn, Lars R.
Security Management, v33, n7, p8A(8)
July, 1989
ISSN: 0145-9406 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 4469 LINE COUNT: 00330

... silent duress alarm to the ACP or host.
Card-based systems incorporating alarm monitoring circuits (**intrusion detection**) and control functions (output relays to control various devices) are usually of the central processing...

...output). The following illustration is a simple system with one host, two ACPs, and one **intrusion detection** station (AID). The IDS has alarm input points and relay output points (control points). (see...for example, masking operation 19, the research and development lab on the third floor. Alarm **points assigned** to this masking operation are masked until the masking operation is reversed (1ser leaves the...

...kept away from the security system.
These are all examples of access point and alarm **point assignments** . Of course, an access point with a special assignment (such as an alarm masking point...

...AT SOME FUNCTION-RELATED card assignments such as the following: * time assignment * day assignment * access **point assignment** * activate additional relay or relays (always) * activate additional relay or relays (during time zone) * guard...

19890700

23/3,K/5 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

03500565 SUPPLIER NUMBER: 06321829 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Index of employers. (hospital profiles) (Nursing Opportunities supplement)
RN, v51, n1, pS6(377)
Jan, 1988
ISSN: 0033-7021 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 210302 LINE COUNT: 18943

... Care. Some of our specialty services include: MICU/SICU, Progressive Care, Hemodialysis, Pediatrics and Substance **Abuse** programs. Nurses play a vital role in our health care team. Unique scheduling plans such...

19880100
?

26/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

01732368 SUPPLIER NUMBER: 16514441
Quality unbound. (using data mining technology to improve the quality of data in databases)
Parsaye, Kamran; Chignell, Mark
Database Programming & Design, v8, n1, p38(4)
Jan, 1995
ISSN: 0895-4518 LANGUAGE: ENGLISH RECORD TYPE: ABSTRACT

...ABSTRACT: is a prerequisite for any large database application. The program should include continuous data quality **audits** with appropriate tools, cleanup and restructuring of data schemas, and standards and software for maintaining...

...naming, inconsistent field lengths, inconsistent field orders, inconsistent descriptions, incomplete entries, inconsistent identities, and inconsistent **value assignment** . A rule-based constraints approach to data integrity increases the chance that the constraints are...

19950100

26/3,K/2 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

01591901 SUPPLIER NUMBER: 13724609 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Data quality control with smart databases. (Cover Story)
Parsaye, Kamran; Chignell, Mark
AI Expert, v8, n5, p22(5)
May, 1993
DOCUMENT TYPE: Cover Story ISSN: 0888-3785 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2296 LINE COUNT: 00188

...ABSTRACT: naming, inconsistent field lengths, inconsistent field orders, inconsistent descriptions, incomplete entries, inconsistent identities, and inconsistent **value assignment** . A rules-based constraints approach lets comprehensive integrity constraints be expressed more easily in terms...

19930500

26/3,K/3 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

01455881 SUPPLIER NUMBER: 11471645 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Planning makes perfect: companies need to implement contingency plans with personnel in mind. (Contingency Planning)
Radding, Alan
MIDRANGE Systems, v4, n20, p31(4)
Oct 15, 1991
ISSN: 1041-8237 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2237 LINE COUNT: 00177

... is a tedious chore with little immediate payoff. The business group has to gather information, **audit** systems and procedures, inventory equipment and supplies, **assign values** , and set priorities. In short, they must document what the unit has, how it operates...

19911015

26/3,K/4 (Item 4 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2002 The Gale Group. All rts. reserv.

01386925 SUPPLIER NUMBER: 09732481 (USE FORMAT 7 OR 9 FOR FULL TEXT)
JIT and quality assurance form a new partnership in manufacturing operations. (Just-In-Time)
Gupta, Y.P.; Willborn, Walter W.O.
Industrial Engineering, v22, n12, p34(7)
Dec, 1990
ISSN: 0019-8234 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 5115 LINE COUNT: 00432

... place.
Once the program is effectively audited and continuously improved customers, in conducting their external **audit** , will find assessing the trucker a meaningful task. Standards for quality assurance programs and auditing...

...been shown that to promote cooperation between the two parties it is important that an **assigned point** of contact between them be established and the shipper clearly delineates the quality improvement objectives...

19901200

26/3,K/5 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2002 The Gale group. All rts. reserv.

04194574 SUPPLIER NUMBER: 16512743 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Measuring service quality in special libraries: lessons from service marketing.
White, Marilyn Domas; Abels, Eileen G.
Special Libraries, v86, n1, p36(10)
Wntr, 1995
ISSN: 0038-6723 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 4337 LINE COUNT: 00367

... services, providers in many service sectors often generate a tangible output. An accountant, for example, **audits** a firm's books and presents the results in a report. An information specialist searches...

...computerized database and generates a bibliography for a client. In the information related literature, the **values assigned** to the product are often confounded with the **values assigned** to the service.[6]
Definitions of Service Quality
Service quality is a judgment about the...

19950100

26/3,K/6 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

06278753 Supplier Number: 54413275 (USE FORMAT 7 FOR FULLTEXT)
Building Trust in Digital Certificates.(Technology Information)
Moskowitz, Robert
Network Computing, p105(1)
April 19, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1545

... of the content of CPs consists of operational requirements, such as CRL update timings or **audit** -trail retention periods. Such requirements could be stated in XML, and even some of the...

...such as key generation environment (user system, tempest system and so

on) could have XML **values assigned** . With this capability, an administrator could define the rules for an application in XML and...
19990419

26/3,K/7 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2002 The Gale Group. All rts. reserv.

04829393 Supplier Number: 47105783
Customs audit makes Nike sweat.
Mongelluzzo, Bill
Journal of Commerce and Commercial, pA1
Feb 6, 1997
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:
Nike Corp. still has not completed a compliance **audit** initiated 10 months ago by US Customs. This new law shifts the burden of accurately classifying and **assigning value** to merchandise onto importers, instead of customs. Nike prepared for the **audit** by developing a customs manual and a training program for US and overseas employees. Nike...

...team estimated that completion would take 60 days. Customs in the last year has opened **audits** on around 150 of the top 1,000 importing firms in key industries, completing approximately...
19970206

26/3,K/8 (Item 1 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

00766722
Accelerating collection of accounts receivable with computers is discussed by L Clapper, pres of CFO Assoc (Mt Prospect, Ill), which provides financial management services to small businesses.
CASHFLOW Magazine May, 1982 p. 41,42

Publication Year: **1982**

... the ability to prepare invoices and statements; the ability to assess finance charges, based on **rates assigned** ; **audit** trail; corrections; tie-ins to order processing and general ledger; and report writing.
...

26/3,K/9 (Item 2 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

00749253
FAA Administrator, JL Helms, asks Congress for authorization of the first 5 yrs of a 20-yr plan to modernize the national airspace system, warning that unless a decision is made now 'we suffer the consequences starting not later than 1986.
Aviation Week & Space Technology March 1, 1982 p. 36

Publication Year: **1982**

... FAA's Aviation System Acquisition Review Committee under Helms to review programs at critical decision **points** ; **appointing** a project manager for each major system acquisition; and establishing an independent **audit** function to evaluate program performance, schedule, and cost. The modernization program would provide general aviation...

26/3,K/10 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

10887268 SUPPLIER NUMBER: 54141371 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Embracing risk.(includes related article on internal auditing in risk management)(internal auditing of risk management)
Maynard, Gregg R.
Internal Auditor, 56, 1, 24(5)
Feb, 1999
ISSN: 0020-5745 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3538 LINE COUNT: 00308

... process, all auditable activities are first identified, an activity commonly referred to as "defining the **audit** universe." **Audit** management then **assigns values** to each auditable activity based on objective factors, such as the net dollars at risk, the number of transactions processed, the volume of assets or liabilities under control, and previous **audit** or regulatory ratings. Through spreadsheet analysis, these objective factors are weighted numerically according to importance...

19990201

26/3,K/11 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

10869143 SUPPLIER NUMBER: 54067834 (USE FORMAT 7 OR 9 FOR FULL TEXT)
How to live to talk about regulatory audits.
Cavaletti, Carla
Futures (Cedar Falls, Iowa), 28, 2, 78(3)
Feb, 1999
ISSN: 0746-2468 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2245 LINE COUNT: 00186

... chances of being audited, though, depend on two elements. One is what the NFA's **Audit** Priority System reveals to the compliance staff. The system is a computer program that operates by **assigning points** to members depending on various factors. For instance, if a member has had complaints filed...

...is audited include its use of media advertising, the time elapsed since the previous NFA **audit** and referrals from outside the NFA. Regardless, though, of the number of points a member...

19990201

26/3,K/12 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

10337304 SUPPLIER NUMBER: 20899228 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The responsibilities and obligations of the tax matters partner.
Garrison, Larry R.
Tax Adviser, 29, n6, 404(411)
June, 1998
ISSN: 0039-9957 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 6537 LINE COUNT: 00512

... Section 1222(a), a large partnership may elect to pay the additional tax on the **audit** adjustment at the entity level; the tax is computed by netting the adjustments of income and loss to the partnership and multiplying the result by the highest income tax **rate** .
Appointing a Representative
An ELP is required to designate a partner or other person who has...

19980600

26/3,K/13 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

10165052 SUPPLIER NUMBER: 20178811 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Uncovering the real market: how to conduct your own marketing audit.
Nevitt, Jennifer A.
Journal of Property Management, v62, n5, p38(6)
Sep-Oct, 1997
ISSN: 0022-3905 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2183 LINE COUNT: 00186

...ABSTRACT: efforts. Another technique is the rent-comparable analysis, which is helpful in calculating market rents, **assigning values** to amenities and comparing properties against the competition. It is also beneficial to assess the...

19970919

26/3,K/14 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09914236 SUPPLIER NUMBER: 17231467 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The design of an integrated group decision support system for technology assessment.
Noori, Hamid
R & D Management, v25, n3, p309(14)
July, 1995
ISSN: 0033-6807 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 7655 LINE COUNT: 00637

... the firm's strengths, weaknesses, opportunities and constraints, and to use this understanding to indirectly **assign weighting** factors to all criteria and subcriteria relevant to technology decision. This process of working through...people have a poor understanding of how they make preference trade-offs. When asked to **assign weights** according to the relative importance of decision factors, people often give subjective weights that bear...

...less information is actually being used to arrive at the decision. (4.) The company internal **audit** considers several key sets of factors in the decision analysis. These key factors comprise the...

19950700

26/3,K/15 (Item 6 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

09048417 SUPPLIER NUMBER: 18730024 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Corporate tax compliance and financial reporting.(Fundamental Tax Reform: Possibilities and Problems)
Mills, Lillian F.
National Tax Journal, 49, n3, 421-435
Sep, 1996
ISSN: 0028-0283 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 7383 LINE COUNT: 00639

... coefficient ((alpha).sub.1) will represent the proposed adjustment rate by the IRS.
PTS equals **audit points assigned** by the Coordinated Examination Program. PTS represents size and complexity and includes a factor for prior **audit** hours. If the IRS is more successful at detecting avoidance in large, complex firms due...

...a dummy variable which equals one if the firm is publicly held. PTS is audit **points assigned** by the IRS. NPPE is beginning depreciable property net of accumulated depreciation. ITC is investment...

19960900

26/3,K/16 (Item 7 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

07242416 SUPPLIER NUMBER: 15382649 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Allstate's risk assessment approach to selecting operational audit topics. (includes related article)
Reding, Kurt F.; DiGirolamo, Kristine Kay
Internal Auditor, v51, n2, p48(4)
April, 1994
ISSN: 0020-5745 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2047 LINE COUNT: 00179

... Decision Matrix allows the auditor to consider multiple key factors identified as important to the **audit** situation. A numerical score is calculated for each **audit** topic. The score is based on **weights assigned** to each key factor (most important to least important) and each **audit** topic under each key factor (most favorable topic for a given factor to least favorable topic). Highest priority is given to the **audit** topic receiving the highest total score.
* Conclusion
As the demand for operational audits increases, streamlining...

19940400

26/3,K/17 (Item 8 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

06199077 SUPPLIER NUMBER: 13600357 (USE FORMAT 7 OR 9 FOR FULL TEXT)
How to establish quality control of the sales force.
Roseman, Ed
Medical Marketing & Media, v27, n10, p44(7)
Oct, 1992
ISSN: 0025-7354 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 3087 LINE COUNT: 00254

... It features a matrix that takes into account a number of factors: representative input, objective **audit** information, and subjective information. We **assign weights** by product and rank physicians according to who will give us the best return. We...

19921000

26/3,K/18 (Item 9 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

05910019 SUPPLIER NUMBER: 12471777 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Five keys to a complete sanitation system. (includes related article) (Food Plant Ideas)
Graham, Don
Prepared Foods, v161, n5, p50(3)
April, 1992
ISSN: 0747-2536 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1707 LINE COUNT: 00140

... program and sanitation operations.
The plant sanitation manager or QA manager also should conduct an

audit periodically. They should **assign points** for each area so the area supervisor can relate the levels in that particular area...

19920400

26/3,K/19 (Item 10 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

05866225 SUPPLIER NUMBER: 12132017 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Will your tax return light up the IRS computer? (Cover Story)
Pincus, Carol R.
Medical Economics, v69, n6, p212(12)
March 16, 1992
DOCUMENT TYPE: Cover Story ISSN: 0025-7206 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2521 LINE COUNT: 00188

... have one strike against you.
There's nothing arbitrary about how the IRS picks its **audit** targets. Every return that's filed is fed through a computer programmed to **assign points** to certain hot spots. You can be sure, for example, that the computer zeros in...

...assigned a certain number of points, and high-scoring returns get kicked out for possible **audit** .
The exact items that get flagged and how many points they're assigned is top...

19920316

26/3,K/20 (Item 11 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

05524964 SUPPLIER NUMBER: 11541735 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Supplier evaluation revisited. (need for companies' purchasing agents to evaluate and rate their suppliers; includes related articles)(Purchasing 2000)
Porter, Anne Millen
Purchasing, v111, n6, p58(5)
Oct 24, 1991
ISSN: 0033-4448 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 3426 LINE COUNT: 00276

... supply-base management aims. Often, as in the case of Ford Q1, the on-site **audit assigns points** and produces a rating that can be compared with a minimum standard. That minimum standard...

19911024

26/3,K/21 (Item 12 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

05223104 SUPPLIER NUMBER: 11424686 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The Universal Motors assembly and stamping plant; transferring high-tech production to Mexico.
Shaiken, Harley
Columbia Journal of World Business, v26, n2, p124(14)
Summer, 1991
ISSN: 0022-5428 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 9685 LINE COUNT: 00755

... aging, sports model (3,212).
Representatives from the company's divisional offices perform a

monthly **audit** on completed cars in the factory to ensure that the plant's own daily quality checks conform to company standards.(21) Each vehicle is **assigned points** depending on the severity of the defect, a higher score indicating a more severe defect. The original plant goal was 240. The last two **audits** in 1988, however, both landed below 200, an impressive achievement. These **audits** have also shown significant improvement each model year since the plant's inauguration, declining from...

19910622

26/3,K/22 (Item 13 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

04847083 SUPPLIER NUMBER: 09045064 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Strategic safety planning: a systems view. (Focus)
Waring, Alan
Occupational Hazards, v52, n10, p121(4)
Oct, 1990
ISSN: 0029-7909 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2814 LINE COUNT: 00228

... if not exclusively, on numerical measures. Few would deny the value of being able to **assign scores** and quantify safety performance. Quantitative measures are essential to safety auditing. However, there is an internal conundrum in all **audit** systems which seek to quantify aspects of human activity by index measurement. They rely largely...

19901000

26/3,K/23 (Item 14 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

04613936 SUPPLIER NUMBER: 09262061 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Develop a consistent supplier audit. (quality assurance)
Handzo, C. Stephen
Purchasing World, v34, n4, p54(3)
April, 1990
ISSN: 0093-1659 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 1461 LINE COUNT: 00121

... auditing process is an auditing and reporting form. The auditing form is used during an **audit** as a tool to assist in organizing auditors' questioning and to **assign point** values to each category evaluated. The form assists auditors in making an objective assessment of...

19900400

26/3,K/24 (Item 15 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

02796405 SUPPLIER NUMBER: 04514597
Capital project management system. (Management information systems.)
Kottlowski, David
Management Accounting (USA), v67, n9, p10(2)
March, 1986
ISSN: 0025-1690 LANGUAGE: ENGLISH RECORD TYPE: ABSTRACT

...ABSTRACT: information about project expenses, ensure compliance with company expenditure authorization policies, account for expenditures, and **assign values** to assets for depreciation purposes. The selection of the Capital Project Management System (CPMS) software...

...to track expenditures and convert them to fixed assets upon completion

of a project, and **audit** trails included. accuracy and an accountability record.

19860300

26/3,K/25 (Item 16 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2002 The Gale Group. All rts. reserv.

02335000 SUPPLIER NUMBER: 03667119 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Beware, the IRS audit.
Wiener, Gloria J.
Restaurant Business, v84, p84(3)
March 1, 1985
ISSN: 0097-8043 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 902 LINE COUNT: 00069

... claimed by taxpayers at all income levels, the IRS has developed a mathematical formula that **assigns** **weighted** ratings to various items on all returns. Your figures are compared to the national average: the lower your rating, the lower your chances of an **audit** .
IRS examiners screen returns with high ratings to decide whether or not to conduct an...

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 07/12/2006

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

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/12/2006

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

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	$1400	$300	$0	$1700	10/12/2006

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.

PTOL-85 (Rev. 07/06) Approved for use through 04/30/2007.

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)

20350 7590 07/12/2006

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

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.

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.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

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	$1400	$300	$0	$1700	10/12/2006

EXAMINER	ART UNIT	CLASS-SUBCLASS
JACKSON, JENISE E	2131	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.

1 _____

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.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

20350 7590 07/12/2006

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

EXAMINER	
JACKSON, JENISE E	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/12/2006

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 666 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 666 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.

PTOL-85 (Rev. 07/06) Approved for use through 04/30/2007.

Notice of Allowability	Application No.	Applicant(s)	
	09/766,343	SCHNEIER ET AL.	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- 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 2/7/06.

2. ☒ The allowed claim(s) is/are 1-5, 7-23, 25-44.

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)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AVAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Reasons For Allowance

1. Status of Claims: Claims 6 and 24 were cancelled. Claims 1-5, 7-23, 25-44 are allowable for the features listed below:

2. 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, 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.

3. 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 are given a score/attack

severity as to how certain attacks would effect 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. systems is merely a system that simulates attacks to determine how these attacks will affect or have the potential to effect the network.

4. 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.

5. 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.

6. 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 1-5, 7-23, 25-44 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) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. 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).

May 9, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Notice of References Cited	Application/Control No. 09/766,343	Applicant(s)/Patent Under Reexamination SCHNEIER ET AL.	
	Examiner Jenise E. Jackson	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,119,236	09-2000	Shipley, Peter M.	726/22
*	B	US-6,088,804	07-2000	Hill et al.	726/25
*	C	US-6,519,703	02-2003	Joyce, James B.	726/22
	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 Country Code-Number-Kind Code	Date 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.

Issue Classification	Application/Control No. 09/766,343	Applicant(s)/Patent under Reexamination SCHNEIER ET AL.
	Examiner Jenise E. Jackson	Art Unit 2131

ISSUE CLASSIFICATION

ORIGINAL		INTERNATIONAL CLASSIFICATION									
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED				
726	3	H	0	6F	7	'04	H	0	4K	1	'00
CROSS REFERENCES		6	0	6F	11	'00	6	0	6F	15	'16
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)						6	0	6F	15	'173
726	1 2 6 11						6	0	6F	15	'16
726	12 13 22 23										
726	25										
709	223 226 229										

Jenise Jackson 5/9/06
(Assistant Examiner) (Date)

Pamela Harrison
(Legal Instruments Examiner) (Date)

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100
(Primary Examiner) (Date)

Total Claims Allowed: 42

O.G. Print Claim(s)	O.G. Print Fig.
37	2

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	37	31		61		91		121		151		181
2	2	38	32		62		92		122		152		182
3	3	39	33		63		93		123		153		183
4	4	40	34		64		94		124		154		184
5	5	41	35		65		95		125		155		185
	6	42	36		66		96		126		156		186
6	7	18	37		67		97		127		157		187
7	8	19	38		68		98		128		158		188
8	9	20	39		69		99		129		159		189
9	10	21	40		70		100		130		160		190
10	11	22	41		71		101		131		161		191
11	12	23	42		72		102		132		162		192
12	13	24	43		73		103		133		163		193
13	14	25	44		74		104		134		164		194
14	15		45		75		105		135		165		195
15	16		46		76		106		136		166		196
16	17		47		77		107		137		167		197
17	18		48		78		108		138		168		198
26	19		49		79		109		139		169		199
27	20		50		80		110		140		170		200
28	21		51		81		111		141		171		201
29	22		52		82		112		142		172		202
30	23		53		83		113		143		173		203
	24		54		84		114		144		174		204
31	25		55		85		115		145		175		205
32	26		56		86		116		146		176		206
33	27		57		87		117		147		177		207
34	28		58		88		118		148		178		208
35	29		59		89		119		149		179		209
36	30		60		90		120		150		180		210

Search Notes

Application/Control No.	Applicant(s)/Patent under Reexamination
09/766,343	SCHNEIER ET AL.
Examiner	**Art Unit**
Jenise E. Jackson	2131

SEARCHED			
Class	Subclass	Date	Examiner
726	1-3, 6, 11-13, 22-23	updated 5/9/06	JEJ
726	25	↓	↓
709	223, ~~226~~, 229	↓	↓

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
726	1-2, 6 11-13, 22-~~23~~	5/9/06	JEJ
726	25	" "	↓
709	223, 226 229	" "	

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
West updated	4/27/06	JEJ
STN updated	5/9/06	JEJ

Index of Claims

Application/Control No.	Applicant(s)/Patent under Reexamination
09/766,343	SCHNEIER ET AL.
Examiner	**Art Unit**
Jenise E. Jackson	2131

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	5/9/06
	1	
	2	
	3	
	4	
	5	
	~~6~~	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	~~24~~	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

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. 7642

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
09/766,343	01/19/2001 RULE	713	2131	028490-0007

APPLICANTS

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

** CONTINUING DATA **********

This appln claims benefit of 60/190,326 03/16/2000

** FOREIGN APPLICATIONS **********

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
** 04/25/2001

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☑ no 35 USC 119 (a-d) conditions met ☐ yes ☑ no ☐ Met after Allowance Verified and Acknowledged Examiner's Signature Initials	MN	9	44	3

ADDRESS
20350

#10

TITLE
Method and system for dynamic network intrusion monitoring, detection and response

FILING FEE RECEIVED	FEES: Authority has been given in Paper	
1272	No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

PART B - FEE(S) TRANSMITTAL

OIPE
OCT 10 2006
PATENT & TRADEMARK OFFICE

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)

20350 7590 07/12/2006

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

10/11/2006 RMEBRAH1 00000073 201430 09766343

01 FC:1501 1400.00 DA
02 FC:1504 300.00 DA
03 FC:8001 3.00 DA

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.

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.

Paula S. Cunningham	(Depositor's name)
Paula S Cunningham	(Signature)
October 4, 2006	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,343	01/19/2001	Bruce Schneier	028490-0007	7642

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	$1400	$300	$0	$1700	10/12/2006

EXAMINER	ART UNIT	CLASS-SUBCLASS
JACKSON, JENISE E	2131	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.

1 Philip H. Albert
2 Townsend and Townsend and Crew
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: COUNTERPANE INTERNET SECURITY, INC.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): 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 _____ Date 9/10/06

Typed or printed name Philip H. Albert Registration No. 35,819

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.

OIPE IAP96
OCT 10 2006
PATENT & TRADEMARK OFFICE

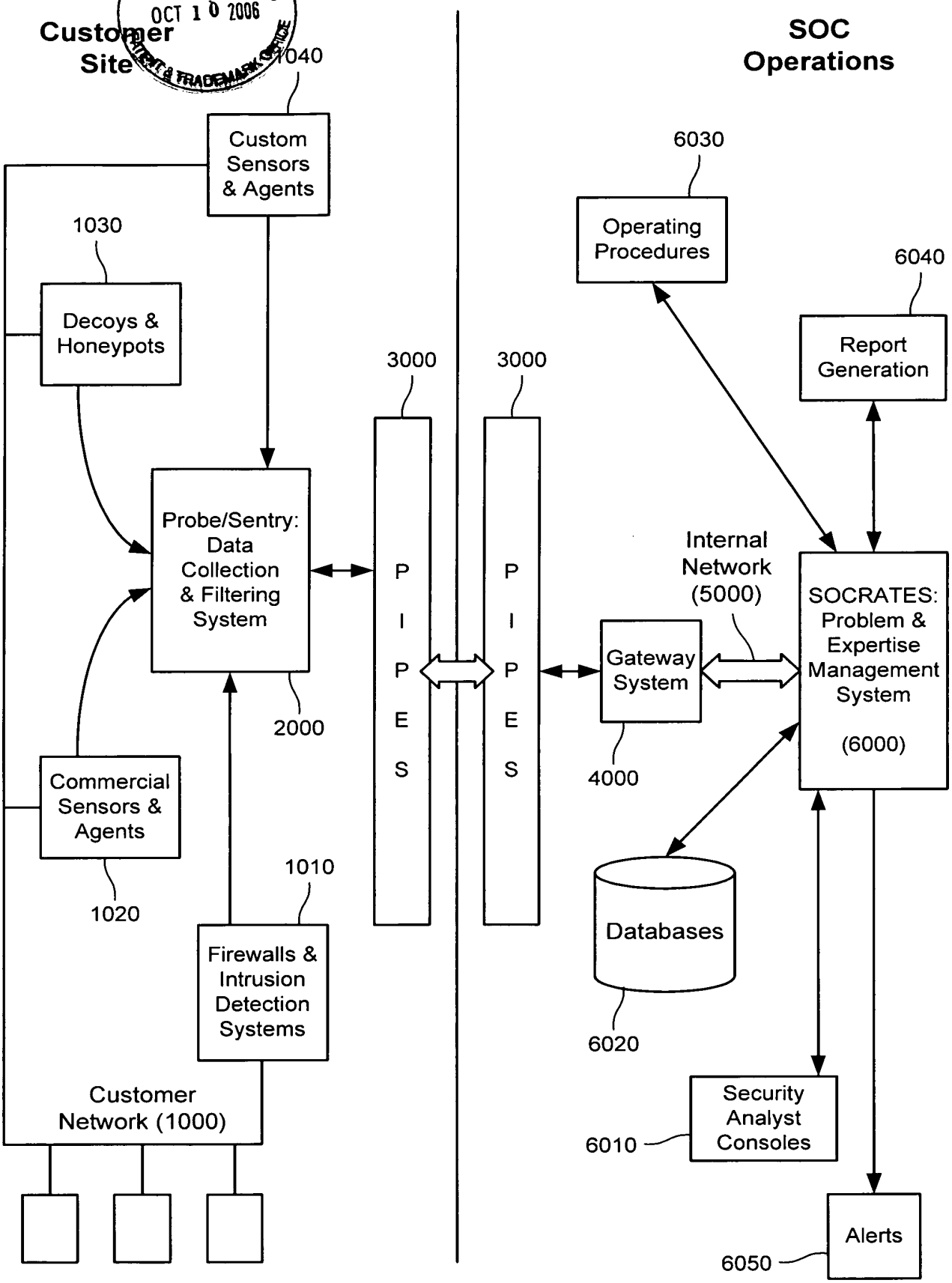


FIG. 1

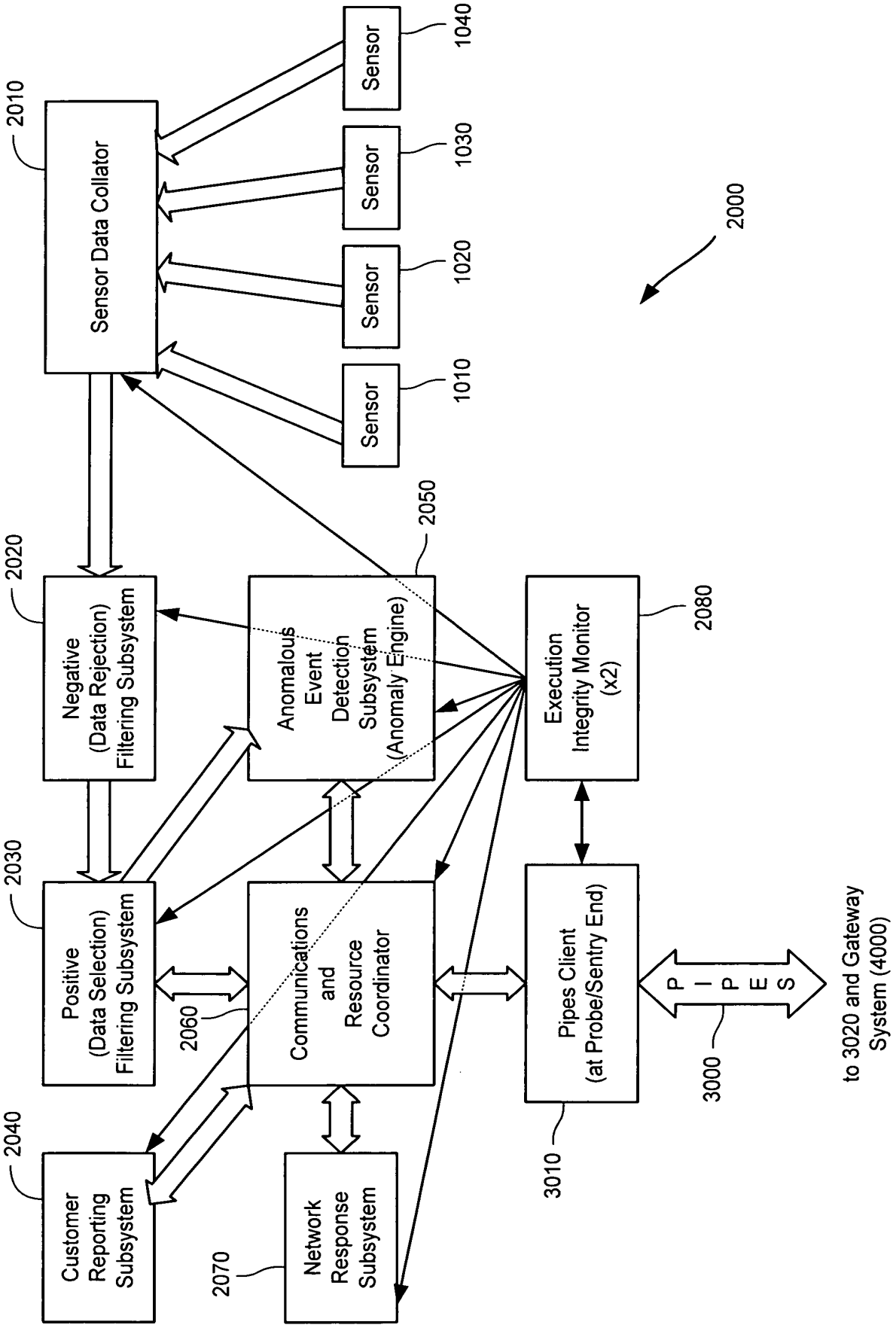

2000
2010
Sensor Data Collator
Sensor
1040
Sensor
1030
Sensor
1020
Sensor
1010
2020
Negative (Data Rejection) Filtering Subsystem
2050
Anomalous Event Detection Subsystem (Anomaly Engine)
2080
Execution Integrity Monitor (x2)
2030
Positive (Data Selection) Filtering Subsystem
2060
Communications and Resource Coordinator
Pipes Client (at Probe/Sentry End)
3010
P I P E S
3000
to 3020 and Gateway System (4000)
2040
Customer Reporting Subsystem
2070
Network Response Subsystem

FIG. 2

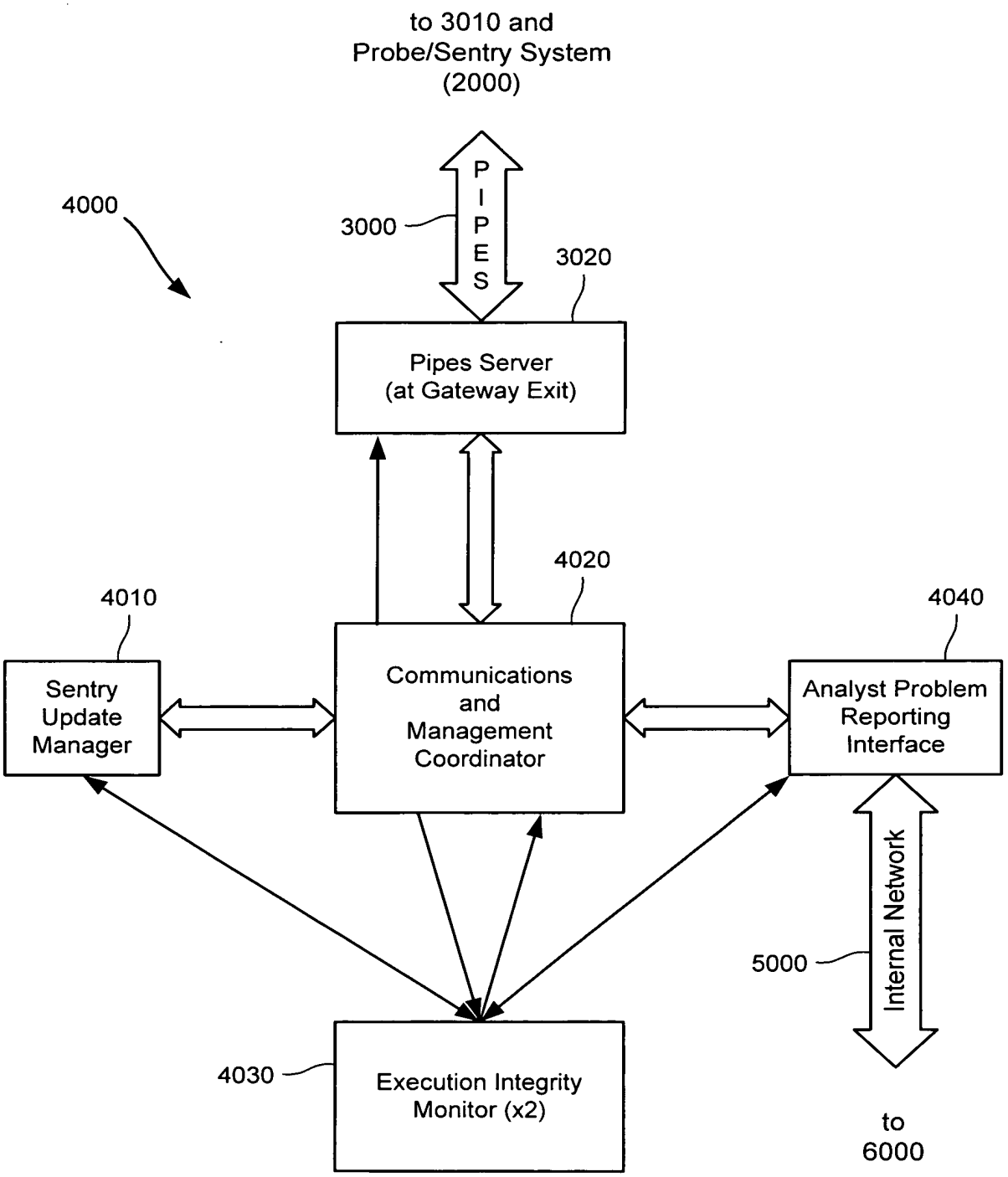

to 3010 and
Probe/Sentry System
(2000)
4000
3000
P
I
P
E
S
3020
Pipes Server
(at Gateway Exit)
4020
4010
4040
Sentry
Update
Manager
Communications
and
Management
Coordinator
Analyst Problem
Reporting
Interface
Internal Network
5000
4030
Execution Integrity
Monitor (x2)
to
6000

FIG. 3

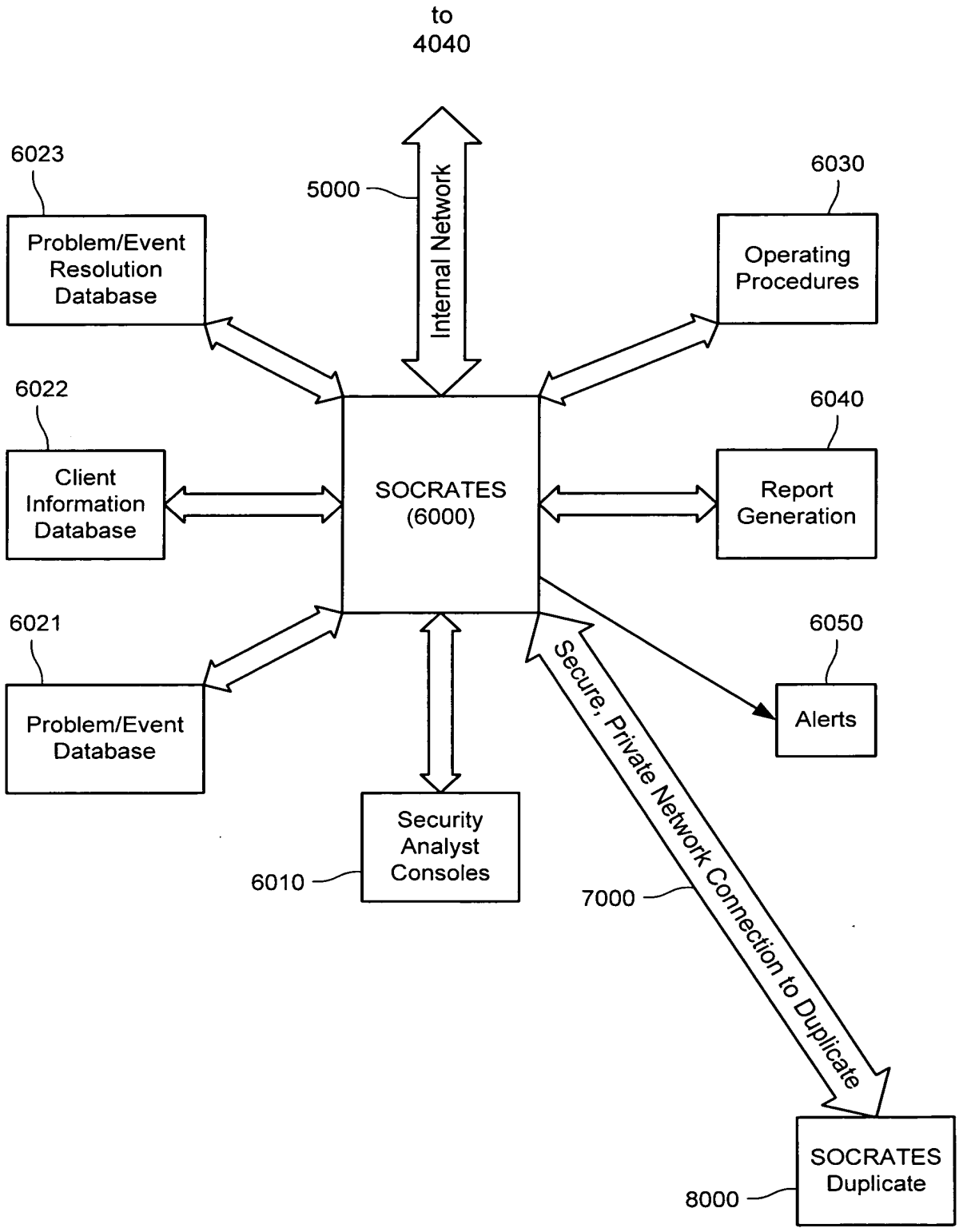

to
4040
6023
Problem/Event Resolution Database
5000
Internal Network
6030
Operating Procedures
6022
Client Information Database
SOCRATES (6000)
6040
Report Generation
6021
Problem/Event Database
6050
Alerts
Security Analyst Consoles
6010
7000
Secure, Private Network Connection to Duplicate
SOCRATES Duplicate
8000

FIG. 4

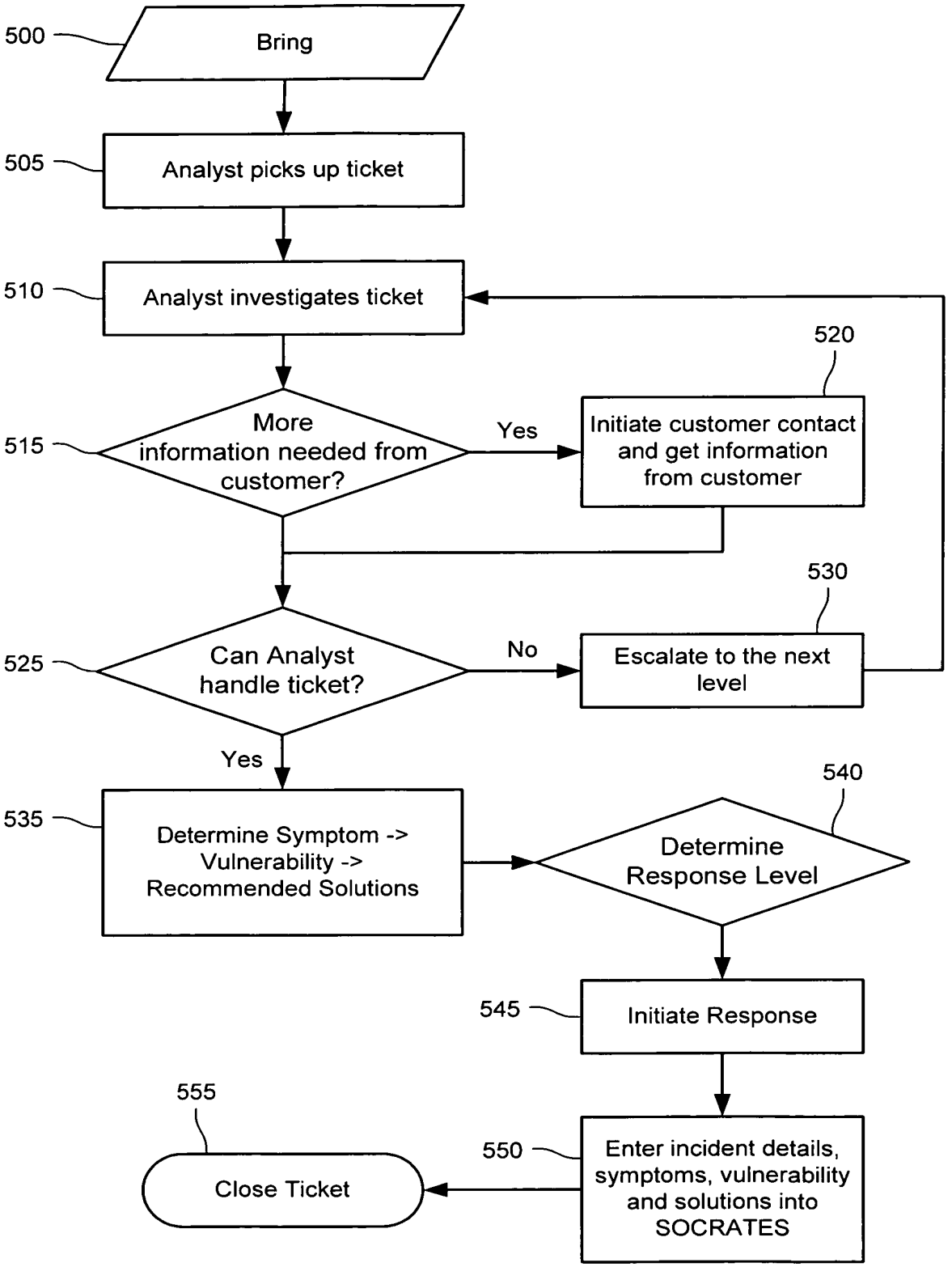

500
Bring
505
Analyst picks up ticket
510
Analyst investigates ticket
515
More information needed from customer?
Yes
520
Initiate customer contact and get information from customer
525
Can Analyst handle ticket?
No
530
Escalate to the next level
Yes
535
Determine Symptom -> Vulnerability -> Recommended Solutions
540
Determine Response Level
545
Initiate Response
550
Enter incident details, symptoms, vulnerability and solutions into SOCRATES
555
Close Ticket

FIG. 5

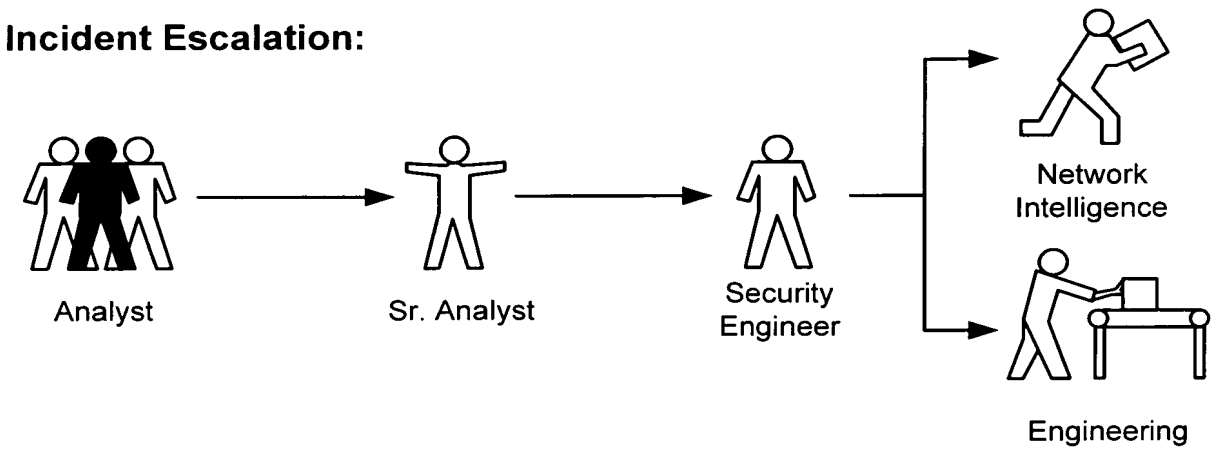

Incident Escalation:
Analyst
Sr. Analyst
Security Engineer
Network Intelligence
Engineering
Customer Service Escalation:
Analyst
Customer Service
Management
Technical Support Escalation:
OutSource Field Engineering
Network Intelligence
Security Engineer
Engineering
Customer Service
Management

FIG. 6

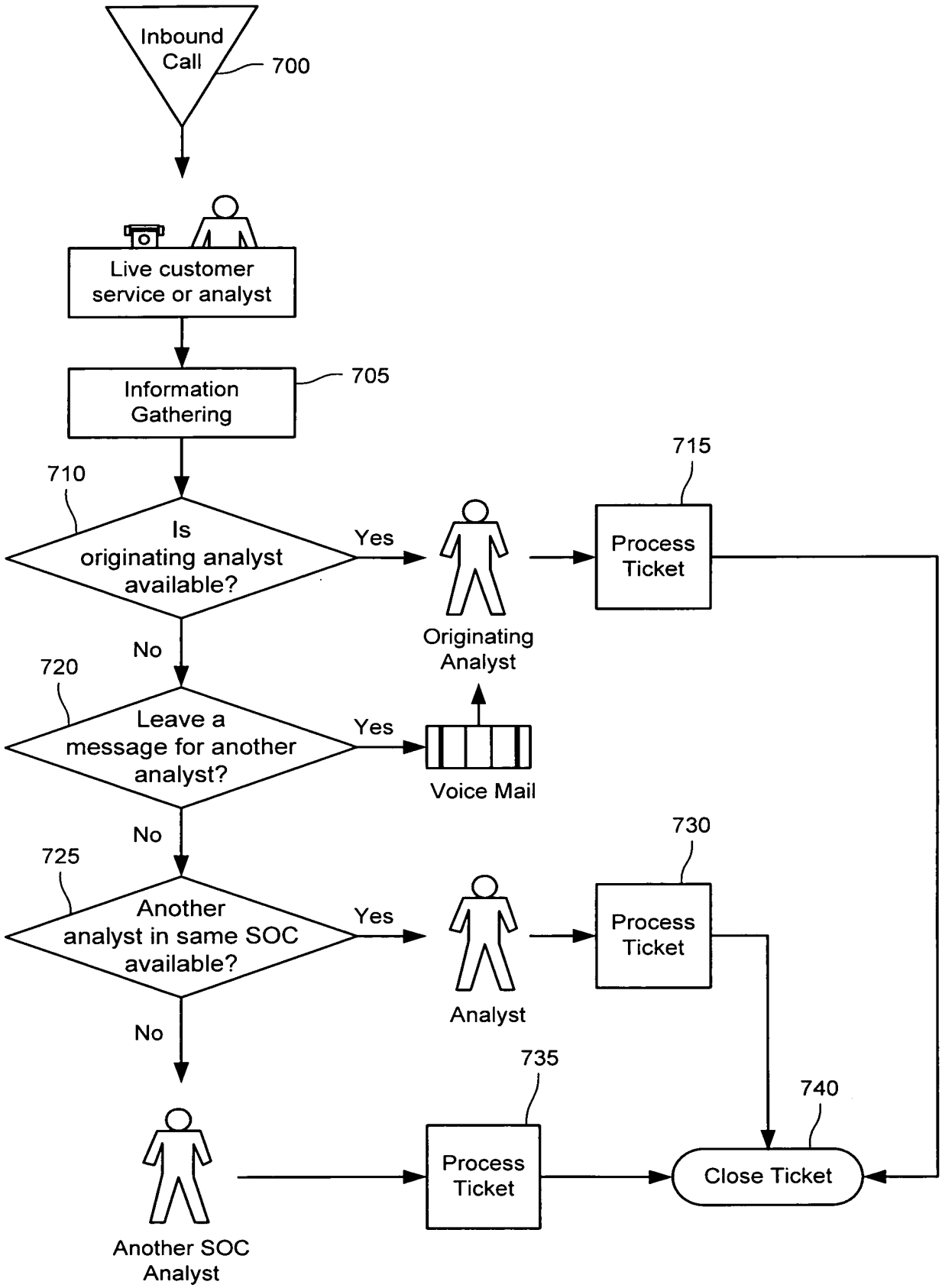

Inbound Call
700
Live customer service or analyst
Information Gathering
705
710
Is originating analyst available?
Yes
No
715
Process Ticket
Originating Analyst
720
Leave a message for another analyst?
Yes
No
Voice Mail
725
Another analyst in same SOC available?
Yes
No
730
Process Ticket
Analyst
735
Process Ticket
740
Close Ticket
Another SOC Analyst

FIG. 7

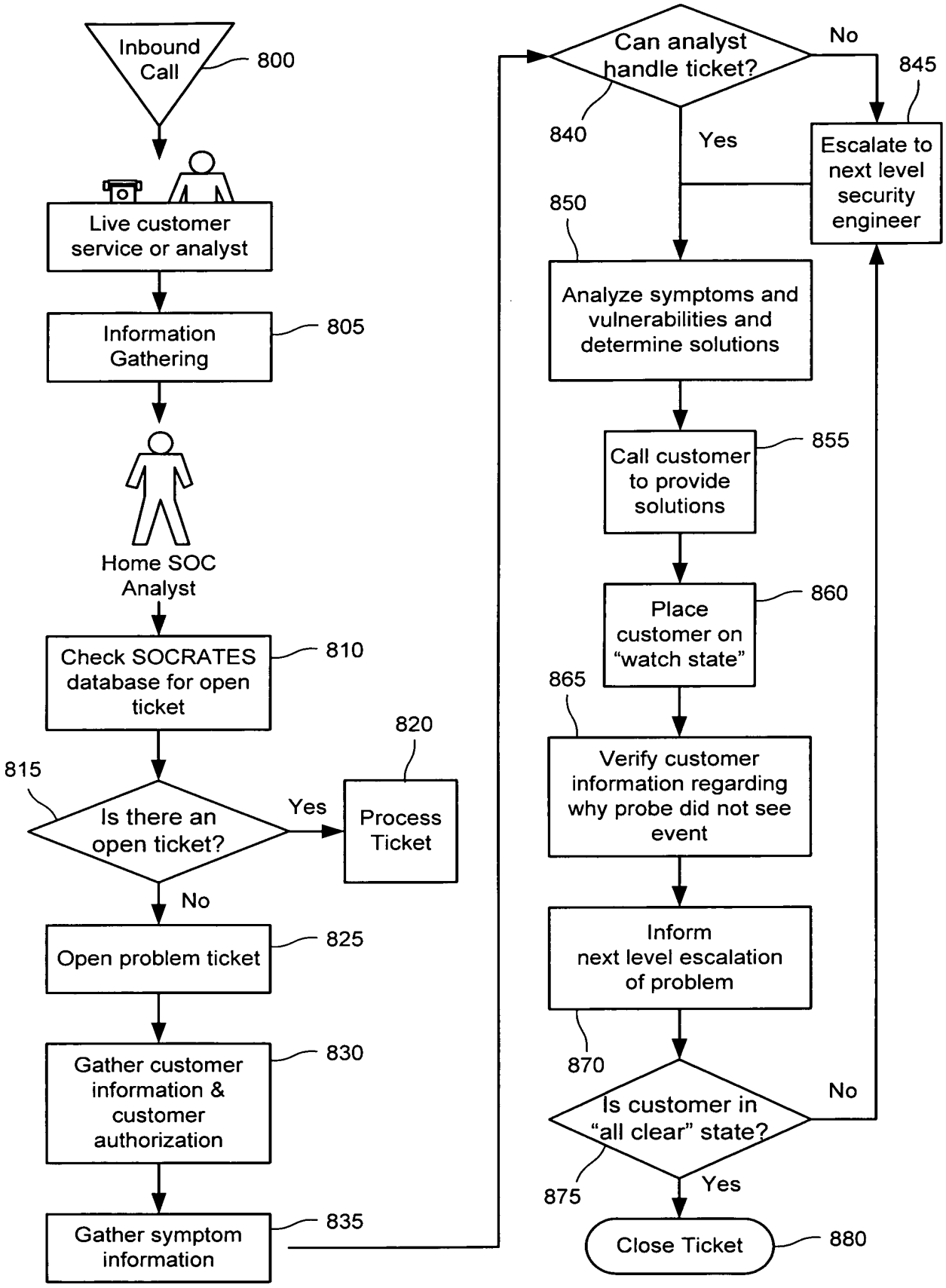

Inbound Call
800
Live customer service or analyst
Information Gathering
805
Home SOC Analyst
Check SOCRATES database for open ticket
810
Is there an open ticket?
815
Yes
Process Ticket
820
No
Open problem ticket
825
Gather customer information & customer authorization
830
Gather symptom information
835
Can analyst handle ticket?
840
No
845
Escalate to next level security engineer
Yes
850
Analyze symptoms and vulnerabilities and determine solutions
Call customer to provide solutions
855
Place customer on "watch state"
860
865
Verify customer information regarding why probe did not see event
Inform next level escalation of problem
870
Is customer in "all clear" state?
875
No
Yes
Close Ticket
880

FIG. 8B

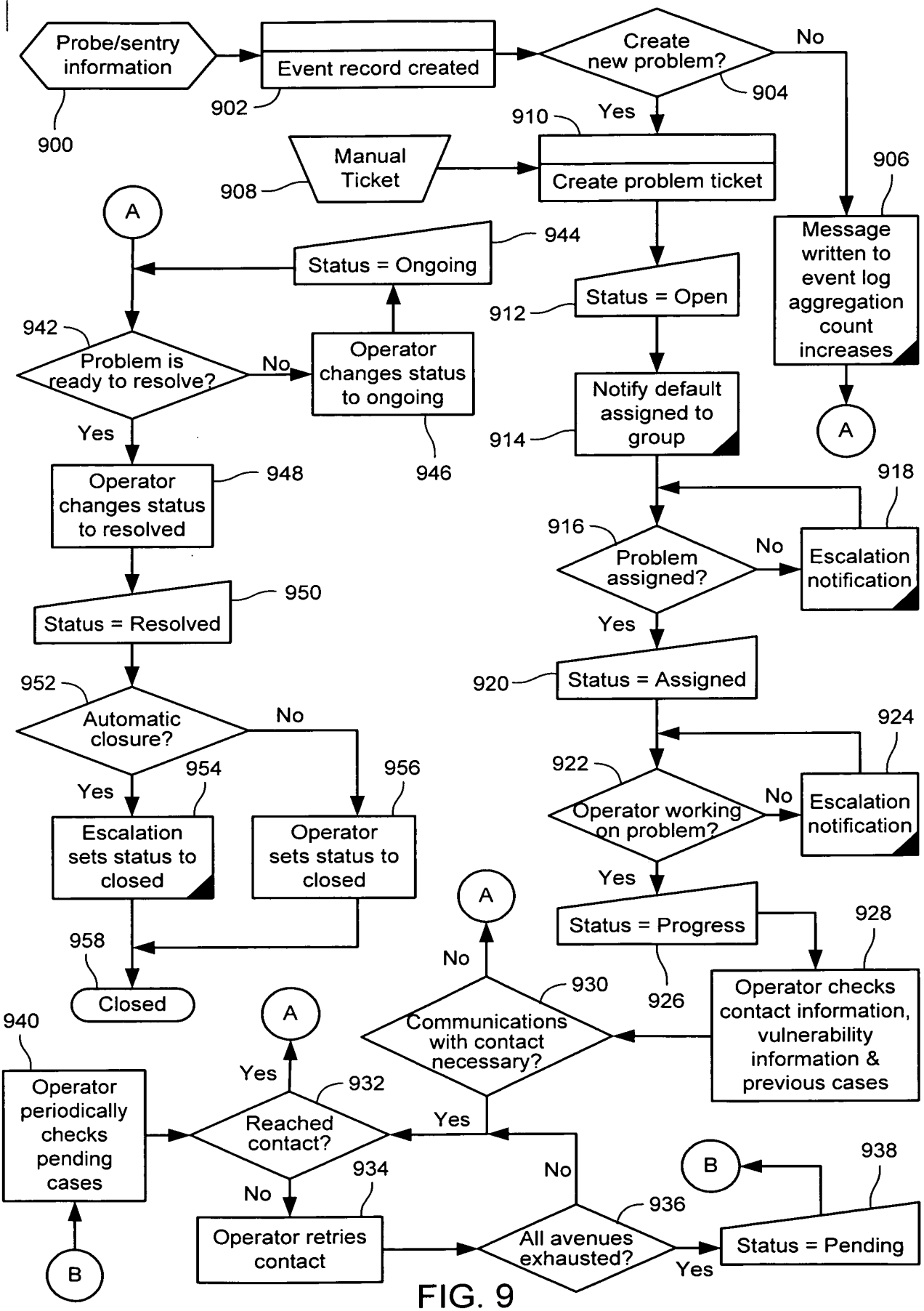

Probe/sentry information
900
Event record created
902
Create new problem?
904
No
Yes
910
Manual Ticket
908
Create problem ticket
906
Message written to event log aggregation count increases
A
Status = Ongoing
944
Status = Open
912
942
Problem is ready to resolve?
No
Operator changes status to ongoing
946
Notify default assigned to group
914
Yes
Operator changes status to resolved
948
Status = Resolved
950
916
Problem assigned?
No
Escalation notification
918
Yes
Status = Assigned
920
952
Automatic closure?
No
Yes
954
956
Escalation sets status to closed
Operator sets status to closed
922
Operator working on problem?
No
Escalation notification
924
Yes
Status = Progress
926
928
Operator checks contact information, vulnerability information & previous cases
958
Closed
A
No
930
Communications with contact necessary?
940
Operator periodically checks pending cases
Yes
932
Reached contact?
Yes
No
934
Operator retries contact
No
936
All avenues exhausted?
Yes
B
938
Status = Pending
B

FIG. 9

OIPE
OCT 10 2006
IAP86
PATENT & TRADEMARK OFFICE

Supplemental Application Data Sheet

Application Information

Application number::	09/766,343
Filing Date::	01/19/01
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 Intrusion Monitoring, Detection and Response
Attorney Docket Number::	022133-000510US
Request for Early Publication::	No
Request for Non-Publication::	No
Suggested Drawing Figure::	9
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::	101 East Minnehaha Parkway
State or Province of Residence::	MN
Country of Residence::	US
Street of Mailing Address::	
City of Mailing Address::	101 East Minnehaha Parkway
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 Rd., #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::	CA
City of Residence::	San Jose
State or Province of Residence::	
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	An Appn claiming benefit under 35 USC 119(e) of	60/190,326	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::	California
Country of mailing address::	U.S.
Postal or Zip Code of mailing address::	94043

OIPE IAP86
OCT 10 2006
PATENT & TRADEMARK OFFICE

PTO/SB/21 (07-06)

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	14

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

ENCLOSURES *(Check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☒ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) (please identify below):

Return Postcard; Part B Issue Fee Transmittal; Supplemental ADS

Remarks The Commissioner is authorized to charge any additional fees to Deposit Account 20-1430.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Townsend and Townsend and Crew LLP		
Signature			
Printed name	Philip H. Albert		
Date	October 4, 2006	Reg. No.	35,819

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	Paula S. Cunningham		
Typed or printed name	Paula S. Cunningham	Date	10/4/2006

60884629 v1

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.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/766,343	01/02/2007	7159237	028490-0007	7642

20350 7590 12/13/2006

TOWNSEND AND TOWNSEND AND CREW, 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 842 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 Customer Service Center of the Office of Patent Publication 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, San Jose, CA;

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

TOWNSEND and TOWNSEND and CREW LLP

By: _____

PATENT
Docket No.: 022133-000510US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Bruce Schneier et al.

Patent No.: 7,159,237

Issued: January 2, 2007

Application No.: 09/766,343

Filed: January 19, 2001

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

Confirmation No.: 7642

Examiner: Jenise E. Jackson

Art Unit: 2131

REQUEST FOR CERTIFICATE OF CORRECTION

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

Sir:

Pursuant to 37 CFR 1.322 Applicant submits a Certificate of Correction correcting printing errors made at the time of printing of the patent. No fee is required for this Certificate. The desired corrections are set forth on form PTO/SB/44, enclosed.

Date: APRIL 17, 2007

_____
Philip H. Albert
Reg. No. 35,819

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (415) 576-0200
Fax: (415) 576-0300
PHA:rlj
61030503 v1

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,159,237

APPLICATION NO.: 09/766,343

ISSUE DATE : January 2, 2007

INVENTOR(S) : Schneier et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Cover Page:

Insert (63), "This Application claims benefit of Provisional Application 60/190,326, filed on January 19, 2001".

MAILING ADDRESS OF SENDER (Please do not use customer number below):

TOWNSEND AND TOWNSEND AND CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, CA 94111-3834

61030500 v1

Electronic Acknowledgement Receipt

EFS ID:	1691303
Application Number:	09766343
International Application Number:	
Confirmation Number:	7642
Title of Invention:	METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE
First Named Inventor/Applicant Name:	Bruce Schneier
Customer Number:	20350
Filer:	Philip H. Albert/Robert Jackson
Filer Authorized By:	Philip H. Albert
Attorney Docket Number:	028490-0007
Receipt Date:	17-APR-2007
Filing Date:	19-JAN-2001
Time Stamp:	18:09:58
Application Type:	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	Request for Certificate of Correction	022133_000510US_RequestforCertificate.pdf	49904	no	2
Warnings:					

Information:	
Total Files Size (in bytes):	49904

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.

SPE RESPONSE FOR CERTIFICATE OF CORRECTION

Paper No.: _____

DATE : 6-6-07

TO SPE OF : ART UNIT 2131

SUBJECT : Request for Certificate of Correction for Appl. No.: 09/766343 Patent No.: 7159237

Please respond to this request for a certificate of correction within 7 days.

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Should Coce be Approved

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

Certificates of Correction Branch

703-308-9390 ext. 117

Thank You For Your Assistance

The request for issuing the above-identified correction(s) is hereby:

Note your decision on the appropriate box.

- ☐ Approved — All changes apply.
- ☐ Approved in Part — Specify below which changes do not apply.
- ☐ Denied — State the reasons for denial below.

Comments: _____

_____

_____

_____

_____

_____ _____

SPE Art Unit

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

Patent Number	7159237
Patent Date	1/02/2007
First Named Inventor	Schneier et al.
Art Unit	2131
Examiner Name	Jenise E. Jackson
Attorney Docket Number	022133-000510US

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

☒ Firm *or* Individual Name	Roger Nash BT Intellectual Property Department				roger.2.nash@bt.com
Address	ppC5, BT Centre 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.

61259923v1

Electronic Acknowledgement Receipt

EFS ID:	2757004
Application Number:	09766343
International Application Number:	
Confirmation Number:	7642
Title of Invention:	METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE
First Named Inventor/Applicant Name:	Bruce Schneier
Customer Number:	20350
Filer:	Philip H. Albert/Susan Aikins
Filer Authorized By:	Philip H. Albert
Attorney Docket Number:	022133-000510US
Receipt Date:	23-JAN-2008
Filing Date:	19-JAN-2001
Time Stamp:	16:48:17
Application Type:	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_022133-000510US.pdf	40945 3e70dff3174a2e321ea892519afee093251a74e7	no	1

Warnings:	
Information:	

Total Files Size (in bytes):	40945

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.

SPE RESPONSE FOR CERTIFICATE OF CORRECTION

Paper No.: _____

DATE : 6-6-07

TO SPE OF : ART UNIT 2131

SUBJECT : Request for Certificate of Correction for Appl. No.: 09/766343 Patent No.: 7159237

Please respond to this request for a certificate of correction within 7 days.

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Should Cofe be Approved

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

E Young

Certificates of Correction Branch

703-308-9390 ext. 117

Thank You For Your Assistance

The request for issuing the above-identified correction(s) is hereby:

Note your decision on the appropriate box.

☒ Approved	All changes apply.
☐ Approved in Part	Specify below which changes do not apply.
☐ Denied	State the reasons for denial below.

Comments: _____

Kristine Kincaid — SPE

2139 — Art Unit

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,159,237 B2
APPLICATION NO. : 09/766343
DATED : January 2, 2007
INVENTOR(S) : Schneier et al.

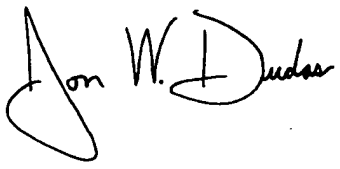
It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page

Insert Item (63), --This Application claims benefit of Provisional Application 60/190,326, filed on January 19, 2001--.

Signed and Sealed this

Seventh Day of October, 2008



JON W. DUDAS
Director of the United States Patent and Trademark Office

PTO/SB/81A (12-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
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 - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Patent Number	7,159,237
Issue Date	January 2, 2007
First Named Inventor	Bruce SCHNEIER
Title	METHOD AND SYSTEM FOR 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/96) submitted herewith or filed on _____

SIGNATURE of Inventor or Patent Owner

Signature		Date	1/21/15
Name	JAMIE NEWELL	Telephone	
Title and Company	SECRETARY, IG AMERICAS INC.		

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

EFS ID:	24793132
Application Number:	09766343
International Application Number:	
Confirmation Number:	7642
Title of Invention:	METHOD AND SYSTEM FOR DYNAMIC NETWORK INTRUSION MONITORING, DETECTION AND RESPONSE
First Named Inventor/Applicant Name:	Bruce Schneier
Correspondence Address:	Roger Nash BT Intellectual Property Department ppC5, BT Centre 81 Newgate Street. London - EC1A 7AJ GB 4420-736-8118 roger.2.nash@bt.com
Filer:	Raymond Y. Mah/Deborah White
Filer Authorized By:	Raymond Y. Mah
Attorney Docket Number:	022133-000510US
Receipt Date:	02-FEB-2016
Filing Date:	19-JAN-2001
Time Stamp:	13:10:19
Application Type:	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		POA_ChangeofAddress_7159237.pdf	2847066 bf9fb8b1b111068b1fc70a4373ea4d8fd4861c11	yes	2

	Multipart Description/PDF files in .zip description		
	Document Description	Start	End
	Assignee showing of ownership per 37 CFR 3.73	1	1
	Power of Attorney	2	2

Warnings:	
Information:	
Total Files Size (in bytes):	2847066

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.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: BT AMERICAS INC.

Application No./Patent No.: 7,159,237 Filed/Issue Date: January 2, 2007

Titled:

BT AMERICAS INC. , a CORPORATION

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

states that it is:

1. [X] 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. [X] 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 024964, Frame 0835, 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).

[X] 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.

_____ 1/21/15

Signature Date

JAMIE NEWELL SECRETARY

Printed or Typed Name 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.

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

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
09/766,343	01/19/2001	Bruce Schneier	022133-000510US

CONFIRMATION NO. 7642

POWER OF ATTORNEY NOTICE

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

OC00000028068335

Date Mailed: 02/26/2016

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.

/deelliott/

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
09/766,343	01/19/2001	Bruce Schneier	022133-000510US

CONFIRMATION NO. 7642

POWER OF ATTORNEY NOTICE

Roger Nash
BT Intellectual Property Department
ppC5, BT Centre
81 Newgate Street.
London, EC1A 7AJ
UNITED KINGDOM

OC000000081006789

Date Mailed: 03/01/2016

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**.

/ltaba/

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
09/766,343	01/19/2001	Bruce Schneier	RYM-36-1

CONFIRMATION NO. 7642

23117
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

POA ACCEPTANCE LETTER

OC000000081006865

Date Mailed: 03/01/2016

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**.

/ltaba/

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

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
		District of Delaware

PLAINTIFF	DEFENDANT
BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC.	FORTINET, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT 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 ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT 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