TITLE

AUTOMATED COMPUTER SYSTEM SECURITY COMPROMISE

This application claims the benefit of U.S. Provisional Application No. 60/304,270, filed July 10, 2001, and U.S. Provisional Application No. 60/313,793, filed August 20, 2001.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates generally to analyzing computer system security by compromising the security in a systematic manner.

Related Art

Computer systems that are connected to a computer network, such as the Internet, must employ security measures to prevent unauthorized users from accessing these systems. The security measures must be properly designed and implemented in order to prevent unauthorized access. However, it is difficult to evaluate the effectiveness of such security measures, particularly in view of the increasing sophistication of techniques used to gain unauthorized access to computer systems.

The effectiveness of the security measures of a computer system may be evaluated by performing a computer security audit in which various aspects of computer security are analyzed and evaluated.

ForcePoint LLC
EX-1010-PT2
Page001

The security audit may include a penetration test, which is a process by which a security auditor attempts to gain unauthorized access to the computer system.

Conventionally, a penetration test is performed using a multitude of *ad hoc* methods and tools, rather than according to a formalized standard or procedure. A typical penetration test includes the following stages:

1. Information gathering: The security auditor gathers technical details about the target system and information regarding the owner of the target system.

2. Information analysis and planning: The auditor analyzes the information to plan an overall approach by which to perform the penetration testing. This tends to be a difficult and time consuming task and requires experienced and knowledgeable personnel having a highly specialized skill base.

3. Vulnerability detection: The auditor searches the target system for security vulnerabilities based on the top-level plan developed in the information analysis and planning stage. Security vulnerabilities include, for example, system misconfigurations that enable an unauthorized user to gain access using a known series of steps.

The vulnerability search may be performed using an automated vulnerability scanner, which is a software package that determines whether certain known flaws may be used to gain unauthorized access to the target. Manual vulnerability scanning also may be performed to probe for common vulnerabilities that, for various reasons, may have been missed by an automated scanner. However, such vulnerability scanning techniques merely list the vulnerabilities, rather than actually attempt to exploit them.

ForcePoint LLC
EX-1010-PT2
Page002

The automated and manual vulnerability searches may be supplemented by research performed by the security auditor to determine previously unknown vulnerabilities. Such research typically is performed using a copy (also called a mirror) of the software application being probed and/or the associated hardware.

4. Compromising and accessing the target system: The auditor attempts to compromise the target system based on the results of the vulnerability detection stage using publicly available or custom-developed programs.

Publicly available programs designed to exploit system vulnerabilities tend to be unreliable and require testing and customization before use. In general, exploiting detected vulnerabilities, regardless of the tools being used, requires experienced and knowledgeable personnel having a highly specialized skill base. In addition, a considerable laboratory infrastructure may be required to develop and test vulnerability exploitation tools, particularly when the target system employs a number of different operating system platforms.

5. Analysis and reporting: This stage includes consolidating and presenting the information obtained during the previous stages and developing recommendations for remedying the security vulnerabilities identified during the penetration test. Manually maintaining a record of all of the actions taken and information gathered during testing is extremely time consuming and prone to error. Moreover, the preparation of complete and accurate records is subject to the discipline of the personnel conducting the test.

6. Clean up: The compromising and accessing stage typically results in significant changes being made to the target system. In the clean up stage, the auditor returns the system to its original

ForcePoint LLC
EX-1010-PT2
Page003

configuration. To perform a successful clean up, a detailed and exact list of all actions performed during testing must be maintained, yet there are only rudimentary tools available for maintaining such information.

In view of the shortcomings discussed above, there is a need for a system and method for performing an automated penetration test employing computer system compromise that takes an entirely fresh approach and overcomes the drawbacks of the conventional techniques.

SUMMARY OF THE INVENTION

The present invention generally provides a novel system, method, and computer code for performing automated penetration testing for analyzing computer system security by compromising the security in a systematic manner.

One aspect of the present invention provides a system, method, and computer code for performing penetration testing of a target computer network by installing a remote agent in the target computer network. A local agent is provided in a console and configured to receive and execute commands. A user interface provided in the console and configured to send commands to and receive information from the local agent, process the information, and present the processed information. A database is configured to store the information received from the local agent. A network interface is connected to the local agent and configured to communicate via a network with the remote agent installed in the target computer network. Security vulnerability exploitation modules are provided for execution by the local agent and/or the remote agent.

Embodiments of this aspect may include one or more of the following features. The user interface may enable a user to select one of the modules and initiate execution of the selected module on

either the local agent or the remote agent. The user interface may provide a graphical representation of the target computer network.

Another aspect of the present invention provides an agent for use in a system for performing penetration testing of a target computer network. The agent includes a proxy server configured to receive and execute system calls received via a network and a virtual machine configured to execute scripting language instructions received via the network.

Embodiments of this aspect may include one or more of the following features. The agent may include an execution engine configured to control the proxy server and the virtual machine. The system calls and the scripting language instructions may be routed to the proxy server and the virtual machine, respectively, by the execution engine. The agent may include a remote procedure call module configured to receive commands from the network formatted in a remote procedure call protocol and pass the commands to the execution engine.

Another aspect of the present invention provides an agent including a proxy server configured to receive and execute system calls received via a network and a virtual machine configured to execute scripting language instructions received via the network. The agent further includes a secure communication module configured to provide secure communication between the virtual machine and the network. An execution engine is configured to control the proxy server and the virtual machine. The system calls and the scripting language instructions are routed to the proxy server and the virtual machine, respectively, by the execution engine. A remote procedure call module is configured to receive commands via the network formatted in a remote procedure call protocol and pass the commands to the execution engine. A second secure communication module

ForcePoint LLC
EX-1010-PT2
Page005

is configured to provide secure communication between the remote procedure call module and the network.

Another aspect of the present invention provides a system, method and computer code for performing penetration testing of a target network in which a first module is executed in a console having a user interface. The first module is configured to exploit a security vulnerability in a first target host of the target network. A first remote agent is installed in the first target host. The first remote agent is configured to communicate with the console and a second remote agent. A second module is executed in the first remote agent. The second module is configured to exploit a security vulnerability in a second target host of the target network.

Embodiments of this aspect may include the feature of installing a second remote agent in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

Another aspect of the present invention provides a system, method, and computer code for performing penetration testing of a target network. A first module is executed to exploit a security vulnerability of a first target host of the target network. A first remote agent is installed in the first target host as a result of exploiting the security vulnerability of the first target host. A system call is sent to the first remote agent via a network. The system call is executed in the first target host using a proxycall server of the first remote agent to exploit a security vulnerability of a second target host.

In another aspect, a first module is executed to exploit a security vulnerability of a first target host of the target network. A first remote agent is installed in the first target host as a result of

ForcePoint LLC
EX-1010-PT2
Page006

exploiting the security vulnerability of the first target host. A second module that generates a system call is executed in the first remote agent. The system call is executed in the first target host to exploit a security vulnerability of a second target host.

In another aspect, a first module is executed to exploit a security vulnerability of a first target host of the target network. A first remote agent is installed in the first target host as a result of exploiting the security vulnerability of the first target host. A second module is executed in the first remote agent that generates a system call. A second remote agent is installed in the second target host as a result of exploiting a security vulnerability of the second target host. The system call generated by the second module is sent to the second remote agent via a network. The system call is executed in the second target host using a proxycall server of the second remote agent.

In another aspect, a first module is executed to exploit a security vulnerability of a first target host of the target network. A first remote agent is installed in the first target host as a result of exploiting the security vulnerability of the first target host. A second remote agent is installed in the second target host as a result of exploiting a security vulnerability of the second target host. A system call is sent to the first remote agent and is sent from the first remote agent to the second remote agent. The system call is executed in the second target host using a proxycall server of the second remote agent.

In another aspect, a first remote agent is installed in the first target host. The first remote agent has a proxy server configured to receive and execute system calls. A system call received via a network is executed in the first remote agent. A second remote agent is installed in the first target host. The second remote agent has a proxy server configured to receive and execute system calls

ForcePoint LLC
EX-1010-PT2
Page007

and a virtual machine configured to execute scripting language instructions. A scripting language instruction or a system call received via the network is executed in the second remote agent.

These and other objects, features and advantages will be apparent from the following description of the preferred embodiments of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more readily understood from a detailed description of the preferred embodiments taken in conjunction with the following figures.

Fig. 1 is a block diagram of a system for performing automated penetration testing of a target network in accordance with the present invention.

Fig. 2 is a block diagram of a console for automated penetration testing connected through the Internet to a first target host.

Fig. 3 is a block diagram of the console connected through the Internet to a first target host, which is connected through a target network to a second target host.

Fig. 4 is a block diagram showing components of the console.

Fig. 5 is a block diagram of a level 0 agent.

Fig. 6 is a block diagram of a level 1 agent.

Fig. 7 is a block diagram of a level 2 agent connected to upstream and downstream agents by two different networks.

ForcePoint LLC
EX-1010-PT2
Page008

Fig. 8 is a block diagram of a level 2 agent connected to upstream and downstream agents by a single network.

Fig. 9 is a block diagram of a level 3 agent.

Fig. 10 is a block diagram of a configuration in which a module is executed by the local agent in the console and system calls are executed in the operating system of the console.

Fig. 11 is a block diagram of a configuration in which a module is executed by the local agent in the console and system calls are executed in the operating system of the first target host.

Fig. 12 is a block diagram of a configuration in which a module is executed by the remote agent in the first target host and system calls are executed in the operating system of the first target host.

Fig. 13 is a block diagram of a configuration in which a module is executed by the remote agent in the first target host and system calls are executed in the operating system of the second target host.

Fig. 14 is a block diagram of a configuration in which a module is executed by the local agent in the console and system calls are executed in the operating system of the second target host.

Fig. 15 is a basic graphical user interface display screen presented by the user interface of the console.

Fig. 16 is a display screen following the running a Network Discovery Module.

Fig. 17 is a display screen following initiation of the Network Discovery module for a second time.

Fig. 18 is a display screen showing the results of the second running of the Network Discovery module and the running of the Remote Procedure Call (RPC) Mapper module.

ForcePoint LLC
EX-1010-PT2
Page009

Fig. 19 is a display screen in which the entities in the model of the target network can be examined and modified using an entity editor.

Fig. 20 is a display screen following two executions of the General Exploit module and the installation of a level 0 agent in a target host.

Fig. 21 is a display screen showing a window in which a Python console is running using the level 0 agent as a source.

Fig. 22 is a display screen following the execution of a port scanning module using the level 0 agent as a source.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

According to the present invention, as shown in Fig. 1, an automated penetration test is performed to identify, analyze, exploit, and document security vulnerabilities in a target network 100. The penetration test is executed by a console 105 that may be, for example, a personal computer running Microsoft Windows 2000 Professional, Server, or Advanced Server operating systems. The target network 100 may be connected to a network, such as for example the Internet 110. In the case of such example, the console also would be connected to the Internet 110 and would gain access to the target network 100 through the Internet 110.

The target network 100 has a first target host 115, e.g., a firewall. The firewall is a security device that typically is the only host in the target network that is connected directly to the Internet. It handles Internet traffic to and from the target network and serves to protect the target network from unauthorized access. The target network 100 has a number of other hosts connected to it – all of which could be the eventual targets of the penetration test.

The console 105, shown in Fig. 2, compromises the security measures protecting the first target host 115 by executing a series of modules. The modules may be selected and initiated by the user. Alternatively, the console may execute a predetermined sequence of modules or may determine a sequence of modules to be executed based on the information gathered during the penetration testing.

In the initial stage, typically, modules are executed to gather information about the first target host 115. For example, the console 105 may execute a port scanner that analyzes the ports of the first target host 115 and determines all of the services that are being run, such as an Internet web server, an email server, a finger service, etc. Further information might be acquired by running modules designed to exploit the services identified by the port scanner. For example, if the first target host 115 is running a finger service, then that service will be targeted by a module to determine software version, user names, etc. As a further example of an information gathering module, a network discovery module may be used to determine the number of hosts in the target network 100 and the Internet Protocol (IP) address of each host.

Following execution of the information gathering modules, the console executes modules, called exploits, to exploit security vulnerabilities in the first target host 115 based on the information that has been retrieved. For example, information may be obtained regarding a firewall operating system being run on the first target host 115, such as the software brand and revision number. Based on this information, the console 105 executes an exploit that has been written to take advantage of security vulnerabilities for that particular firewall.

Once a service running on the first target host 115 has been compromised, the console 105 installs a remote agent 120 on the first target host. The remote agent 120 is a program that operates on the

first target host 115 to perform a number of functions, such as receiving and executing control commands and modules from the console 105 and sending back information to the console 105.

As shown in Fig. 3, once the remote agent 120 has been installed on the first target host 115, it is used by the console 105 to gain access to the target network 100 and compromise the security of the other hosts that make up the target network 100, such as the second target host 125. For example, the remote agent 120 on the first target host 115 executes exploits, such as those discussed above, or system calls received from the console 105 to gather information and exploit other security vulnerabilities in the target network 100. To hosts connected to the target network 100, such commands or queries appear to originate from the first target host 115 and therefore may be more readily accepted. This is particularly true for networks that employ hierarchies of trust, which means that commands from known, i.e., trusted, sources are subject to less stringent security measures than commands from unknown sources.

Once the security of the second target host 125 has been compromised, the remote agent 120 in the first target host 115 installs a remote agent 130 in the second target host 125. Each of the installed agents 120 and 130 sends and receives modules, commands, and data from other installed agents, which is referred to as chaining. For example, the agent 130 in the second target host 125 receives modules and commands from the agent 120 in the first target host 115, which, in turn, receives the modules and commands from the console. The agent 130 in the second target host 125 also sends data back to the agent 120 in the first target host 115, which, in turn, sends the data back to the console 105.

The agent 130 in the second target host 125 executes the modules received from the upstream agents to gather information from and exploit security vulnerabilities in a third target host, in a

ForcePoint LLC
EX-1010-PT2
Page012

manner similar to that discussed above. Once the security measures have been compromised, the agent in the second target host installs an agent in the third target host. The penetration of the target network may continue in this manner until all of the target hosts have been compromised or until the final target of the penetration testing has been compromised.

The term "exploiting security vulnerabilities", as used herein, is a broad concept that includes any means for gaining access to and/or obtaining information from a target host. The concept includes, without limitation, the execution of modules that are designed to take advantage of specific security vulnerabilities that have been identified in a target host. For example, the first target host 115 may have been misconfigured by the owner in a manner that is detectable and allows installation of a remote agent 120. This concept also includes, without limitation, the execution of information gathering modules, such as port scanners and network discovery modules. This concept further includes, without limitation, the exploitation of security vulnerabilities of a target host that result from the compromise of other target hosts. For example, once a remote agent 120 has been installed in the first target host 115, it may be possible to gather information and install remote agents on other target hosts due to hierarchies of trust within the target network. This concept further includes, without limitation, obtaining access to a target host by virtue of a lack of security features or measures.

As shown in Fig. 4, a local agent 135 installed in the console 105 communicates with and controls the remote agents 120 and 130 through a network interface 140, such as a network interface card. The console 105 provides a module repository 145 to store modules that perform various functions related to system penetration and compromise. During the penetration test, these modules are sent to the local agent 135 in the console 105 or a remote agent 120 or 130 in a target host 115 or 125 to

be executed. For example, a module that performs packet sniffing may be sent to and executed on the remote agent 120 in order to monitor data packets passing through the first target host 115.

The console 105 also provides a user interface 150 that enables the user to control and monitor the performance of the penetration test. The user interface 150 may be a graphical user interface that displays a representation of the target network 100. The user interface 150 also reports the results of the activities performed by the agents installed in the target network.

A database 155 in the console 105 stores information sent back by remote agents 120 and 130. The database 155 could be a standard flat file, for example a text file, although a more complex structure, such as a relational database, also may be used. In addition, data may be exported to an external relational database. Each structured element of information is represented as an object in the database 155. The database 155 can accommodate multiple distributed instances of the same object that can be independently updated. The database 155 synchronizes the multiple instances of the objects to allow revision of the instances with the most recent data.

The information that is stored as objects in the console database 155 includes an activity log of all actions performed by the remote agents 120 and 130, such as executing modules, port scanning the host, passing modules to downstream remote agents, and installing remote agents in other hosts. The information also includes configuration data relating to the deployment of the remote agents, such as identification of the hosts in which the remote agents are installed and the possible communication channels that might be used to connect to them. The information also includes all of the data generated by execution of commands and modules by the remote agents, such as known hosts in the target network, operating systems, open ports, user accounts, cracked passwords, etc. The remote agents may store a subset of the database to provide caching of module data and to

make such data available to downstream modules. The cached data is eventually sent back to the console database.

Another type of object that can be managed by the database 155 is referred to as an entity, which is an object that represents a physical component in the target network 100, such as a host. Entities contain information similar to that discussed above, but also may have the capability to perform certain functions. For example, an entity may be capable of serializing and deserializing itself to and from XML markup language for transfer in and out of the database. This allows information produced by modules executed by remote agents to be shared between agents and with the console.

The data stored in the console database 155 is used for a number of purposes, such as to analyze the security vulnerabilities of the target network 100 and plan the exploitation of these vulnerabilities to penetrate further into the target network 100. The data also allows the console to reverse any changes made to the target network 100 during the penetration testing. In addition, the data allows the client for whom the penetration testing is performed to have a complete picture of actions performed during the testing. For example, the data may be exported into a relational database, as mentioned above, or may be used to generate reports using XML.

In general terms, an agent, such as the local and remote agents discussed above, is a program that is controlled by or used as a proxy by another program. The controlling program may be resident on the same host as the agent, as in the case of the user interface that controls the local agent on the console. Alternatively, the controlling program may be on a separate host, as in the case of the local agent on the console that controls the remote agent on the first target host. Hence, in this example, the local agent in the console serves both as an agent and as a controlling program.

Fig. 5 shows an example of a basic agent, which is referred to as a level 0 agent 205, running on a host 210 that is connected to a network 215. The level 0 agent 205 communicates through the network 215 to a controlling program running on an upstream agent, such as the local agent 135 in the console 105 or an intermediate agent positioned between the console and the level 0 agent. The level 0 agent 205 provides a syscall proxy server 220 that enables it to act as a proxy for the controlling program. This configuration is referred to as a system call proxy or proxycall configuration.

For example, referring again to Fig. 4, a level 0 agent 205 may be installed as the remote agent 120 on the first target host 115 and may be controlled by a module executed by the local agent 135 in the console 105 such as, for example, a remote exploit. The module includes commands that result in system calls ("syscalls"), which are instructions that access the operating system of the host. Rather than executing the syscall on the console 105, the syscalls are sent by a proxy client in the local agent 135 to the syscall proxy server 220 in the remote agent 120. The syscall proxy server 220 executes the syscalls on the first target host 115. Thus, syscalls are executed on the host of the remote agent 120, e.g., the first target host 115, rather than the host of the local agent 135, e.g., the console 105.

By acting as a syscall proxy, the remote agent 120 allows the local agent 135 to execute commands as if the local agent 135 were resident on the first target host 115. The syscall proxy configuration allows large, complex programs, such as the automated penetration testing program resident on the console 105, to execute system calls on a target host without actually being resident on the target host. Only the relatively small agent needs to be installed on the target host.

The level 0 agent 205 is a relatively simple program and may be about 100 bytes in size or smaller. Due to its small size, the level 0 agent 205 is typically the first type of agent to be installed in the target host during penetration testing. It may be used to gather information and/or exploit vulnerabilities in the target host to enable further penetration of the target host. Thus, the level 0 agent helps open the way for the installation of more complex agents, as discussed below.

The level 0 agent is often installed directly as the result of exploiting a security vulnerability, e.g., during exploitation of a buffer overflow or user-supplied format string vulnerability in an application running on the target host. The installed agent runs in the process space of the compromised application, e.g., an Internet web server or email server, and opens a socket to provide an unencrypted communication channel to the console or upstream agent. The syscall proxy server 220 in the level 0 agent 205 can execute one syscall at a time.

Fig. 6 shows an example of a more complex agent, which is referred to as a level 1 agent 225. The level 1 agent 225, like the level 0 agent 205, provides a syscall proxy server 220 to execute commands received from the console 105 or an upstream agent. The level 1 agent 225 can spawn separate syscall proxy servers 220 for corresponding syscalls received from the upstream agent, so several syscalls can be executed simultaneously. The level 1 agent 225 also can allocate memory and other resources within the host. Hence, the level 1 agent 225 can run in its own process space rather than relying solely on the process space of a compromised application. The ability to run in its own process space gives the level 1 agent 225 more autonomy and control over its own lifetime and more control over the resources of the host 210.

The level 1 agent 225 also provides a secure communication channel 230 with authentication and encryption of data. Data transmitted by the level 1 agent 225 back to the console 105 or upstream

agent is encrypted to ensure that information about the compromised system cannot be detected by third parties that may be monitoring network communications. The data is authenticated, e.g., using a digital signature, so that only the console that created the agent can communicate with it. This prevents different users who may be running the security compromise system from communicating with each other's agents.

Fig. 7 shows an example of a more complex agent, which is referred to as a level 2 agent 305. The level 2 agent 305, like the level 1 agent 225, provides a syscall proxy server 220 and secure communication 230 capability. The syscall proxy server 220 allows the level 2 agent to execute syscalls received from a module running on an upstream agent in a manner similar to the level 0 and level 1 agents. For example, a module running on the local agent 135 in the console 105 such as, for example, a remote exploit, may generate system calls that are intended to be executed in the operating system of the target host, rather than the console. Such syscalls are sent to the syscall proxy server 220 of the remote agent in the target host to be executed.

The level 2 agent 305 also provides a virtual machine 310 that can execute modules written in high-level, platform-independent, scripting languages, such as Python, Perl, Java, and Tcl. A module, in general, is an element of program code containing an individual operation or group of operations that are to be executed. Most of the modules used in the automated penetration test are designed to exploit security vulnerabilities in or gather information from a target host. Such modules may be obtained in a variety of ways. For example, laboratory testing may be performed on widely used software products to determine possible security vulnerabilities and how to exploit them. A module is then written for each software product based on the results of this testing. As a further example, such modules are commonly written and made available on the Internet by

ForcePoint LLC
EX-1010-PT2
Page018

members of the on-line security research community or by hackers or crackers, i.e., persons who attempt to gain unauthorized access to computer systems.

One advantage of executing modules in a virtual machine 310 is that it allows the level 2 agent 305 to perform computationally-intensive operations on the target host 210 without receiving a continuous flow of instructions, as in the case of syscall proxying. Indeed, syscall proxying may not be feasible for computationally-intensive operations because of the delays in transmitting instructions that result from network latency. Thus, the virtual machine 310 of the level 2 agent 305 can take greater advantage of the processor and other resources of the target host 210.

Another advantage of executing modules in a virtual machine 310 is that the modules need not be included as an integral part of the agent, but instead may be transferred to the agent on demand. This obviates the need to port the modules to the target host 210 operating system. Thus, modules can be run in a variety of target hosts without being rewritten for each different target host operating system. Moreover, the size of the agent is substantially reduced. In addition, because there are many widely available programs and modules written in standard scripting languages, the amount of custom programming required to create modules to execute on the target host is reduced.

The virtual machine 310 can communicate with, control, and install modules in downstream agents by opening a network connection to the target host 210 to access a network 315. The communication with the downstream agents may be established by a secure communication module 230 that forms a secure communication channel with data encryption and authentication. The virtual machine 310 can also handle native calls, which are syscalls that are intended to be executed in the operating system of the target host 210 on which the virtual machine 310 is installed. For example, an information gathering module may execute a syscall in the operating

system of the target host 210 on which the virtual machine 310 is installed in order to access the Internet through a network interface.

In the example shown in Fig. 7, the network 315 accessed by the virtual machine 310 is separate from the network 215 used to communicate with the console 105 or upstream agent. The network 315 accessed by the virtual machine 310 may be a target network 100, such as shown in Figs. 1 and 3, that cannot be reached from an outside host. Alternatively, as shown in Fig. 8, the network 320 accessed by the virtual machine 310 may be the same network 320 used to communicate with the console 105 or upstream agent. For example, as shown in Fig. 1, both the second and third target hosts are connected to the target network, and a virtual machine in an agent on the second target host may communicate with an agent installed on the third target host.

The virtual machine 310 and the syscall proxy server 220 in the level 2 agent 305 are controlled by an execution engine 325 that determines which modules are executed and how they are executed. For example, the execution engine 325 provides task control capability to start, pause, resume, and cancel module execution. The execution engine 325 also controls the execution of native modules 330, which are modules written to be executed directly in the operating system of the target host 210.

The execution engine 325 provides transparent multitasking capabilities by taking advantage of either the multi-threading or multi-processing capabilities of the underlying operating system to enable concurrent execution of modules and syscalls by spawning new threads or processes as necessary. Task-specific storage is provided to enable an executing module to access context information. For example, upon initialization, the execution engine may set up synchronization

objects (known as mutexes) and task-specific storage for module context using, e.g., the ThreadLocalStorage routine in Win32 or the thread-specific routine in PTHREADS.

The execution engine 325 is isolated in certain respects from the rest of the system architecture, aside from the modules that are controlled by it. For example, the execution engine 325 operates independently of the proxycall architecture. In addition, necessary parameters for the modules to execute on the agent are provided by the module context, rather than by the execution engine 325.

The module context provides all of the information necessary for a specific execution instance (the execution instance being, e.g., a task or executing module). Such information includes the module parameters, designation of remote or local execution, description of the peer (for remote execution), etc. The module context is available from any subsystem of the agent that is involved in the module execution, e.g., a proxycall client. The module accesses the module context from the agent during execution of the module.

The level 2 agent receives commands and instructions through a remote procedure call (RPC) component 327, which then passes the received data to the execution engine 325. The RPC component 327 employs a standard protocol to control communication with the console or upstream agent using a predefined data packet format. To implement this protocol, the console uses an internal representation of all the deployed agents that includes all of the properties and capabilities for establishing a communication channels with the deployed agents.

Communications between the console and deployed level 1 and level 2 agents are established as follows. First, the console establishes an internal connection with the internal representation of the remote agent with which it is attempting to communicate. The internal representation of the

remote agent uses its communications component to establish a communication channel across the network with the remote level 1 or level 2 agent. The communication channel then is created using a component of the system that can multiplex communications from several modules into one or many communications channels with a remote agent.

The RPC component 327 implements a bi-directional communication mechanism using the communications channel described above as an underlying transport mechanism. The RPC component implements and executes commands that control the execution of modules on the remote agents as well as the transfer of information between agents. For example, the RPC component is used to start, pause and stop module execution. The RPC component also is used to transfer modules to remote agents, retrieve module execution results from remote agents, and control the configuration and status of remote agents.

Fig. 9 shows an example of a level 3 agent 335, which is similar to the level 2 agent 305 shown in Fig. 8, but includes a user interface 340 through which the level 3 agent 335 is controlled. The user interface 340 allows the level 3 agent 335 to function as the local agent 135 component of the console 105, as shown in Fig. 2. The level 3 agent 335, like the level 2 agent 305, includes secure communication capability 230, a virtual machine 310, a syscall proxy server 220, native module capability 330, an RPC send/dispatch component 327, and an execution engine 325.

The proxycall and virtual machine capabilities discussed above enable the agents to execute modules in a number of different configurations. Fig. 10 shows a configuration in which a module 400 is executed by the local agent 135 in the console 105. System calls generated by the module 400 are handled by the local agent 135 as native syscalls and are executed in the operating system 405 of the console 105. For example, when a module 400 executes a command for querying the

status of a port on a target host 115, a system call is made to the operating system 405 of the console 105 in order to access the network interface 140 and transmit the request to the target host 115 through the Internet 110.

Another configuration in which a module is executed by the local agent 135 in the console 105 is shown in Fig. 11. In this configuration, however, system calls generated by the module 400 are transmitted to a remote agent 120 installed in the first target host 115. The system calls are handled by the syscall proxy server of the remote agent 120 and are executed in the operating system 410 of the first target host 115. For example, when a module 400 executes a command for retrieving a file from the second target host 125 through the target network 100, the syscall generated by this command is executed in the operating system 410 of the first target host 115. From the perspective of the second target host 125, the command appears to have been executed on the first target host 115 and therefore is more likely to be trusted and implemented by the second target host 125.

Fig. 12 shows a configuration in which a module 400 is executed by a remote agent 120 in a target host, e.g., the first target host 115. System calls generated by the module 400 are handled by the remote agent 120 as native syscalls and are executed in the operating system of the first target host 410. This configuration allows the module 400 to take advantage of the resources of the first target host 115. In addition, it enables the module 400 to run without generating network traffic between the console 105 and the target network 100.

Another configuration in which a module is executed by a remote agent in a target host is shown in Fig. 13. In this configuration, however, the system calls generated by the module 400 are transmitted to a remote agent 130 installed in another target host, e.g., the second target host 125.

ForcePoint LLC
EX-1010-PT2
Page023

System calls generated by the module 400 are handled by the syscall proxy server of the remote agent 130 and are executed in the operating system 415 of the second target host 125.

As above, this configuration allows the module to take advantage of the resources of the first target host 115, and enables the module to run without generating network traffic between the console 105 and the target network 100. Another advantage of this configuration is that, from the perspective of the other hosts in the target network 100, the module 400 commands appear to originate from the second target host 125. Consequently, such commands are more likely to be trusted and implemented by the other hosts of the target network. In other words, using the remote agent 130, the system effectively assumes the identity of the compromised host and takes advantage of the privileges of the compromised host within the target network.

Fig. 14 shows another configuration in which a module is executed by the local agent in the console. In this configuration, however, system calls generated by the module 400 are transmitted to a remote agent 120 installed in the first target host 115, which in turn passes the system calls to a remote agent 130 installed in the second target host 125. The system calls are handled by the syscall proxy server of the remote agent 130 in the second target host 125 and are executed in the operating system 415 of the second target host 125. As in the case above, from the perspective of the other hosts in the target network, the module commands appear to originate from the second target host. Consequently, such commands are more likely to be trusted and implemented by the other hosts of the target network.

As discussed above, the local agent 135 in the console 105 provides a user interface 150. As shown in Fig. 15, the user interface presents to the user a Windows-based graphical user interface (GUI) screen. The screen has several component windows that present information in various

ForcePoint LLC
EX-1010-PT2
Page024

formats and allow control to be executed over various aspects of the penetration testing. Of course, the components of the screen may be moved and sized based on the user's preferences.

The visibility view, in the central portion of the screen, presents a graphical representation, i.e., a model, of the target network. In this example, the graphical representation is in the form of a hierarchical listing of entities, i.e., a tree listing. Each entity represents a physical component of the target network, e.g., a host. Initially, the visibility view shows only two entities, the local host (e.g., the console) and the local agent that is running on the local host. As further discussed below, as each stage of the penetration testing is performed, the model of the target network is updated to reflect newly gained information.

Tabs are arranged on the left side of the screen to organize the available functions, modules, and tools offered by the program. Clicking on a tab causes it to move to the top of the window and display the available modules under that category. For example, the Remote Exploits tab provides various modules that may be run on the local agent to exploit security vulnerabilities in a target network without being located in the target network. An executed modules window is provided on the top right side of the screen to display a history of the modules that have been executed during the penetration testing and their status. A module output window is provided on the bottom right side of the screen to display the output of the modules.

Fig. 16 shows an example of how the user interface screen appears after the Network Discovery module has been run. The Network Discovery module, which is grouped under the Information Gathering tab, is typically run early in the penetration testing to determine the topology of the target network. The executed modules window shows that the Network Discovery module has been run and provides the start and finish times and the current status, which in this case indicates that the

execution of the module is finished. The module output window provides a table of host names, Internet protocol (IP) addresses, operating system (OS), and other information output by the module.

Following the execution of the Network Discovery module, the visibility view displays a graphical representation of the target network in the form of a tree listing. The tree shows that the local host on the console (local host) has a local agent that is connected to a first target host having IP address 192.168.66.0/24. The first target host, in turn, is connected to other hosts within the target network. The entities in the tree listing may be collapsed or expanded according to hierarchical level by clicking on the arrow symbols on the left-hand side of the entities. As each module is run during the penetration testing, the visibility view is automatically updated to show a more complete model of the target network.

Fig. 17 shows an example of the screen display for initiating the execution of the Network Discovery module for a second time. The user double clicks on the Network Discovery module tab, and the screen presents a module parameter entry box. The user is prompted to enter the IP address of the target network, which is typically known by the user prior to performing penetration testing. For instance, the user may determine the IP address from a domain name server lookup of the domain name of the target host. In this example, the Network Discovery module is targeting the host with IP address 192.168.22.0/24. In the visibility view, the previously targeted host (192.168.66.0/24) has been collapsed to a single top-level entry in the tree listing. As an alternative to entering the target host IP address, the module tab may be dragged and dropped onto the target host in the tree listing for which information is to be gathered.

As discussed above, modules may be run on local or remote agents in a variety of configurations. The system calls generated by the modules are executed on the default source host, which in the example of Fig. 17 is the local agent. The default source is either the most recently used source or a source selected in the visibility view prior to execution of the module. For instance, if a module is executed using the local agent as a source host, the local agent remains the default source until a new source is selected. Thus, double clicking on the Network Discovery tab results in that module being run with on the local agent and gathering information from the target host entered in the module parameter entry box.

As shown in Fig. 18, the output of the Network Discovery module is presented in the visibility view as a list of connected hosts under the target host (192.168.22.0/24). The executed module window indicates that the Network Discovery module has been run a second time. In addition, the Remote Procedure Call (RPC) Mapper module has been run, which attempts to identify all of the ports in the target host that are available to receive RPC commands. The RPC Mapper was initiated by dragging and dropping it onto the target host, which in this case is 192.168.22.2. The output of the RPC Mapper is shown in the module output window in the log/debug format, which includes information to enable the user to track and rectify errors in the module. The output identifies the RPC ports and their associated protocols.

As shown in Fig. 19, the entities in the model of the target network can be examined and modified using an entity editor. Each entity has properties that reflect aspects of the information gathered on the corresponding physical component in the target network. For example, a host entity has properties such as system architecture (arch), operating system, interfaces, ports, etc. The host entity also has an agent property that lists the agents running on that host.

ForcePoint LLC
EX-1010-PT2
Page027

The properties of each entity are updated automatically as modules are run during the penetration testing. For example, the entity corresponding to host 192.168.22.2 has a listing of ports available for RPC service. This listing is the result of running the RPC Mapper module directed toward this host, as described above. In certain instances, different modules may result in different property states, for example, two different results regarding the operating system being run on a particular host. In such a case, the program will prompt the user to resolve the apparent conflict based on experience or outside knowledge.

Even in the absence of a conflict, the state of these properties may be changed by the user based on experience and knowledge gained from other sources. For example, the user may know, based on experience, that a host having a particular architecture, e.g., Sparc Version 8, may run a particular operating system, e.g., Solaris. In such a case, the user edits the host entity and changes the operating system property from unknown to Solaris. This allows the user to build a more complete and accurate model of the target network.

Once sufficient information has been gathered regarding the target network, modules may be executed to exploit security vulnerabilities in the target network. As shown in Fig. 20, such modules are grouped under the Local Exploits and Remote Exploits tabs on the user interface screen depending upon whether they run within the target host (i.e., locally) or remotely. In this example, the executed module window shows that a module called "General Exploit" has been run twice. The first execution of the module was unsuccessful, as indicated by the icon to the left of the module name and by the term "aborted" in the status column. The second execution was successfully completed. In addition to the modules grouped under the exploit tabs, there are a series of modules under the Agents tab that relate to the installation and execution of remote agents

in the target network. In this example, a level 0 agent has been installed in the host with address 192.168.22.6.

The installation of the level 0 agent may be accomplished by clicking on two entries under the Agents tab. First, a level 0 agent service is initiated, which is a process that runs on the target host. As discussed above, the level 0 agent service may share the process space of an existing service on the target host, such as an email server. Then, a level 0 agent is installed and executed in the level 0 agent service. Alternatively, the program may present a single entry under the Agents tab that performs all of the steps required to install and execute the level 0 agent.

Once the level 0 agent has been installed, the user can begin to take advantage of the agent by executing modules on it. The user sets the level 0 agent to be the source for the execution of modules by right clicking on the agent and selecting "Set as source". As shown in Fig. 21, the level 0 agent may be displayed as highlighted or bold in the visibility view to indicate to the user that it is the current default source. All subsequent modules are run on the level 0 agent source until the default is changed.

In this example, the Python Console module has been initiated. As discussed above, Python is a high-level, platform-independent, scripting language. The Python console allows the user to enter and execute Python commands and to save commands as a module. The Python command interpreter runs on the local agent, however, the syscalls generated by the command interpreter are executed by the syscall proxy server of the level 0 agent, which is the selected source.

In contrast, a module may run on a remote agent that has the capability to execute modules, such as a level 2 agent. As discussed above, the level 2 agent has a virtual machine that enables it to

execute scripting language modules. In such a case, the module is resident on and executes on the remote agent. Syscalls generated by the module are executed either as a native call on the remote host (see Figs. 7 and 8) or by a syscall proxy server on a downstream agent. The module may be installed together with the remote agent, or may be downloaded after the remote agent has been installed. This capability for 100% remote execution is advantageous, because it allows the module to run without receiving a continuous series of commands, thereby avoiding the generation of excessive network traffic. Moreover, a module for exploiting a security vulnerability may have certain timing requirements that, due to network latency, cannot be met if commands must be received over the network.

Regardless of whether a module is being run on the local agent or a remote agent, the syscalls generated by the module will be executed on the selected source, which in the example of Fig. 21 is the level 0 agent installed on target host 192.168.22.6. Thus, the Python commands executed in the Python console generate syscalls that are executed on this selected target host. For example, the Python command "print socket.gethostname()", shown in the Python console window, generates a syscall to retrieve the name of the target host, "diavolo". The remaining commands shown in the window generate syscalls to create a socket in the target host, which can be used to retrieve information from the target host.

It will be appreciated that each of these embodiments discussed above provides a novel system and method for analyzing computer system security by compromising the security in a systematic manner.

It also will be appreciated that because the system provides a database of modules for exploiting security vulnerabilities, the system described herein actually attempts to exploit detected vulnerabilities, rather than merely listing them.

It also will be appreciated that because the system provides a virtual machine to execute modules in agents installed in target hosts, the modules can be run on a variety of platforms and operating systems without further customization and testing. In addition, publicly available programs to exploit security vulnerabilities can be used without an extensive laboratory infrastructure for rewriting and testing.

It also will be appreciated that because the system maintains a database of all operations performed during the penetration testing, the target system can be reliably returned to its original configuration.

While the present invention has been described with respect to what is presently considered to be the preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. To the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

WHAT IS CLAIMED:

1. A system for performing penetration testing of a target computer network by installing a remote agent in the target computer network, the system comprising:

a local agent provided in a console and configured to receive and execute commands;

a user interface provided in the console and configured to send commands to and receive information from the local agent, process the information, and present the processed information;

a database configured to store the information received from the local agent;

a network interface connected to the local agent and configured to communicate via a network with the remote agent installed in the target computer network; and

security vulnerability exploitation modules for execution by the local agent and/or the remote agent.

2. The system of claim 1, wherein the user interface enables a user to select one of the modules and initiate execution of the selected module on either the local agent or the remote agent.

3. The system of claim 1, wherein the user interface provides a graphical representation of the target computer network.

4. A method for performing penetration testing of a target computer network, comprising:

installing a remote agent in the target computer network;

executing a command using a local agent provided in a console;

receiving information from the local agent in a user interface provided in the console;

presenting the information received from the local agent to a user;

storing the information received from the local agent in a database;

communicating via a network with the remote agent installed in the target computer network; and

providing security vulnerability exploitation modules for execution by the local agent and/or the remote agent.

5. The method of claim 4, further comprising:

selecting, using the user interface, one of the modules; and

initiating execution of the selected module on either the local agent or the remote agent.

6. The method of claim 4, further comprising providing a graphical representation of the target computer network using the user interface.

7. Computer code for performing penetration testing of a target computer network, the computer code comprising code for:

installing a remote agent in the target computer network;

executing a command using a local agent provided in a console;

ForcePoint LLC
EX-1010-PT2
Page033

receiving information from the local agent in a user interface provided in the console;

presenting the information received from the local agent to a user;

storing the information received from the local agent in a database;

communicating via a network with the remote agent installed in the target computer network; and

providing security vulnerability exploitation modules for execution by the local agent and/or the remote agent.

8. The computer code of claim 7, further comprising code for:

selecting, using the user interface, one of the modules; and

initiating execution of the selected module on either the local agent or the remote agent.

9. The computer code of claim 7, further comprising code for providing a graphical representation of the target computer network using the user interface.

10. An agent for use in a system for performing penetration testing of a target computer network, the agent comprising:

a proxy server configured to receive and execute system calls received via a network; and

a virtual machine configured to execute scripting language instructions received via the network.

11. The agent of claim 10, further comprising an execution engine configured to control the proxy server and the virtual machine, wherein the system calls and the scripting language instructions are routed to the proxy server and the virtual machine, respectively, by the execution engine.

12. The agent of claim 11, further comprising a remote procedure call module configured to receive commands from the network formatted in a remote procedure call protocol and pass the commands to the execution engine.

13. An agent for use in a system for performing penetration testing of a target computer network, the agent comprising:

a proxy server configured to receive and execute system calls received via a network;

a virtual machine configured to execute scripting language instructions received via the network;

a secure communication module configured to provide secure communication between the virtual machine and the network;

an execution engine configured to control the proxy server and the virtual machine, wherein the system calls and the scripting language instructions are routed to the proxy server and the virtual machine, respectively, by the execution engine;

a remote procedure call module configured to receive commands via the network formatted in a remote procedure call protocol and pass the commands to the execution engine; and

a second secure communication module configured to provide secure communication between the remote procedure call module and the network.

14. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module in a console having a user interface, the first module being configured to exploit a security vulnerability in a first target host of the target network;

installing a first remote agent in the first target host, the first remote agent being configured to communicate with the console and a second remote agent; and

executing a second module in the first remote agent, the second module being configured to exploit a security vulnerability in a second target host of the target network.

15. The method of claim 14, further comprising installing a second remote agent in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

16. A system for performing penetration testing of a target network, comprising:

a console having a user interface;

a first module configured to execute in the console to exploit a security vulnerability in a first target host of the target network;

a first remote agent installed in the first target host, the first remote agent being configured to communicate with the console and a second remote agent; and

ForcePoint LLC
EX-1010-PT2
Page036

a second module configured to execute in the first remote agent to exploit a security vulnerability in a second target host of the target network.

17. The system of claim 16, further comprising a second remote agent installed in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

18. Computer code for performing penetration testing of a target network, the computer code comprising code for:

executing a first module in a console having a user interface, the first module being configured to exploit a security vulnerability in a first target host of the target network;

installing a first remote agent in the first target host, the first remote agent being configured to communicate with the console and a second remote agent; and

executing a second module in the first remote agent, the second module being configured to exploit a security vulnerability in a second target host of the target network.

19. The computer code of claim 18, further comprising code for installing a second remote agent in the second target host of the target network, the second remote agent being configured to communicate with the first remote agent.

20. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

sending a system call to the first remote agent via a network; and

executing the system call in the first target host using a proxycall server of the first remote agent to exploit a security vulnerability of a second target host.

21. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing in the first remote agent a second module that generates a system call; and

executing the system call in the first target host to exploit a security vulnerability of a second target host.

22. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing a second module in the first remote agent that generates a system call;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending the system call generated by the second module to the second remote agent via a network; and

executing the system call in the second target host using a proxycall server of the second remote agent.

23. A method for performing penetration testing of a target network, comprising the steps of:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending a system call to the first remote agent;

sending the system call from the first remote agent to the second remote agent; and

executing the system call in the second target host using a proxycall server of the second remote agent.

24. A method for performing penetration testing of a target network, comprising the steps of:

installing a first remote agent in the first target host, the first remote agent having a proxy server configured to receive and execute system calls;

executing in the first remote agent a system call received via a network;

installing a second remote agent in the first target host, the second remote agent having a proxy server configured to receive and execute system calls and a virtual machine configured to execute scripting language instructions; and

executing in the second remote agent a scripting language instruction or a system call, the system call being received via the network.

25. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

sending a system call to the first remote agent via a network; and

executing the system call in the first target host using a proxycall server of the first remote agent to exploit a security vulnerability of a second target host.

26. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing in the first remote agent a second module that generates a system call; and

executing the system call in the first target host to exploit a security vulnerability of a second target host.

27. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

executing a second module in the first remote agent that generates a system call;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending the system call generated by the second module to the second remote agent via a network; and

executing the system call in the second target host using a proxycall server of the second remote agent.

28. Computer code for performing penetration testing of a target network, the code comprising code for:

executing a first module to exploit a security vulnerability of a first target host of the target network;

installing a first remote agent in the first target host as a result of exploiting the security vulnerability of the first target host;

installing a second remote agent in the second target host as a result of exploiting a security vulnerability of the second target host;

sending a system call to the first remote agent;

sending the system call from the first remote agent to the second remote agent; and

executing the system call in the second target host using a proxycall server of the second remote agent.

29. Computer code for performing penetration testing of a target network, the code comprising code for:

installing a first remote agent in the first target host, the first remote agent having a proxy server configured to receive and execute system calls;

executing in the first remote agent a system call received via a network;

installing a second remote agent in the first target host, the second remote agent having a proxy server configured to receive and execute system calls and a virtual machine configured to execute scripting language instructions; and

executing in the second remote agent a scripting language instruction or a system call, the system call being received via the network.

ForcePoint LLC
EX-1010-PT2
Page042

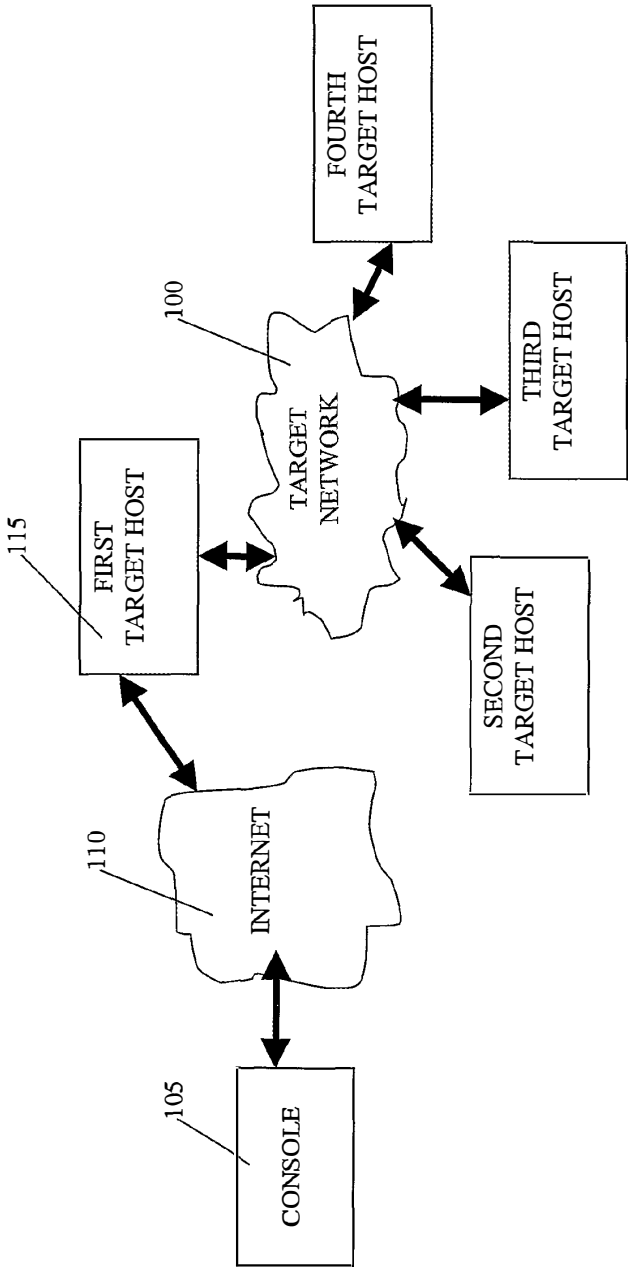


Fig. 1

ForcePoint LLC
EX-1010-PT2
Page043

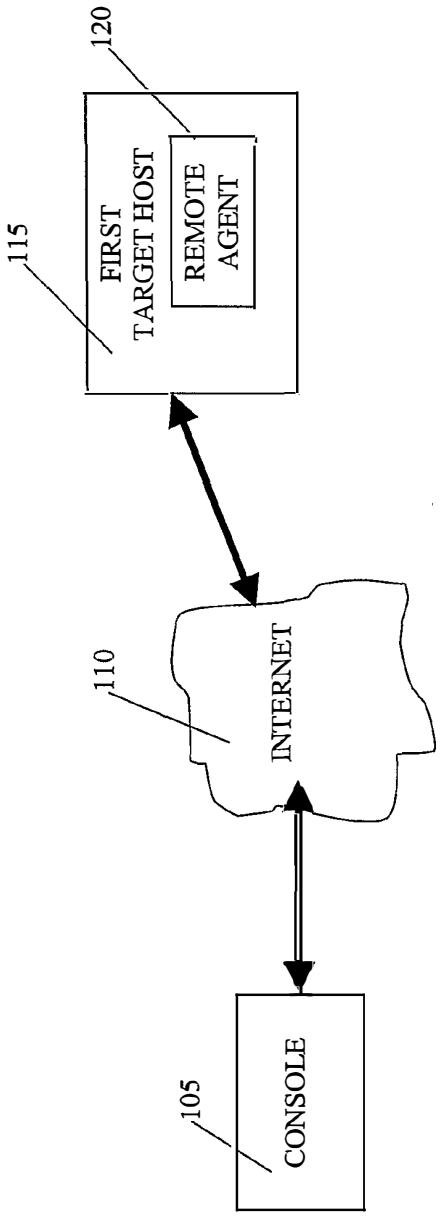

120
FIRST TARGET HOST
REMOTE AGENT
115
110
INTERNET
105
CONSOLE

Fig. 2

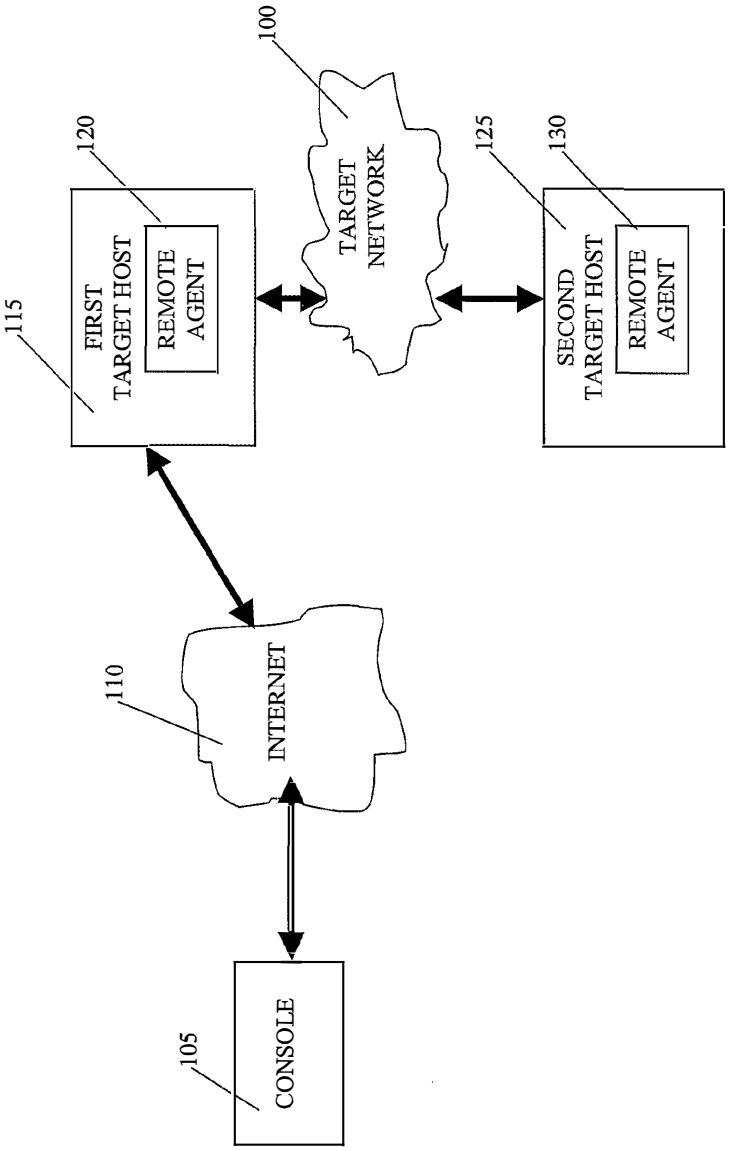

100
TARGET NETWORK
120
FIRST TARGET HOST
REMOTE AGENT
115
125
130
SECOND TARGET HOST
REMOTE AGENT
INTERNET
110
CONSOLE
105

Fig. 3

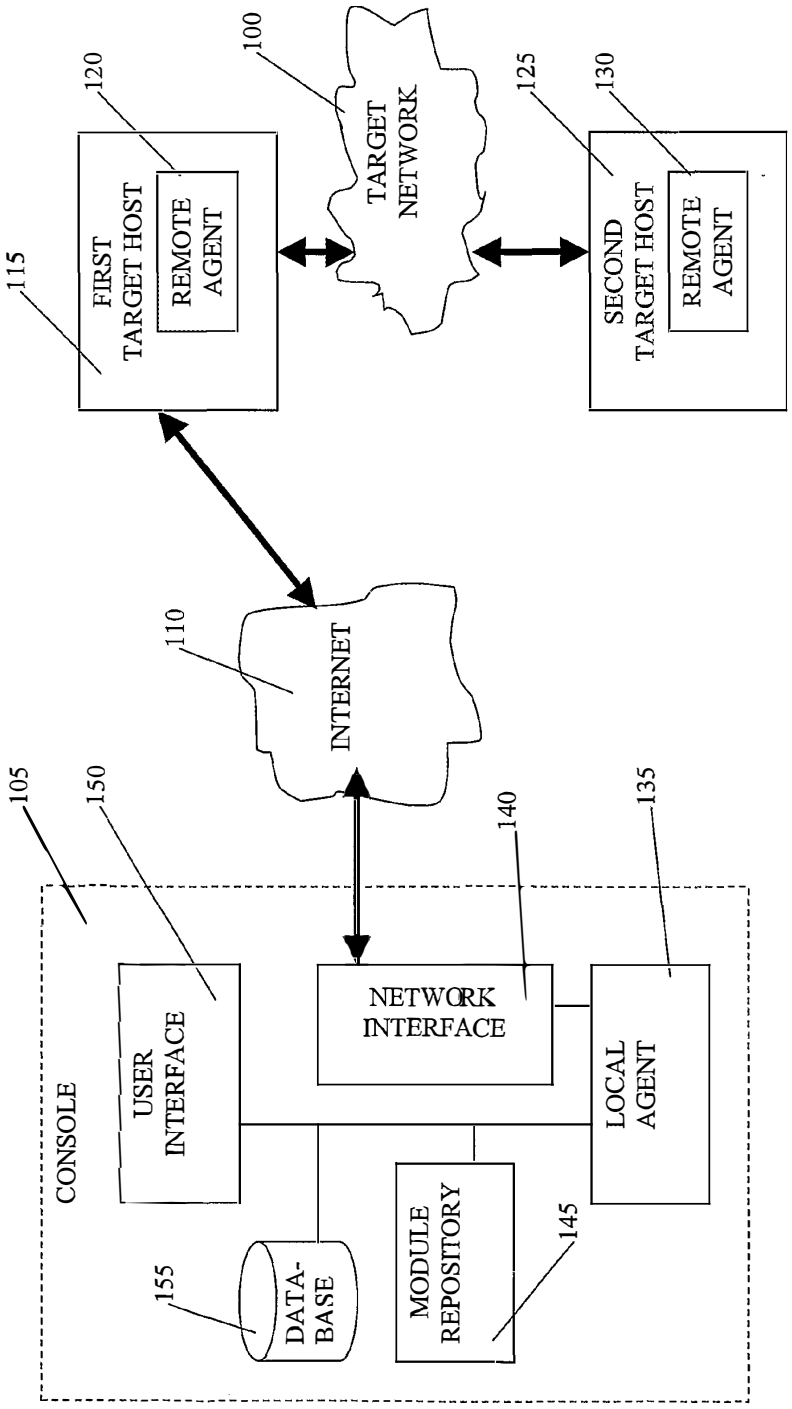


Fig. 4

ForcePoint LLC
EX-1010-PT2
Page046

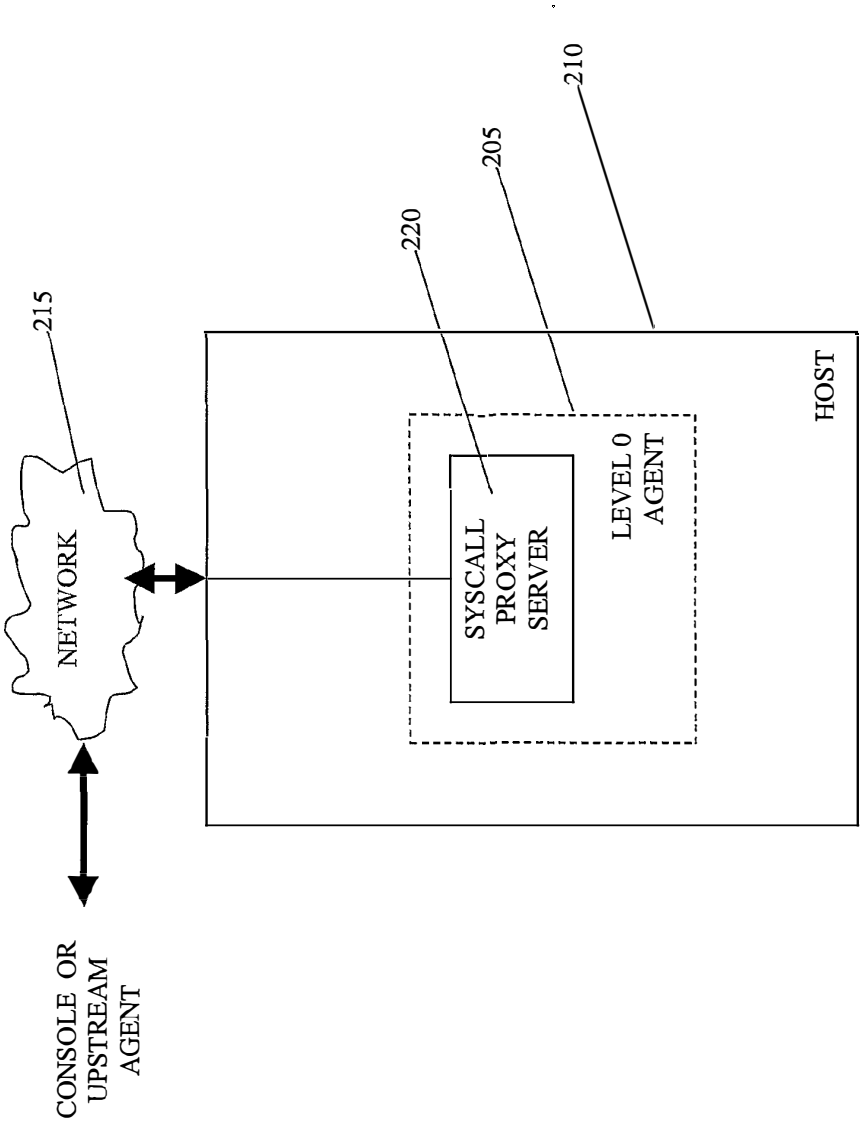

210
205
220
215
HOST
LEVEL 0 AGENT
SYSCALL PROXY SERVER
NETWORK
CONSOLE OR UPSTREAM AGENT

Fig. 5

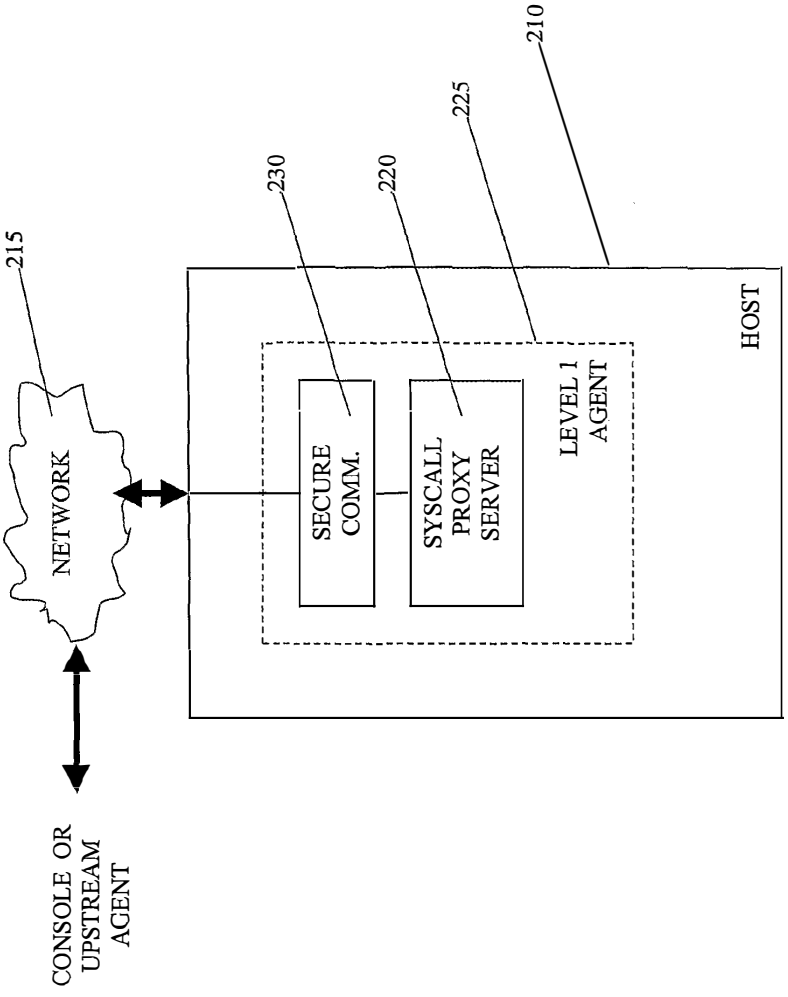


Fig. 6

ForcePoint LLC
EX-1010-PT2
Page048

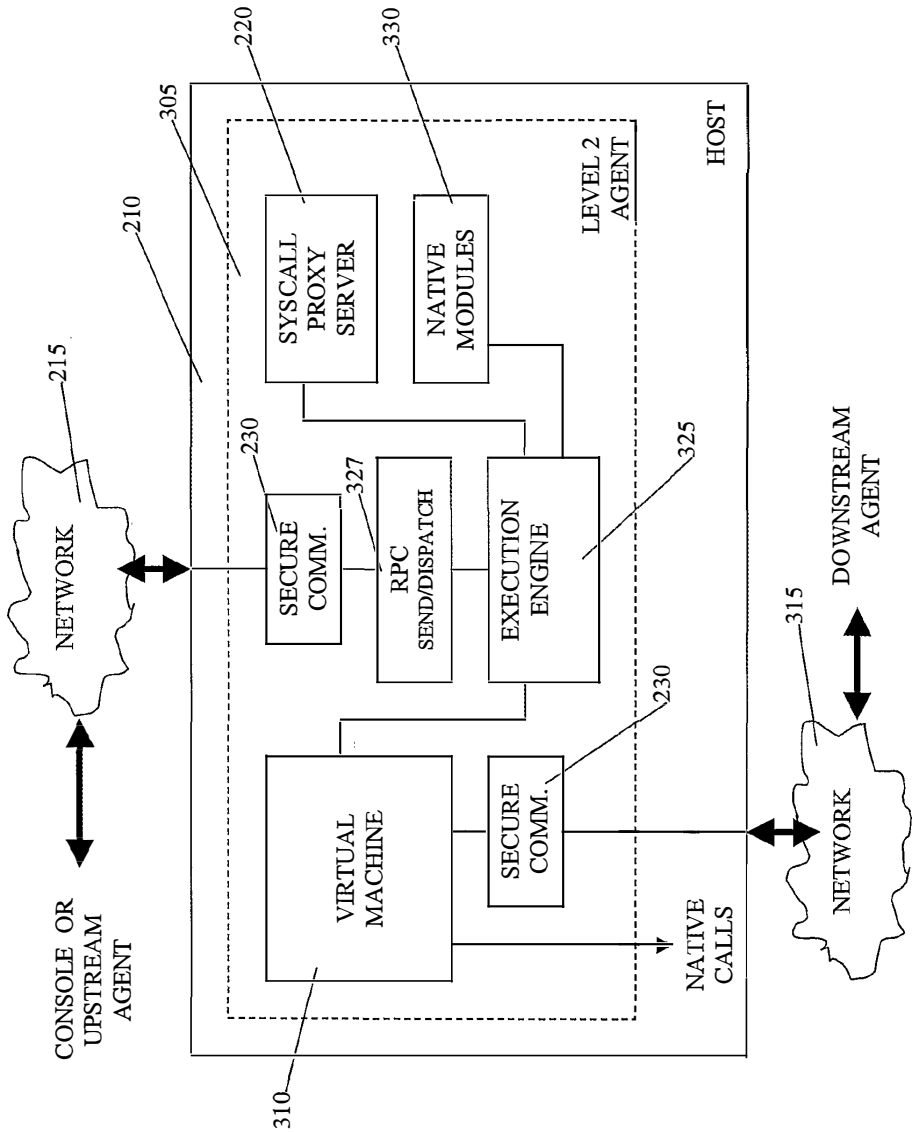

220
330
305
210
HOST
LEVEL 2 AGENT
SYSCALL PROXY SERVER
NATIVE MODULES
215
230
327
325
NETWORK
SECURE COMM.
RPC SEND/DISPATCH
EXECUTION ENGINE
DOWNSTREAM AGENT
315
230
VIRTUAL MACHINE
SECURE COMM.
NETWORK
CONSOLE OR UPSTREAM AGENT
NATIVE CALLS
310

Fig. 7

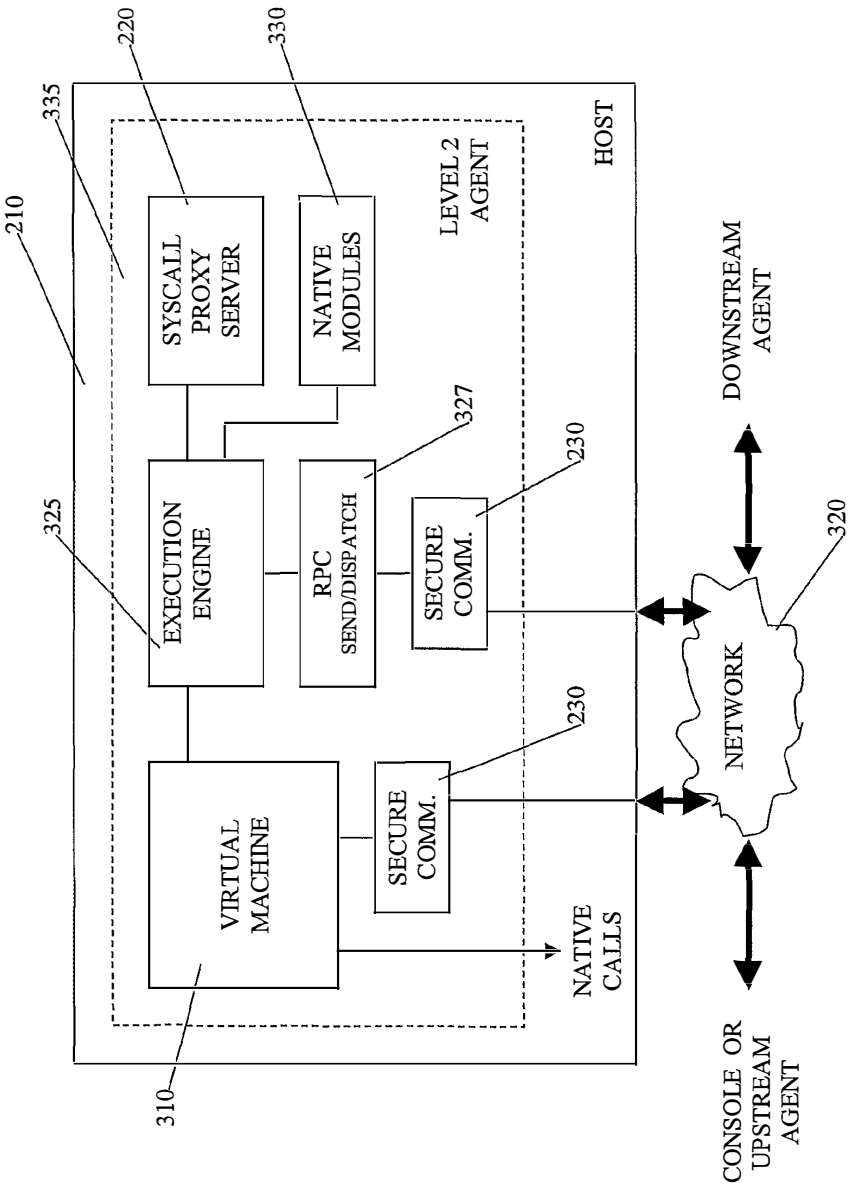

210
220
330
335
325
327
230
230
320
310
HOST
LEVEL 2 AGENT
SYSCALL PROXY SERVER
NATIVE MODULES
EXECUTION ENGINE
RPC SEND/DISPATCH
SECURE COMM.
SECURE COMM.
VIRTUAL MACHINE
NETWORK
NATIVE CALLS
DOWNSTREAM AGENT
CONSOLE OR UPSTREAM AGENT

Fig. 8

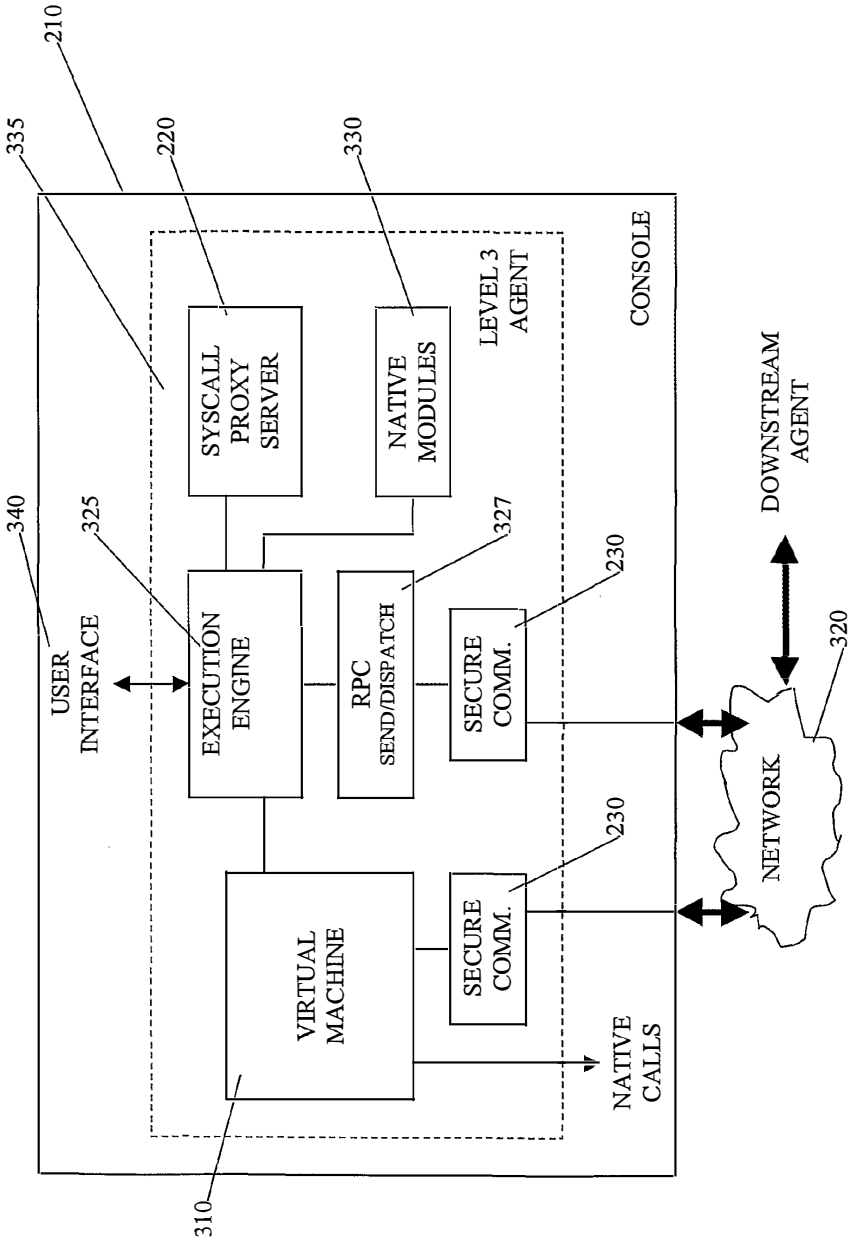

210
335
220
330
CONSOLE
LEVEL 3 AGENT
SYSCALL PROXY SERVER
NATIVE MODULES
DOWNSTREAM AGENT
340
325
327
230
USER INTERFACE
EXECUTION ENGINE
RPC SEND/DISPATCH
SECURE COMM.
320
NETWORK
230
VIRTUAL MACHINE
SECURE COMM.
NATIVE CALLS
310

Fig. 9

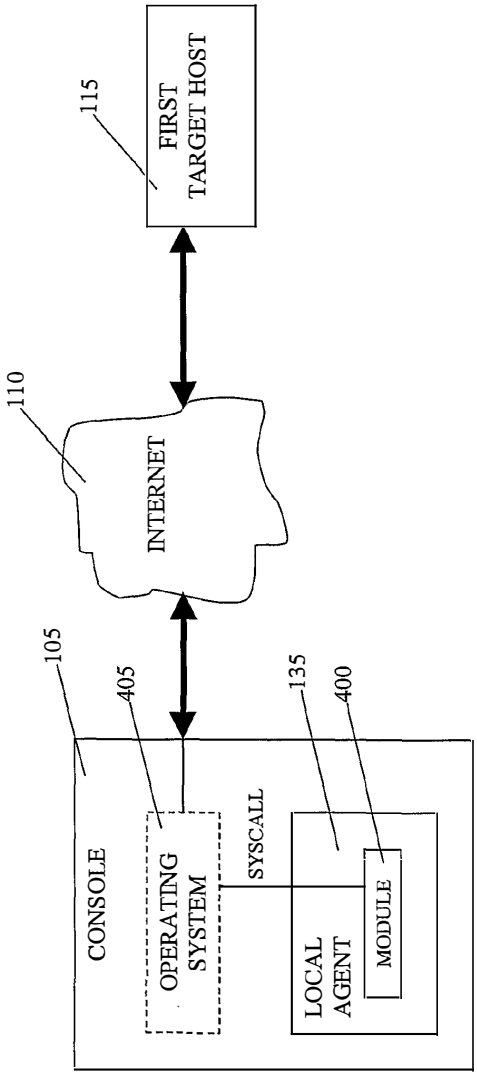

115
FIRST TARGET HOST
110
INTERNET
105
405
135
400
CONSOLE
OPERATING SYSTEM
SYSCALL
LOCAL AGENT
MODULE

Fig. 10

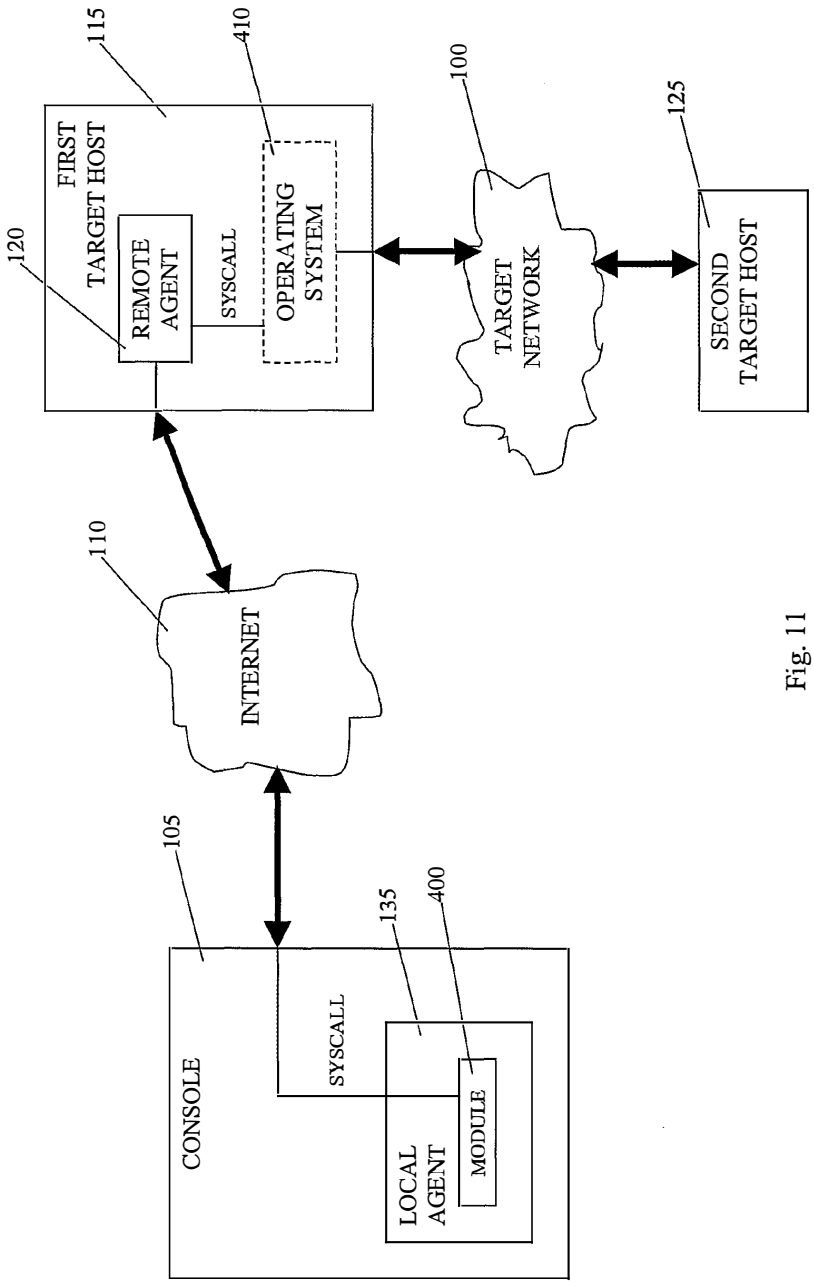

115
410
100
125
FIRST
TARGET HOST
OPERATING
SYSTEM
120
REMOTE
AGENT
SYSCALL
TARGET
NETWORK
SECOND
TARGET HOST
110
INTERNET
105
135
400
CONSOLE
SYSCALL
LOCAL
AGENT
MODULE

Fig. 11

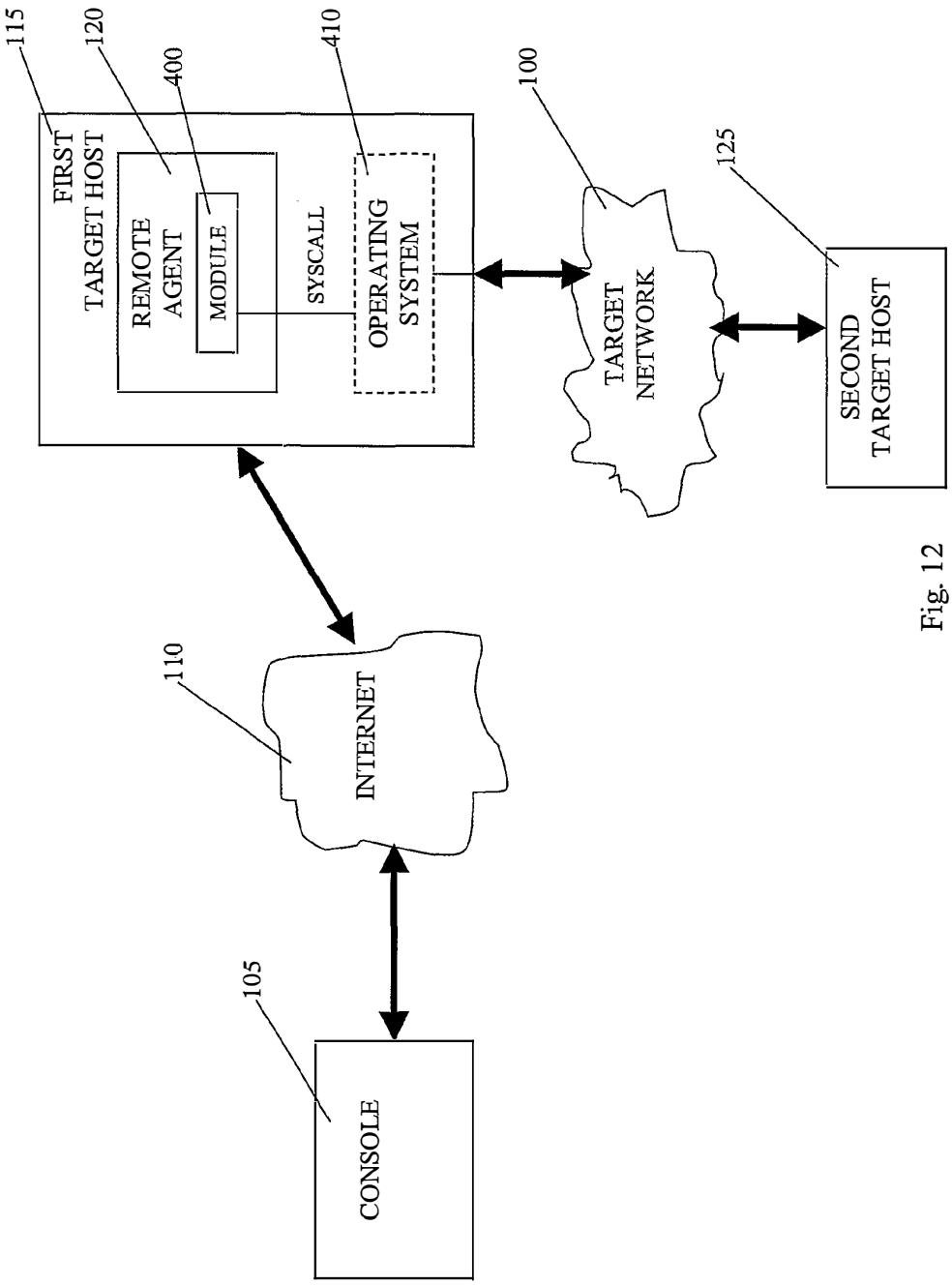

115
120
400
410
100
125
FIRST TARGET HOST
REMOTE AGENT
MODULE
SYSCALL
OPERATING SYSTEM
TARGET NETWORK
SECOND TARGET HOST
110
INTERNET
105
CONSOLE

Fig. 12

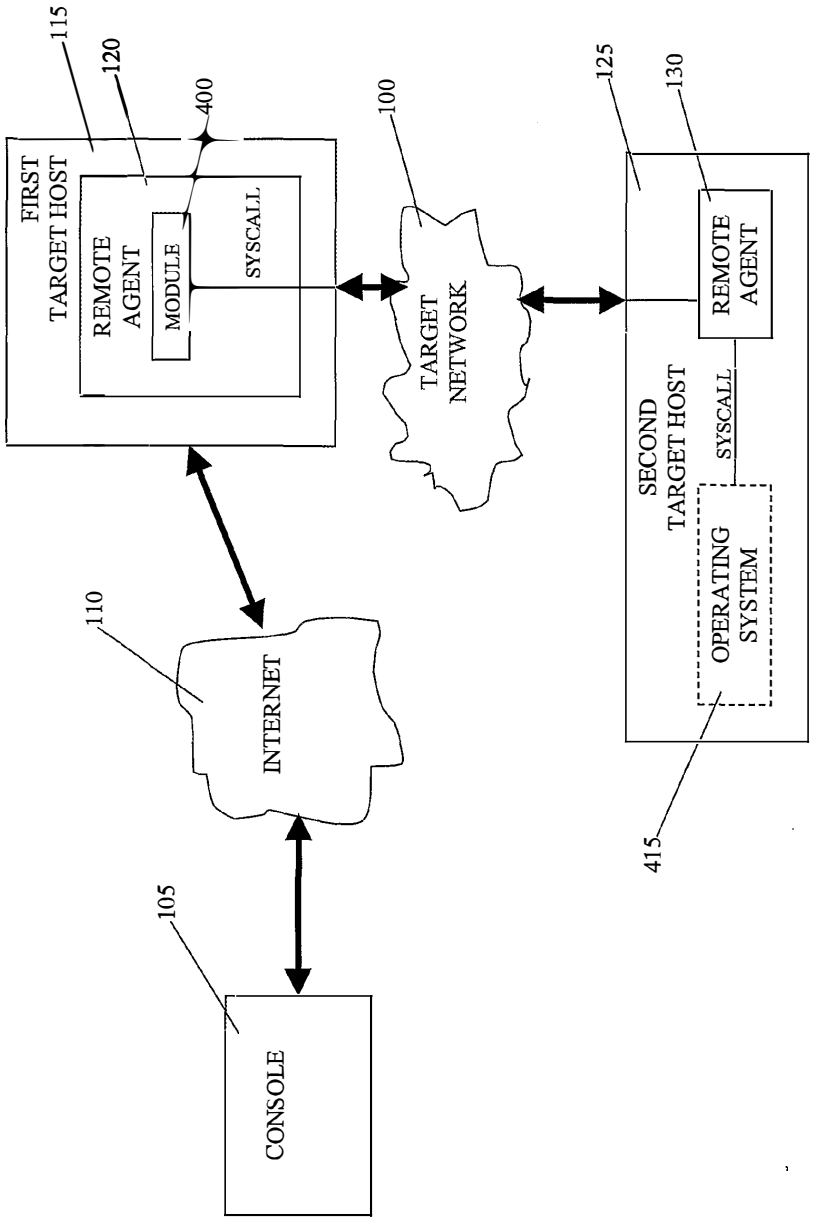

115
120
400
100
125
130
FIRST TARGET HOST
REMOTE AGENT
MODULE
SYSCALL
TARGET NETWORK
REMOTE AGENT
SECOND TARGET HOST
SYSCALL
OPERATING SYSTEM
415
110
INTERNET
105
CONSOLE

Fig. 13

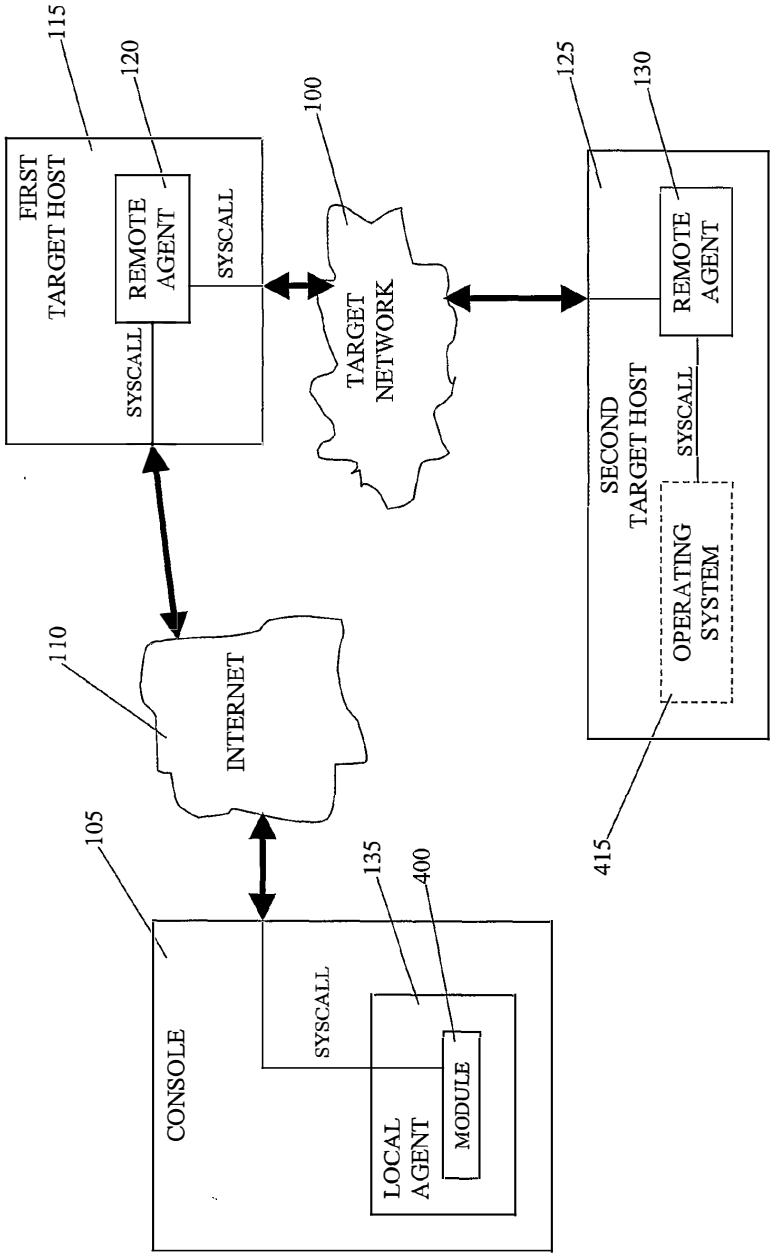

115
120
100
125
130
FIRST TARGET HOST
REMOTE AGENT
SYSCALL
SYSCALL
TARGET NETWORK
REMOTE AGENT
SECOND TARGET HOST
SYSCALL
OPERATING SYSTEM
110
INTERNET
105
135
400
CONSOLE
SYSCALL
LOCAL AGENT
MODULE
415

Fig. 14

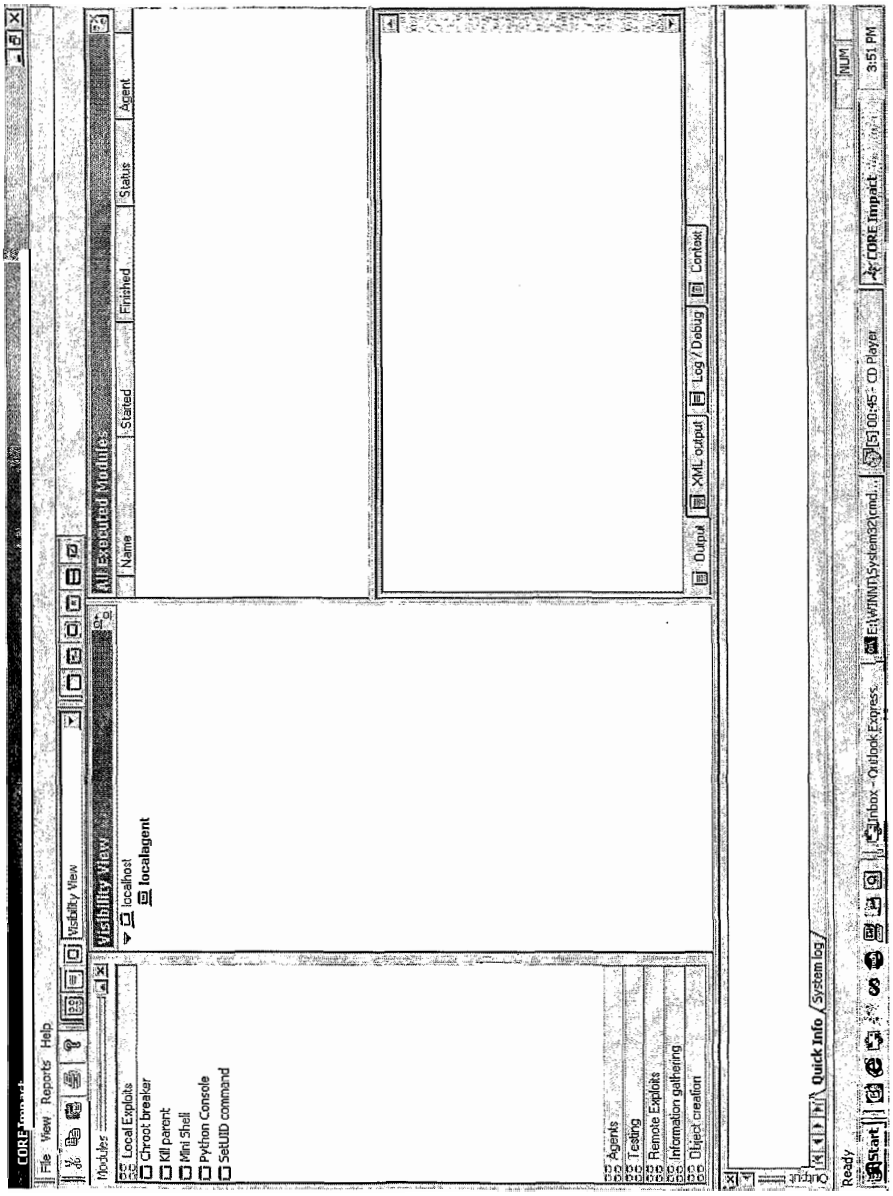


Fig. 15

ForcePoint LLC
EX-1010-PT2
Page057

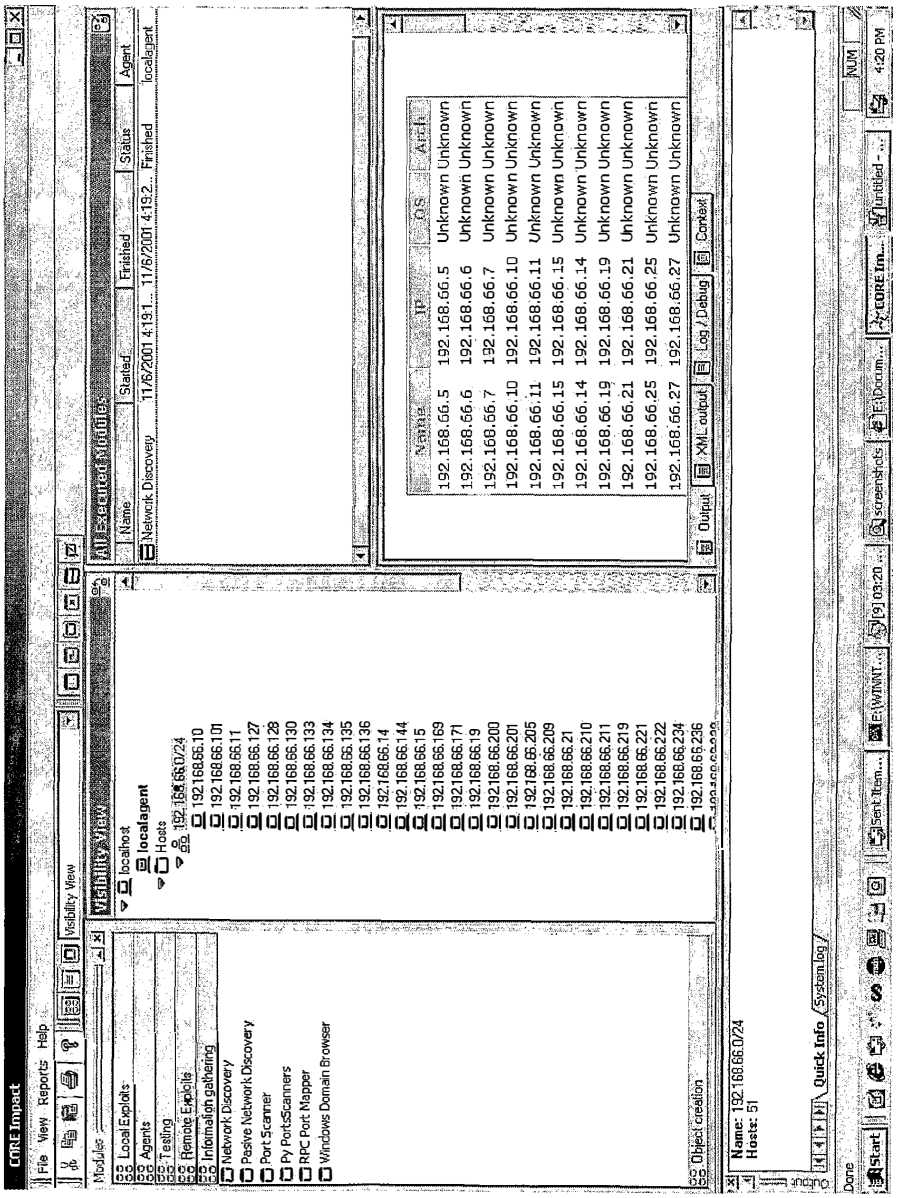

CORE Impact
File View Reports Help
Visibility View
Module
Local Exploits
Agents
Testing
Remote Exploits
Information gathering
Network Discovery
Passive Network Discovery
Port Scanner
Py PortScanners
RPC Port Mapper
Windows Domain Browser
Object creation
localhost
localagent
Hosts
192.168.66.0/24
192.168.66.10
192.168.66.101
192.168.66.11
192.168.66.127
192.168.66.128
192.168.66.130
192.168.66.133
192.168.66.134
192.168.66.135
192.168.66.136
192.168.66.14
192.168.66.144
192.168.66.15
192.168.66.169
192.168.66.171
192.168.66.19
192.168.66.200
192.168.66.201
192.168.66.205
192.168.66.209
192.168.66.21
192.168.66.210
192.168.66.211
192.168.66.219
192.168.66.221
192.168.66.222
192.168.66.234
192.168.66.236
All Executed Modules
Name
Started
Finished
Status
Agent
Network Discovery
11/6/2001 4:19:1...
11/6/2001 4:19:2...
Finished
localagent
Name
IP
OS
Arch
192.168.66.5 Unknown Unknown
192.168.66.6 Unknown Unknown
192.168.66.7 Unknown Unknown
192.168.66.10 Unknown Unknown
192.168.66.11 Unknown Unknown
192.168.66.15 Unknown Unknown
192.168.66.14 Unknown Unknown
192.168.66.19 Unknown Unknown
192.168.66.21 Unknown Unknown
192.168.66.25 Unknown Unknown
192.168.66.27 Unknown Unknown
Output
XML output
Log / Debug
Context
Name: 192.168.66.0/24
Hosts: 51
Quick Info
System.log
Done
Start
Sent Item...
E:\WINNT...
03:20 ...
screenshots
E:\Docum...
CORE Im...
Untitled - ...
NUM
4:20 PM

Fig. 16

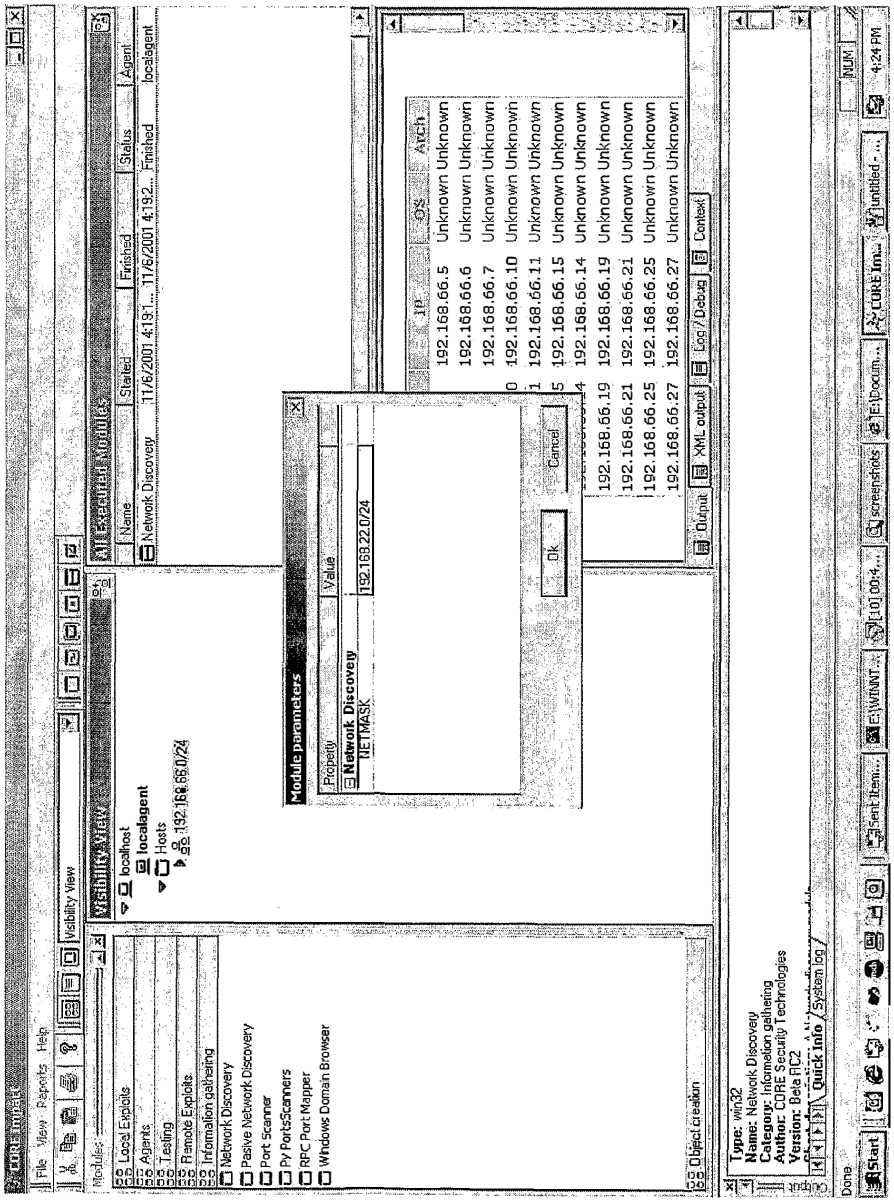


Fig. 17

ForcePoint LLC
EX-1010-PT2
Page059

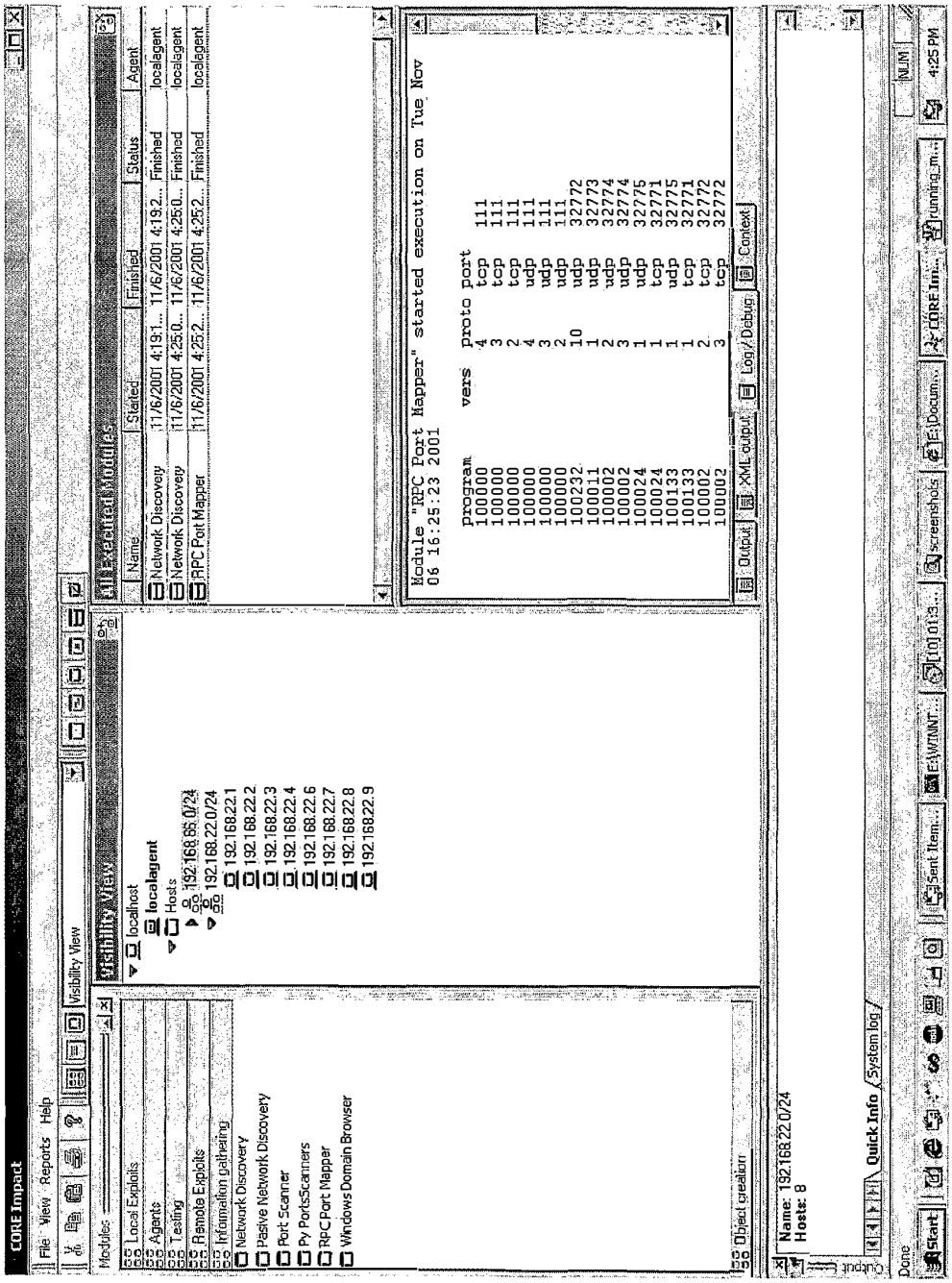

CORE Impact
File View Reports Help
Modules
Visibility View
Local Exploits
Agents
Testing
Remote Exploits
Information gathering
Network Discovery
Pasive Network Discovery
Port Scanner
Py PortsScanners
RPCPort Mapper
Windows Domain Browser
Object creation
localhost
localagent
Hosts
192.168.66.0/24
192.168.22.0/24
192.168.22.1
192.168.22.2
192.168.22.3
192.168.22.4
192.168.22.6
192.168.22.7
192.168.22.8
192.168.22.9
Execution Modules
Name
Started
Finished
Status
Agent
Network Discovery 11/6/2001 4:19:1... 11/6/2001 4:19:2... Finished localagent
Network Discovery 11/6/2001 4:25:0... 11/6/2001 4:25:0... Finished localagent
RPC Port Mapper 11/6/2001 4:25:2... 11/6/2001 4:25:2... Finished localagent
Module "RPC Port Mapper" started execution on Tue Nov 06 16:25:23 2001
program vers proto port
100000 4 tcp 111
100000 3 tcp 111
100000 2 tcp 111
100000 4 udp 111
100000 3 udp 111
100000 2 udp 111
100232 10 udp 32772
100011 1 udp 32773
100002 2 udp 32774
100002 3 udp 32774
100024 1 udp 32775
100024 1 tcp 32771
100133 1 udp 32775
100133 1 tcp 32771
100002 2 tcp 32772
100002 3 tcp 32772
Output
XML output
Log / Debug
Context
Name: 192.168.22.0/24
Hosts: 8
Quick Info
System log
Done
Start
Sent Item...
E:\WINNT...
[101013...
screenshots
E:\Docum...
CORE Im...
running_m...
NUM
4:25 PM

Fig. 18

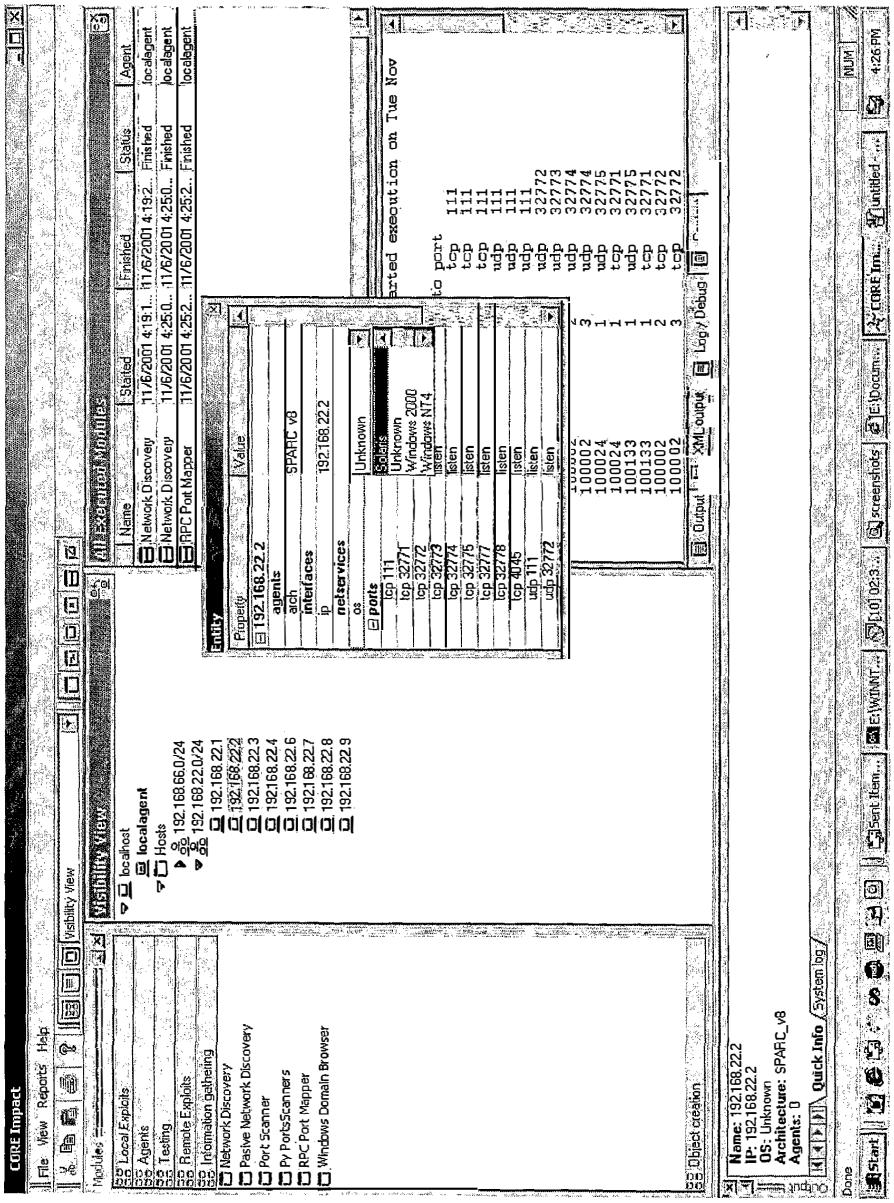

CORE Impact
File View Reports Help
Visibility View
Modules
Local Exploits
Agents
Testing
Remote Exploits
Information Gathering
Network Discovery
Passive Network Discovery
Port Scanner
Py PortsScanners
RPC Port Mapper
Windows Domain Browser
localhost
localagent
Hosts
192.168.66.0/24
192.168.22.0/24
192.168.22.1
192.168.22.2
192.168.22.3
192.168.22.4
192.168.22.6
192.168.22.7
192.168.22.8
192.168.22.9
Execution Modules
Name
Started
Finished
Status
Agent
Network Discovery 11/6/2001 4:19:1... 11/6/2001 4:19:2... Finished localagent
Network Discovery 11/6/2001 4:25:0... 11/6/2001 4:25:0... Finished localagent
RPC Port Mapper 11/6/2001 4:25:2... 11/6/2001 4:25:2... Finished localagent
Entity
Property
Value
192.168.22.2
agents
arch SPARC v8
interfaces
ip 192.168.22.2
netservices
os Unknown
ports
tcp 111 Solaris
tcp 32771 Unknown
tcp 32772 Windows 2000
tcp 32773 Windows NT4
tcp 32774 listen
tcp 32775 listen
tcp 32777 listen
tcp 32778 listen
tcp 4045 listen
udp 111 listen
udp 32772 listen
100004 2
100002 3
100024 1
100024 1
100133 1
100133 1
100002 2
100002 3
Output
XML output
Log / Debug
arted execution on Tue Nov
to port
tcp 111
tcp 111
tcp 111
udp 111
udp 111
udp 32772
udp 32773
udp 32774
udp 32774
udp 32775
tcp 32771
udp 32775
tcp 32771
tcp 32772
tcp 32772
Object creation
Name: 192.168.22.2
IP: 192.168.22.2
OS: Unknown
Architecture: SPARC_v8
Agents: 0
Quick Info
System log
Done
Start
Sent Item...
E:\WINNT...
[10] 02:3...
screenshots
E:\Docum...
CORE Im...
Untitled -...
NUM
4:26 PM

Fig. 19

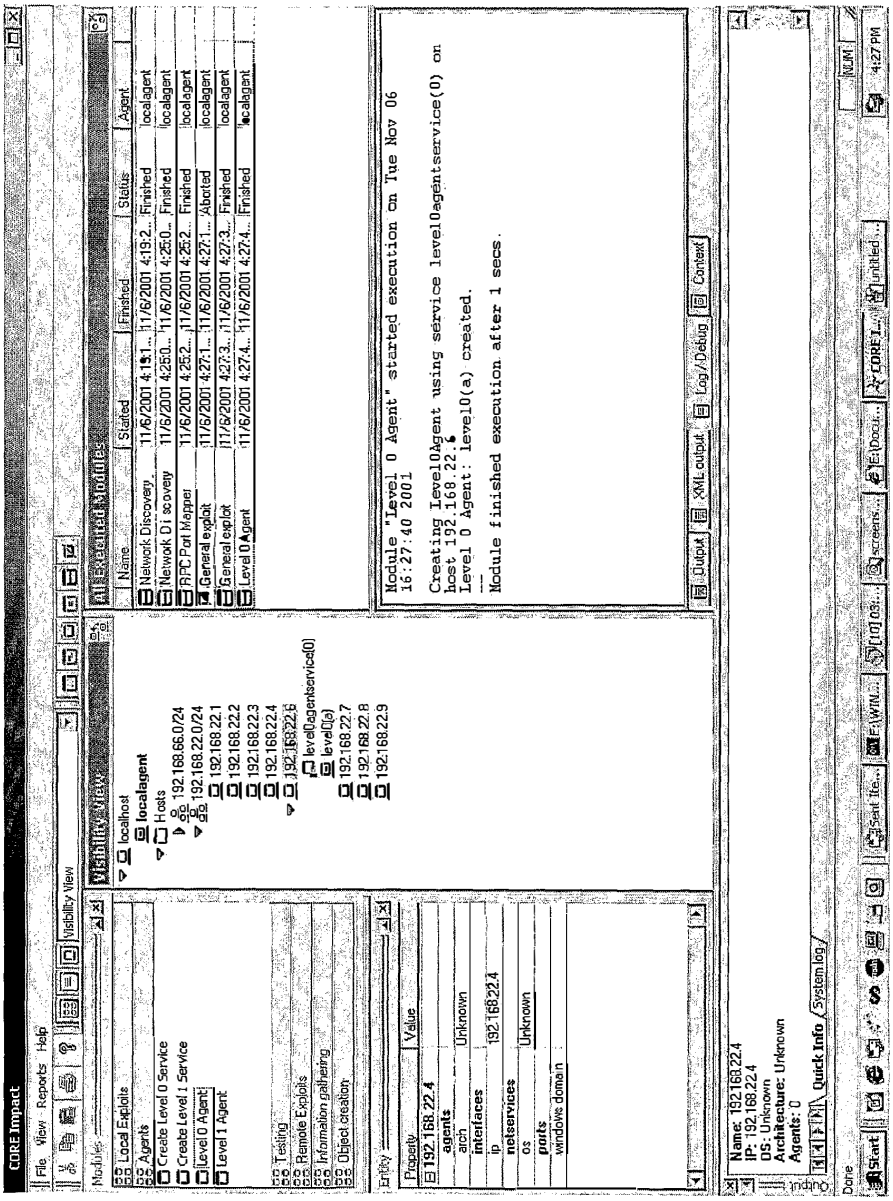

CORE Impact
File View Reports Help
Visibility View
Modules
Local Exploits
Agents
Create Level 0 Service
Create Level 1 Service
Level 0 Agent
Level 1 Agent
Testing
Remote Exploits
Information gathering
Object creation
Visibility View
localhost
localagent
Hosts
192.168.66.0/24
192.168.22.0/24
192.168.22.1
192.168.22.2
192.168.22.3
192.168.22.4
192.168.22.6
level0agentservice(0)
level0(a)
192.168.22.7
192.168.22.8
192.168.22.9
Executed Modules
Name
Started
Finished
Status
Agent
Network Discovery
Network Discovery
RPC Port Mapper
General exploit
General exploit
Level 0 Agent
11/6/2001 4:19:1...
11/6/2001 4:19:2...
Finished
localagent
11/6/2001 4:25:0...
11/6/2001 4:25:0...
Finished
localagent
11/6/2001 4:25:2...
11/6/2001 4:25:2...
Finished
localagent
11/6/2001 4:27:1...
11/6/2001 4:27:1...
Aborted
localagent
11/6/2001 4:27:3...
11/6/2001 4:27:3...
Finished
localagent
11/6/2001 4:27:4...
11/6/2001 4:27:4...
Finished
localagent
Module "Level 0 Agent" started execution on Tue Nov 06
16:27:40 2001
Creating Level0Agent using service level0agentservice(0) on
host 192.168.22.4
Level 0 Agent: level0(a) created.
Module finished execution after 1 secs.
Output
XML output
Log/Debug
Context
Property
Value
192.168.22.4
agents
arch
Unknown
interfaces
ip
192.168.22.4
netservices
Unknown
os
ports
windows domain
Name: 192.168.22.4
IP: 192.168.22.4
OS: Unknown
Architecture: Unknown
Agents: 0
Quick Info
System log
Done
Start
Sent Ite...
F:\WIN...
[no] os:...
screens...
E:\[docu...
CORE I...
Untitled ...
NUM
4:27 PM

Fig. 20

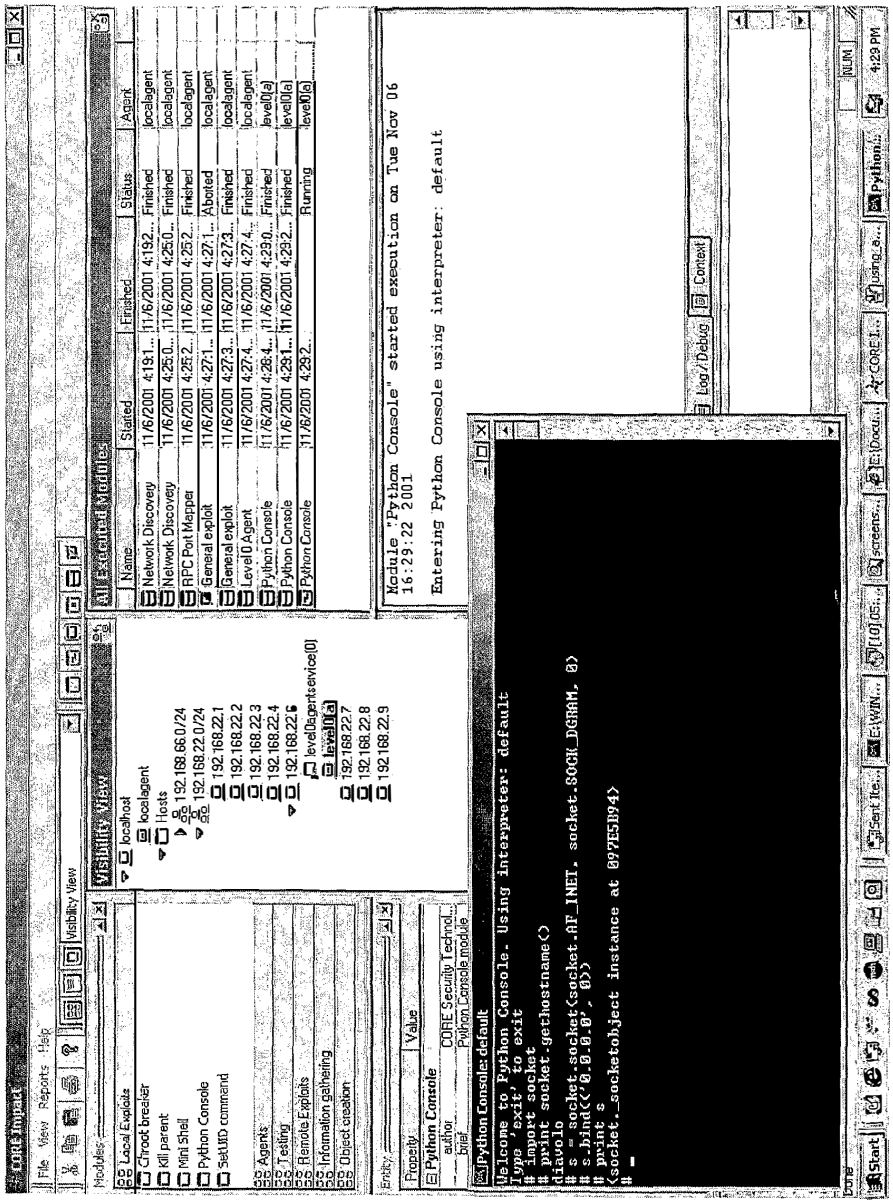


Fig. 21

ForcePoint LLC
EX-1010-PT2
Page063

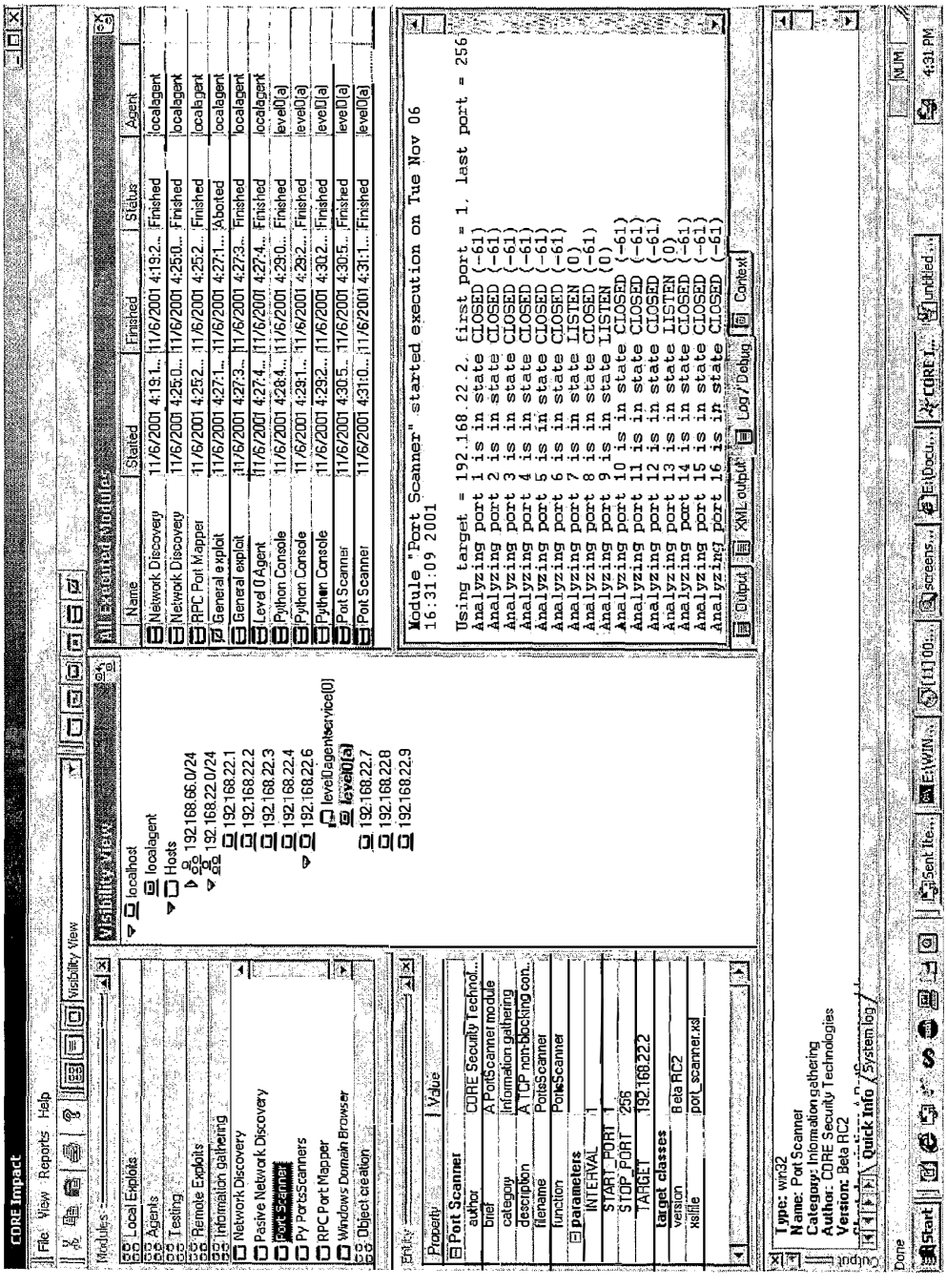


Fig. 22

ForcePoint LLC
EX-1010-PT2
Page064

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/22457

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/30
US CL : 707/104.1, 707/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 707/104.1, 707/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,070,244 A (ORCHIER ET AL) 30 May 2000 (30.05.2000), column 1, lines 50-67; column 2, lines 1-67	1-29
A,P	US 6,408,391 B1 (HUFF ET AL) 18 June 2002 (18.06.2002), column 2, lines 55-67; column 3, lines 1-67	1-29

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 September 2002 (12.09.2002)	30 OCT 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Apu Mofiz Telephone No. 7036054240

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/029940 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/26092

(22) International Filing Date: 15 August 2002 (15.08.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/969,686 2 October 2001 (02.10.2001) US

(71) Applicant *(for all designated States except US)*: **NETWORKS ASSOCIATES TECHNOLOGY, INC.** [US/US]; 3965 Freedom Circle, Santa Clara, CA 95054 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **SINGLETON, Richard, B.** [GB/GB]; 4 Coral Close, Eaton Bray, Bedfordshire LU6 2AS (GB).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 12400 Wilshire Boulevard, 7th floor, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/029940 A2

(54) Title: MASTER SECURITY POLICY SERVER

(57) Abstract: A master policy server manages security polices for client computers through a network of local policy servers. Each local policy server is responsible for the security policies on a group of clients and maintains a data store containing the security policies and security information pertaining to the clients. Periodically, the master policy server and the local policy server synchronize, at which time the master policy server replicates updated policies to the local policy servers and the policy servers upload client security statistics to the master policy server for consolidation into a global status.

ForcePoint LLC
EX-1010-PT2
Page066

MASTER SECURITY POLICY SERVER

FIELD OF THE INVENTION

This invention relates generally to computer security, and more particularly to managing security policies through a centralized server.

COPYRIGHT NOTICE/PERMISSION

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever. The following notice applies to the software and data as described below and in the drawings hereto: Copyright © 2001, Networks Associates Technology, Inc., All Rights Reserved.

BACKGROUND OF THE INVENTION

Organizations often manage their computer security policies from a central location, typically employing a single computer server to manage the security polices on networked user (client) computers. The clients poll the server several times a day to check for, and optionally download, updated security policies and to upload their status to the server. Assuming a client and the server exchange a large amount of data several times a day, the data traffic between the server and even a small number clients can cause significant degradation for overall network communications.

SUMMARY OF THE INVENTION

A master policy server manages security polices for client computers through a network of local policy servers. Each local policy server is responsible for the security policies on a group of clients and maintains a data store containing the security policies and security information pertaining to the clients. Periodically, the master policy server and the local policy server synchronize, at which time the master policy server replicates

updated policies to the local policy servers and the local policy servers upload client security statistics to the master policy server for consolidation into a global status. A local policy server may also request an updated security policy outside of the synchronization timeframe. Similarly, the master policy server may also request the client statistics from a local policy server outside of the synchronization timeframe.

Because the local policy servers consolidate the statistics from the clients prior to uploading it to the master policy server, the amount of data flowing through the network to the master policy server is greatly reduced. Similarly, because the master policy server replicates the security policies to a few local policy servers instead of to each client, the amount of data flowing through the network from the master policy server is also reduced.

The present invention describes systems, clients, servers, methods, and computer-readable media of varying scope. In addition to the aspects and advantages of the present invention described in this summary, further aspects and advantages of the invention will become apparent by reference to the drawings and by reading the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram illustrating a system-level overview of an embodiment of the invention;

Figure 2A is a flowchart of a method to be performed by a master server according to an embodiment of the invention;

Figure 2B is a flowchart of a method to be performed by a local server operating in conjunction with the master server of Figure 2A;

Figure 3A is a diagram of one embodiment of an operating environment suitable for practicing the present invention; and

Figure 3B is a diagram of one embodiment of a computer system suitable for use in the operating environment of Figure 3A.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of embodiments of the invention, reference is made to the accompanying drawings in which like references indicate similar elements, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical, functional, and other changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

A system level overview of the operation of an embodiment of the invention is described by reference to Figure 1, which illustrates a security policy distribution system 100. The system 100 utilizes a master policy server 101 to manage security policies on client (user) computers through a network 129 of local policy severs A 103, B 105 and C 107. For example, local policy server A103 manages client A-1 115 through client A-N 117, while local policy server B 105 manages client B-1 119 through B-N 121. Although the clients are represented as individual systems in Figure 1, it will be appreciated that they may be grouped together by hardware and software platform type, domain name, site location, or physical or logical region.

Each local policy server has a local data store 109, 111, 113 that contains the security policies and security information collected from the client computers it manages. Each type of hardware and software platform acting as a client computer may be associated with a exemplary security policy or may share exemplary security policies with other platforms. The security policy may contain configuration parameters for anti-virus programs, firewalls, and other security software that protect a client computer from compromise by a third-party.

Communication between the local policy servers 103, 105, 107 and the master policy server 101 through network 129 is intermittent. Each local policy server 103, 105, 107 is responsible for periodically querying the master policy server 101 to determine if the security policies applicable to its clients have changed. The local policy servers also periodically, or upon request, send client security statistics derived from the security

information on local data stores 109, 111, 113 to the master policy server 101, which acts as a consolidation point for status information regarding the overall security of the system 100. The statistics from the local policy servers are stored in a global data store 127. When a global status for the system 100 is requested, the master policy server 101 derives the status from the statistics in the global data store 127 and, optionally, from additional statistics obtained from the local policy servers. More detailed status information for particular clients or groups of clients is obtained from the appropriate local policy server.

In one embodiment, the master policy server 101 and the local policy servers 103, 105, 107 synchronize security policies and statistics at times when less data traffic is generally experienced on the network 129. When the local policy servers are physically located in different time zones, the synchronization may occur at several points during a twenty-four hour period. In an alternate embodiment, the local policy servers can schedule checks for updated policies in addition to the synchronization process. Furthermore, it will be appreciated that the synchronization at a local policy server may happen more than once a day. The network 129 connecting the master policy server and the local policy servers is secured using any of several well-known secure transmission protocols when the security policies are being uploaded to the master policy server 101 or replicated to the local policy servers 103, 105, 107. Otherwise, no particular network transmission protocols are required in the system 100.

When the system 100 is installed, the system administrator may create the initial security policies at one of the local policy servers 103, 105, 107 for transfer to the master policy server 101 and subsequent replication to the other local policy servers, or directly at the master policy server 101. Similarly, updates to the security policies may be performed at a local policy server or at the master policy server. In one embodiment, the master policy server 101 maintains global level security policy configurations and the local policy servers 103, 105, 107 derive their local level configuration and set-up policies for their clients from the global level configurations.

The number of local policy servers is dependent upon the number of clients at each site and the physical locations of the sites. Because the master policy server 101 only sends and receives data from the local policy servers 103, 105, 107 instead of each

ForcePoint LLC
EX-1010-PT2
Page070

of the clients, a single master policy server and common TCP/IP wide-area networks are generally able to handle the amount of data being transferred in the system 100. Alternate embodiments in which additional levels of servers are incorporated between the local policy servers 103,105, 107 and the master policy server 101 are also contemplated and are considered within the scope of the invention.

The operations of an embodiment of a security policy distribution system 100 have been described in terms of a single master policy server and three local policy servers as illustrated in Figure 1, but the invention is not so limited. Next, the particular methods of the invention that perform the operations for the system 100 are described in terms of computer software with reference to a series of flowcharts. The methods to be performed by a computer constitute computer programs made up of computer-executable instructions illustrated as blocks (acts). Describing the methods by reference to a flowchart enables one skilled in the art to develop such programs including such instructions to carry out the methods on suitably configured computers (the processing unit of the computer executing the instructions from computer-readable media). The computer-executable instructions may be written in a computer programming language or may be embodied in firmware logic. If written in a programming language conforming to a recognized standard, such instructions can be executed on a variety of hardware platforms and for interface to a variety of operating systems. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein. Furthermore, it is common in the art to speak of software, in one form or another (e.g., program, procedure, process, application, module, logic...), as taking an action or causing a result. Such expressions are merely a shorthand way of saying that execution of the software by a computer causes the processor of the computer to perform an action or a produce a result.

Referring first to Figure 2A, the acts to be performed by a computer executing a master server method 200 to perform the operations described for the master policy server 101 in Figure 1 is shown. The master server method 200 is invoked by one or more of a series of predetermined events. If a new policy has been created, either at the master policy server 101, or at one of the local policy servers, 103, 105, 107, (block 201),

the master server method 200 obtains and stores the security policy at block 203. If the master server method 200 receives a request for a new policy from a local policy server (block 205), the master server method 200 replicates the policy to the requestor at block 207. It will be appreciated that the master policy server will replicate those policies which are requested by the local policy server, i.e., those policies particular to the client platforms which the local policy server is managing. If the master server method 200 receives a request for system status (block 209), the master server method 200 determines if the request is for historical or current status (block 213). If the report is for current status, the master server method 200 obtains the current statistics from the local servers at block 215. The appropriate status is returned to the requester at the block 217. Otherwise, the event that invoked the master server method 200 is a scheduled synchronization event and the master server method 200 synchronizes security policies and statistics with the appropriate local policy servers at block 211.

A local server method 230 is illustrated in Figure 2B that performs the operations previously described for the local policy servers 103, 105, 107 in Figure 1. As with the master server method 200, the local server method 230 is invoked by one or more of a predetermined sequence of events. If a new policy has been configured on the local policy server (block 231), the local server method 230 sends the new policy to the master policy server at block 233 for replication to the other local policy servers. If the event is a scheduled check for the availability of new policies (block 235), the local server method 230 requests appropriate new policies from the master policy server at block 237 and receive and apply any new policies at block 239. If the local server method 230 receives a request for current status from the master server method 200 (block 241), it send its current statistics to the master policy server at block 243. Otherwise, the event is a scheduled synchronization event and the local server method 230 synchronizes with the master policy server at block 245, sending statistics from the local data store to the master policy server and receiving any updates to the security policies.

The methods performed by a master policy server and local policy server have been shown by reference to flowcharts in Figures 2A and 2B, respectively, including all the acts from 201 until 217 and from 231 until 245. It will be appreciated that more or fewer processes may be incorporated into the methods illustrated in Figures 2A-B

without departing from the scope of the invention, and that no particular order is implied by the arrangement of blocks shown and described herein.

The following description of Figures 3A-B is intended to provide an overview of computer hardware and other operating components suitable for performing the methods of the invention described above, but is not intended to limit the applicable environments. One of skill in the art will immediately appreciate that the invention can be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention can also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network.

Figure 3A shows several computer systems that are coupled together through a network 3, such as the Internet. The term "Internet" as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (web). The physical connections of the Internet and the protocols and communication procedures of the Internet are well known to those of skill in the art. Access to the Internet 3 is typically provided by Internet service providers (ISP), such as the ISPs 5 and 7. Users on client systems, such as client computer systems 21, 25, 35, and 37 obtain access to the Internet through the Internet service providers, such as ISPs 5 and 7. Access to the Internet allows users of the client computer systems to exchange information, receive and send e-mails, and view documents, such as documents which have been prepared in the HTML format. These documents are often provided by web servers, such as web server 9 which is considered to be "on" the Internet. Often these web servers are provided by the ISPs, such as ISP 5, although a computer system can be set up and connected to the Internet without that system being also an ISP as is well known in the art.

The web server 9 is typically at least one computer system which operates as a server computer system and is configured to operate with the protocols of the World Wide Web and is coupled to the Internet. Optionally, the web server 9 can be part of an ISP which provides access to the Internet for client systems. The web server 9 is shown

coupled to the server computer system 11 which itself is coupled to web content 10, which can be considered a form of a media database. It will be appreciated that while two computer systems 9 and 11 are shown in Figure 3A, the web server system 9 and the server computer system 11 can be one computer system having different software components providing the web server functionality and the server functionality provided by the server computer system 11 which will be described further below.

Client computer systems 21, 25, 35, and 37 can each, with the appropriate web browsing software, view HTML pages provided by the web server 9. The ISP 5 provides Internet connectivity to the client computer system 21 through the modem interface 23 which can be considered part of the client computer system 21. The client computer system can be a personal computer system, a network computer, a Web TV system, or other such computer system. Similarly, the ISP 7 provides Internet connectivity for client systems 25, 35, and 37, although as shown in Figure 3A, the connections are not the same for these three computer systems. Client computer system 25 is coupled through a modem interface 27 while client computer systems 35 and 37 are part of a LAN. While Figure 3A shows the interfaces 23 and 27 as generically as a "modem," it will be appreciated that each of these interfaces can be an analog modem, ISDN modem, cable modem, satellite transmission interface (e.g. "Direct PC"), or other interfaces for coupling a computer system to other computer systems. Client computer systems 35 and 37 are coupled to a LAN 33 through network interfaces 39 and 41, which can be Ethernet network or other network interfaces. The LAN 33 is also coupled to a gateway computer system 31 which can provide firewall and other Internet related services for the local area network. This gateway computer system 31 is coupled to the ISP 7 to provide Internet connectivity to the client computer systems 35 and 37. The gateway computer system 31 can be a conventional server computer system. Also, the web server system 9 can be a conventional server computer system.

Alternatively, as well-known, a server computer system 43 can be directly coupled to the LAN 33 through a network interface 45 to provide files 47 and other services to the clients 35, 37, without the need to connect to the Internet through the gateway system 31.

Figure 3B shows one example of a conventional computer system that can be used as a client computer system or a server computer system or as a web server system. It will also be appreciated that such a computer system can be used to perform many of the functions of an Internet service provider, such as ISP 5. The computer system 51 interfaces to external systems through the modem or network interface 53. It will be appreciated that the modem or network interface 53 can be considered to be part of the computer system 51. This interface 53 can be an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (e.g. "Direct PC"), or other interfaces for coupling a computer system to other computer systems. The computer system 51 includes a processing unit 55, which can be a conventional microprocessor such as an Intel Pentium microprocessor or Motorola Power PC microprocessor. Memory 59 is coupled to the processor 55 by a bus 57. Memory 59 can be dynamic random access memory (DRAM) and can also include static RAM (SRAM). The bus 57 couples the processor 55 to the memory 59 and also to non-volatile storage 65 and to display controller 61 and to the input/output (I/O) controller 67. The display controller 61 controls in the conventional manner a display on a display device 63 which can be a cathode ray tube (CRT) or liquid crystal display. The input/output devices 69 can include a keyboard, disk drives, printers, a scanner, and other input and output devices, including a mouse or other pointing device. The display controller 61 and the I/O controller 67 can be implemented with conventional well known technology. A digital image input device 71 can be a digital camera which is coupled to the I/O controller 67 in order to allow images from the digital camera to be input into the computer system 51. The non-volatile storage 65 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data is often written, by a direct memory access process, into memory 59 during execution of software in the computer system 51. One of skill in the art will immediately recognize that the term "computer-readable medium" includes any type of storage device that is accessible by the processor 55 and also encompasses a carrier wave that encodes a data signal.

It will be appreciated that the computer system 51 is one example of many possible computer systems which have different architectures. For example, personal computers based on an Intel microprocessor often have multiple buses, one of which can

be an input/output (I/O) bus for the peripherals and one that directly connects the processor 55 and the memory 59 (often referred to as a memory bus). The buses are connected together through bridge components that perform any necessary translation due to differing bus protocols.

Network computers are another type of computer system that can be used with the present invention. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network connection into the memory 59 for execution by the processor 55. A Web TV system, which is known in the art, is also considered to be a computer system according to the present invention, but it may lack some of the features shown in Figure 3B, such as certain input or output devices. A typical computer system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

It will also be appreciated that the computer system 51 is controlled by operating system software which includes a file management system, such as a disk operating system, which is part of the operating system software. One example of an operating system software with its associated file management system software is the family of operating systems known as Windows® from Microsoft Corporation of Redmond, Washington, and their associated file management systems. The file management system is typically stored in the non-volatile storage 65 and causes the processor 55 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the non-volatile storage 65.

A security policy distribution system that is managed by a master security policy server has been described. Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention.

The terminology used in this application with respect to network communications is meant to include all communication media and environments, including local and wide area networks, public and private communications environments, and wired and wireless

communications media. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.

ForcePoint LLC
EX-1010-PT2
Page077

CLAIMS

What is claimed is:

1. A computerized method of distributing security policies comprising:
maintaining a security policy at a master policy server; and
periodically synchronizing the master policy server and a local policy server to replicate the security policy at the local policy server.

2. The computerized method of claim 1, wherein the synchronizing further comprises obtaining security statistics from the local policy server by the master policy server.

3. The computerized method of claim 2 further comprising:
deriving a global status from the statistics.

4. The computerized method of claim 1, further comprising:
obtaining security statistics by the master policy server upon request to the local policy server.

5. The computerized method of claim 1 further comprising:
replicating the security policy to the local policy server upon request to the master policy server.

6. The computerized method of claim 1 further comprising:
creating the security policy at the local policy server; and
transferring the security policy to the master policy server.

7. The computerized method of claim 1 further comprising:
creating the security policy at the master policy server.

8. The computerized method of claim 1, wherein the synchronizing is performed securely across a communications medium coupling the master policy server and the local policy server.

9. The computerized method of claim 1, further comprising:

managing security for a plurality of client platforms by the local policy server, the security policy comprising security parameters particular to each client platform.

10. The computerized method of claim 9, further comprising:

deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy comprising the global security parameters.

11. A computer-readable medium having executable instructions to cause a computer to perform a method comprising:

maintaining a security policy at a master policy server; and

periodically synchronizing the master policy server and a local policy server to replicate the security policy at the local policy server.

12. The computer-readable medium of claim 11, wherein the synchronizing further comprises obtaining security statistics from the local policy server by the master policy server.

13. The computer-readable medium of claim 12, wherein the method further comprises:

deriving a global status from the statistics.

14. The computer-readable medium of claim 11, wherein the method further comprises:

obtaining security statistics by the master policy server upon request to the local policy server.

15. The computer-readable medium of claim 11, wherein the method further comprises:

replicating the security policy to the local policy server upon request to the master policy server.

16. The computer-readable medium of claim 11, wherein the method further comprises:

creating the security policy at the local policy server; and

transferring the security policy to the master policy server.

17. The computer-readable medium of claim 11, wherein the method further comprises:

creating the security policy at the master policy server.

18. The computer-readable medium of claim 11, wherein the synchronizing is performed securely across a communications medium coupling the master policy server and the local policy server.

19. The computer-readable medium of claim 11, wherein the method further comprises:

managing security for a plurality of client platforms by the local policy server, the security policy comprising security parameters particular to each client platform.

20. The computer-readable medium of claim 19, wherein the method further comprises:

deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy comprising the global security parameters.

21. A computer system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus; and

a master server process executed from the memory by the processor to cause the processor to maintain a security policy and to periodically synchronize with a local policy server through the network interface to replicate the security policy at the local policy server.

22. The computer system of claim 21, wherein the master server process further causes the processor to obtain security statistics from the local policy server through the network interface during synchronization.

23. The computer system of claim 22, wherein the master server process further causes the processor to derive a global status from the statistics.

24. The computer system of claim 21, wherein the master server process further causes the processor to request security statistics from the local policy server through the network interface.

25. The computer system of claim 21, wherein the master server process further causes the processor to receive a request from the local policy server and to replicate the security policy to the local policy server in response.

26. The computer system of claim 21, wherein the master server process further causes the processor to create the security policy.

27. The computer system of claim 21, wherein the master server process further causes the processor to couple the network interface to a secure communications medium for synchronization.

28. A computer system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus; and

a local server process executed from the memory by the processor to cause the processor to periodically synchronize with a master policy server through the network interface to receive a security policy from a master policy server.

29. The computer system of claim 28, wherein the local server process further causes the processor to transfer security statistics to the master policy server through the network interface during synchronization.

30. The computer system of claim 28, wherein the local server process further causes the processor to receive a request for security statistics from the master policy server and to transfer the security statistics to the master policy server through the network interface in response.

31. The computer system of claim 28, wherein the local server process further causes the processor to request a security policy from the master policy server through the network interface and to receive the security policy in response.

32. The computer system of claim 28, wherein the local server process further causes the processor to create the security policy and to transfer the security policy to the master policy server through the network interface.

33. The computer system of claim 28, wherein the local server process further causes the processor to manage security for a plurality of client platforms, the security policy comprising security parameters particular to each client platform.

34. The computer system of claim 33, wherein the local server process further causes the processor to derive the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy server comprising the global security parameters.

35. An apparatus comprising:

network means for interfacing to a network; and

master policy means for maintaining a security policy and for periodically synchronizing with a local policy means through the network interface to replicate the security policy at the local policy means.

36. The apparatus of claim 35, wherein the master policy means is further operable for obtaining security statistics from the local policy means through the network means during synchronization.

37. The apparatus of claim 36, wherein the master policy means is further operable for deriving a global status from the statistics.

38. The apparatus of claim 35, wherein the master policy means is further operable for requesting security statistics from the local policy means through the network means.

39. The apparatus of claim 35, wherein the master policy means is further operable for receiving a request from the local policy means through the network means and for replicating the security policy to the local policy means through the network means in response.

40. The apparatus of claim 35, wherein the master policy means is further operable for creating the security policy.

41. The apparatus of claim 35, wherein the network means is further operable for coupling to a secure communications medium for synchronization between the master policy means and the local policy means.

42. An apparatus comprising:

network means for interfacing to a network; and

local policy means for periodically synchronizing to a master policy means through the network means to receive a security policy form the master policy means.

43. The apparatus of claim 42, wherein the local policy means is further operable for transferring security statistics to the master policy means through the network means during synchronization.

44. The apparatus of claim 42, wherein the local policy means is further operable for receiving a request for security statistics from the master policy means through the network means and for transferring the security statistics to the master policy means through the network means in response.

45. The apparatus of claim 42, wherein the local policy means is further operable for requesting a security policy from the master policy means through the network means and for receiving the security policy from the master policy means through the network means in response.

46. The apparatus of claim 42, wherein the local policy means is further operable for creating the security policy and for transferring the security policy to the master policy means through the network means.

47. The computer system of claim 42, wherein the local security means is further operable for managing security for a plurality of client platforms, the security policy comprising security parameters particular to each client platform.

48. The computer system of claim 47, wherein the local security means is further operable for deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy means comprising the global security parameters.

ForcePoint LLC
EX-1010-PT2
Page084

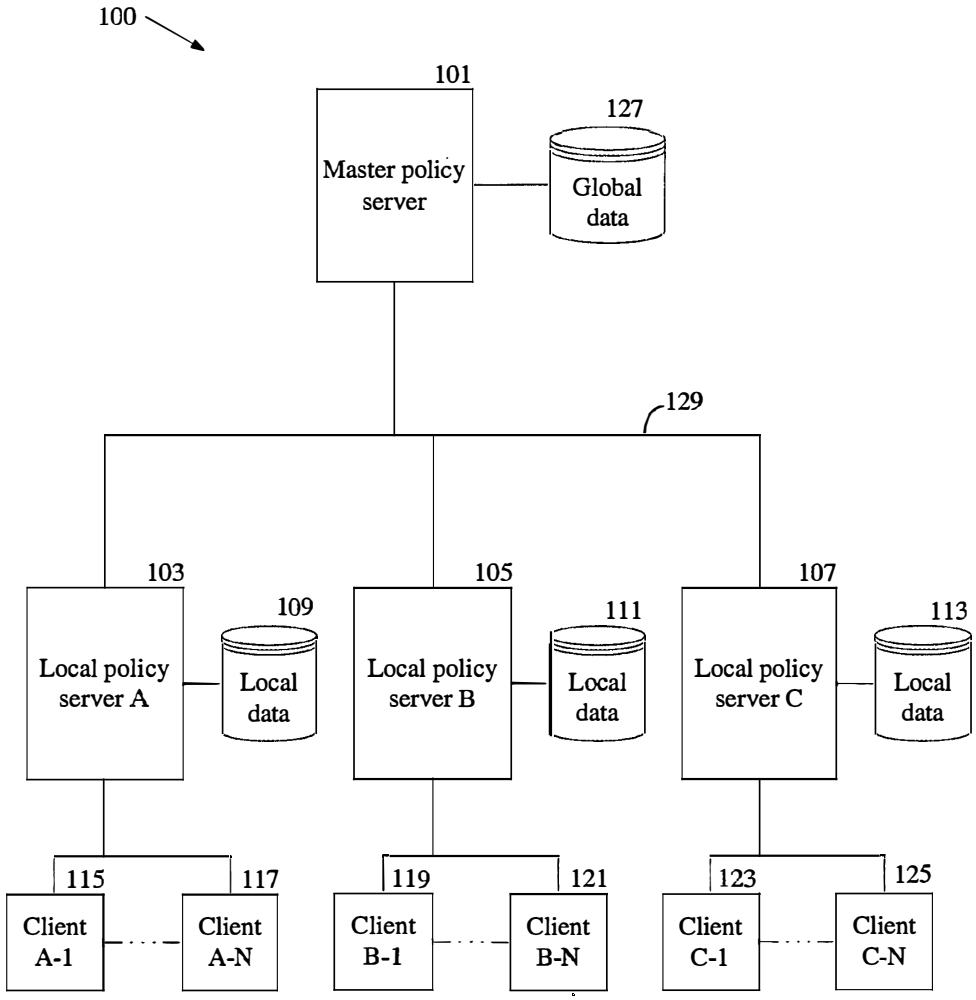

100
101
Master policy server
127
Global data
129
103
Local policy server A
109
Local data
105
Local policy server B
111
Local data
107
Local policy server C
113
Local data
115
117
Client A-1
Client A-N
119
121
Client B-1
Client B-N
123
125
Client C-1
Client C-N

Figure 1

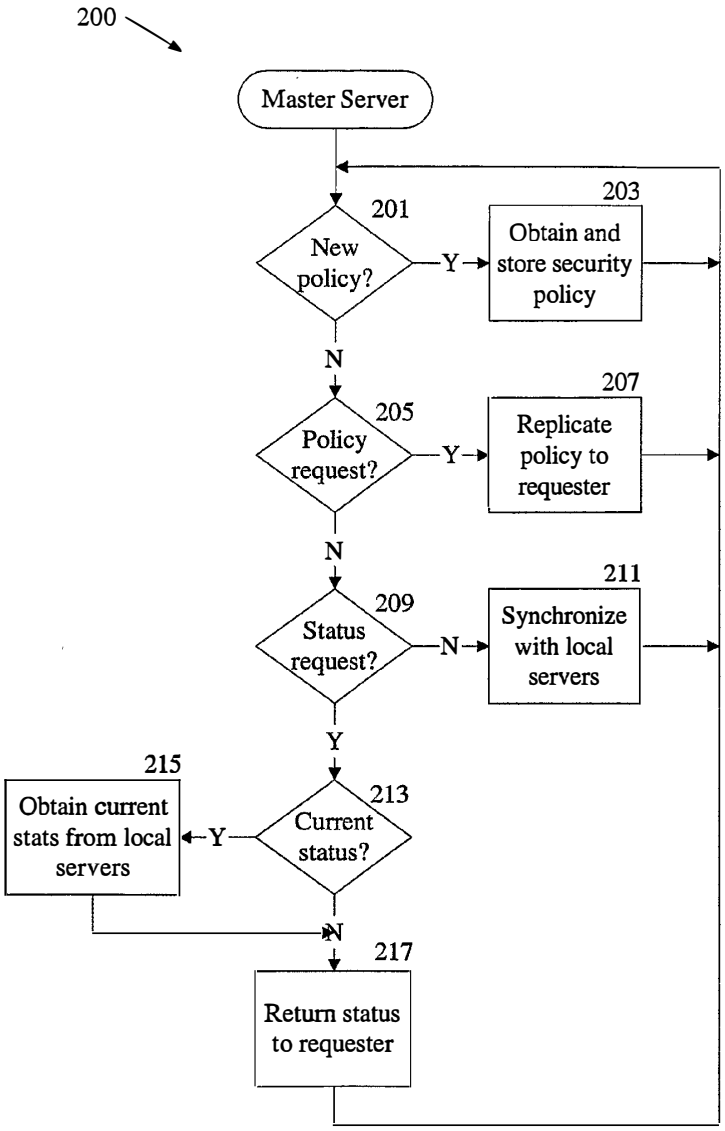

200
Master Server
201
New policy?
Y
203
Obtain and store security policy
N
205
Policy request?
Y
207
Replicate policy to requester
N
209
Status request?
N
211
Synchronize with local servers
Y
213
Current status?
Y
215
Obtain current stats from local servers
N
217
Return status to requester

Figure 2A

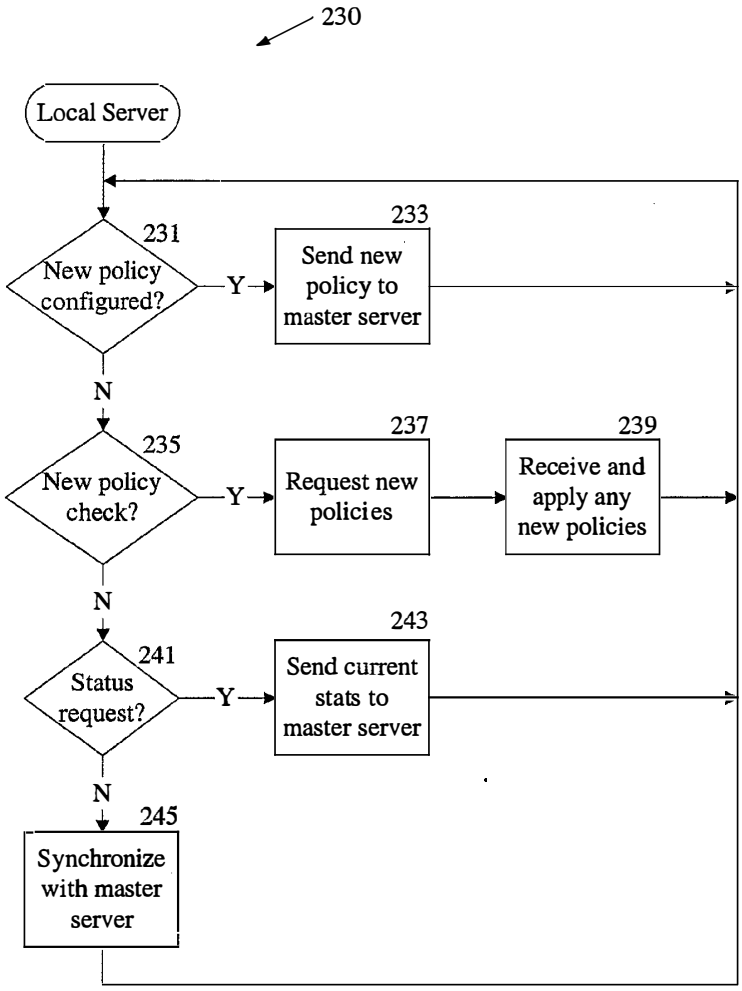

230
Local Server
231
New policy configured?
Y
233
Send new policy to master server
N
235
New policy check?
Y
237
Request new policies
239
Receive and apply any new policies
N
241
Status request?
Y
243
Send current stats to master server
N
245
Synchronize with master server

Figure 2B

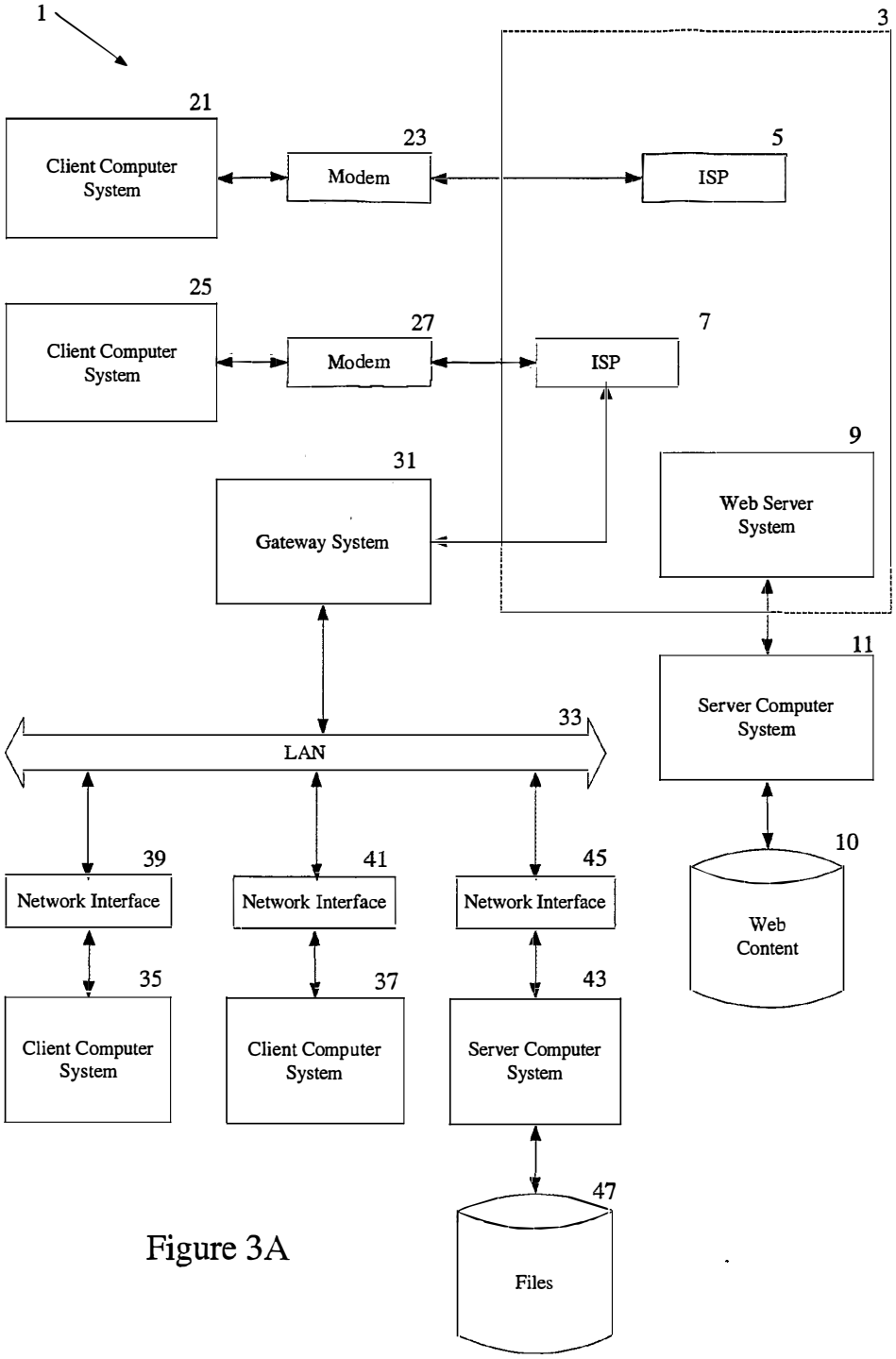

1
3
21
Client Computer System
23
Modem
5
ISP
25
Client Computer System
27
Modem
7
ISP
9
Web Server System
31
Gateway System
11
Server Computer System
33
LAN
39
Network Interface
41
Network Interface
45
Network Interface
10
Web Content
35
Client Computer System
37
Client Computer System
43
Server Computer System
47
Files

Figure 3A

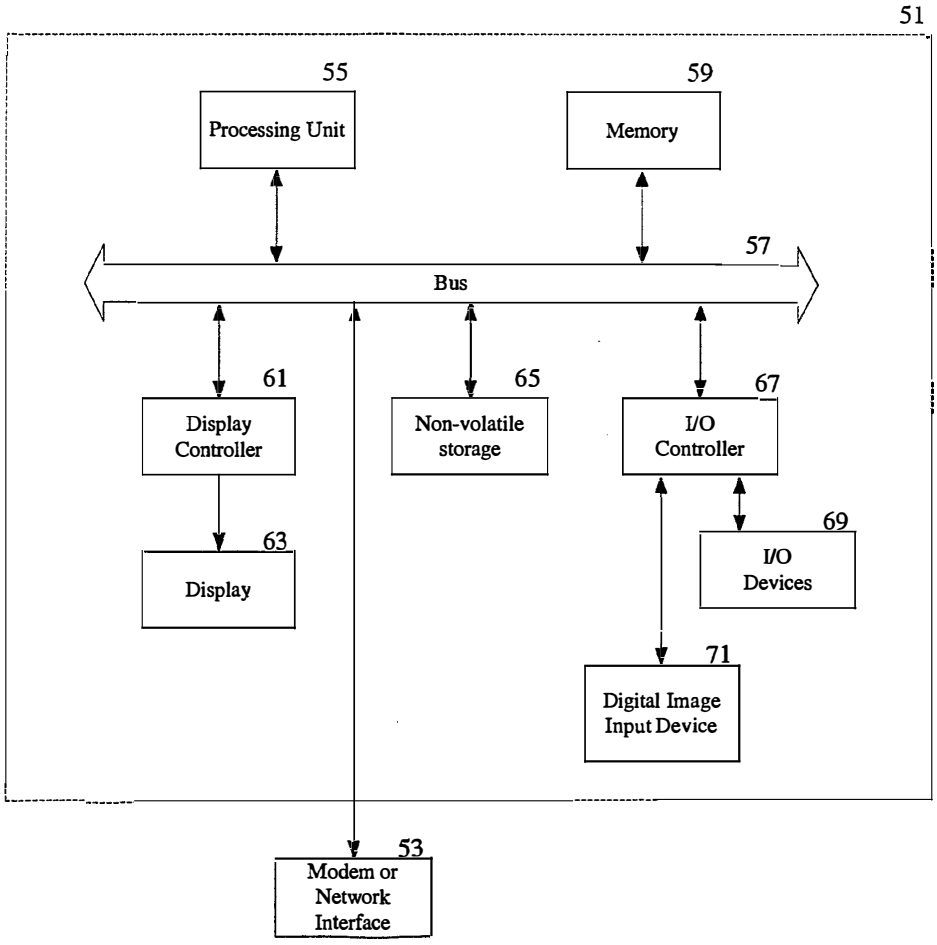

51
55
Processing Unit
59
Memory
57
Bus
61
Display Controller
65
Non-volatile storage
67
I/O Controller
63
Display
69
I/O Devices
71
Digital Image Input Device
53
Modem or Network Interface

Figure 3B

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/029941 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/US02/28513

(22) International Filing Date:
6 September 2002 (06.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/969,686 2 October 2001 (02.10.2001) US

(71) Applicant: **NETWORKS ASSOCIATES TECHNOLOGY, INC.** [US/US]; 3965 Freedom Circle, Santa Clara, CA 95054 (US).

(72) Inventor: **SINGLETON, Richard, B.**; 4 Coral Close, Eaton Bray, Bedfordshire LU6 2AS (GB).

(74) Agents: **MALLIE, Michael, J.** et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 03/029941 A2

(54) Title: MASTER SECURITY POLICY SERVER

(57) Abstract: A master policy server manages security polices for client computers through a network of local policy servers. Each local policy server is responsible for the security policies on a group of clients and maintains a data store containing the security policies and security information pertaining to the clients. Periodically, the master policy server and the local policy server synchronize, at which time the master policy server replicates updated policies to the local policy servers and the local policy servers upload client security statistics to the master policy server for consolidation into a global status.

ForcePoint LLC
EX-1010-PT2
Page090

MASTER SECURITY POLICY SERVER

FIELD OF THE INVENTION

This invention relates generally to computer security, and more particularly to managing security policies through a centralized server.

COPYRIGHT NOTICE/PERMISSION

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever. The following notice applies to the software and data as described below and in the drawings hereto: Copyright © 2001, Networks Associates Technology, Inc., All Rights Reserved.

BACKGROUND OF THE INVENTION

Organizations often manage their computer security policies from a central location, typically employing a single computer server to manage the security polices on networked user (client) computers. The clients poll the server several times a day to check for, and optionally download, updated security policies and to upload their status to the server. Assuming a client and the server exchange a large amount of data several times a day, the data traffic between the server and even a small number clients can cause significant degradation for overall network communications.

SUMMARY OF THE INVENTION

A master policy server manages security polices for client computers through a network of local policy servers. Each local policy server is responsible for the security policies on a group of clients and maintains a data store containing the security policies and security information pertaining to the clients. Periodically, the master policy server and the local policy server synchronize, at which time the master policy server replicates

updated policies to the local policy servers and the local policy servers upload client security statistics to the master policy server for consolidation into a global status. A local policy server may also request an updated security policy outside of the synchronization timeframe. Similarly, the master policy server may also request the client statistics from a local policy server outside of the synchronization timeframe.

Because the local policy servers consolidate the statistics from the clients prior to uploading it to the master policy server, the amount of data flowing through the network to the master policy server is greatly reduced. Similarly, because the master policy server replicates the security policies to a few local policy servers instead of to each client, the amount of data flowing through the network from the master policy server is also reduced.

The present invention describes systems, clients, servers, methods, and computer-readable media of varying scope. In addition to the aspects and advantages of the present invention described in this summary, further aspects and advantages of the invention will become apparent by reference to the drawings and by reading the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a diagram illustrating a system-level overview of an embodiment of the invention;

Figure 2A is a flowchart of a method to be performed by a master server according to an embodiment of the invention;

Figure 2B is a flowchart of a method to be performed by a local server operating in conjunction with the master server of Figure 2A;

Figure 3A is a diagram of one embodiment of an operating environment suitable for practicing the present invention; and

Figure 3B is a diagram of one embodiment of a computer system suitable for use in the operating environment of Figure 3A.

ForcePoint LLC
EX-1010-PT2
Page092

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of embodiments of the invention, reference is made to the accompanying drawings in which like references indicate similar elements, and in which is shown by way of illustration specific embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical, functional, and other changes may be made without departing from the scope of the present invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

A system level overview of the operation of an embodiment of the invention is described by reference to Figure 1, which illustrates a security policy distribution system 100. The system 100 utilizes a master policy server 101 to manage security policies on client (user) computers through a network 129 of local policy severs A 103, B 105 and C 107. For example, local policy server A103 manages client A-1 115 through client A-N 117, while local policy server B 105 manages client B-1 119 through B-N 121. Although the clients are represented as individual systems in Figure 1, it will be appreciated that they may be grouped together by hardware and software platform type, domain name, site location, or physical or logical region.

Each local policy server has a local data store 109, 111, 113 that contains the security policies and security information collected from the client computers it manages. Each type of hardware and software platform acting as a client computer may be associated with a exemplary security policy or may share exemplary security policies with other platforms. The security policy may contain configuration parameters for anti-virus programs, firewalls, and other security software that protect a client computer from compromise by a third-party.

Communication between the local policy servers 103, 105, 107 and the master policy server 101 through network 129 is intermittent. Each local policy server 103, 105, 107 is responsible for periodically querying the master policy server 101 to determine if the security policies applicable to its clients have changed. The local policy servers also periodically, or upon request, send client security statistics derived from the security

ForcePoint LLC
EX-1010-PT2
Page093

information on local data stores 109, 111, 113 to the master policy server 101, which acts as a consolidation point for status information regarding the overall security of the system 100. The statistics from the local policy servers are stored in a global data store 127. When a global status for the system 100 is requested, the master policy server 101 derives the status from the statistics in the global data store 127 and, optionally, from additional statistics obtained from the local policy servers. More detailed status information for particular clients or groups of clients is obtained from the appropriate local policy server.

In one embodiment, the master policy server 101 and the local policy servers 103, 105, 107 synchronize security policies and statistics at times when less data traffic is generally experienced on the network 129. When the local policy servers are physically located in different time zones, the synchronization may occur at several points during a twenty-four hour period. In an alternate embodiment, the local policy servers can schedule checks for updated policies in addition to the synchronization process. Furthermore, it will be appreciated that the synchronization at a local policy server may happen more than once a day. The network 129 connecting the master policy server and the local policy servers is secured using any of several well-known secure transmission protocols when the security policies are being uploaded to the master policy server 101 or replicated to the local policy servers 103, 105, 107. Otherwise, no particular network transmission protocols are required in the system 100.

When the system 100 is installed, the system administrator may create the initial security policies at one of the local policy servers 103, 105, 107 for transfer to the master policy server 101 and subsequent replication to the other local policy servers, or directly at the master policy server 101. Similarly, updates to the security policies may be performed at a local policy server or at the master policy server. In one embodiment, the master policy server 101 maintains global level security policy configurations and the local policy servers 103, 105, 107 derive their local level configuration and set-up policies for their clients from the global level configurations.

The number of local policy servers is dependent upon the number of clients at each site and the physical locations of the sites. Because the master policy server 101 only sends and receives data from the local policy servers 103, 105, 107 instead of each

ForcePoint LLC
EX-1010-PT2
Page094

of the clients, a single master policy server and common TCP/IP wide-area networks are generally able to handle the amount of data being transferred in the system 100. Alternate embodiments in which additional levels of servers are incorporated between the local policy servers 103,105, 107 and the master policy server 101 are also contemplated and are considered within the scope of the invention.

The operations of an embodiment of a security policy distribution system 100 have been described in terms of a single master policy server and three local policy servers as illustrated in Figure 1, but the invention is not so limited. Next, the particular methods of the invention that perform the operations for the system 100 are described in terms of computer software with reference to a series of flowcharts. The methods to be performed by a computer constitute computer programs made up of computer-executable instructions illustrated as blocks (acts). Describing the methods by reference to a flowchart enables one skilled in the art to develop such programs including such instructions to carry out the methods on suitably configured computers (the processing unit of the computer executing the instructions from computer-readable media). The computer-executable instructions may be written in a computer programming language or may be embodied in firmware logic. If written in a programming language conforming to a recognized standard, such instructions can be executed on a variety of hardware platforms and for interface to a variety of operating systems. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein. Furthermore, it is common in the art to speak of software, in one form or another (e.g., program, procedure, process, application, module, logic...), as taking an action or causing a result. Such expressions are merely a shorthand way of saying that execution of the software by a computer causes the processor of the computer to perform an action or a produce a result.

Referring first to Figure 2A, the acts to be performed by a computer executing a master server method 200 to perform the operations described for the master policy server 101 in Figure 1 is shown. The master server method 200 is invoked by one or more of a series of predetermined events. If a new policy has been created, either at the master policy server 101, or at one of the local policy servers, 103, 105, 107, (block 201),

ForcePoint LLC
EX-1010-PT2
Page095

the master server method 200 obtains and stores the security policy at block 203. If the master server method 200 receives a request for a new policy from a local policy server (block 205), the master server method 200 replicates the policy to the requestor at block 207. It will be appreciated that the master policy server will replicate those policies which are requested by the local policy server, i.e., those policies particular to the client platforms which the local policy server is managing. If the master server method 200 receives a request for system status (block 209), the master server method 200 determines if the request is for historical or current status (block 213). If the report is for current status, the master server method 200 obtains the current statistics from the local servers at block 215. The appropriate status is returned to the requester at the block 217. Otherwise, the event that invoked the master server method 200 is a scheduled synchronization event and the master server method 200 synchronizes security policies and statistics with the appropriate local policy servers at block 211.

A local server method 230 is illustrated in Figure 2B that performs the operations previously described for the local policy servers 103, 105, 107 in Figure 1. As with the master server method 200, the local server method 230 is invoked by one or more of a predetermined sequence of events. If a new policy has been configured on the local policy server (block 231), the local server method 230 sends the new policy to the master policy server at block 233 for replication to the other local policy servers. If the event is a scheduled check for the availability of new policies (block 235), the local server method 230 requests appropriate new policies from the master policy server at block 237 and receive and apply any new policies at block 239. If the local server method 230 receives a request for current status from the master server method 200 (block 241), it send its current statistics to the master policy server at block 243. Otherwise, the event is a scheduled synchronization event and the local server method 230 synchronizes with the master policy server at block 245, sending statistics from the local data store to the master policy server and receiving any updates to the security policies.

The methods performed by a master policy server and local policy server have been shown by reference to flowcharts in Figures 2A and 2B, respectively, including all the acts from 201 until 217 and from 231 until 245. It will be appreciated that more or fewer processes may be incorporated into the methods illustrated in Figures 2A-B

ForcePoint LLC
EX-1010-PT2
Page096

without departing from the scope of the invention, and that no particular order is implied by the arrangement of blocks shown and described herein.

The following description of Figures 3A-B is intended to provide an overview of computer hardware and other operating components suitable for performing the methods of the invention described above, but is not intended to limit the applicable environments. One of skill in the art will immediately appreciate that the invention can be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention can also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network.

Figure 3A shows several computer systems that are coupled together through a network 3, such as the Internet. The term "Internet" as used herein refers to a network of networks which uses certain protocols, such as the TCP/IP protocol, and possibly other protocols such as the hypertext transfer protocol (HTTP) for hypertext markup language (HTML) documents that make up the World Wide Web (web). The physical connections of the Internet and the protocols and communication procedures of the Internet are well known to those of skill in the art. Access to the Internet 3 is typically provided by Internet service providers (ISP), such as the ISPs 5 and 7. Users on client systems, such as client computer systems 21, 25, 35, and 37 obtain access to the Internet through the Internet service providers, such as ISPs 5 and 7. Access to the Internet allows users of the client computer systems to exchange information, receive and send e-mails, and view documents, such as documents which have been prepared in the HTML format. These documents are often provided by web servers, such as web server 9 which is considered to be "on" the Internet. Often these web servers are provided by the ISPs, such as ISP 5, although a computer system can be set up and connected to the Internet without that system being also an ISP as is well known in the art.

The web server 9 is typically at least one computer system which operates as a server computer system and is configured to operate with the protocols of the World Wide Web and is coupled to the Internet. Optionally, the web server 9 can be part of an ISP which provides access to the Internet for client systems. The web server 9 is shown

ForcePoint LLC
EX-1010-PT2
Page097

coupled to the server computer system 11 which itself is coupled to web content 10, which can be considered a form of a media database. It will be appreciated that while two computer systems 9 and 11 are shown in Figure 3A, the web server system 9 and the server computer system 11 can be one computer system having different software components providing the web server functionality and the server functionality provided by the server computer system 11 which will be described further below.

Client computer systems 21, 25, 35, and 37 can each, with the appropriate web browsing software, view HTML pages provided by the web server 9. The ISP 5 provides Internet connectivity to the client computer system 21 through the modem interface 23 which can be considered part of the client computer system 21. The client computer system can be a personal computer system, a network computer, a Web TV system, or other such computer system. Similarly, the ISP 7 provides Internet connectivity for client systems 25, 35, and 37, although as shown in Figure 3A, the connections are not the same for these three computer systems. Client computer system 25 is coupled through a modem interface 27 while client computer systems 35 and 37 are part of a LAN. While Figure 3A shows the interfaces 23 and 27 as generically as a "modem," it will be appreciated that each of these interfaces can be an analog modem, ISDN modem, cable modem, satellite transmission interface (e.g. "Direct PC"), or other interfaces for coupling a computer system to other computer systems. Client computer systems 35 and 37 are coupled to a LAN 33 through network interfaces 39 and 41, which can be Ethernet network or other network interfaces. The LAN 33 is also coupled to a gateway computer system 31 which can provide firewall and other Internet related services for the local area network. This gateway computer system 31 is coupled to the ISP 7 to provide Internet connectivity to the client computer systems 35 and 37. The gateway computer system 31 can be a conventional server computer system. Also, the web server system 9 can be a conventional server computer system.

Alternatively, as well-known, a server computer system 43 can be directly coupled to the LAN 33 through a network interface 45 to provide files 47 and other services to the clients 35, 37, without the need to connect to the Internet through the gateway system 31.

ForcePoint LLC
EX-1010-PT2
Page098

Figure 3B shows one example of a conventional computer system that can be used as a client computer system or a server computer system or as a web server system. It will also be appreciated that such a computer system can be used to perform many of the functions of an Internet service provider, such as ISP 5. The computer system 51 interfaces to external systems through the modem or network interface 53. It will be appreciated that the modem or network interface 53 can be considered to be part of the computer system 51. This interface 53 can be an analog modem, ISDN modem, cable modem, token ring interface, satellite transmission interface (e.g. "Direct PC"), or other interfaces for coupling a computer system to other computer systems. The computer system 51 includes a processing unit 55, which can be a conventional microprocessor such as an Intel Pentium microprocessor or Motorola Power PC microprocessor. Memory 59 is coupled to the processor 55 by a bus 57. Memory 59 can be dynamic random access memory (DRAM) and can also include static RAM (SRAM). The bus 57 couples the processor 55 to the memory 59 and also to non-volatile storage 65 and to display controller 61 and to the input/output (I/O) controller 67. The display controller 61 controls in the conventional manner a display on a display device 63 which can be a cathode ray tube (CRT) or liquid crystal display. The input/output devices 69 can include a keyboard, disk drives, printers, a scanner, and other input and output devices, including a mouse or other pointing device. The display controller 61 and the I/O controller 67 can be implemented with conventional well known technology. A digital image input device 71 can be a digital camera which is coupled to the I/O controller 67 in order to allow images from the digital camera to be input into the computer system 51. The non-volatile storage 65 is often a magnetic hard disk, an optical disk, or another form of storage for large amounts of data. Some of this data is often written, by a direct memory access process, into memory 59 during execution of software in the computer system 51. One of skill in the art will immediately recognize that the term "computer-readable medium" includes any type of storage device that is accessible by the processor 55 and also encompasses a carrier wave that encodes a data signal.

It will be appreciated that the computer system 51 is one example of many possible computer systems which have different architectures. For example, personal computers based on an Intel microprocessor often have multiple buses, one of which can

ForcePoint LLC
EX-1010-PT2
Page099

be an input/output (I/O) bus for the peripherals and one that directly connects the processor 55 and the memory 59 (often referred to as a memory bus). The buses are connected together through bridge components that perform any necessary translation due to differing bus protocols.

Network computers are another type of computer system that can be used with the present invention. Network computers do not usually include a hard disk or other mass storage, and the executable programs are loaded from a network connection into the memory 59 for execution by the processor 55. A Web TV system, which is known in the art, is also considered to be a computer system according to the present invention, but it may lack some of the features shown in Figure 3B, such as certain input or output devices. A typical computer system will usually include at least a processor, memory, and a bus coupling the memory to the processor.

It will also be appreciated that the computer system 51 is controlled by operating system software which includes a file management system, such as a disk operating system, which is part of the operating system software. One example of an operating system software with its associated file management system software is the family of operating systems known as Windows® from Microsoft Corporation of Redmond, Washington, and their associated file management systems. The file management system is typically stored in the non-volatile storage 65 and causes the processor 55 to execute the various acts required by the operating system to input and output data and to store data in memory, including storing files on the non-volatile storage 65.

A security policy distribution system that is managed by a master security policy server has been described. Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention.

The terminology used in this application with respect to network communications is meant to include all communication media and environments, including local and wide area networks, public and private communications environments, and wired and wireless

ForcePoint LLC
EX-1010-PT2
Page100

communications media. Therefore, it is manifestly intended that this invention be limited only by the following claims and equivalents thereof.

ForcePoint LLC
EX-1010-PT2
Page101

CLAIMS

What is claimed is:

1. A computerized method of distributing security policies comprising:
maintaining a security policy at a master policy server; and
periodically synchronizing the master policy server and a local policy server to replicate the security policy at the local policy server.

2. The computerized method of claim 1, wherein the synchronizing further comprises obtaining security statistics from the local policy server by the master policy server.

3. The computerized method of claim 2 further comprising:
deriving a global status from the statistics.

4. The computerized method of claim 1, further comprising:
obtaining security statistics by the master policy server upon request to the local policy server.

5. The computerized method of claim 1 further comprising:
replicating the security policy to the local policy server upon request to the master policy server.

6. The computerized method of claim 1 further comprising:
creating the security policy at the local policy server; and
transferring the security policy to the master policy server.

7. The computerized method of claim 1 further comprising:
creating the security policy at the master policy server.

ForcePoint LLC
EX-1010-PT2
Page102

8. The computerized method of claim 1, wherein the synchronizing is performed securely across a communications medium coupling the master policy server and the local policy server.

9. The computerized method of claim 1, further comprising:

managing security for a plurality of client platforms by the local policy server, the security policy comprising security parameters particular to each client platform.

10. The computerized method of claim 9, further comprising:

deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy comprising the global security parameters.

11. A computer-readable medium having executable instructions to cause a computer to perform a method comprising:

maintaining a security policy at a master policy server; and

periodically synchronizing the master policy server and a local policy server to replicate the security policy at the local policy server.

12. The computer-readable medium of claim 11, wherein the synchronizing further comprises obtaining security statistics from the local policy server by the master policy server.

13. The computer-readable medium of claim 12, wherein the method further comprises:

deriving a global status from the statistics.

14. The computer-readable medium of claim 11, wherein the method further comprises:

obtaining security statistics by the master policy server upon request to the local policy server.

ForcePoint LLC
EX-1010-PT2
Page103

15. The computer-readable medium of claim 11, wherein the method further comprises:

replicating the security policy to the local policy server upon request to the master policy server.

16. The computer-readable medium of claim 11, wherein the method further comprises:

creating the security policy at the local policy server; and

transferring the security policy to the master policy server.

17. The computer-readable medium of claim 11, wherein the method further comprises:

creating the security policy at the master policy server.

18. The computer-readable medium of claim 11, wherein the synchronizing is performed securely across a communications medium coupling the master policy server and the local policy server.

19. The computer-readable medium of claim 11, wherein the method further comprises:

managing security for a plurality of client platforms by the local policy server, the security policy comprising security parameters particular to each client platform.

20. The computer-readable medium of claim 19, wherein the method further comprises:

deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy comprising the global security parameters.

21. A computer system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus; and

ForcePoint LLC
EX-1010-PT2
Page104

a master server process executed from the memory by the processor to cause the processor to maintain a security policy and to periodically synchronize with a local policy server through the network interface to replicate the security policy at the local policy server.

22. The computer system of claim 21, wherein the master server process further causes the processor to obtain security statistics from the local policy server through the network interface during synchronization.

23. The computer system of claim 22, wherein the master server process further causes the processor to derive a global status from the statistics.

24. The computer system of claim 21, wherein the master server process further causes the processor to request security statistics from the local policy server through the network interface.

25. The computer system of claim 21, wherein the master server process further causes the processor to receive a request from the local policy server and to replicate the security policy to the local policy server in response.

26. The computer system of claim 21, wherein the master server process further causes the processor to create the security policy.

27. The computer system of claim 21, wherein the master server process further causes the processor to couple the network interface to a secure communications medium for synchronization.

28. A computer system comprising:

a processor coupled to a memory through a bus;

a network interface coupled to the processor through the bus; and

ForcePoint LLC
EX-1010-PT2
Page105

a local server process executed from the memory by the processor to cause the processor to periodically synchronize with a master policy server through the network interface to receive a security policy from a master policy server.

29. The computer system of claim 28, wherein the local server process further causes the processor to transfer security statistics to the master policy server through the network interface during synchronization.

30. The computer system of claim 28, wherein the local server process further causes the processor to receive a request for security statistics from the master policy server and to transfer the security statistics to the master policy server through the network interface in response.

31. The computer system of claim 28, wherein the local server process further causes the processor to request a security policy from the master policy server through the network interface and to receive the security policy in response.

32. The computer system of claim 28, wherein the local server process further causes the processor to create the security policy and to transfer the security policy to the master policy server through the network interface.

33. The computer system of claim 28, wherein the local server process further causes the processor to manage security for a plurality of client platforms, the security policy comprising security parameters particular to each client platform.

34. The computer system of claim 33, wherein the local server process further causes the processor to derive the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy server comprising the global security parameters.

35. An apparatus comprising:

network means for interfacing to a network; and

ForcePoint LLC
EX-1010-PT2
Page106

master policy means for maintaining a security policy and for periodically synchronizing with a local policy means through the network interface to replicate the security policy at the local policy means.

36. The apparatus of claim 35, wherein the master policy means is further operable for obtaining security statistics from the local policy means through the network means during synchronization.

37. The apparatus of claim 36, wherein the master policy means is further operable for deriving a global status from the statistics.

38. The apparatus of claim 35, wherein the master policy means is further operable for requesting security statistics from the local policy means through the network means.

39. The apparatus of claim 35, wherein the master policy means is further operable for receiving a request from the local policy means through the network means and for replicating the security policy to the local policy means through the network means in response.

40. The apparatus of claim 35, wherein the master policy means is further operable for creating the security policy.

41. The apparatus of claim 35, wherein the network means is further operable for coupling to a secure communications medium for synchronization between the master policy means and the local policy means.

42. An apparatus comprising:

network means for interfacing to a network; and

local policy means for periodically synchronizing to a master policy means through the network means to receive a security policy form the master policy means.

ForcePoint LLC
EX-1010-PT2
Page107

43. The apparatus of claim 42, wherein the local policy means is further operable for transferring security statistics to the master policy means through the network means during synchronization.

44. The apparatus of claim 42, wherein the local policy means is further operable for receiving a request for security statistics from the master policy means through the network means and for transferring the security statistics to the master policy means through the network means in response.

45. The apparatus of claim 42, wherein the local policy means is further operable for requesting a security policy from the master policy means through the network means and for receiving the security policy from the master policy means through the network means in response.

46. The apparatus of claim 42, wherein the local policy means is further operable for creating the security policy and for transferring the security policy to the master policy means through the network means.

47. The computer system of claim 42, wherein the local security means is further operable for managing security for a plurality of client platforms, the security policy comprising security parameters particular to each client platform.

48. The computer system of claim 47, wherein the local security means is further operable for deriving the security policy parameters particular to each client platform from global security parameters, the security policy at the master policy means comprising the global security parameters.

ForcePoint LLC
EX-1010-PT2
Page108

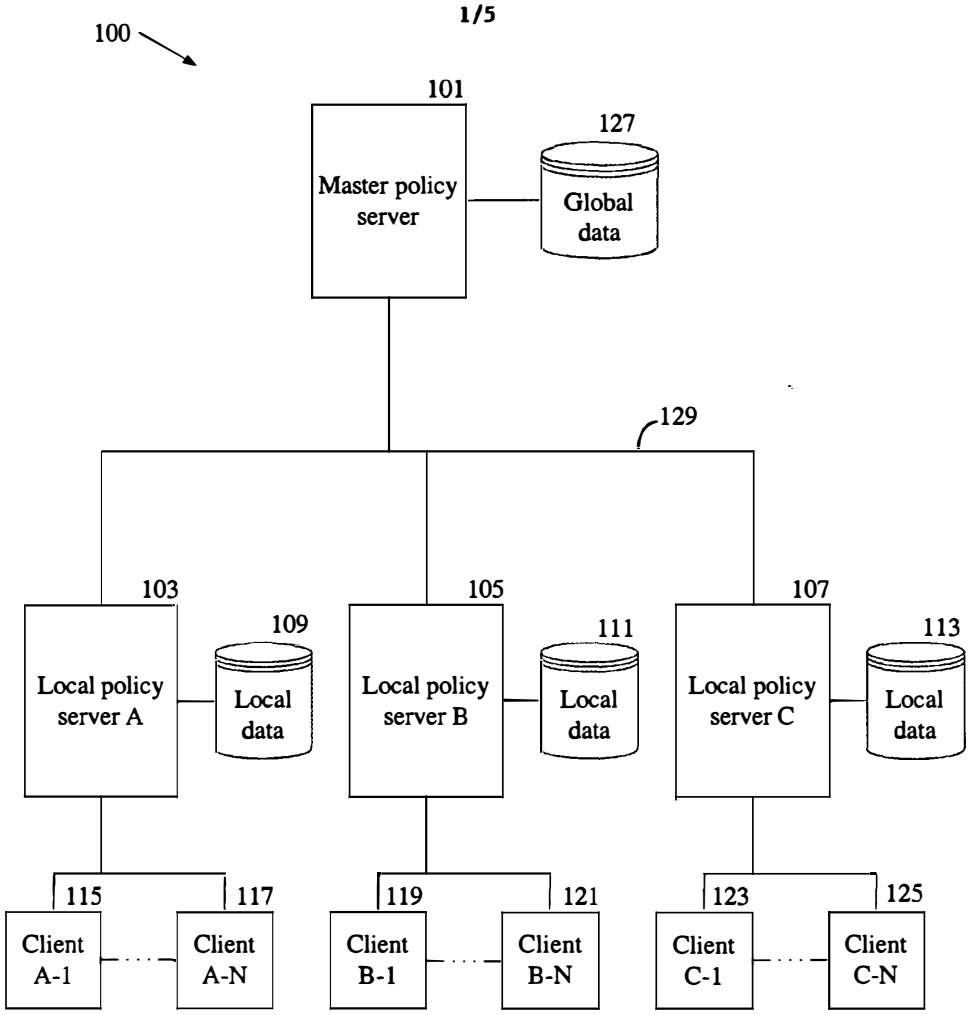

100
101
Master policy server
127
Global data
129
103
Local policy server A
109
Local data
105
Local policy server B
111
Local data
107
Local policy server C
113
Local data
115
Client A-1
117
Client A-N
119
Client B-1
121
Client B-N
123
Client C-1
125
Client C-N

Figure 1

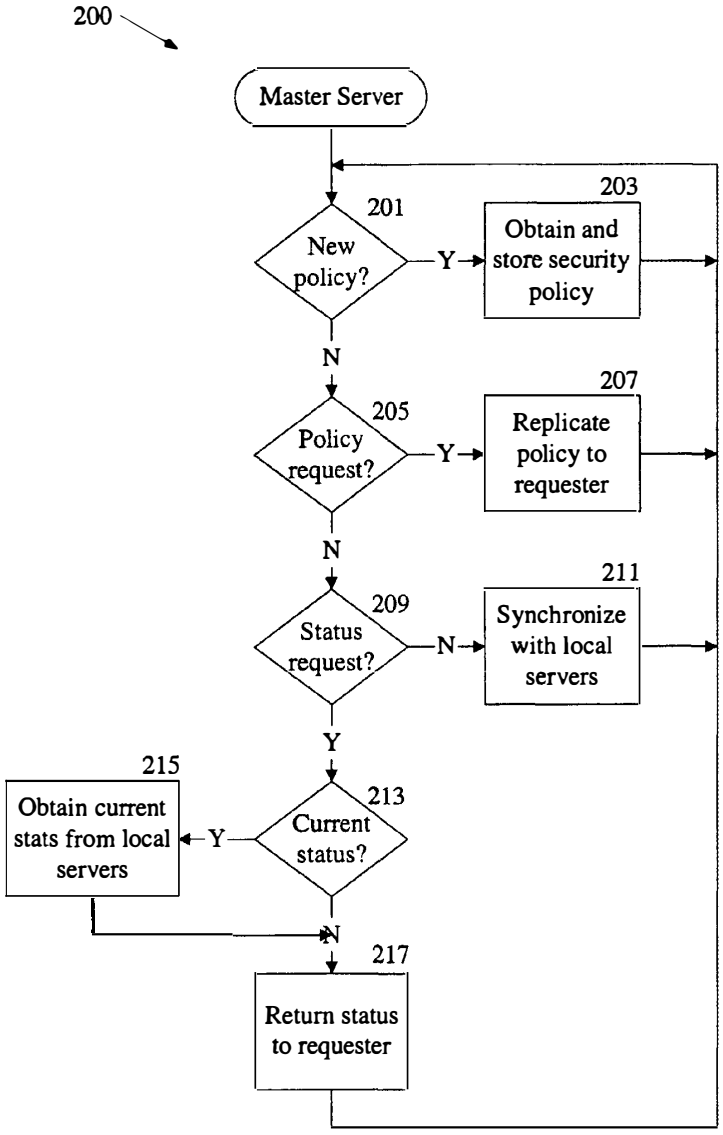

200
Master Server
201
New policy?
Y
203
Obtain and store security policy
N
205
Policy request?
Y
207
Replicate policy to requester
N
209
Status request?
N
211
Synchronize with local servers
Y
213
Current status?
Y
215
Obtain current stats from local servers
N
217
Return status to requester

Figure 2A

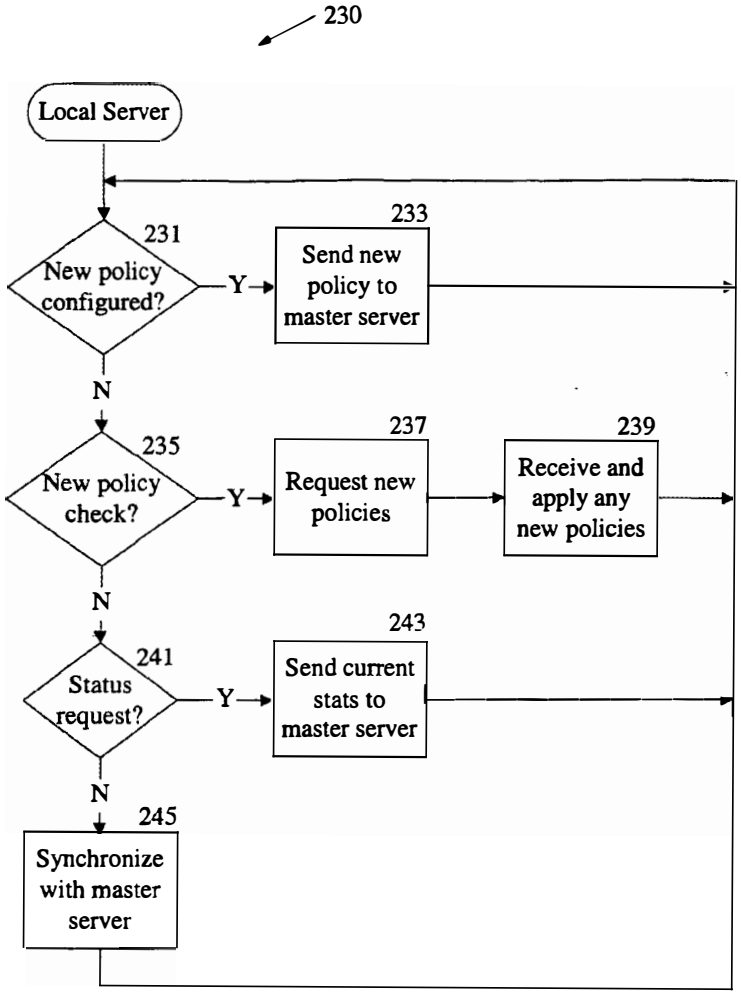

230
Local Server
231
New policy configured?
Y
233
Send new policy to master server
N
235
New policy check?
Y
237
Request new policies
239
Receive and apply any new policies
N
241
Status request?
Y
243
Send current stats to master server
N
245
Synchronize with master server

Figure 2B

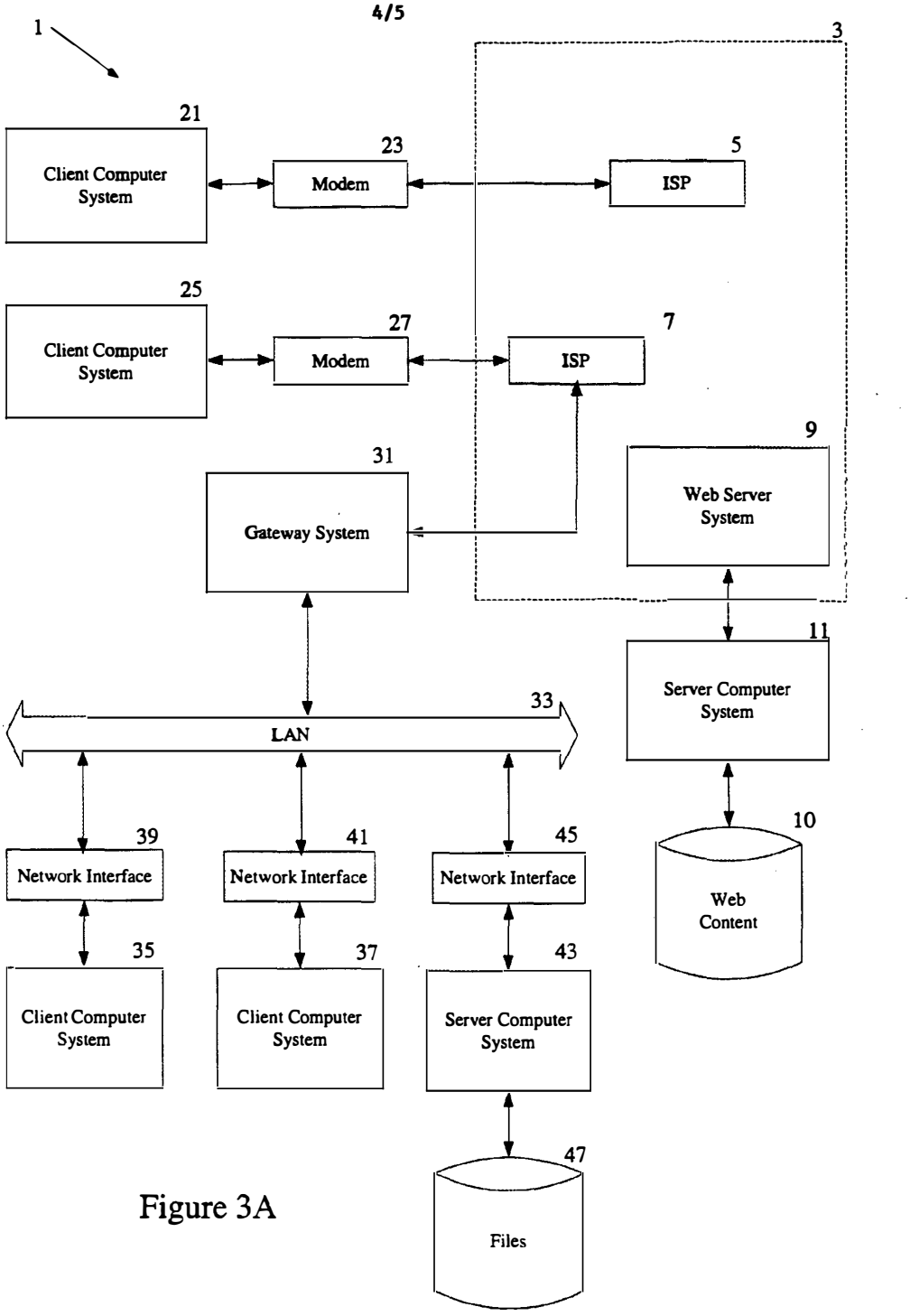

1
3
21
Client Computer System
23
Modem
5
ISP
25
Client Computer System
27
Modem
7
ISP
9
Web Server System
31
Gateway System
11
Server Computer System
33
LAN
39
Network Interface
41
Network Interface
45
Network Interface
10
Web Content
35
Client Computer System
37
Client Computer System
43
Server Computer System
47
Files

Figure 3A

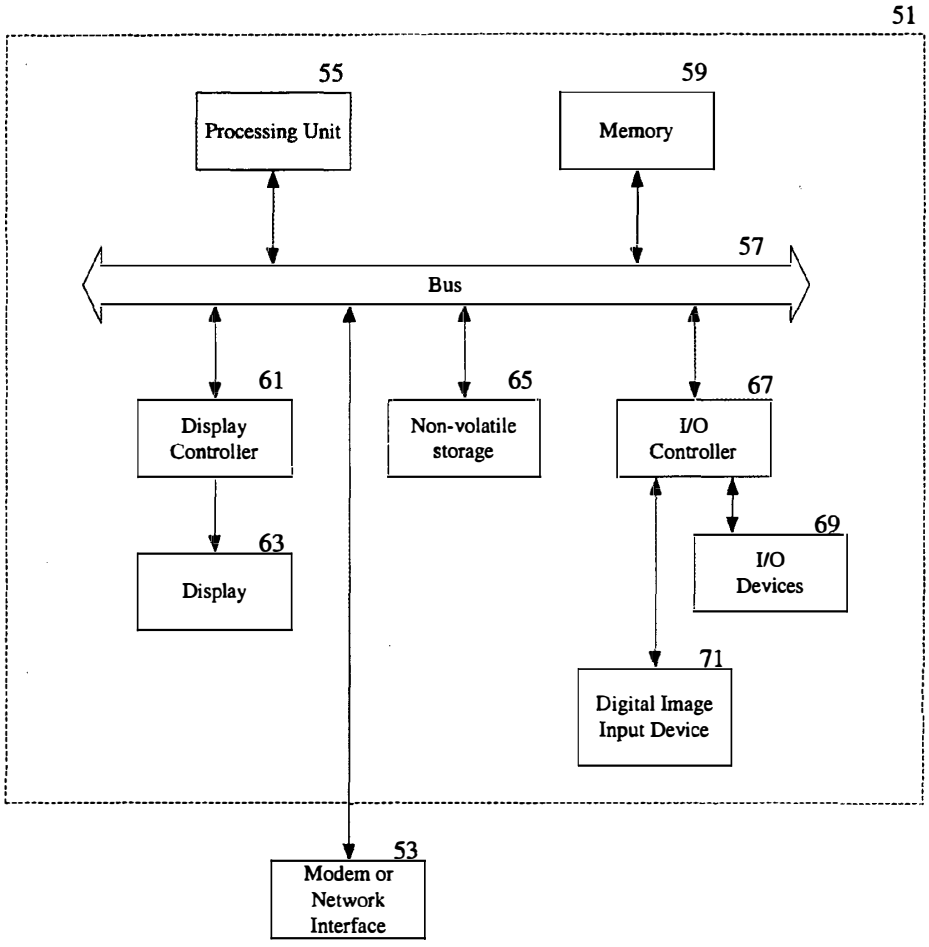

51
55
Processing Unit
59
Memory
57
Bus
61
Display Controller
65
Non-volatile storage
67
I/O Controller
63
Display
69
I/O Devices
71
Digital Image Input Device
53
Modem or Network Interface

Figure 3B

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 October 2004 (07.10.2004)

PCT

(10) International Publication Number
WO 2004/086168 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/006328

(22) International Filing Date: 2 March 2004 (02.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/394,447 20 March 2003 (20.03.2003) US

(71) Applicant *(for all designated States except US)*: **PATCHLINK CORPORATION** [US/US]; 3370 North Hayden Road, Suite 123PMB175, Scottsdale, AZ 85251 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOSHIR, Sean** [US/US]; 3370 North Hayden Road, Suite 123PMB175, Scottsdale, AZ 85251 (US). **ANDREW, Christopher, A., H.** [US/US]; 3290 West Mulberry Drive, Chandler, AZ 85248 (US). **GORDON, Jonathan, M.** [US/US]; 5001 East Hilton Ave., Mesa, AZ 85206 (US). **BACON, Michael** [US/US]; 6932 West Briles Road, Peoria, AZ 85383 (US).

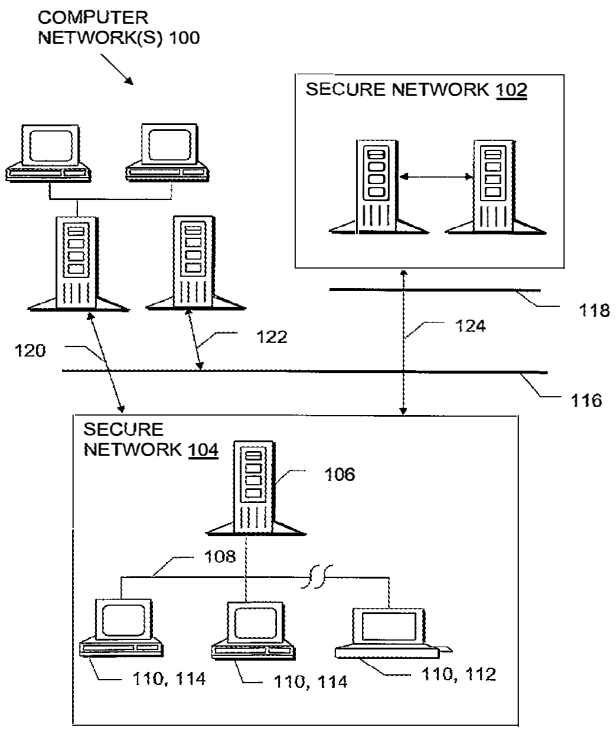
(74) Agents: **SHAHPAR, Shahpar** et al.; Snell & Wilmer LLP, One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-2202 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

[Continued on next page]

(54) Title: NON-INVASIVE AUTOMATIC OFFSITE PATCH FINGERPRINTING AND UPDATING SYSTEM AND METHOD



(57) Abstract: Methods, systems, and configured storage media are provided for discovering software updates (232), discovering if a given computer (202) can use the software update, and then updating the computers with the software as needed automatically across a network (200). Furthermore, when a failure is detected (316), the rollout is stopped (318) and the software can be automatically removed (322) from those computers that already were updated. The Software update can be stored originally at an address that is inaccessible through the network firewall (214) by intermediately uploading the software update to an update computer (220) which is not a part of the network but has access to a package computer (230) through the firewall.

WO 2004/086168 A2

Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NON-INVASIVE AUTOMATIC OFFSITE PATCH FINGERPRINTING AND UPDATING SYSTEM AND METHOD

COPYRIGHT NOTICE

A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever. The copyright owner does not hereby waive any of its rights to have this patent document maintained in secrecy, including without limitation its rights pursuant to 37 C.F.R. § 1.14.

FIELD OF THE INVENTION

The present invention relates to systems and methods which update existing software across a remote network. The invention relates more specifically to checking for the need for updating and then updating the software as required across a client-server system without the need for human oversight, and without requiring that a target network administrative machine keep copies of software patches.

TECHNICAL BACKGROUND OF THE INVENTION

The 'state of the art' in the computer software industry remains such that software is often delivered with various anomalies in its desired behavior. These anomalous behaviors have come to be called "bugs".

The original computer bug is in the operations log of the Harvard University Mark II Aiken Relay Calculator, now preserved in the Smithsonian. The operators removed a moth that had become trapped between relay switches in the computer, and wrote the entry "First actual case of bug being found." Problems with computer hardware and software have since been called "bugs", with the process of removing problems called "debugging".

Each time software is "debugged", a change to that piece of software is created – this change sometimes results in an additional piece of software called a "patch" or

ForcePoint LLC
EX-1010-PT2
Page116

"fix". The industry's software vendors often call these patches by the more formal names "Service Packs" or "Support Packs."

This process has become so prevalent in the industry that software vendors use various naming and numbering schemes to keep track of their available "Support Packs". The difficulty of keeping these "Support Packs" straight is increased when vendors fail to agree on a standard scheme of naming and numbering.

Microsoft, for instance, for its Windows NT family of operating system software products has no less than six major "Service Packs" available to be applied to solve problems its customers may experience. More generally, the total number of patches, fixes, solutions, and/or service packs for any given operating system may be enormous.

When an application is installed, it may contain one or more of these operating systems file patches along with the standard computer files. The patches are generally included because the application vendor discovered some anomalous behavior in one or more of the operating system files, and so sent a "fix" in the form of a different version of one of these troublesome files. This would cause relatively little difficulty if only one application vendor performed this service, or if the file modified by the application vendor is used only by that vendor's application. However, this is often not the case.

When another application is installed, that application may include a more recent version of a shared piece of code. One subset of these shared operating system files are called DLL's (dynamically linked libraries), though they also go by other names. These shared operating system files are often executable, and they expect a fixed number of parameters, certain kinds of parameters, and so on. If the nature of the shared file has changed (e.g., the parameter set is different, the name is different, the function is different), the calling application may no longer behave correctly. Many common computer functions such as "print" are referenced in this fashion.

Many software vendors try to provide the "latest" version of the operating system file. However, when a different application is loaded onto a computer, it may overwrite and subtly (or not-so-subtly) change an operating system file that the original application needed to function as planned.

ForcePoint LLC
EX-1010-PT2
Page117

Assume an administrator for an organization is charged with keeping one hundred servers up and running while supporting three thousand users connecting to these servers. The administrator is also responsible for installing user requested or management dictated applications – either shrink wrapped purchases or internally developed applications. The administrator also has responsibility for the timely distribution, locally or remotely, of time sensitive documents.

Now imagine that six service packs must be installed on the network and distributed to all of the clients. Applying the six service packs could easily result in seven visits to each and every one of the hundred servers for a total of seven hundred visits. This number assumes one extra visit per machine because the application of one of the service packs may cause more problems than it fixed, so it had to be undone.

If the three thousand clients were all running the same workstation operating system, that could mean another twenty-one thousand visits to apply the patches. Remember this all has to be accomplished while installing and patching the internally developed applications and the shrink-wrapped products. Distribution of software patches and files and their subsequent application becomes the first indication of what might be called "administrator agony".

While all the installation is occurring, the individual servers must still be monitored. When a server needs attention the administrator is often contacted by another person, who may frantically report that their server is down and must be fixed. If the administrator had some method to monitor these devices, he or she could become more responsive and further reduce the impact of problems. Monitoring needs are a second indication of "administrator agony". There is often high turnover in the administrator's job, and the users of these systems may experience lower productivity.

Traditionally, the administrator had been helped by being given extra staff. Of course this remedy is not without problems – the addition of personnel increases the number of communication channels between them. The people involved in installation and updates need a tracking device or system so they don't perform or attempt to perform the same unit of work. This lack of coordination between team members is a third indication of "administrator agony".

ForcePoint LLC
EX-1010-PT2
Page118

Proposed solutions are currently available in varying forms, implementations, and coverage or completeness. Typically these proposed solutions are available as shrink-wrap products that are installable (e.g. patchable) locally in the administrator's environment. Some emerging products are helpful, but many conventional solutions are invasive in that they require massive modification of the administrator's environment. The shrink-wrap solution requires additional invasive full product installations in the administrator's network, thereby adding to the problem, and lacks a central "command center" to coordinate the support or distribution plan. Emerging solutions may provide a somewhat lesser degree of invasion, but nonetheless require a special connection between the administrator and the solution, and they often do not provide a center for coordinated efforts.

Furthermore, it is not always obvious exactly what patches, if any, a given piece of software has received. Updates don't always clearly announce their presence. So, it is not always clear whether a specific computer has previously received a specific patch. Accordingly, there is a need for improved tools and techniques for updating computers across a network. Such tools and techniques are described and claimed herein.

BRIEF SUMMARY OF THE INVENTION

The present invention relates to methods, articles, signals, and systems for determining if software needs updating, and if so, then updating the software across a network with reduced demands on a human administrator. If the update fails, the computer(s) upon which the update software was installed may be restored to a non-updated state. The invention is defined by the appended claims, which take precedence over this summary.

In various embodiments, the invention facilitates software deployment, software installation, software updating, and file distribution based on software and patch finger printing across multiple operating systems and devices, across a network. Any computer with a network connection and with an update agent running on it may connect to an update server, and then process whatever tasks the administrator has designated for that agent.

ForcePoint LLC
EX-1010-PT2
Page119

Figures 2 shows an overview of one such system. A network 200, shown with only two target computers and an update computer for simplicity of illustration, is protected from the internet by a firewall 214. The software that is needed to update network target computers 202, 208 resides on package computers 230, 234 that are located inside or outside the firewall and barred by the firewall 214 from direct communications with the target computers 202, 208. However, an update server 220 does have access 216 to the network 200, potentially through internal firewalls – as well as access through the firewall 214. The system is designed to work both as an onsite purchased solution as well as a fully offsite hosted solution, and can operate through firewalls and proxy circuits at any level within the Intranet/Extranet infrastructure.

Patch fingerprints 902 give a recipe to allow a repository component to determine if a given software package (associated with the patch fingerprint) , patch, driver, etc. should be loaded onto a computer in the system. These fingerprints are stored in a patch component database location 900 that may be inside or outside the firewall 214. It may be at a separate location or it may be installed on the update server 528. The repository component also includes an inventory library database 918 that contains basic hardware and software information about each of the network target computers 202, 208. Using the information in the patch fingerprint, the inventory library, and specific information gleaned from each network target computer, the system is able to intelligently recommend which patches and drivers are required for a given computer.

As shown in Figure 5, the preferred embodiment of the invention employs an additional agent known as the discovery agent 548 installed on the target computer 500, which routinely discovers the hardware and software on that machine. This inventory information is then reported back to an inventory library 918 located somewhere else in the repository component. In addition to the computer inventory, the discovery agents also return scan results for patch fingerprints, which indicate whether it is appropriate to install a specific patch associated with each patch fingerprint.

The Inventory Database thus collects a complete inventory of the software, hardware and current patch fingerprints that are installed on any particular target

ForcePoint LLC
EX-1010-PT2
Page120

computer within the network. With this information, the update server 528 can present the user with detailed reports of the current patch status for all computers within the network. This illustrates the number of computers needing the patch as well as the computers already installed with the patch.

In addition, Finger Print definitions 906 are also normally associated with an update package suitable for deployment by the system. Once the need for a particular patch has been established by scanning for its signature(s) on all or any computers within the network it can then be quickly deployed by the administrator by merely selecting the date and time.

In some embodiments, fingerprint definitions 906 may be combined with one or more of the following to form a portable patch definition file: vendor bulletin(s) discussing the patch(es), report(s) prepared by embodiments of the invention for administrators, target computer 500 signature(s), deployment package(s). This patch definition file provides information that can be used to update other networks. The patch definition file (a.k.a. "patch metafile") provides a portable uniform data representation which can be employed by embodiments of the invention to move or replicate patches among update servers 528 of different networks. Suitable networks 100 include without limitation networks that are not connected to the Internet and/or to each other, such as military networks that are isolated to provide greater security. This movement/replication can be done by email, tape write/read, and/or other conventional data transfer means. The patch metafile may also aid the interchange and interoperability of patches between inventive embodiments supplied by different vendors.

The patches that need to be loaded onto specific target computers are listed on the update server 220 in update lists 222 associated with update agents 204, 210; in the illustration, list 224 is associated with Target1 202, and list 226 is associated with Target2 208. The update lists specify at least one location (through means such as a universal resource locator, or URL) where the patch can be found, and optionally include a date which is the earliest date that the software can be installed.

In operation, the update agent 204 of Target1 202 checks its update list 224 at the onsite or offsite update server 220 to see if a new package should be installed. If one is there, the update agent 204 checks to see if the package is already in memory on

ForcePoint LLC
EX-1010-PT2
Page121

the update server 220. If so, the update agent 204 attempts to install the software patch directly from the update server 220. If not, the update agent 204 attempts to install the software patch directly from the package computer location 232. In some instances, this is successful, in which case the update list 224 is updated.

In other cases, a download 218 will be obstructed by the firewall 214. If this happens, the update agent 210 informs the update server 220 and then the update server 220 itself will attempt to retrieve the package and place it in memory 228. From that memory on the update server, the software is installed directly to the target machine.

A monitor checks to see that the software installs properly on the target 202, 208, and then continues checking (or can be notified) to ensure that the updated software runs correctly and that the target computer itself doesn't experience any problems in what appear to be unrelated areas. Should the package fail to install properly, or create problems for the software program that was patched, or create other problems on the target computer, the package can be automatically removed and the computer restored to its preinstalled state or another acceptable state in which the update has been removed or disabled, and the target computer is in a workable state. If the package has been installed on more than one computer, they all can be removed. If the error occurs in the middle of a rollout to many computers, the rollout can be halted and the software removed or disabled. The monitor may be located on the update server 220, on a repository site 600, at least partially in the update agent 204, 210, and/or in a combination of such locations.

When there is a problem with an installation, or when an installation is successful, an administrator can be notified by email, by pager, or by some other notification means.

The update agent 204, 210 can also be used to survey its own target computer, and this information can be stored in a database offsite or at another location. This information can then be used to determine what updates a given target computer needs in order to have the most appropriate configuration. When a new software patch becomes available, the stored information can be used to determine if a particular target computer needs the patch.

ForcePoint LLC
EX-1010-PT2
Page122

It should be noted that target computer can include any type of server or workstation, regardless of operating system or installed software. Moreover, the scope of the invention applies to many other devices including wireless devices (mobile phone, personal digital assistant, pocket computer, etc.), intelligent switch devices, hubs, routers, and any other type of Internet-attachable device.

Other aspects and advantages of the present invention will become more fully apparent through the following description.

BRIEF DESCRIPTION OF THE DRAWINGS

To illustrate the manner in which the advantages and features of the invention are obtained, a more particular description of the invention will be given with reference to the attached drawings. These drawings only illustrate selected aspects of the invention and thus do not limit the invention's scope. In the drawings:

Figure 1 is a diagram illustrating one of the many distributed computing systems suitable for use according to the present invention.

Figure 2 is a diagram illustrating systems according to the present invention.

Figure 3 is a diagram illustrating methods according to the present invention.

Figure 4 is a diagram further illustrating methods according to the present invention.

Figure 5 is a diagram further illustrating systems according to the present invention.

Figure 6 is a diagram further illustrating systems according to the present invention.

Figure 7 is a diagram further illustrating systems according to the present invention.

Figure 8 is a diagram further illustrating methods according to the present invention.

Figure 9 is a diagram further illustrating systems according to the present invention.

ForcePoint LLC
EX-1010-PT2
Page123

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides systems, methods, articles, and signals which help update existing software across a remote network. The invention relates more specifically to updating software across a client-server system with little or no need for human oversight, and without requiring copies of the software patches on an administrative machine on the network whose clients are being updated. The update is automatic, and it can detect errors within a specific update and automatically rollback a faulty update to leave the network in a usable state.

Separate figures discussed herein illustrate various embodiments of the present invention, but the discussion of a given figure is not necessarily limited to a particular type of embodiment. For example, those of skill will appreciate that the inventive methods may also be used in configured storage media and/or computer system implementations according to the invention. To prevent unnecessary repetition, the discussion of methods thus applies to articles and systems, and vice versa, unless indicated otherwise. It will also be appreciated that method steps or system components may be renamed, regrouped, repeated, or omitted, and that method steps may be ordered differently and/or performed in overlapping execution, unless the claims as properly understood call for particular steps or components and/or require a particular order of execution.

For the reader's convenience, some pertinent information on related technologies such as networks and firewalls is provided below. The invention goes beyond previously known technologies, but it may partially comprise or rely on earlier advances in computing and networking and/or be used together with such earlier advances.

Systems Generally

As shown in Figure 1, computer networks 100 such as secure computer networks 102, 104, may be configured according to the invention. Suitable computer networks 100, 102, 104 include, by way of example, local networks, wide area networks, and/or portions of the internet. "Internet" as used herein includes variations such as a private internet, a secure internet, a value-added network, a virtual private network, or an intranet. Secure networks may be secured with a security perimeter

ForcePoint LLC
EX-1010-PT2
Page124

which is defined by firewall software 116, 118 routing limitations, encryption, virtual private networking, and/or other means. The network 100, 102, 104 may also include or consist of a secure intranet, which is a secure network such as a local area network that employs TCP/IP and/or HTTP protocols internally. The computers 110 connected by the network for operation according to the invention may be workstations 114, laptop computers 112, disconnectable mobile computers (such as PDAs or other wireless devices), servers, computing clusters, mainframes, or a combination thereof. The computer hardware may be general-purpose, special purpose, stand-alone, and/or embedded. The network 100 may include other networks, such as one or more LANs, wide-area networks, wireless networks (including infrared networks), internet servers and clients, intranet servers and clients, or a combination thereof, which may be protected by their own firewalls.

A given network 100 may include Novell Netware® network operating system software (NETWARE is a registered trademark of Novell, Inc.), NetWare Connect Services, VINES, Windows NT, Windows 95, Windows 98, Windows 2000, Windows ME, Windows XP, Windows 2K3, LAN Manager, or LANtastic network operating system software, UNIX, TCP/IP, AppleTalk and NFS-based systems, Distributed Computing Environment software, and/or SAA software, for instance (VINES is a trademark of Banyan Systems; NT, WINDOWS 95, WINDOWS 98, WINDOWS 2000, WINDOWS ME, WINDOWS XP and LAN MANAGER are trademarks of Microsoft Corporation; LANTASTIC is a trademark of Artisoft; SAA is a mark of IBM). The network may include a local area network which is connectable to other networks through a gateway or similar mechanism.

One system according to the invention includes one or more servers 106 that are connected by network signal lines 108 to one or more network clients 110. The servers and network clients may be configured by those of skill in the art in a wide variety of ways to operate according to the present invention. The servers may be configured as internet servers, as intranet servers, as directory service providers or name servers, as software component servers, as file servers, or as a combination of these and other functions. The servers may be uniprocessor or multiprocessor machines. The servers 106 and clients 110 each include an addressable storage medium such as random access memory and/or a non-volatile storage medium such as

ForcePoint LLC
EX-1010-PT2
Page125

a magnetic or optical disk. The signal lines 108 may include twisted pair, coaxial, or optical fiber cables, telephone lines, satellites, microwave relays, modulated AC power lines, and other data transmission "wires" known to those of skill in the art, including wireless connections. Signals according to the invention may be embodied in such "wires" and/or in the addressable storage media.

In addition to the network client computers, a printer, an array of disks and other peripherals may be attached to a particular system. A given computer may function both as a client 110 and a server 106; this may occur, for instance, on computers running Microsoft Windows NT software. Although particular individual and network computer systems and components are mentioned, those of skill in the art will appreciate that the present invention also works with a variety of other networks and computers.

Suitable software and/or hardware implementations of the invention are readily provided by those of skill in the art using the teachings presented here and programming languages and tools such as Java, Pascal, C++, C, Perl, shell scripts, assembly, firmware, microcode, logic arrays, PALs, ASICs, PROMS, and/or other languages, circuits, or tools.

Configured Media Generally

The servers 106 and the network clients 110 and individual computers 110, 114 are capable of using floppy drives, tape drives, optical drives or other means to read a storage medium. A suitable storage medium includes a magnetic, optical, or other computer-readable storage device. Suitable storage devices include floppy disks, hard disks, tape, CD-ROMs, PROMs, RAM and other computer system storage devices. The substrate configuration represents data and instructions which cause the computer system to operate in a specific and predefined manner as described herein. Thus, the medium tangibly embodies a program, functions, and/or instructions that are executable by the servers and/or network client computers and/or individual computers to perform updating, monitoring, administrative and/or other steps of the present invention substantially as described herein.

ForcePoint LLC
EX-1010-PT2
Page126

Firewalls

Network administrators generally do not allow just any information into their system. Rather, they use a firewall 116, 118 to protect the network. A firewall is hardware and/or software device that screens incoming messages (often based on content, origin, or nature of request) and only allows to pass those that are deemed safe. Three main types of firewalls are screening routers (also called packet filters), proxy server circuit-level gateways, and proxy server application-level gateways. Screening routers can base decisions on external information about a network packet such as its domain name and IP address, so messages that come from acceptable domain names and IP addresses can be allowed through 120, 124 while refusing messages from other locations 122. Proxy server circuit-level gateways disguise information about an internal system when passing the information to an external system. The IP addresses of the internal computers are typically replaced with the IP address of the proxy. At this level, authentication can be required. Proxy server application-level gateways provide all of the features of screening routers and circuit level gateways while also allowing the contents of the packets themselves to be evaluated. Messages can be rejected for content as well as for security violations.

Software Installation

System administrators often need to change the software on a specific machine. A new piece of software must be installed for the first time, as when a new application is added to a machine. An already-installed piece of software can be updated, as when a new version of an existing piece of software will be installed on a specific machine; this is also referred to as "replacing" the software. A data file of an existing piece of software can be updated without otherwise changing the software configuration, as when tax tables are updated on an accounting program, or when anti-virus software files are updated. If a problem is discovered in an existing piece of software, then a fix or patch can be installed. Any or all of these changes to the state of a specific machine or machines are referred to in this patent as "installation". Similarly, the words "package," "patch," and "update" should be given the broadest possible meaning. For example, package could refer to an entire program including all the necessary files, to one or more data files, to a software patch to an existing file, to

ForcePoint LLC
EX-1010-PT2
Page127

a change to a configuration file, to a *.dll file, a driver file for a specific piece of hardware attached to a computer and/or a computer network, and so on. "Update" refers to at least attempting to install a package on a computer.

Methods Generally

With reference to Figures 3, 4, and 5, one embodiment of a method operating according to the present invention includes a target computer 500 in a pre-update state. The target computer 500 is the computer that the invention will at least attempt to update; not every embodiment of the invention requires that the update be successful. An update server 528 is connected across a network 524 to the target computer. In some implementations the target computer has a network connection, such as a connection through a winsock layer. Typically, the target computer is protected by a firewall 526, as explained above, but the update server can drill through the firewall to access the target computer.

Many existing enterprise software management tools use agents. Examples include Microsoft SMS software, Microsoft Active Directory software, IBM Tivoli products, Symantec anti-virus software, McAfee anti-virus software, and Novell ZENworks software (marks of their respective owners). In large networks, agents can wake up and report in parallel to a server when they have information to report. By contrast, tools that lack agents rely on remote API calls, which are polled continuously by the server, making them linearly scaleable in performance rather than parallel processing as seen in the preferred embodiment.

Agents in embodiments of the present invention can receive compressed files to conserve network bandwidth. Compression also enhances security, because decompression errors may indicate that a patch has been tampered with.

An inventive agent can also resume a download when a mobile target bearing the agent is disconnected and then reconnected to the network at another location, unlike patch management tools that lack agents and therefore download entire service packs or files after being interrupted. Tools lacking agents may also generate uncontrolled spikes in bandwidth utilization as patches are deployed, whereas some embodiments of the present invention permit an update server to be controlled by an

ForcePoint LLC
EX-1010-PT2
Page128

administrator so that the server uses only a specified amount of bandwidth per agent connection (bandwidth throttling).

Conventional patch tools that rely on a permanent LAN/domain connection and lack client agents may rely on a remote registry service, which provides registry information to a remote computer. The remote registry service is not available on the Windows 95, Windows 98, or Windows ME platforms. Such a service can be a security risk in organizations whose client computers are on the Internet, because they allow remote computers to read the registry of a client, thereby providing information that can be used to guide infiltration or other attacks on the client's security. Embodiments of the present invention preferably avoid using a remote registry service, due to the security risk.

An update agent 508 is located at each computer that is to be updated. The update agent is a software component (usually not very large) that may be installed initially, either in the traditional manner or by using the invention, on the network target machines such as workstation(s) and/or server(s). The update agent is capable of operating in the place of the human administrator, at the direction of the human administrator, to perform work in a manner similar to what could be performed if the human administrator was actually present at the machine. The update agent knows how to perform four basic tasks: 1) how to contact the update server 528 to retrieve a list of tasks, 2) how to start the tasks in the task list received, 3) how to process policy information for hours of operation and so forth, and 4) how to register with the Update Server.

The update agent is capable of updating, configuring, or replacing itself without the need for manual intervention after the initial install. Typically a small boot-strap agent will be installed initially, but will grow in abilities as the administrator dictates or as required to fulfill administrator requests. The update agents of different sorts of target computers 500, such as onsite administrator computers, server computers, and client machines, can all start out as the same version of a single agent. Machines in a given network can all have a the same agent installed, or machines can have unique agents installed. When there is more than one client, each can have a different update agent initially, or a mix of agents can be installed on different client machines, as is chosen by the administrator, or as is set up as a default.

ForcePoint LLC
EX-1010-PT2
Page129

Similarly, multiple servers and administrators can also have a mix of different agents initially installed. As the agents for the individual target computers change, they can all change in concert or they can diverge. In some embodiments, the agents may all start out different and then converge in functionality.

The offsite location of the update server 528 is a location distinct from the target computer. The location may be offsite at a completely different vendor, or offsite at a different physical location from the target computer 500 but at a location managed by the same entity, at the same physical location. It may be at a different-appearing location from the target computer 500, such as at a subcontractor location, or at some other distinct-appearing location. The important point is that as far as an individual target computer operating system is concerned, the work appears to be off-site. One embodiment locates the update server on the target computer 500 but in a fashion (such as in a different partition) that appears offsite.

The actual update material that is to be installed on the target computer is often stored at a separate location (known as the package computer) apart from the update server and the target computer. The software update itself can be any of a wide variety of software that can be updated across a network, such as an incremental software patch, a new software program never before installed on the target computer, an update to an old program, software scripts, data files, or even an update of the update agent.

If a known condition is met, during a placing step 300, a task id is placed on an update task list 222. The known condition could be that the patch is not currently on the computer, that the administrator has given assent, the owner of the target computer 500 has permission from the owner of the package, the fact that no one has specifically denied placing privileges, or some other known or inventive condition. The update task list located on the update server is associated with a specific target computer 500, and specifies at least one download address where the software update can be found. The download address can be in any format that is understandable to the computers. The invention does not depend upon any specific addressing convention. Two common addressing formats in use currently are the "Universal Resource Locator" and "fully qualified domain name" formats. Other formats are PURLs (Persistent Uniform Resource Locators) and URN's (Uniform Resource Names), and

ForcePoint LLC
EX-1010-PT2
Page130

other naming schemes may be known in the future. Other information that may be included in the task identifier, such as a date the download will first be attempted. Multiple download addresses, each of which specifies a location where the software update can be found, may all be associated with a specific software update.

During a starting task step 304, the software update is at least attempted to be uploaded from the package computer 567 to the update server 528. During an optional choose package computer step 306, if more than one download location is placed on task id list 226, the location that the software update will be downloaded from is chosen. The choice can be made by any known or inventive method, such as using the first location on the list, using the location that a test message returns from most rapidly, using the first available machine, and so on.

Once a location for the update is known, the software download is attempted from the location of the package computer 548 to the memory 530 of the update server 528. If the download is unsuccessful, then in one inventive method another location from the list of possible locations in the task update list is chosen, and the download of the software update is retried. In some implementations, if the download can't be completed for some reason, the update server 528 waits for a time and tries to download from the package computer 567 again. If the download is successful, then the update server 528 attempts to download 312 the software update to the target computer 500.

Once the download is in cache or other memory in the update computer a second download 312 is attempted to download the software package from the update server to the target computer. In some embodiments of the method, the second download 312 is delayed 310 by some predetermined criterion. This delay may be from the start of the first download, with the delay period based on an estimate of the time needed to download the software update from the package computer to the update server. The second download may also be delayed to a specific time of day when the target computer 500 has less of a chance of being used, such as after a business closes for the day. Other known or inventive delay criteria may also be used.

A monitor 302 checks the installation, performing the role typically played by an administrator, to determine the results of the installation 314. Once the results are known, an administrator can be notified 328. Notification can be by sending an email

ForcePoint LLC
EX-1010-PT2
Page131

330, by paging someone, by sending a pre-recorded phone message, or by any other known or inventive method and means.

If the monitoring step detects a failure 316, then the task that failed is suspended 318. The first download 308 to the update server 528 could fail, as could the second download from the update server 528 to the target computer 500. If there are multiple target computers having the software update installed, the Nth installation could fail, and so on. Determining results preferably goes beyond simply ensuring that the software update appears to have installed properly, and in some embodiments of the invention extends for a time beyond the installation. For example, one embodiment of the monitor will test a patch application by having it installed on only one target computer, assuring that it downloads properly, installs it and then watching it for some period of time until the administrator who sets the time delay gains enough confidence in the patch to allow it to be applied to other target computers. Should the application of this patch cause abnormal activity, as noticed by undesirable behaviors either in the program whose software was modified or elsewhere in the computer, the rollout can be automatically suspended until the problem is resolved.

Furthermore, in some instances when failure is detected the software update is disabled or removed 324 from the target computer, and that machine is returned substantially to its pre-update state or another acceptable (working) non-update state. This may mean that the installed software is taken off the target machine 322; or that not only is the software removed, but all the ancillary files (.dll's, .exe's, etc.) are restored to their pre-update state. In other instances it may mean that the target computer or some portion thereof was backed up before the software update was installed, and the backup itself is restored onto the machine.

If there are multiple target computers 500, failure may be detected by the monitor after the software has been installed on one or more machines. In this case, the software update can be removed 322 from not only the target computer 500 where the failure was spotted, but it can also be removed 326 from all of the other target computers 500 where the software was previously installed 326. The removal request can come from an administrator or removal can be performed automatically after failure is detected 316.

ForcePoint LLC
EX-1010-PT2
Page132

The monitor 302 may perform more tasks than simply waiting to hear if a software package has installed successfully. For example, in some instances the monitor waits for a time period 400 after the installation and if it has not heard otherwise, assumes that the installation was successful.

Administrators and administrator helpers can benefit greatly from a central repository where they can enter and retrieve information regarding requests for help. One such method is help desk "ticketing". Ticketing records the requestor, the type of request, when help was requested, when the response to the request was completed, and other useful information. A PatchLink HelpDesk service provides facilities for administrators to manage their network requests and network resources, both people and computer resources, via one central repository. PatchLink HelpDesk software provides these facilities across the internet without an invasive application install on the administrator's network that introduces yet another resource that has to be managed, backed up, and updated – this is taken care of transparently at an offsite Management Center.

A website, reachable by a standard web browser or some other known or inventive network connection, provides the facilities to use the help desk services. A preferred implementation is currently at the PatchLink web site, reachable at www.patchlink.com. Simple web forms support the data collection required to begin the enrollment process. Once the enrollment process is complete, the administrator can license one or more services on a recurring subscription basis.

The enrollment process is begun when the administrator initiates the process by signing up and indicating a desired level of participation. A preferred embodiment of the invention has three different user levels: guest, regular, and executive. A guest is allowed to view the web site and can read the user forums but cannot post to the forums. A regular member can perform guest functions and can also chat in chat rooms, and post to forums. An executive member has a subscription to the site. He or she can perform regular member functions, and can also use the more advanced features of the site, such as offsite automatic package updates (e.g., PatchLink Update services), offsite monitoring (e.g., PatchLink Monitor services), and the offsite help desk functions (e.g., PatchLink HelpDesk services).

ForcePoint LLC
EX-1010-PT2
Page133

One embodiment of the method entails an email being sent to a customer care agent assigned to the customer's telephone area code. The customer care agent telephones the pending user to complete the enrollment process. The customer care agent collects the necessary identity information and payment information, and then upgrades the pending user's account to permit use of the account, making the pending user an administrator/ user. The areas the administrator/user can participate in or use is controlled by entries in the licensed product's table of the update host's database. These entries are created by the customer care agent during the enrollment process.

Recall that all these services are available to the administrator via a browser or other network connection across the internet. When a monitor enters a ticket into the help desk and initiates a rollout in some instantiations of the inventive method, the monitor then decides whether a failure has occurred 316, 406. To decide the monitor may look at what software updates have recently been installed, how long ago the installations occurred, the current hardware and software configuration, and so on. Which incidents are considered failure can be, without limitation, set by an administrator; defaults can be used, and judgment of the help desk personnel can be taken into account.

In a detect success step 408 the target computer 500 sends a message 410 to the update server after the download from the update server to the target computer has completed successfully. The monitor can presume success 404 if a specified time period has passed without noticing or being notified of a failure.

Failure can be detected in other ways 316, 406. For instance the target computer can notify the monitor that a failure has occurred; a user can notify the monitor through the help desk or through a direct link that a failure has occurred; when a target computer does not contact the monitor within a specified time from the beginning of the second download 312 onto the target machine, a human administrator can declare that a failure has occurred; and so on. Notice that even after the monitor has declared the outcome of a download to be a success, later events, such as an indication of failure from the help desk, can cause the monitor to declare the download to be a failure.

ForcePoint LLC
EX-1010-PT2
Page134

In one embodiment of the invention, the update server 528 waits for a confirmation of a successful installation (by the monitor, or by another known or inventive contact method) before the next target computer 500 has the software update placed on its update list 222. The update server checks for a target computer 500 that is eligible for the software update but has not yet received it 412. If one is found 414 the appropriate task identifier, specifying the target machine, the software update, and the location, are added 416 to the update server's 528 task update list. This way, rather than a mass update where all eligible computers have the software installed on them *en masse*, the rollout proceeds one computer at a time until, after a default or user-defined number of successful installations, the rollout is deemed a success; at that juncture the software update is made available to more than one target computer at a time.

It is not always clear by looking at a specific target computer 500 what software packages and patches have been installed. The invention includes a method to analyze a target computer 500 to ensure that a given patch has not already been installed on the computer 500 before the invention attempts to install that patch. The following discussion includes references to Figures 8 and 9 and continuing reference to Figure 5.

A patch fingerprint which defines a specific software update is described in greater detail below. The patch fingerprint is located 800 by monitoring a patch component database location 900 for a new patch fingerprint 902. The word "new" here indicates that the patch has not yet been downloaded into the repository component 600, or for some reason needs to be downloaded into the repository component again, even though it has been downloaded previously. There may be one or many patch component locations; those locations may be on a separate computer connected to the system through a network link, on the update server 528, on the target computer 599, on the package computer 567, on a non-networked location such as a CD, a tape, a floppy disk, etc., or some other known or inventive location.

Once the patch fingerprint 906 is located 800, it is placed 802 into the repository component 600. The usual method of placement is to download 804 the patch fingerprint 906 into the repository component, but in some embodiments the

ForcePoint LLC
EX-1010-PT2
Page135

fingerprint 906 will be on the same file system, so the patch fingerprint will be copied without using the network, such as copying between partitions.

The illustrated patch fingerprint comprises one or more general inventory install dependencies 912 that can be used to take a high-level look to see if a specific patch can be installed on a machine. It also includes a signature block 910 that can be used to request specific information from a target computer 500, and an existence test 908 which can use the signature block information to determine if a specific patch has been loaded on a machine.

In some versions of the invention, the inventory install dependencies 912 describe at least some of the necessary software and hardware that must be installed on the target computer 500. These dependencies 912 are compared 808 with information about the target computer 806 previously stored in the inventory library 918. If the install information and the inventory information don't match, then the patch is not installed. In some versions of the invention a message is sent to at least one administrator containing a list of components required (such as necessary hardware and software) for the install.

If the necessary inventory information is on the target computer 500, or if the inventory info is not used, then the signature block is sent 810 from the repository computer 600 to target computer 500. The information requested in the signature block 814, which may consist of more specific install information, is gathered 812 by the discovery agent 548 and then sent back to the repository component 818. In some versions of the invention, the discovery agent also gathers other information 816 about the target computer such as usage statistics, hardware and software installed, configurations, etc. This information can then be used to populate the inventory library 918.

Once the signature information 910 has been sent to the repository component 600, an evaluator 914 evaluates at least a portion of the specific install information requested by the signature block using the existence test 908, and in some instances the inventory install information 912, to determine if the patch is absent 822 on the target computer 500.

As an optional step, once it has been determined if the patch is absent a message is sent 824 to at least one address associated with an administrator. This

ForcePoint LLC
EX-1010-PT2
Page136

message may be sent using a variety of methods, including email, pager, fax, voicemail, instant messaging, SNMP notification, and so on.

Patch Fingerprint

With continuing reference to Figures 5, 8 and 9, one embodiment of the system verifies that a software package can be or should be installed on a given target computer 500 before attempting installation. To do so, a patch fingerprint 906 is used, e.g., by an agent on a client. The patch fingerprint defines how to determine if a given software package/incremental patch has been previously installed. It may also define a minimum hardware/software configuration necessary for the patch installation. These patch fingerprints 906 are stored in a fingerprint library 904. The fingerprint library 904 is located on a repository component 600. This repository component 600 may be located on the update server 528, or may be in a separate location accessible to the update server 528 and the target computer 500. Some versions of the invention also include an inventory library 918 which contain target inventories. Each target inventory 920 contains the hardware and software information about a defined set of target computers 500. This defined set may include as few as one computer or as many as all of the computers in a given network, or some number in between.

The fingerprint library 904 can be automatically replenished. In some embodiments, at least one, but possibly several, patch component database locations 900 are monitored 800 for new patches 902. In some embodiments of the invention a signal from the locations 900 indicates to the repository component 600 that new patches 902 are available 800. In the preferred implementation the fingerprint library 904 is updated with new patch fingerprints at specific time intervals. After the repository component 600 is aware of the new patch fingerprint, the patch fingerprint is placed into the repository component 802, usually by using a downloader 924 to download the new patch fingerprint. Patch fingerprints may be entered into the repository components in other ways, however. For example, one or more patch fingerprints may be manually installed into the fingerprint library by an administrator.

Inventory Library

The repository component 600 also contains an inventory library 918. A discovery agent 548, which in some embodiments initially resides on the update

ForcePoint LLC
EX-1010-PT2
Page137

server 528, is installed from the update server 528 to the target computer 500 using known or inventive methods. This discovery agent 548, described in greater detail below, inventories at least some of target computer 500's software information 606, hardware information 608 including specific software updates and patches installed, usage information 604, registry information 612, web information 610, configuration information 614, services 618, file information, patch signatures which have been utilized, etc.

This information, or a subset or superset thereof, is then sent, in some embodiments in compressed form, to the target computer inventory 920 in the inventory library 918. Result information can be quite voluminous, and hence may be compressed for efficient upload and to minimize bandwidth usage on the customers network. A preferred implementation sends the data using an XML data transfer, though any other known or inventive data transfer method can be used. Transfer of inventory information may also be encrypted within a customer network to prevent unwanted wire-level snooping of system configuration information.

Report Generator

With this information, a report generator 922 can present a user with detailed reports of the current patch status for all computers within the network, illustrating the number of computers needing the patch, the computers already installed with the patch, computers that can't receive the patch until hardware or software is upgraded and so on. In addition, the report generator 922 can provide a partial or complete inventory of the computers attached to the network. In some embodiments the report generator 922 provides graphical presentations of the inventory for analysis by the administrator, both to track location of hardware as well as to ensure software license compliance. However the repository component 600 also uses the inventory library 918 information as well as detected fingerprint information to distribute relevant signatures 910 from the patch fingerprint 906 to the discovery agent 548, thus greatly optimizing the patch discovery process by eliminating unnecessary scanning work at the target computer 500.

ForcePoint LLC
EX-1010-PT2
Page138

Discovery Agent

One optional step to decide if a given software program or patch can be installed is by verifying that the necessary hardware, if applicable, is present, and/or the necessary software is present. For example, some programs may require a specific operating system, some programs may require a certain processor. As an example, if an update of Microsoft Word software is to be installed, it is necessary that Microsoft Word software be on the machine. These high-level dependencies are stored, in some versions, in the inventory install block 912 in the patch fingerprint. The information in the inventory install block is generally high level enough that it can be pulled out of the target inventory 920 of the specific target computer 500 stored in the inventory library 918.

In some implementations of the invention the patch fingerprint 906 also includes installation dependency information 912. This, as explained above, is information about the target computer 500 that can be expected to be found in the inventory library, and so can be checked without querying the target computer 500. This includes software that should be present (such as a specific version of a program, a patch, a data file or a driver) a hardware component that should be present, or specific hardware and/or software that shouldn't be present.

If the inventory library does not have an up-to-date inventory for the target computer 500, the discovery agent can be used to scan the target computer 500 for inventory information; it does not necessarily need to also scan simultaneously for signature information. In the preferred implementation, the first time that the discovery agent 548 runs on a given target computer it scans only for inventory information and then loads that information into the inventory library 918; it ignores the patch fingerprint information. At other times when the discovery agent 548 runs it may ignore inventory information and may, rather, be used to look up specific signature information 910 to test for the existence of a specific patch. When the signature block information is looked for, values such as registry entries and INI file values may be inspected for existence, or the actual value may be returned to the repository component 600.

Each Patch fingerprint comprises a signature block 910 and an existence test 908. The patch signature block is a set of information requests, the information itself

ForcePoint LLC
EX-1010-PT2
Page139

to be gleaned from a target computer 500 which will then be used to determine if all necessary bug fix and security patches are installed. Examples of patch signature block information include but are not limited to file, hardware, registry and configuration information, a specific file name or directory name, all or part of a path that a file is expected to be found in, a specific version number of a file, a created date of a file, a specific file version of a file, and a specific registry value.

In one implementation the fingerprint library 904 is a SQL database. The patch signatures 910 are extracted from the SQL fingerprint library and then sent to all target computers that meet the dependency criteria for operating system and installed software as specified in the inventory install information 912.

A preferred implementation employs an XML-based request input file. The result file sent back to the update server 528 also employs XML formatting. This result file contains the signature information for the target computer, and may also contain the software and hardware inventory updates. The inventory and signature information sent to the update server can be quite voluminous, and so are compressed and may also be encrypted in the preferred implementation. The following is a sample patch signature that will gather registry information for Microsoft Outlook as well as the EXEs date and time, and information in the registry :

```
<file componentid="1" reportID="1">
        <name>outlook.exe</name>
        <path></path>
        <version>9.0.2416</version>
        <created></created>
        <size></size>
        <root>HKEY_LOCAL_MACHINE</root>
        <Key>SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\OUTLOOK.EXE</key>
        <value>Path</value>
</file>
```

Once the discovery agent on the target computer has returned its scan results for the signature, the existence test 908 logic is used by the evaluator 914 to infer whether that particular computer actually has the patch or not. This algorithm

ForcePoint LLC
EX-1010-PT2
Page140

minimizes the number of tests that must be done by the evaluator: its sole responsibility is to discover information – allowing the data analysis to be done by the repository component 600 itself. Distributing the workload in this fashion provides a better implementation for scanning and analyzing huge numbers of workstations and servers.

Each existence test is specific to a given patch. A sample existence test might appear as: if registry QQ contains value ZFILEVAL or (if file _Z123.bat was changed on date 12/12/2000 at 11:52 pm and file Z is of size ZFILESIZE) then the patch ZPATCH is present. The preferred embodiment of the patch fingerprint library is an SQL database, but other known or inventive databases can be used.

Note that a patch fingerprint may also contain dependencies to other Finger Print definitions: for example, "MS-023 IIS Vulnerability Fix" patch might hypothetically require the presence of "Microsoft Windows Service Pack 2". This is used to further optimize where the patch signatures are actually sent. These may sometimes be used in the install dependencies info 912 and other times in the signature block 910, depending on circumstances.

In addition, fingerprint definitions 906 are also normally associated with a software package 554 suitable for deployment by the system. Once the need for a particular patch has been established by scanning its signature(s) on a computer or all computers within the network, it can then be quickly deployed by the administrator by merely selecting the date and time.

A fingerprint definition 906 may also contain a logical expression that should be evaluated to assess whether the other elements within the patch signature should be evaluated to TRUE (patched) or FALSE (not patched). The expression is a simple logical statement such as (A AND B) | C where A, B, and C refer to other fingerprint definitions within the patch signature.

In some implementations the downloader 924 regularly checks the patch component database for new patch fingerprints. When a new patch fingerprint is located, it is downloaded into the repository component. The evaluator compares the dependencies needed for the specific patch implementation listed in the install info 912 with each of the target computer 500 specifications listed in the inventory library. Then an update list is created which may identify all of the target computers 500 that

ForcePoint LLC
EX-1010-PT2
Page141

need the patch, all of the target computers that don't possess the patch, all of the target computers that can receive the patch, as they have the necessary dependencies, and/or all of the target computers 500 that have already received the patch. This update list may now be used to update the target computers, and/or may be sent to an administrator by a notifier 916.

In some instances of the invention the patch component database is owned by someone other than the target computer 500 owner. Only if this patch update host has given permission to the target computer 500 owner will the downloader be allowed to download the new patch fingerprints into the repository component. The permission may comprise a purchase agreement, a lease agreement, subscription for download permission and an evaluation agreement.

If any modifications are made that may be of interest to the administrator, the notifier 916 will send a notification message containing the new patch updates that have become available or the patch-related state changes that have occurred in his network configuration. Notifications can be sent via e-mail, pager, telephony, SNMP broadcast or Instant Message.

Target Computer

In one embodiment, the inventive system comprises three pieces: a target computer 500, an update server 528, and a package computer 548. The target computer 500 has a memory 502, and a network connection 504, which in at least one implementation of the invention is a winsock layer. A socketless protocol can be implemented, or any other known or inventive network connection can be used. The update server 528 has a memory 530 that may include an optional backup storage 534, and a network connection 532. The package computer 567 has a memory 550, and a network connection 552. Figure 5 shows one target computer 500 for convenience but there may be many more in a given embodiment. Likewise, one update server 528, and one package computer 567 is shown for convenience, the invention may only require one but also support two or more. In a preferred embodiment these pieces are all separate computers, but they can be virtual pieces of the same computer, such that they appear to be distinct. For example, the "package computer" piece may reside on a different partition of the update server or the same partition.

ForcePoint LLC
EX-1010-PT2
Page142

The target computer contains a network connection 544, which may be protected from the outside by a firewall 526 as is discussed above. Different target computers within a network may run on different platforms; for instance, some may be Windows machines, some Unix machines, etc. The same update server 528 can be used for all the platforms, or different update servers 528 can be specified by platform type, or the update servers 528 can be assigned to target computers 500 using a different schema.

The target computer 500 also contains an update agent 508. The update agent is a software component that can be installed using the inventive method on multiple machines at a time or, in some embodiments of the system, can be installed in the traditional manner on the target computer 500. Once registered, the update agent 508 knows how to perform three basic tasks: 1) how to contact an update server 528 to retrieve its list of tasks from its update list 536, 2) how to start the tasks in the task list received, and 3) how to retrieve policy information received from the update server 528 that control polling interval, hours of operation, and so forth.

Update agent

The update agent of target computer 500 contacts the update server 528 to determine if there is work for the agent 508 to do. The update server 528 determines this by analyzing an agent's update list queue 536. This update list 536 contains, at a minimum, a software location reference 538, but can also contain a date 540 that indicates the earliest date that the software package 554 can be installed, and multiple software location references, if the same software package is available from multiple locations. The types of software 554 that can be updated comprise, without restriction, patch files 556 that update a currently installed software application on the target computer, data files 558, script files 562, new application files 564, executable files, 560 driver updates, new software versions and updates to the update agent file itself 566 .

When the update agent discovers an entry on its associated update list 536, with an appropriate date 540, if any, the installer 510 initially checks to see if a copy of the software package already exists in memory 530 on the update server 528. If found, it then downloads the software package directly from the update server. This

ForcePoint LLC
EX-1010-PT2
Page143

situation may arise when a previous target computer 500 has requested the software package 554 from the update server 528.

If the software package is not found, the installer 510 then attempts to download the update directly from the package computer location given in the software location reference 538 to the target computer memory 502 using its network connection. This will be possible if there is no firewall 526, or if the update server can connect to the package computer location 548.

When an administrator builds a package that instructs the update agent 508 to retrieve the files from a "non trusted" source such as the package computer 567, the installer 510 will be unable to retrieve the resource directly. However, the update agent can ask the update server 528 to retrieve the package. In some implementations there are multiple update servers and the update agent 508 decides which one of them to access using some predetermined criterion. Examples include selecting the first update server 528 that is available, selecting the least-busy update server, selecting the update server that is "closest" in networking terms, and so on.

In one implementation of the invention, if the update server 528 can reach the offsite package computer 567, it reports to the update agent 508 that it can reach the resource and estimates the time the retrieval will take. This estimate informs the agent how long it should wait before the requested resource is available. If the calculation estimation is not exact, as it probably will not be because of internet traffic fluctuations and server response time variances, then if the agent asks for the resource again the update server will provide another wait time length and the agent will wait once again. This cycle will repeat until the update server 528 has the resource available in memory and can deliver it to the agent upon the next request.

As a particular software package could be requested multiple times by different agents 508, in one implementation of the invention, the update server 528 will store this resource in a local cache 530 from which it can fulfill additional retrieval requests. To prevent the update server 528 from filling up all its available memory with old software packages, one embodiment stores the number of times the package is accessed and the time of the latest access for the stored software package and estimates a "time to live" amount of time for that resource to stay in its cache. A separate task running in the update server 528 will check periodically for resources

ForcePoint LLC
EX-1010-PT2
Page144

that have "outlived" their usefulness and recover the update host's storage resources by deleting the stored software package update from the cache 530.

In one embodiment the update server will make the packages available to the list of agents one at a time. If an agent 508 or an outcome finder 512 reports that the application of the patch failed, or if the patch puts the agent's target computer 500 in such a state that it can no longer communicate with the update server, then the update server will suspend the rollout automatically on the administrator's behalf. At this point, the administrator, or some other designated person can be notified 516 of the outcome.

An outcome finder 512 determines if the software package installation was successful and then communicates its finding to the update server 528. If the outcome is unsuccessful, as discussed above, a restorer 514 places the target computer in an acceptable non-updated state. The outcome finder 512 does not necessarily monitor only the actual software installation; rather it can be set up to watch uses of the software that was patched, the entire target computer, and/or computers that are networked to the target computer, for some designated period of time. The outcome finder can also have different levels of success. For instance, the installation itself (file copying) can be considered a low level of success, while the target computer not misbehaving for a period of time thereafter can be considered a higher level of success, with different actions taken according to the success level. Success or failure can then be monitored as described earlier, and installation retried, suspended, etc. as necessary.

Some embodiments store a backup 506, 534 of a target computer 500 or a portion thereof before installing the software package on the target computer 500. Sometimes the backup is stored 534 on the update server, sometimes on the target computer 506, 500 which is having its software updated, and sometimes it is stored offsite at a repository site 600. When the outcome finder 512 reports a problem with a software installation, the restorer 514 can use the backup 534 to return the target computer to a non-updated state.

In one embodiment of the invention, the update server 528 waits for a confirmation of a successful installation (by the outcome finder 512, or by another known or inventive contact method) before the next target computer 500 has the

ForcePoint LLC
EX-1010-PT2
Page145

software location reference 538 to the package placed on its update list 536 at the update server 528. In a preferred embodiment, when an installation finishes, an administrator is notified 516 of the results by email 518, pager 520, voice mail 522, SNMP notification 568, instant messaging 570, fax or by some other means. If the installation failed, the specific machine that the installation failed on may be identified. In some embodiments, after a default or user-defined number of successful installations, the package is made available to more than one user at a time.

These update lists 536 facilitate the administrator's designation of pre-built packages, or custom built packages, to be delivered or rolled-out to managed workstations clients or servers, which we refer to as target computers 500. When these packages are to be made available, updates are scheduled by the administrator to be performed by the invention; this may automate a previous task requiring the administrator's visit to a client to install a patch or service pack.

The update agent 508 may be aware of the platform it is operating upon, and may be programmable or scriptable to perform actions on behalf of the administrator. In one implementation these features are exposed to the administrator through Package Builder wizards. A "software package" can be any combination of files, service packs, hotfixes, software installations and scripts. This presents an opportunity for the administration of remote machines, since almost anything that could be performed at a remote machine can be accomplished via the agent acting on behalf of the administrator.

One implementation of the invention allows scripts 562 to be run before (pre-install) and after (post-install) the package installation. An example of a pre-install script may be: (in pseudo-code)

check for available disk space

If disk space available greater than ValueX (where ValueX = room needed for install plus a buffer) then continue with installation.

Else, alert outside administration that an error has occurred, and terminate.

An example of an post-install script (again, in pseudo-code):

If install was successful, then notify an outside source that install successful.

If install was unsuccessful, then notify an outside source that install was unsuccessful.

ForcePoint LLC
EX-1010-PT2
Page146

Referring now to Figures 6 and 7, the network 200 may include many different sorts of target computers, each with an agent that may be specifically constructed for the specific target platform. For example, a network running Microsoft Windows PCs, Apple Macintosh computers, and UNIX computers, may have three types of agents. This provides a benefit in that the agent is capable of surveying its target computer and reporting this computer information 602 to the update server 528 and/or to a separate repository site 600 for storage. In some instances of the system, a discovery agent 548 is provided which performs the scan, as discussed elsewhere. In other instances the scan is performed by the update agent 508, or a downloaded script file 562. Hardware configurations 608, software configurations 606, information about the usage of various hardware and software components 604, web sites visited, emails sent and received 610, can all be sent to the offsite location 600. Once this information is available at the update server, an administrator can view the entire managed network from one place.

When the inventive system is implemented on an existing network, the discovery agent 548 may perform a survey of the software in existence at least on the target computer 500, with existing software configurations 700 detected and stored within the repository site 600 memory. Some systems may survey the entire network 200. When updates are called for, the system knows which ones are needed without needing to resurvey the network machines to check their current status.

A recommended configuration 704 for the target computer 500 is placed on the update server 528 or on the repository site 600. The recommended configuration may be decided on in many ways, either inventive or known to those of skill in the database arts, for example, by hardware configuration, by software configuration, by type of computer, by last package update, and so on. The discovery agent 548 then compares the current 700 and recommended 704 configurations and prepares a proposed list of updates 708 for the target computer 500. The update list may include service packs for installed software, previously uninstalled software, updated data files, and the like. The process of preparing the suggested list may take into account not only the current software configuration but also information such as the hardware configuration 608, and how often a particular program, data file, etc. is accessed 604,

ForcePoint LLC
EX-1010-PT2
Page147

as well as other information that is known to one of skill in the art. An administrator may be automatically notified of the update list.

Assuming that the target computer current configuration 700 generates a proposed update list 706, an administrator may be automatically notified 708. At this point, the computer use may be restricted until the new target computer is updated at least partially, until the administrator gives permission, or until some other inventive or known condition is met. This proposed update list 706 may also be used to define an update list 536 used to actually update the computer, as explained elsewhere.

Packages are composed of modules representing files, e.g., software files or data files, and scripts, which are sequences of actions to take upon files in the package. Alternatively one or more script file(s) may be included within the package content, and executed by the agent in order to install the patch. In some embodiments of the invention, a human administrator receives notice of the availability of new software patches. In other embodiments, the notices are sent directly to the offsite update server 528 which decides when to roll them out. The offsite update server can be configured to store in permanent memory the packages that have already been stored on each target computer. When a new package becomes available, or during the installation of an existing package, existing evidence of the software packages that need to be installed, as well as information about previous installations, is available in some embodiments at the offsite update server 528, and in other instances at the repository site 600.

The packages that are to be updated do not need to be owned by the target computer 500 user to receive access to it. In one embodiment of the system, the software package is owned by a third party which leases the software to the user. In another embodiment, the software package is owned by the update server user who then leases and provides access to the software package to the target computer 500 user.

Security and Critical Patch Management, Features

The present invention provides tools and techniques for managing and distributing critical patches that resolve known security vulnerabilities and other stability issues or enhancements, etc. in various operating systems. Suitable operating

ForcePoint LLC
EX-1010-PT2
Page148

systems include, without limitation, all Microsoft operating systems (e.g., 95, 98, ME, NT, W2K, XP, .W2K3), UNIX operating systems (e.g., Linux, Solaris, AIX, HP-UX, SCO, etc), and Novell NetWare operating systems. Operating system product names are the marks of their respective owners.

In the past, in order to manage security or otherwise critical patches, corporations and other computer users have frequently checked vendor web sites, e.g., by reading news reports or textual alerts posted around the world wide web or were sent notifications via email subscription or newsgroup etc, to find out about new patches. Upon learning that a vendor whose software is used by the corporation has released a new patch to fix or enhance application software, driver software, and/or hardware, the corporation's software administrative personnel have generally had to manually download the latest relevant patches, test them for compatibility with the corporation's machines in various layouts and configurations, and then distribute the patch(es) manually or using their traditional software distribution tools.

By contrast, the present invention can provide notification 824 of critical updates to computers in a proactive manner, whether or not they have Internet access. It can operate proactively by performing patch downloads without requiring an express administrator command to perform each download. It can also assist with distribution and installation of software updates, software packages, and other data to networked desktop, server, mobile, and other computers.

One embodiment of the present invention includes content replication through an update server 528 that retrieves the latest critical updates from a master archive such as a package computer 567. Retrieval may use 128-bit SSL or other familiar protocols for secure transmission. As new updates are added to the master archive, the updates' metadata are downloaded automatically to the update servers and/or the fingerprint library 904. If metadata indicates a patch is critical, the patch can be downloaded to the update server and cached there for rapid deployment. Each patch has an associated installer 912, prerequisite signature 910, and other fingerprint identification 906.

In some embodiments information is sent in one direction only, namely, from the master archive to the update server, thereby enhancing security of the master archive. In addition, in some embodiments all transmitted information is encrypted,

ForcePoint LLC
EX-1010-PT2
Page149

CRC (cyclic redundancy code) checked, compressed, digitally signed, and downloaded 308 over a 128-bit SSL connection. The SSL connection employs a secure network protocol that validates and confirms the authenticity of the master archive as the patch source. Other secure network protocols may also be used. In other embodiments, some of these elements are omitted, e.g., no CRC check is done and/or no digital signature is used, etc.

The update server 528 acts as the patch source for client target computers 500. The update server, which contains the replication service and administrative tools for managing updates and software packages, can scan clients 500 and schedule patch deliveries to them using protocols such as HTTP, HTTPS, and XML. In some embodiments, the update server uses Microsoft's Internet Information Services. The update server can be implemented to automatically cache critical updates it receives from the master archive. In some embodiments the administrator can set a replication schedule, can trigger replication manually, or can have the replication software in the update server replicate and distribute software automatically in response to expected or measured network inactivity.

In some embodiments, administrators can create software packages 554, which they can then deploy like any other patch. That is, a "patch" in the general sense need not presuppose a previously installed close-related piece of software that is being modified, but may comprise a piece of software new to the target. For example, a package containing Microsoft Office 2000 could be deployed to every desktop. Administrators of custom applications can similarly create packages to rollout custom applications and their patches. Some embodiment administrators may also utilize built-in software distribution features to distribute any software packages to any target computer.

In some embodiments the update server 528 is configured with software and/or hardware which displays an enterprise report matrix or other summary of the patch status of the machines in a corporation or other enterprise. The report is displayed to a network administrator and/or other personnel charged with maintaining the enterprise's computer functionality. The administrator influences (and in some cases totally controls) which updates or packages from the update server are pushed to the clients 500, by setting policies, defining groups, responding to alerts, and/or taking

ForcePoint LLC
EX-1010-PT2
Page150

other steps which are discussed here or already familiar. In some embodiments the administrator has full control over the deployment of patches, including control of reboots and the power to set or modify client agent policies.

Patches may be tested internally before they are widely deployed through the enterprise, since a given patch may behave differently in different enterprises. PatchLink.com Corporation ("PatchLink"), which provides commercial software and services for patch management, and which is the assignee of this application and its ancestors, continually researches, tests, and approves patches before they are released by PatchLink. For instance, when a hot fix for the Microsoft W2K (Windows 2000) operating system is released by Microsoft, it may then be installed and tested by PatchLink on two hundred or more different W2K configurations, such as standard W2K, W2K with SQL server, W2K with Office, and W2K with Exchange (marks of Microsoft), and so on, in combination with various service packs and other hot fixes, before it is released by PatchLink to a master archive 567.

In some embodiments, the client agent 508 checks 332 an intranet-hosted update server to determine which updates are needed at the client in question. It reports gathered information, such as the current configuration 700, back to the update server, which creates the report matrix for the administrator. In some embodiments, the administrator specifies and approves patch deployment using a deployment wizard. Administrator-approved updates and packages are downloaded 312 in the background, thereby reducing inconvenience to users of the computers receiving the download, and then auto-installed according to a schedule set by the administrator. Administrator-defined rules can control the behavior of the patch install process.

One embodiment of the present invention provides a proactive service that enables administrators to have the embodiment automatically download 308, 312 and install 510 software packages and updates, such as critical operating system fixes and security patches.

A built-in security feature of some embodiments of the invention uses digital security identification. Before installing 520 a downloaded update on a target 500, this feature verifies the digital certificate, CRC check, compression, and encryption on each file or package. On the update server 528, access to administrative pages and other controls is restricted to authorized administrators. In some embodiments,

ForcePoint LLC
EX-1010-PT2
Page151

replication (downloading) of updates uses SSL and the embodiment checks the validity of downloads to the update server; if the SSL certificates do not properly identify a recognized source (e.g., PatchLink.com) then the download fails, and the server sends an email alert to the administrator. In some embodiments, all information in all downloads (master archive to update server, update server to target) is encrypted, CRC checked, compressed, digitally signed, and sent over 128-bit SSL connections only. In other embodiments, these elements are amended (e.g., 40-bit encryption) and/or omitted.

A patch signature 910 feature permits an embodiment to scan the target 500 and determine if the prerequisite(s) for each patch have been met, e.g., by having the agent check for the proper software version and the proper hardware drivers on the target. The patch signature and the patch fingerprinting features may each be used to make a detection report which is viewable in an enterprise report matrix. A workstation inventory feature uses a discovery agent 508 to pinpoint the needed software and hardware drivers for a target computer. The discovery agent may also scan the target for necessary signatures for fingerprints. PatchLink.com has a master archive which now hosts one of the largest automated patch Fingerprinted repositories in the world.

A background download 312 feature in some embodiments provides a secure background transfer service with built-in bandwidth throttling, so the network administrator can decide how the bandwidth should be utilized during large deployments. Some embodiments provide administrators with a configurable agent 508 policy which permits them to define the agent's communication interval and operating hours. For instance, an administrator may set the policy to roll out patches to production servers only between midnight and 2:00 am. In some cases, agents may have more than one policy active at a given time.

A chained installation feature allows an administrator to reduce or minimize repetitive rebooting by using the Microsoft Qchain.exe tool. If multiple updates which require multiple reboots are to be installed 510, the administrator can use the present invention's capabilities in conjunction with Qchain to deploy the updates with fewer reboots; in some cases only a single reboot will be needed. This reduction in reboots increases the uptime of mission critical computers 500 that are being updated.

ForcePoint LLC
EX-1010-PT2
Page152

Qchain rearranges the DLLs into an order that will put the latest update in effect. Administrators can choose this option during deployment.

Using a download resumption feature, an embodiment detects interruption 316 of a download, e.g., by a service outage. If the target 500 is a mobile workstation, the user can then simply disconnect it and reconnect it at a different location that is not out of service. If the update server can be accessed (via TCP/IP, for instance), the embodiment will resume its download 312 from at or near the point in the download at which it was interrupted, instead of starting again from the beginning to retransmit the entire package.

A mobile-user support feature allows administrators to deploy patches and software updates to target computers 500 which are not connected to the network when the deployment begins. When a mobile target subsequently connects to the network, the embodiment will automatically scan it and perform the necessary operations to bring that target up to date.

Embodiments feature client agents 508 which communicate with the update server 528 for secure downloads 312. Using agents also permits increased performance and scalability in enterprise-wide embodiments, permitting a single update server to service thousands of clients. The agents can work across firewalls 116, 214, and operate on any computer 500 with a TCP/IP (or other) connection to the enterprise network.

Some embodiments feature support for multi-vendor patches 554, which may also be referred to as "comprehensive patch scanning". The update server 528 is not limited to patches from a single vendor, but instead supports inventive management of patches from multiple vendors. For instance, the update server may coordinate with target agents to scan targets 500 for patch-related security vulnerabilities in software from Microsoft, IBM, Adobe, Corel, Symantec, McAfee, Compaq, WinZip, Citrix, Novell, and many others (marks of the respective companies). This provides a more secure network.

A grouping feature of some embodiments allows administrators to group selected target computers 500 into sets called, e.g., "containers" or "groups". Operations that are applicable to an individual target computer can then also be applied to containers/groups holding a proper subset of the possible target computers,

ForcePoint LLC
EX-1010-PT2
Page153

namely, to every target computer 500 (or every suitable target computer in view of patch signatures and fingerprints) belonging to the specified container. This feature facilitates administrator management of deployments, fingerprint reporting, inventory reporting, mandatory patch baseline policy, and/or client agent policies, depending on the embodiment. For instance, each container may have properties that specify its members, its client agent 508 policies, and its mandatory patch baseline policy. Administrators can select individual clients 500, previously-defined client groups, and/or user-defined groups for deployment. In some embodiments computers can be automatically grouped according to the patch(es) they require.

In some embodiments, the administrator can specify Group Managers and delegate limited administrative control to them. From the Group Manager perspective, the view and control of the inventive embodiment is then narrowed to cover only those computers 500 that have been assigned to the managed group by the administrator, all of which preferably use the same update server 528. The administrator can still view and otherwise manage all computers in the network, not merely those in a particular group.

A mandatory patch baseline policy feature in some embodiments permits an administrator to specify a minimal (baseline) configuration for one or more of a network's computers. The embodiment will proactively patch operating systems and/or applications to the organizational standards defined by the baseline policy. Supporting patch policies in an enterprise allows the administrator of an inventive embodiment to set patch policies for his/her company whereby no machine 500 in the company, for instance, can fall below a minimum patch level. For example, if mandatory patch baseline policy for a W2K group includes Microsoft Office 2000, Adobe Acrobat Reader 5.0, and Service Pack 2, then all computers placed in this group (whether placed initially on group definition, or placed later) will have at least those pieces of software installed on them.

A baseline for patches may be associated with a set of computers 500 that is defined by a group (e.g., a user-defined group or an administrator-defined group), or with a set of computers 500 that use a particular operating system (e.g., all W2K computers, regardless of user-or-administrator-defined groups), or with a set of computers 500 that use a particular application (e.g., all computers that use Microsoft

ForcePoint LLC
EX-1010-PT2
Page154

Office XP), or with some combination thereof. For example, in some embodiments the administrator could set a baseline policy rule stating that if Microsoft Office XP is installed then the system should automatically patch in Office XP Service Release 1.

When a mandatory patch baseline policy is used, patches 554 that are dropped (removed) from a target 500 by restoring software from a tape backup, mirrored image, or the like, will be automatically reinstalled after the agent 508 determines the new configuration and that configuration is compared 822 (by the client agent and/or the update server) with the baseline required by the policy. Baseline integrity is thus maintained by these embodiments.

A mandatory patch baseline policy can be used according to the invention to perform automated detection of unwanted software and removal of that unwanted software from target computers within a network. The mandatory deployment patch to be applied when unwanted software is detected would be to UNINSTALL the unwanted items. For example, one such patch would be "Uninstall KaZaA" which would detect and remove the KaZaA file sharing application from a corporate network, thereby reducing the risk that corporate employees violate copyright laws during the course of the business day, or that they consume all available network bandwidth for entertainment purposes. With government agencies and other large entities, eliminating popup software and other things that distract users from their assigned duties can be a high priority.

The invention also provides a feature that may be viewed as the logical opposite of mandatory patching to cure vulnerabilities in a network. This logical opposite, which may be termed the "Forbidden Patch" feature, is used to denote a service pack, hotfix or other software that must not ever be installed. Just as the mandatory patch feature is used to auto-fix a vulnerability, the forbidden patch feature is used to prevent the network administrator from installing software that can break an operational configuration. As an example, assume a company has a payroll system that doesn't work with the latest Microsoft Service Pack for Windows2000. If that Service Pack patch is ever deployed manually or automatically to the payroll server(s), the administrator needs to know at once; otherwise nobody gets paid at the end of the week. Some embodiments of the can scan for and detect the presence of "forbidden patches" and alert the administrator. They may also provide rules so that an

ForcePoint LLC
EX-1010-PT2
Page155

administrator does not inadvertently deploy a forbidden patch to a machine that should not have that patch installed, regardless of whether the applicable group patching policies say otherwise.

A patch compliance assurance feature in some embodiments provides administrators with the option of locking a set of patches 554 for a particular computer or a group of computers 500. That is, certain patches are required, but in a manner weaker than in the mandatory baseline feature. If an attempt is made to change target 500 configuration in a way that violates the patch requirement, an email alert message 824 is sent to the administrator. For example, several W2K computers may belong to an administrator-defined group of "IIS Servers" which is subject to patch compliance. For security, the embodiment accordingly locks down all operating system patches and all Internet Information Server patches. If at some later point such patches (including without limitation DLLs) are replaced, then the embodiment will send an email alert to the administrator identifying the computer 500 name and/or the modifications done to it. The newly non-compliant computer(s) and the reason(s) for non-compliance – a summary of discrepancies between their configuration and the locked configuration – can be identified. In some cases, this compliance feature may be used by administrators to identify users who install new software or remove existing software from their machine. Note that this compliance locking feature may be used by some embodiments in conjunction with the mandatory patch baseline feature, to automatically patch a target 500 that is non-compliant. When a locked patch or other software component is removed, it is then automatically reinstalled, and the administrator is notified 824 by email.

A service change feature in some embodiments allows administrators to lock down the services provided at client workstations (residing in a group or individually), and to then be informed if a user starts or stops a service item without directly contacting the administrator. As users change and/or attempt to change the status of services on a locked client 500, an email alert 824 is sent to the administrator identifying the computer and the (attempted) service changes.

A hardware change feature in some embodiments allows administrators to lock down the hardware configuration provided at client workstations 500 (e.g., in a group), and to then be informed if a user installs or removes a hardware item from

ForcePoint LLC
EX-1010-PT2
Page156

such a workstation without directly contacting the administrator. As users change (or attempt to change) the hardware configuration on a locked client, an email alert is sent 824 to the administrator identifying the computer and the (attempted) hardware changes.

An import/export feature facilitates the updating of computers on networks that are not connected to the Internet, such as highly secure military or government agency computers. Content is transported from the master archive to the target network's update server 528 using a means other than the Internet, such as physically transporting tapes, disks, or other storage media loaded with the content 554 at the master archive, with suitable physical security measures taken during transport. Once the media is accessible to the secure target network's update server 528, the built-in security measures discussed above (encryption, CRC, etc.) can be employed while transmitting the content from the transported media to local storage of that update server. Then that update server can finish updating 304 the secure network's target computers as previously discussed.

A recurring distribution feature in some embodiments facilitates distribution of data or documents 554 that are repeatedly updated, such as an enterprise employee directory or anti-virus definition/data file. One or more such data or document files can be deployed according to a recurring schedule specified by the administrator, to all targets 500, for instance, or to administrator-specified groups or a single target. Other steps, such as recurring server reboots, may also be specified in some cases.

A disaster recovery feature of some embodiments helps administrators recover from system failures such as hard disk crashes or server hardware failures. If an update server 528 fails, the administrator creates another server having the same DNS name as the failed server, and reinstalls the same update server software (with the same serial number if so required) on the new server. Archived, mirrored, or otherwise stored data files 600 used by the embodiment are restored to the new update server as needed. Then the target agents 508 will automatically connect with the new instance of the update server, and normal operations will resume after the target agents provide information (if any) that was lost by the server failure.

An automatic caching feature in some embodiments causes the update server 528 to automatically download and cache in its local update server storage patches

ForcePoint LLC
EX-1010-PT2
Page157

554 that are marked as critical, high-priority, and/or security-related. The update server notifies the administrator as to which patches are critical and which are cached, and scans for target computers 500 that need the patch. By contrast, non-critical patches may be cached at the update server only after they are first deployed. Caching the critical and security patches before their initial deployment provides target computers with a readily available source for the patch when the vendor whose software is vulnerable may be overwhelmed by patch requests. During Code Red and Nimda virus attacks, for instance, some users had to wait hours for a connection to the Microsoft web site to get the patches, because of the extremely heavy demand for them. Proactively caching critical and security patches at an inventive update server 528 reduces the risk that operation of target computers 500 will be interrupted or compromised due to a lack of such patches.

Some embodiments have an intelligent multiple patch deployment feature, which matches patches 554 with operating systems, thereby relieving administrators of the need to expressly and fully identify the operating system used on each target computer. For example, assume Microsoft issued a bulletin for its operating systems which specifies different patches 554 for several different operating system platforms. Administrators using this inventive embodiment need only select "Microsoft operating system" for deployment; they can specify target computers 500 regardless of differences in the operating system details of various specified targets. The embodiment compares 820 patch and operating system requirements for compatibility and for the need for a patch, to ensure that the proper patch gets installed on a given target. Thus, the patch for the Microsoft Windows 98 platform will be installed on a target computer that runs the Windows 98 operating system, the patch for the Microsoft NT platform will be installed on a target computer that runs the NT operating system, and so on. This feature speeds up patch deployment by freeing administrators from the need to manually match patches with targets according to the operating systems (or operating system versions, including prior patches) that are involved.

Another feature helps detect applicable patches 554 and manage patch inter-dependencies, thereby helping administrators avoid manually sorting through dozens (or even hundreds) of generally unrelated patches. Instead, the embodiment identifies

ForcePoint LLC
EX-1010-PT2
Page158

applicable patches using their metadata, fingerprint, and/or signature data, based on factors such as the operating system involved, the presence (or absence) of other patches, the interdependency of different patches (identifying which patches rely on which other patches to work properly), and the mandatory patch baseline policy (if any). Then the administrator is shown which patches are applicable for the target(s) 500 in question. For example, one embodiment shows IIS patches to administrators only if IIS is installed on a target computer. If used consistently, this feature helps ensure that when a patch is deployed toward a target, that target has the application in question and the patch will install on that target.

As an example of patch interdependencies, on a Microsoft W2K platform one embodiment will recommend Service Pack 2 to the administrator, and once Service Pack 2 is installed it will then recommend a Security Rollup patch, which depends on Service Pack 2. The embodiment reads both the registry and the file information to correctly perform fingerprinting to validate patch 554 identification.

Some embodiments allow an administrator to review a history or log of recent operations, and to also uninstall a patch 554 or portion thereof, and rollback effects of deploying the patch to the network. This allows the administrator to undo a patch installation that has caused problems. Lost user data will not necessarily be recovered, but the usual steps taken by a conventional uninstaller can be taken using a restorer 514, such as deleting a DLL, removing a registry entry, restoring a path or other system variable value, and so forth. In addition, the configuration status particular to the embodiment, such as signatures, fingerprints, alerts, and reports, is updated to reflect the problems encountered and/or the removal of the patch. The administrator can also be notified if the removed patch appears in a patch dependency and/or in the mandatory patch baseline.

Some embodiments have a "directory-neutral" feature, meaning that they are platform neutral and do not require a directory such as Novell's NDS directory or Microsoft's Active Directory product in order to operate. However, some embodiments can integrate with and cooperate with such directories in particular organizations.

Some embodiments operate according to a selective patch feature, under which patches 554 are not automatically installed unless they are required to meet the

ForcePoint LLC
EX-1010-PT2
Page159

mandatory patch baseline policy. In some, patches marked as critical and/or security patches are also installed automatically. In such embodiments, other patches are not installed until they administrator selects them and expressly authorizes their installation; this permits administrators to test patches internally within their organization before installing them on the organization's computers. Once the patch is adequately tested, it can be added to the mandatory patch baseline for the group of targets 500 in question, so that it will be automatically installed when needed.

Some embodiments support a security policy patch 554 that prevents applications from running on a target machine 500. This provides a policy-driven way to hook into the target computer's file system and stop a particular file (or multiple files) from executing. This could be implemented by patches that rename the executable/DLL file(s) in question and substitute in place thereof code that does nothing, or code that displays an error message to the user, and/or code that notifies the administrator by email.

Operation of inventive embodiments may be further understood by considering the following example scenarios. In one scenario, as new patches 554 are released by their respective vendors, an update server 528 downloads the corresponding fingerprints from a master archive 567. The embodiment then checks to see if any target computers 500 meet the profile (need the patch in question) by sending the patch's fingerprint to targets for scanning by agents 508. The administrator is notified of the new patch and its potential impact on the network, and a report matrix informs the administrator which targets need the patch and which do not. The administrator selects one or more individual target computers and/or groups, and authorizes deployment. Deployment proceeds as discussed herein. The administrator may set the time of deployment, and decide whether to reboot after the installation.

In a managed data center scenario, the center's administrator creates a patch group from each cluster of data servers. The administrator can test critical updates received from a master archive 567, and then deploy tested patches 554 on network targets, either all at once, or in stages to groups. Agent policies can help the administrator specify the hours of operation for each group.

ForcePoint LLC
EX-1010-PT2
Page160

In an embodiment update scenario, the software used by the embodiment is updated by using the embodiment. That is, when a vendor (such as PatchLink.com) provides patches 554 to the software for target agents 508, update servers 528, and/or other embodiment software, those patches can be deployed as discussed herein, using the inventive tools and techniques that would more often be used to deploy patches to operating systems or user applications. For instance, an administrator can select a PatchLink HotFix client patch and deploy it to update client agent software. Client agents may be initially deployed by pushing them to all target computers.

Implementation notes

Additional details regarding particular embodiments are provided below. These implementation details are provided in order to err -- if errors are made -- by including too much information rather than including too little. Applicants should not be penalized for being so forthcoming. In particular, the inclusion of details should not be viewed as an assumption or admission that those details, or similar details, or a similar level of detail, are actually required to support the claims ultimately granted. Nor should the inclusion of particular implementation details be misinterpreted by treating as inventors people who simply implemented inventive ideas conceived by others.

Agents

- Microsoft Windows Agents
- NetWare Agent
- Linux Agent
- Java Agent

Package Construction / Package Maintenance

An administrator uses this module to create a package for distribution through the designated Update agents. This package can be a file distribution or a software package, allowing for more flexibility when updating existing installed software, installing new software, file-replication, etc. throughout the designated managed machines.

Below are the steps for proper package creation:

ForcePoint LLC
EX-1010-PT2
Page161

1. Enter the Package Specifications

- Package Name – Labels the package throughout the updating process.
- Package Type – When Software Package is selected in the Software Package routines, after the source files for the package are placed in their proper destination sequence, the administrator may immediately finish the package creation (using pre-designated default values for the rest of the options). File Distribution requires the administrator to complete all steps in the package creation routine.
- Operating System - Choose the Operating Systems to which the package can be rolled out. Currently, you may select one operating system per package. These include: Linux , NetWare, Windows 2000/NT, Windows NT, Windows 95/98/ME
- (Optional) Import – Imports a previously exported package. This option is useful for creating the same package for multiple operating systems.

2. Add the Source

- Add File – Adds a file from your local workstation or network location that is reachable.
- Add Dir – Adds a directory from your local workstation or network location that is reachable.
- Add URL – Adds a remote file to the package via well-known protocols. The various types of URLs you can add are: Local File – File://, FTP – ftp://, HTTP – http://, Secure HTTP – https://, Anything else you choose as long as the agent recognizes the protocol (this field is editable).
- Remove – Removes a file from the package.
- Properties – Shows the details of how each file is stored within the update server. Also allows for multiple sources in case one source is busy or slow (due to net lag for example). The agent automatically tries the other sources.
- Import File – Imports a specific list of files from a previously exported package.

ForcePoint LLC
EX-1010-PT2
Page162

3. Add the Destination

- Target Computer – A hierarchical tree view of the package file destination. The various default directories shown depend on the operating system for which this package is targeted. The package always displays in the same directory path from which the source files were originally imported (see Step 2). To move the files around simply highlight the directory or file and drag it to its new location.
- Properties – If the directory where the files should install is not displayed, highlight a file and click the Properties button. This displays the base information of where the source file is coming from and an entry field for the destination. Type the new location and click OK and your changes are shown (this may take a while because the paths are reconnected for large package file numbers).
- Export File – Exports a base package to a file (source and destination information) for use later in an import function.

4. Dependencies

- Left Column – A list of existing packages that are ready for rollout (operating system dependent). For example, if you have a Java-based package that must be rolled out to numerous computers, you would select the specific JDK package as your dependency so that the JDK is installed prior to the current package.
- Right Column – The packages placed here (by using the arrow buttons) are the dependencies for your package. Use the + and – buttons to arrange the dependencies in order of importance (most important being the first dependency). Dependencies are processed before your package.
- Asset – If the dependencies are not found the package fails to install. For example, if a Microsoft Office 2000 SR1 package is created, its Asset dependency is Microsoft Office 2000 which must already be installed.
- Install – If the dependencies are not found, install them prior to installing the current package. Using the above example, if MS Office 2000 is not found, it is installed prior to installing the SR1 package.

ForcePoint LLC
EX-1010-PT2
Page163

5. Package Settings

- Backup – Backs up any existing package files found on the destination machines. The editable pull-down list contains the most common directories for the operating system in question. If your directory is not found just type it into the list.
- Confidence Level – The default for all new packages is New. The Confidence Level indicates that this package was tested and its performance has determined its confidence level.
- Availability – The default is Available which indicates the package is available for rollouts. Not Available indicates this created package is unavailable for a rollout.

6. Scripts

- There are three types of package scripts you can use: Command Line – The contents of this script are executed as a standard command line. This script is sent after the files are copied to their destinations. Pre-Script – The contents of this script are executed prior to the files being copied onto the machine. Post-Script – The contents of this script are executed after the files are copied onto the machine.

7. System Settings

- Language – Select the languages for which the package is available. The agent then checks that the language is on the machine and that the package matches before the package is installed.
- Processor Type – Select the processor for which the package is available. The agent then checks that the processor is on the machine and that the package matches before the package is installed.

8. Finish – Click Finish to upload the files and assemble the package. When the assembly process ends the button changes from Finish to Done. Click Done to complete the package creation function.

Define a Group / Modify a Group

This module lets an administrator group machines together, making the rollout procedures easier so that a rollout is as easy for one machine as it is for 500 machines.

ForcePoint LLC
EX-1010-PT2
Page164

Additionally, an administrator might group machines according to their function or location to make bandwidth utilization more efficient for their network.

1. Group Name – The label designation for the group.
2. Machine List – Select all the machines this group will include. A machine shows up only after the update agent is installed and registered.
3. Finish – After the machines are placed in the group, the Finish button changes to Done. Click Done to complete the group function.

Schedule a Rollout / View Existing Rollouts

The rollout schedule defines the date and time the packages are made available to the designated machines.

1. Choose a Package
   - Package Selection List – Choose a package (only one at this time) to install.
2. Choose Machines
   - Add a Group – This button displays a dialog box showing a list of the available groups. Highlight the groups you wish to deploy then click the OK button.
   - Remove a Group – Highlight the groups you do not want the package rolled out to, then click the Remove a Group button.
   - Add a Machine – This button displays a dialog box showing a list of available machines (with registered update agents on them). Highlight the machines to add then click the OK button.
   - Remove a Machine – Highlight the machines you do not want the package rolled out to, then click the Remove a Machine button.
   - Rollback – Removes the package just installed and returns the backup (if one was designated). This option is available only via View Existing Rollouts.
   - Reapply – Re-installs the package.

ForcePoint LLC
EX-1010-PT2
Page165

3. Choose a Rollout Date and Time
   - Calendar – Choose the date for the rollout installation to occur.
   - Time – The time on the server when the package is to be rolled out.
4. Choose Bandwidth and Sequencing
   - Bandwidth – This level determines how much bandwidth on the server downloading of the package will utilize. The minimum value is 30 % and the maximum is 100%.
   - Sequencing – Selecting YES (default value) causes the rollout to go machine by machine throughout the entire rollout process and finish after the last machine is done. If an error occurs anywhere in the rollout process the rollout stops. Selecting NO causes the rollout to install the package on all machines. If an error occurs on one machine, it does not affect the package rollout on another machine.
5. Finish – The rollout is created or updated and is saved after clicking the Done button.

Agent requests will be in the form of HTML Forms using the POST method. Host responses will be well-formed XML 1.0 documents. Most of the returned documents are of such simple structure, a DTD, NameSpace, or Schema will not be included, but they will be syntactically and structurally in compliance with the XML specification. All dates and times are normalized to Coordinated Universal Time (GMT).

This describes the transaction or data flow between the Agent, the requestor, and the Host, the Update Service. All Update transactions will be initiated by the Agent, except for the case where the Host will open, send the agent ID and then close an agreed upon port and protocol at the Agent's IP address to effectively 'Ping' or notify the Agent that it should request a list of work from the host regardless of its request schedule.

ForcePoint LLC
EX-1010-PT2
Page166

First Contact:

Any Agent needing to converse with the update server 528 service, will always make a request to the designated master site for the /update subdirectory. This subdirectory will be configured to return a '302 Object Moved' and its 'new' location.

As demonstrated in the following example, the agent performs a 'HEAD' request on the /update subdirectory of the www.patchlink.com site.

Head Request:
HEAD /update http/1.1

The Host responds that the object is moved, and the new location can be found at the address provided by the Location: header

InstallShield Agent Registration:

During the physical installation of the 'update agent', the Administrator will be required to enter some information before the agent is installed. The Admin will be required to enter the Host Name or IP Address, the Account Identifier, a GUID (Globally Unique Identifier), and the User Name and Password that was specified when registering. This data will be sent to the host to validate the ability to install the agent software, and to generate an ID for the agent.

Agent TaskList

Once InstallShield has successfully installed the BootStrap Agent software on the computer, it's time for the agent to start working. After the agent resolves the update server 528 host site address, it posts a 'TaskList' request. A 'TaskList' is a simple list of 'Task' items the Admin has scheduled for the Agent to perform.

ForcePoint LLC
EX-1010-PT2
Page167

The BootStrap Agent must be able to:

1. Request the initial TaskList.
2. Receive the initial TaskList.
3. Understand the initial TaskList.
4. Download the Full Agent's install file.
5. Run the Agent Install.
6. Report any install problems, if so, continue as instructed
7. Start the full Agent.
8. Poll for new TaskLists
9. Understand SoftPkg IDs and dependencies and download them.
10. Initial "Action Scripts" either by invoking an external Script Engine or by invoking the Script Engine from within the Agent.

The Agent making the initial TaskList request and processing the returned response accomplishes this. For example:

TaskList Request

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: 32

Action=TaskList
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=0.0
&LocalTime=20000628010100
&Status=0

In this request, the Agent's Version is 0.0. This indicates to the host that this is a new installation of the agent and that the host should prepare a 'Task' for the agent that downloads the latest versions of the appropriate agent software. In the following

ForcePoint LLC
EX-1010-PT2
Page168

response, this is shown as the first 'Task' - TaskID="C1D50120-FF13-11d3-95B5-000629526438".

Whenever there has been a change to the Agent's policy, the host will include the policy data in the **'TaskList'** – since this is the initial request from the agent, the policy data is included in this response.

LocalTime is just that the Local time (NOT GMT). This allows the server to know exactly what time it is on the Agent machine. Format is in YYYYMMDDHHMMSS.

Status tells the tasklist processor to just return a simple yes or no status if there are tasks to be done.
Status=0 means to return a normal task list. Status=1 means tell the agent if you have tasks to be done. This allows the agent to come in non-SSL and do a quick check.

Agent Soft Package Request

The first task indicates there is a module to be installed. As shown below, the agent requests the detailed installation information from the host:

Soft Package Request

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: nnnn

Action= SOFTPKG
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=0.0
&TaskID=C1D50120-FF13-11d3-95B5-000629526438

ForcePoint LLC
EX-1010-PT2
Page169

&PkgID=12340000-1111-0000-0000-000000000000
&LocalTime=20000628010100

Note that in this instance, the Agent's version is 0.0. This indicates to the host that the package to update the Agent software should be included in the TaskList response. This allows the host to dynamically determine when there is a newer version of the agent software that is available and directs the agent to update itself.

The host puts together an "Open Software Distribution" document that details the information the agent will need to be able to complete the task:

LocalTime is just that the Local time (NOT GMT). This allows the server to know exactly what time it is on the Agent machine. Format is in YYYYMMDDHHMMSS.

Soft Package (All elements)

A soft package showing all the possible XML components (shows backup).

```
<?xml version="1.0"?>
<!DOCTYPE SOFTPKG SYSTEM
"http://msdn.microsoft.com/standards/osd/osd.dtd">
<SOFTPKG  xmlns:GX="http://www.patchlink.com/standards/osd/update.dtd"
        GX:TaskID="C1D50120-FF13-11d3-95B5-000629526438"
        GX:PkgID="12340000-1111-0000-0000-000000000000"
        Name="12340000-1111-0000-0000-000000000000"
        GX:ReInstall="N" GX:RollBack="N">
  <TITLE>Windows NT update agent</TITLE>
  <IMPLEMENTATION>
    <OS VALUE="win2k"/>
    <OS VALUE="win98"/>
    <DISKSIZE Value="123456"/>
    <CODEBASE>
```


ForcePoint LLC
EX-1010-PT2
Page170

<GX:DIR ModuleID="00000104-0000-0000-0000-000000000000">
<GX:Destination>
<GX:URI DateTime="20000415010100">
<GX:URL>FILE://%TEMP%/</GX:URL>
<GX:ACL Attrib="RWXHSMA Name="$OTHER"/>
<GX:ACL Attrib="RWXHSMA" Group="$GROUP"/>
<GX:ACL Attrib="RWXHSMA" Name="$USER"/>
</GX:URI>
</GX:Destination>
</GX:DIR >
<GX:FILE Expand="N" Overwrite="Y" ModuleID="00000100-0000-0000-0000-000000000000">

Soft Package Status – Success

The return codes RC and SoftPkgRC are in decimal format. SoftPkgRC denotes the overall completion of the package. Some modules could have been successful (RC=0) but another may have caused the error. If a rollout is attempted with a package that has already been install once then the agent will return (RC=0) for all the modules it installed and return (SoftPkgRC=725003) or 0x000b100b Soft Package already installed.

Upon completion of the task, the agent will update the host with the results:

Request

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: nnn

Action=Status
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&TaskID=C1D50120-FF13-11d3-95B5-000629526438

ForcePoint LLC
EX-1010-PT2
Page171

&PKGID=12340000-1111-0000-0000-000000000000
&InstallDate=20000101123456
&SoftPkgRC=0
&SoftPkgRCMsg=Success
&ModuleID=00000100-0000-0000-0000-000000000000
&RC=0
&RCMsg=Success

File Attributes and ACL's

This part describes the GX:ACL element found in GX:Destination (GX:URI) element. The attributes in Update are supplied in to the agent in the Super set form defined below.

The problem with doing basic file attributes is that some file systems blur the boundary between Attributes and ACL's. An attribute is the basic ACL of a file and what is defined here is a small cross platform superset. For instance, Windows NTFS has the Read Only attribute flag but it also has the Read ACL. Therefore, if we are going to make generic attribute flags, then we must expect the meaning to be altered somewhat when used as ACL's. Those on the Unix platform will see no difference, except that like other platforms, you would ignore flags that you do not understand or no defined behavior is listed here.

Three default ACL's are defined and act like basic file attributes; $OTHER, $GROUP, $USER.
On Unix the file system all three of these attribute ACL's would use. However, NT, FAT and NetWare would use only $ OTHER for basic file attributes. Any other names in the ACL's element.data will be construed as a name

ForcePoint LLC
EX-1010-PT2
Page172

ACL and Attribute flags

Letter	Short	Definition
R	Read	Display the file's data, attributes, owner, and permissions
W	Write	Write to the file, append to the file.
X	Execute	Run the file (if it's a program or has a program associated with it for which you have the necessary permissions)
H	Hidden	Hidden file
S	System	System file
M	Modify	Read, write, modify, execute, and change the file's attributes.
A	Archive	File is ready for Archive

The XML syntax:

This denotes an ACL for a User

<GX:ACL Attrib="RWXHSMA" Name="UserName"/>

ACL for a Group. Note that $GROUP will always use Group=

<GX:ACL Attrib="RWXHSMA" Group="GroupName"/>

Soft Package - Rollback

HTTP/1.1 200 OK
Connection: close
Content-Type: text/xml
Content-Length: nnn

ForcePoint LLC
EX-1010-PT2
Page173

```
<?xml version="1.0"?>
<!DOCTYPE SOFTPKG SYSTEM
"http://msdn.microsoft.com/standards/osd/osd.dtd">
<SOFTPKG  xmlns:GX="http://www.patchlink.com/standards/osd/update.dtd"
        GX:TaskID="C1D50120-FF13-11d3-95B5-000629526438"
        GX:PkgID="12340000-1111-0000-0000-000000000000"
        Name="12340000-1111-0000-0000-000000000000"
        GX:ReInstall="N" GX:RollBack="Y">
 <TITLE>Windows NT update agent</TITLE>
 <IMPLEMENTATION>
  <DISKSIZE Value="432"/>
  <CODEBASE>
   <GX:FILE Expand="N" Overwrite="Y" ModuleID="00000100-0000-0000-0000-
000000000000">
    <GX:Destination>
     <GX:URI>
      <GX:URL>FILE://%TEMP%/</GX:URL>
      <GX:FILENAME>HelloWorld.txt</GX:FILENAME>
     </GX:URI>
    </GX:Destination>
    <GX:Backup>
     <GX:URI>
      <GX:URL>FILE://%TEMP%/Backup</GX:URL>
     </GX:URI>
    </GX: Backup >
   </GX:FILE>
  </CODEBASE>
 </IMPLEMENTATION>
</SOFTPKG>
```


ForcePoint LLC
EX-1010-PT2
Page174

This example rolls back the simple file copy with backup shown above. The agent denotes a rollback from the attribute GX:Rollback="Y" in the SOFTPKG element tag. The GX:Source element tags are not supplied.

The destination MUST contain a filename to restore the backup to. (Note: it is not an error if the backup files do not exist prior to rollback (the destination may not have existed when the package was distributed). It is however, an error if the destination files exists and cannot be deleted prior to the rollback.)

ProxyGet

Sometimes an agent may be installed behind a firewall in such a configuration that the agent is only allowed access to the host site. The agent will detect this case when it tries to retrieve a module for a package that is on the vendor's site. When the agent realizes that it cannot establish communications with a standard HTTP get, it can ask the host to retrieve the file on the agent's behalf by using a 'ProxyGet' request – as described below:

Request

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: nnn

Action=ProxyGet
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&URL=http://www.Microsoft.com/hotfix/Q12345.exe

ForcePoint LLC
EX-1010-PT2
Page175

ProxyGetStatus

Request

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: nnn

Action=ProxyGetStatus
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&RefID=107045CF06E011D28D6D00C04F8EF8E0

GetRequest

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: nnn

Action=Get
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&RefID=107045CF06E011D28D6D00C04F8EF8E0

HTTP Get

Request:

GET /download/Q12345.EXE http/1.1

ForcePoint LLC
EX-1010-PT2
Page176

Bandwidth Utilization

Range specified Get Request:

HTTP/1.1 allows a client to request that only part (a range of) the response entity be included within the response. HTTP/1.1 uses range units in the Range and Content-Range header fields. An entity may be broken down into subranges according to various structural units.

range-unit = bytes-unit | other-range-unit

bytes-unit = "bytes"

other-range-unit = token

The only range unit defined by HTTP/1.1 is "bytes". HTTP/1.1 implementations may ignore ranges specified using other units. HTTP/1.1 has been designed to allow implementations of applications that do not depend on knowledge of ranges.

Since all HTTP entities are represented in HTTP messages as sequences of bytes, the concept of a byte range is meaningful for any HTTP entity.

Byte range specifications in HTTP apply to the sequence of bytes in the entity-body (not necessarily the same as the message-body). A byte range operation may specify a single range of bytes, or a set of ranges within a single entity.

When the administrator has selected Bandwidth Utilization features, by specifying them in the agent's policy data, the agent will make 'Range' specified Get requests rather than simple Get requests.

Consider the following Agent Profile:

ForcePoint LLC
EX-1010-PT2
Page177

<Policy IntervalType="S" Interval="60" Start="000000" End="060000"
Retries="3" BackOff="10%" AlwaysUseProxyGet="Y"
FailAction="Stop" UDPPort="1234" TCPPort="1234"
KeepAliveConns="Y"
DownloadRestartable="Y" DownloadChunkSize="1024"
DownloadWaitSchedule="S" DownloadWaitInterval="10"/>

The following shows a request for the first 1024 bytes of the Q12345.Exe file, and the host's response:

Request:

GET /download/Q12345.EXE http/1.1
Range: bytes=0-1023

ProxyGet Request:

POST ***server_object_returned_in_firstcontact*** http/1.1
Content-Type: text/html
Content-Length: nnn

Action=Get
&AccountID=AF011203-7A09-4b67-A38E-1CB8D8702A50
&AgentID=D7292F2D-CCFE-46dc-B036-3B318C2952E3
&AgentVer=2.0
&RefID=107045CF06E011D28D6D00C04F8EF8E0
&RangeBytes=0-1023

ForcePoint LLC
EX-1010-PT2
Page178

Response XML Elements

Element	**POLICY**
Attributes	**IntervalType** – type of time period. • S=Seconds • M=Minutes • H=Hours **Interval** – Number of time periods that agent should check host for Tasklist. **Start** – The time of day the agent should start running and checking for work to do (GMT). **Stop** – The time of day the agent should stop running and checking for work to do (GMT). **Retries** – The number of times to retry a request before applying the Backoff amount. **BackOff** – the amount of IntervalType time to added to the Interval after a failed contact with the host. This may be expressed as a percentage by appending the percent sign (%). **UDPPort**– {nnn} UDP port number used to wake up the Agent. **TCPPort**– {nnn} TCP port number used to wake up the Agent. **TraceLevel** – OFF = 0, INFO = 1, DETAILED = 2, DEBUG = 3 **PurgeIntervalType** – type of time period (see IntervalType) **PurgeInterval** – Number of time periods (PurgeIntervalType) that the agent should scan backups and purge those with a time older than the purge interval.
Child of	TASKLIST
Parent of	

ForcePoint LLC
EX-1010-PT2
Page179

Element	**TASK**
Attributes	**TaskID** – unique task identifier. **PkgID** – The package identifier to be acted upon.
Child of	TASTLISK
Parent of	

Discovery Agent XML tags

<name> tag - This is the name of the file you want to search for.

- <path> tag - Very versatile. This is the path you want to search for the file in.

<Version> tag - This is the version of the file you are looking for.

<created> tag - This is the date the file was created.

Example <version> > 5/30/2001 12:01:04 PM </version>

Note: This exact date format is preferred.

<Size> tag - This is the size of the file you are looking for. Note: Cannot due < or >

<root> tag - This is the root key to look for the registry entry in.

<Key> tag - This is the key in the registry you are looking for.

<value> tag - this is the value in the key you are looking for.

<Data> tag - this is the data you expecting to find in that key.

<class> tag - You can specify any valid WMI class that makes sense. example win32_services

ForcePoint LLC
EX-1010-PT2
Page180

<searchfield> - This is the field that will best determine what wmi entries to look at.

<searchvalue> - This is the value that will best determine what wmi entries to look at.

<checkfield> - This is the field to look in to get the value you are expecting to get.

<checkvalue> - This is the value you are expecting to find.

Example of the <registry> section of the input file.

```
<registry componentid="" reportID="">
    <root> </root>
    <key> </key>
    <value> </value>
    <data> </data>
</registry>
```

Patch Fingerprint Signature example

```
<report reportid="22">
    <file componentid="1" reportID="1">
        <name>outlook.exe</name>
        <path></path>
        <version></version>
        <created></created>
        <size>57393</size>
        <root>HKEY_LOCAL_MACHINE</root>
        <Key>SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\OUTLOOK.EXE</key>
        <value>Path</value>
    </file>
</report>
```


ForcePoint LLC
EX-1010-PT2
Page181

The Above example will find the outlook Path from the registry and then will validate its size.

Summary

The invention provides systems, methods, and configured storage media for assuring that software updates are needed, and that the computers have the necessary software and hardware components, then updating the software across a network with little or no need for human oversight, without requiring copies of the software patches on an administrative machine on the network whose clients are being updated, and which removes the updates from the affected machines, leaving them in a usable state when a problem is discovered during installation or after installation with an installed patch.

As used herein, terms such as "a" and "the" and item designations such as "update server" are inclusive of one or more of the indicated item. In particular, in the claims a reference to an item means at least one such item is required. When exactly one item is intended, this document will state that requirement expressly.

The invention may be embodied in other specific forms without departing from its essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. Headings are for convenience only. The claims are part of the specification which describes the invention. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by patent is:

ForcePoint LLC
EX-1010-PT2
Page182

CLAIMS

1. An automated method for updating software in a system having a first target computer in a non-update state connected across a network to an update server in a pre-update state, the system also having a package computer which may be inaccessible to the first target computer and is accessible to the update server, and a repository component accessible to the first target computer and the update server, the method comprising the steps of:

putting at least one patch fingerprint which defines a specific software update into the repository component;

gathering information about the first target computer;

comparing at least a portion of the gathered information with the patch fingerprint to determine if the specific software update is absent from the target computer;

placing at least one task identifier on an update task list, the task identifier specifying the first target computer, the task identifier also specifying at least one download address which references a location on the package computer that contains a software update for the first target computer;

in response to the task identifier, downloading the software update from the package computer to the update server; and

performing a second download of the software update from the update server to the first target computer.

2. The method of claim 1, further comprising the step of providing a patch definition file which is portable and which can be employed to replicate a patch on update servers in a plurality of networks.

3. The method of claim 1, wherein the method operates proactively by performing the download steps without requiring an express administrator command to perform them.

ForcePoint LLC
EX-1010-PT2
Page183

4. The method of claim 1, wherein the method operates proactively by caching a marked patch at the update server before deploying the patch to target computers, the patch marked as at least one of critical, high-priority, and security-related.

5. The method of claim 1, further comprising at least two steps from the following group of security steps: utilizing encryption to secure patch downloads; utilizing cyclic redundancy codes to secure patch downloads; utilizing digital signatures to secure patch downloads; utilizing a secure network protocol such as SSL to secure patch downloads, wherein at least one of the security steps is available in the particular method embodiment.

6. The method of claim 1, wherein the step of downloading the software update from the update server to the first target computer is performed using a background downloading process, thereby reducing inconvenience to a user of the first target computer.

7. The method of claim 1, wherein the step of downloading the software update from the update server to the first target computer is performed using bandwidth-throttled downloading, thereby allowing a network administrator to decide how bandwidth should be employed during a large deployment.

8. The method of claim 1, wherein downloading is performed subject to a policy which limits the hours of operation, and the policy is set by an administrator, thereby allowing the administrator to decide when patch deployments are allowed to occur.

9. The method of claim 1, further comprising preventing downloads of software updates from the update server to the package computer, thereby enhancing security of the package computer.

10. The method of claim 1, wherein the method further comprises use of a chained installation feature permitting an administrator to have downloaded patches installed on the target computer with fewer reboots than would otherwise be required.

ForcePoint LLC
EX-1010-PT2
Page184

11. The method of claim 1, wherein the method further comprises use of a download resumption feature which detects interruption of a downloading step and then after a reconnection resumes the downloading step from at or near the point in that downloading step at which the interruption occurred, thereby avoiding repetition of the entire downloading step to achieve the download.

12. The method of claim 1, wherein the method further comprises use of a mobile-user support feature which allows an administrator to deploy a patch to the first target computer even though the first target computer is not connected to the network when the task identifier placing step occurs.

13. The method of claim 1, wherein the method comprises downloading multiple patches which originated from multiple vendors.

14. The method of claim 1, wherein the method further comprises the step of grouping a proper subset of target computers to form a group, whereby an operation that is applicable to an individual target computer can also be applied to the group.

15. The method of claim 14, wherein the grouping step forms a group containing target computers that are specified by an administrator.

16. The method of claim 14, wherein the grouping step forms a group containing target computers that are specified by a non-administrative user.

17. The method of claim 14, wherein the grouping step forms a group containing target computers that are specified by identifying an operating system that is used by all of the target computers which are being placed in the group.

18. The method of claim 14, wherein the grouping step forms a group containing target computers that are specified by identifying an application program that is used by all of the target computers which are being placed in the group.

ForcePoint LLC
EX-1010-PT2
Page185

19. The method of claim 14, wherein the method further comprises the step of delegating limited administrative control to a group manager, whereby the group manager receives control over only those target computers that were placed in the group by the grouping step.

20. The method of claim 1, wherein the method further comprises use of a mandatory patch baseline policy which specifies at least in part software that should be installed on the first target computer, and the method proactively downloads and installs on the first target computer a patch that is specified in the mandatory patch baseline policy.

21. The method of claim 20, wherein the mandatory patch baseline policy sets a baseline for target computers that use a particular application.

22. The method of claim 20, wherein the mandatory patch baseline policy mandates removal of unwanted software from a target computer.

23. The method of claim 1, wherein the method further comprises use of a forbidden patch feature which specifies software that should not be installed on the first target computer, and the method attempts to prevent such installation from occurring.

24. The method of claim 20, wherein the method further comprises automatically reinstalling a patch that is specified in the mandatory patch baseline policy after software in the patch was dropped from a target computer that is subject to the mandatory patch baseline policy.

25. The method of claim 1, wherein the method further comprises the steps of grouping a proper subset of target computers to form a group, and using a mandatory patch baseline policy to specify at least in part software that should be installed on the target computers in the group.

ForcePoint LLC
EX-1010-PT2
Page186

26. The method of claim 1, wherein the method further comprises use of a patch compliance assurance feature which specifies software that is locked on the first target computer, and the method proactively notifies an administrator if locked software is removed from the first target computer.

27. The method of claim 1, wherein the method further comprises use of a change control feature which specifies at least one item that is locked on the target computer, and the method proactively notifies an administrator if a locked item is changed on the target computer, wherein the item is at least one of: a hardware item, a service item, and a software item.

28. The method of claim 1, wherein at least the step of downloading the software update from the update server to the first target computer recurs, thereby repeatedly updating a particular file on at least the first target computer.

29. The method of claim 1, further comprising at least one step from a group of disaster recovery steps, the step helping an administrator recover and continue operation after a system failure, wherein the group of disaster recovery steps comprises: creating another server with the same domain name as a failed server, reinstalling update server software on a server, restoring archived data, and restoring mirrored data, and wherein at least one of the disaster recovery steps is available in the particular method embodiment.

30. The method of claim 1, further comprising the steps of maintaining a record of recent operations, and rolling back deployment of a patch, thereby allowing an administrator to undo a target computer patch installation that has caused problems.

31. The method of claim 1, wherein the method further comprises use of a intelligent multiple patch deployment feature which matches patches with target computer operating systems, thereby relieving an administrator of the need to expressly and fully identify the operating system used on the target computer.

ForcePoint LLC
EX-1010-PT2
Page187

32. The method of claim 1, wherein the method installs a security patch on the first target computer, thereby providing an administrator with a policy-driven way to hook into the target computer's file system and stop at least one particular file from executing on the target computer.

33. A configured program storage medium having a configuration that represents data and instructions which will cause at least a portion of a computer system to perform method steps of an automated method for updating software in the system, the system having a first target computer in a non-update state connected across a network to an update server in a pre-update state, the system also having a package computer which is inaccessible to the first target computer and is accessible to the update server, and a repository component accessible to the first target computer and the update server, the method comprising the steps of:

putting at least one patch fingerprint which defines a specific software update into the repository component;

gathering information about the first target computer;

comparing at least a portion of the gathered information with the patch fingerprint to determine if the specific software update is absent from the target computer;

placing at least one task identifier on an update task list, the task identifier specifying the first target computer, the task identifier also specifying at least one download address which references a location on the package computer that contains a software update for the first target computer;

in response to the task identifier, downloading the software update from the package computer to the update server; and

performing a second download of the software update from the update server to the first target computer.

34. The configured storage medium of claim 33, wherein the method further comprises the step of providing a patch definition file which is portable and which can be employed to replicate a patch on update servers in a plurality of networks.

ForcePoint LLC
EX-1010-PT2
Page188

35. The configured storage medium of claim 33, wherein the method operates proactively by performing the download steps without requiring an express administrator command to perform them.

36. The configured storage medium of claim 33, wherein the method operates proactively by caching a marked patch at the update server before deploying the patch to target computers, the patch marked as at least one of critical, high-priority, and security-related.

37. The configured storage medium of claim 33, wherein the method further comprises at least two steps from the following group of security steps: utilizing encryption to secure patch downloads; utilizing cyclic redundancy codes to secure patch downloads; utilizing digital signatures to secure patch downloads; utilizing a secure network protocol such as SSL to secure patch downloads, wherein at least one of the security steps is available in the particular method embodiment.

38. The configured storage medium of claim 33, wherein the step of downloading the software update from the update server to the first target computer is performed using a background downloading process, thereby reducing inconvenience to a user of the first target computer.

39. The configured storage medium of claim 33, wherein the step of downloading the software update from the update server to the first target computer is performed using bandwidth-throttled downloading, thereby allowing a network administrator to decide how bandwidth should be employed during a large deployment.

40. The configured storage medium of claim 33, wherein downloading is performed subject to a policy which limits the hours of operation, and the policy is set by an administrator, thereby allowing the administrator to decide when patch deployments are allowed to occur.

ForcePoint LLC
EX-1010-PT2
Page189

41. The configured storage medium of claim 33, wherein the method further comprises preventing downloads of software updates from the update server to the package computer, thereby enhancing security of the package computer.

42. The configured storage medium of claim 33, wherein the method further comprises use of a chained installation feature permitting an administrator to have downloaded patches installed on the target computer with fewer reboots than would otherwise be required.

43. The configured storage medium of claim 33, wherein the method further comprises use of a download resumption feature which detects interruption of a downloading step and then after a reconnection resumes the downloading step from at or near the point in that downloading step at which the interruption occurred, thereby avoiding repetition of the entire downloading step to achieve the download.

44. The configured storage medium of claim 33, wherein the method further comprises use of a mobile-user support feature which allows an administrator to deploy a patch to the first target computer even though the first target computer is not connected to the network when the task identifier placing step occurs.

45. The configured storage medium of claim 33, wherein the method comprises downloading multiple patches which originated from multiple vendors.

46. The configured storage medium of claim 33, wherein the method further comprises the step of grouping a proper subset of target computers to form a group, whereby an operation that is applicable to an individual target computer can also be applied to the group.

47. The configured storage medium of claim 46, wherein the grouping step forms a group containing target computers that are specified by an administrator.

ForcePoint LLC
EX-1010-PT2
Page190

48. The configured storage medium of claim 46, wherein the grouping step forms a group containing target computers that are specified by a non-administrative user.

49. The configured storage medium of claim 46, wherein the grouping step forms a group containing target computers that are specified by identifying an operating system that is used by all of the target computers which are being placed in the group.

50. The configured storage medium of claim 46, wherein the grouping step forms a group containing target computers that are specified by identifying an application program that is used by all of the target computers which are being placed in the group.

51. The configured storage medium of claim 46, wherein the method further comprises the step of delegating limited administrative control to a group manager, whereby the group manager receives control over only those target computers that were placed in the group by the grouping step.

52. The configured storage medium of claim 33, wherein the method further comprises use of a mandatory patch baseline policy which specifies at least in part software that should be installed on the first target computer, and the method proactively downloads and installs on the first target computer a patch that is specified in the mandatory patch baseline policy.

53. The configured storage medium of claim 52, wherein the mandatory patch baseline policy sets a baseline for target computers that use a particular application.

54. The configured storage medium of claim 52, wherein the method further comprises automatically reinstalling a patch that is specified in the mandatory patch baseline policy after software in the patch was dropped from a target computer that is subject to the mandatory patch baseline policy.

ForcePoint LLC
EX-1010-PT2
Page191

55. The configured storage medium of claim 33, wherein the method further comprises the steps of grouping a proper subset of target computers to form a group, and using a mandatory patch baseline policy to specify at least in part software that should be installed on the target computers in the group.

56. The configured storage medium of claim 33, wherein the method further comprises use of a patch compliance assurance feature which specifies software that is locked on the first target computer, and the method proactively notifies an administrator if locked software is removed from the first target computer.

57. The configured storage medium of claim 33, wherein the method further comprises use of a change control feature which specifies at least one item that is locked on the target computer, and the method proactively notifies an administrator if a locked item is changed on the target computer, wherein the item is at least one of: a hardware item, a service item, and a software item.

58. The configured storage medium of claim 33, wherein at least the step of downloading the software update from the update server to the first target computer recurs, thereby repeatedly updating a particular file on at least the first target computer.

59. The configured storage medium of claim 33, wherein the method further comprises at least one step from a group of disaster recovery steps, the step helping an administrator recover and continue operation after a system failure, wherein the group of disaster recovery steps comprises: creating another server with the same domain name as a failed server, reinstalling update server software on a server, restoring archived data, and restoring mirrored data, and wherein at least one of the disaster recovery steps is available in the particular method embodiment.

60. The configured storage medium of claim 33, wherein the method further comprises the steps of maintaining a record of recent operations, and rolling back

ForcePoint LLC
EX-1010-PT2
Page192

deployment of a patch, thereby allowing an administrator to undo a target computer patch installation that has caused problems.

61. The configured storage medium of claim 33, wherein the method further comprises use of a intelligent multiple patch deployment feature which matches patches with target computer operating systems, thereby relieving an administrator of the need to expressly and fully identify the operating system used on the target computer.

62. The configured storage medium of claim 33, wherein the method installs a security patch on the first target computer, thereby providing an administrator with a policy-driven way to hook into the target computer's file system and stop at least one particular file from executing on the target computer.

ForcePoint LLC
EX-1010-PT2
Page193

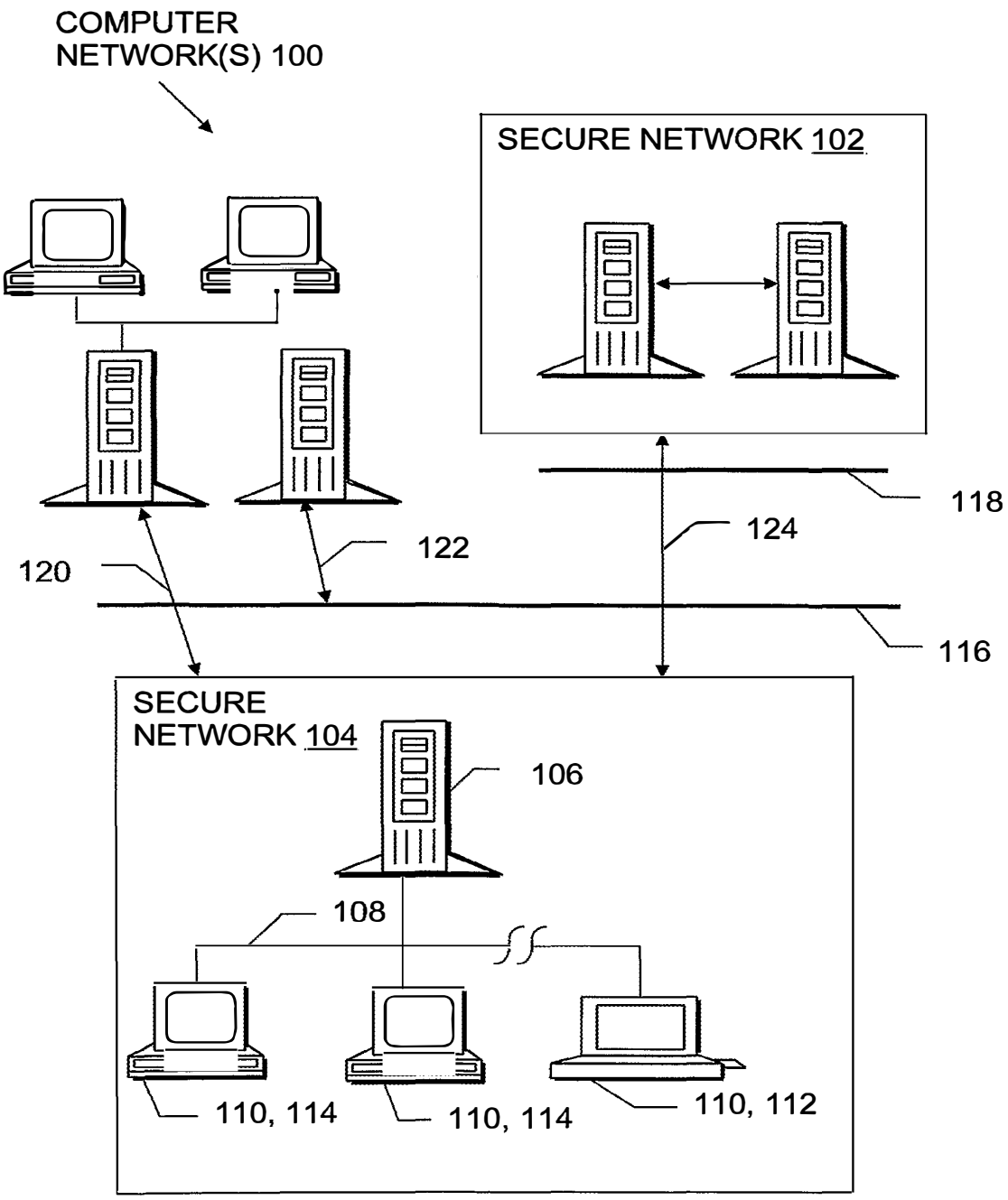

COMPUTER
NETWORK(S) 100
SECURE NETWORK 102
118
124
122
120
116
SECURE
NETWORK 104
106
108
110, 114
110, 114
110, 112

Fig. 1

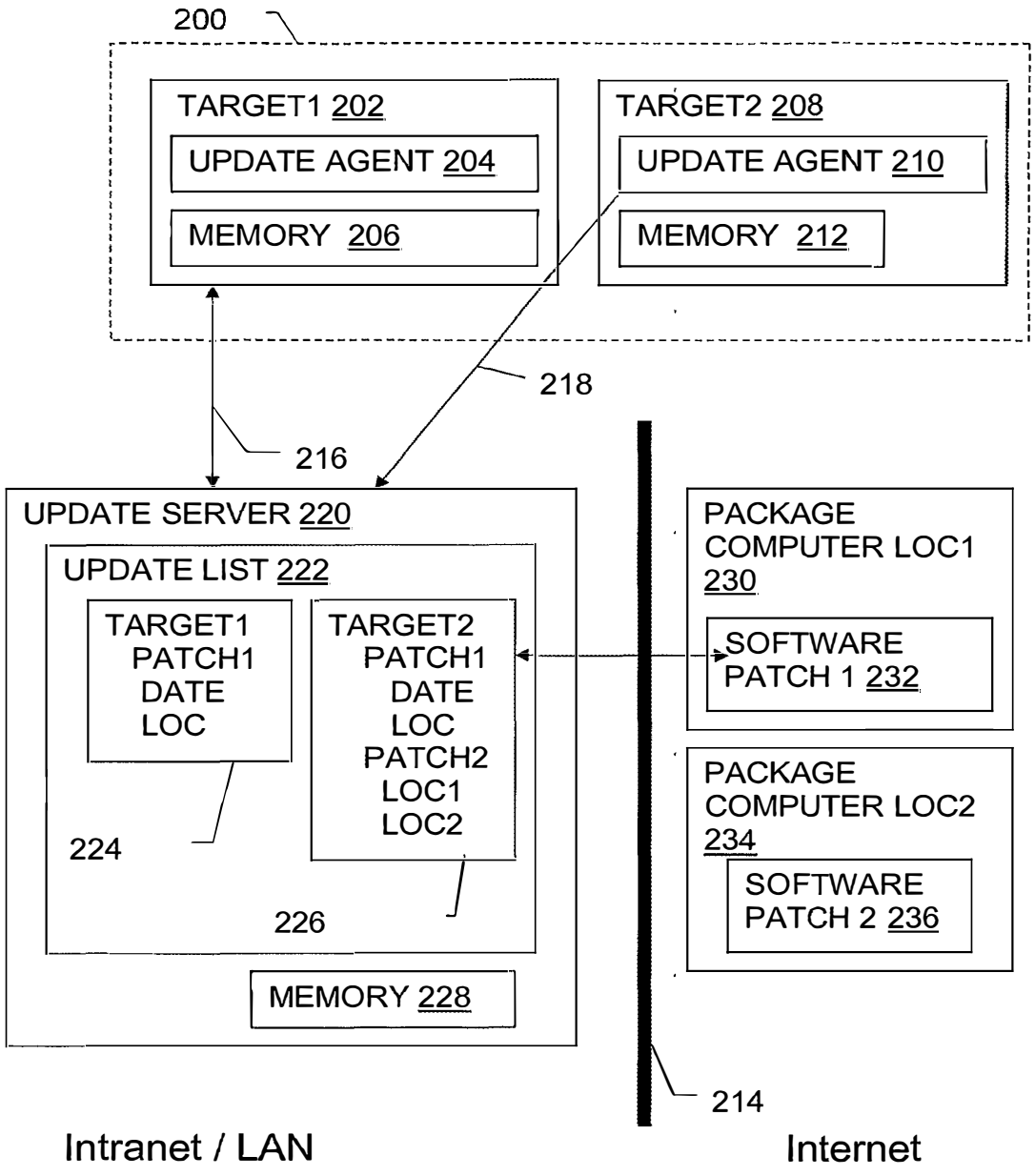

200
TARGET1 202
UPDATE AGENT 204
MEMORY 206
TARGET2 208
UPDATE AGENT 210
MEMORY 212
218
216
UPDATE SERVER 220
UPDATE LIST 222
TARGET1
PATCH1
DATE
LOC
TARGET2
PATCH1
DATE
LOC
PATCH2
LOC1
LOC2
224
226
MEMORY 228
PACKAGE
COMPUTER LOC1
230
SOFTWARE
PATCH 1 232
PACKAGE
COMPUTER LOC2
234
SOFTWARE
PATCH 2 236
214
Intranet / LAN
Internet

Fig. 2

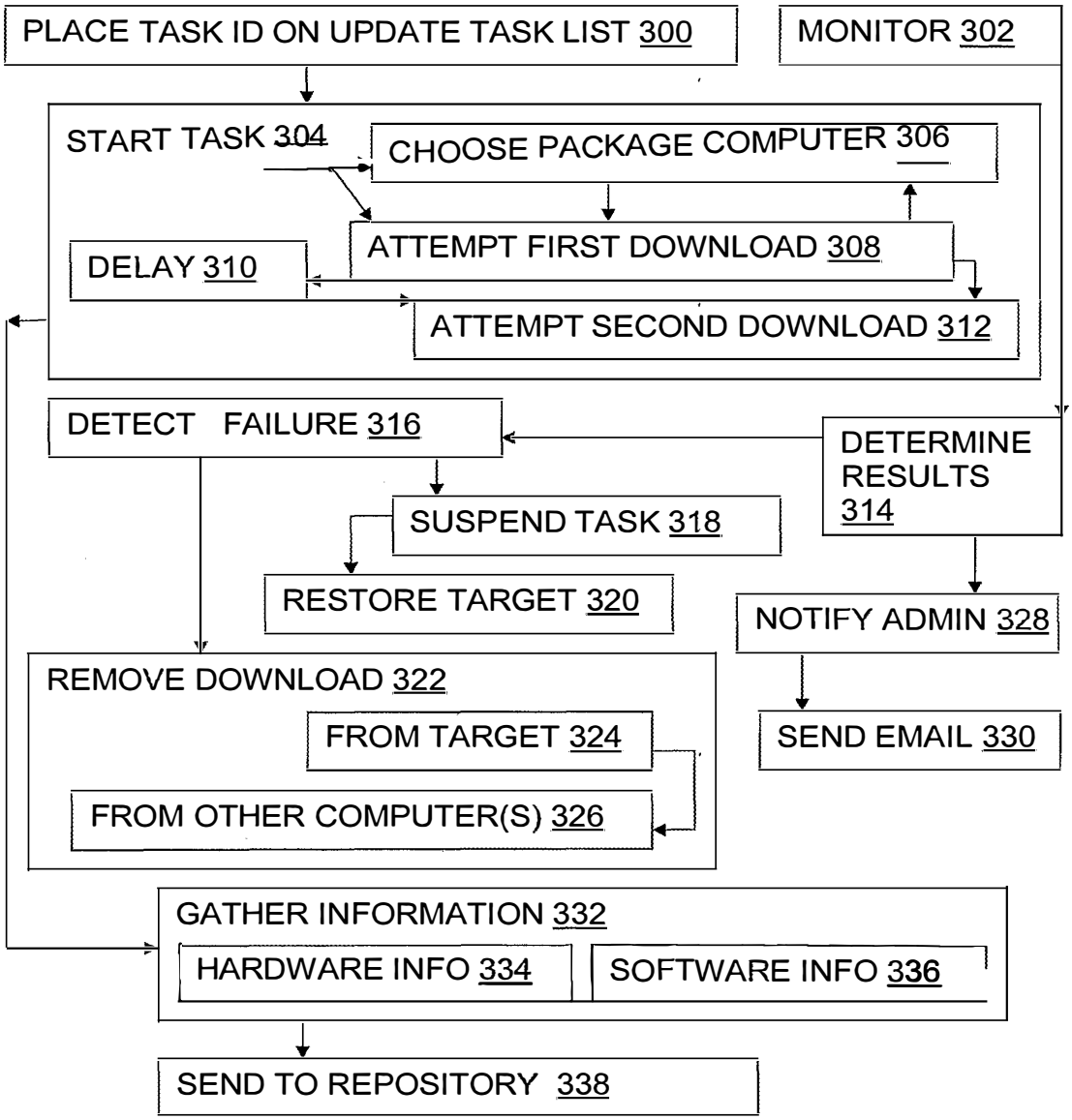

PLACE TASK ID ON UPDATE TASK LIST 300
MONITOR 302
START TASK 304
CHOOSE PACKAGE COMPUTER 306
ATTEMPT FIRST DOWNLOAD 308
DELAY 310
ATTEMPT SECOND DOWNLOAD 312
DETECT FAILURE 316
DETERMINE RESULTS 314
SUSPEND TASK 318
RESTORE TARGET 320
NOTIFY ADMIN 328
REMOVE DOWNLOAD 322
FROM TARGET 324
SEND EMAIL 330
FROM OTHER COMPUTER(S) 326
GATHER INFORMATION 332
HARDWARE INFO 334
SOFTWARE INFO 336
SEND TO REPOSITORY 338

Fig. 3

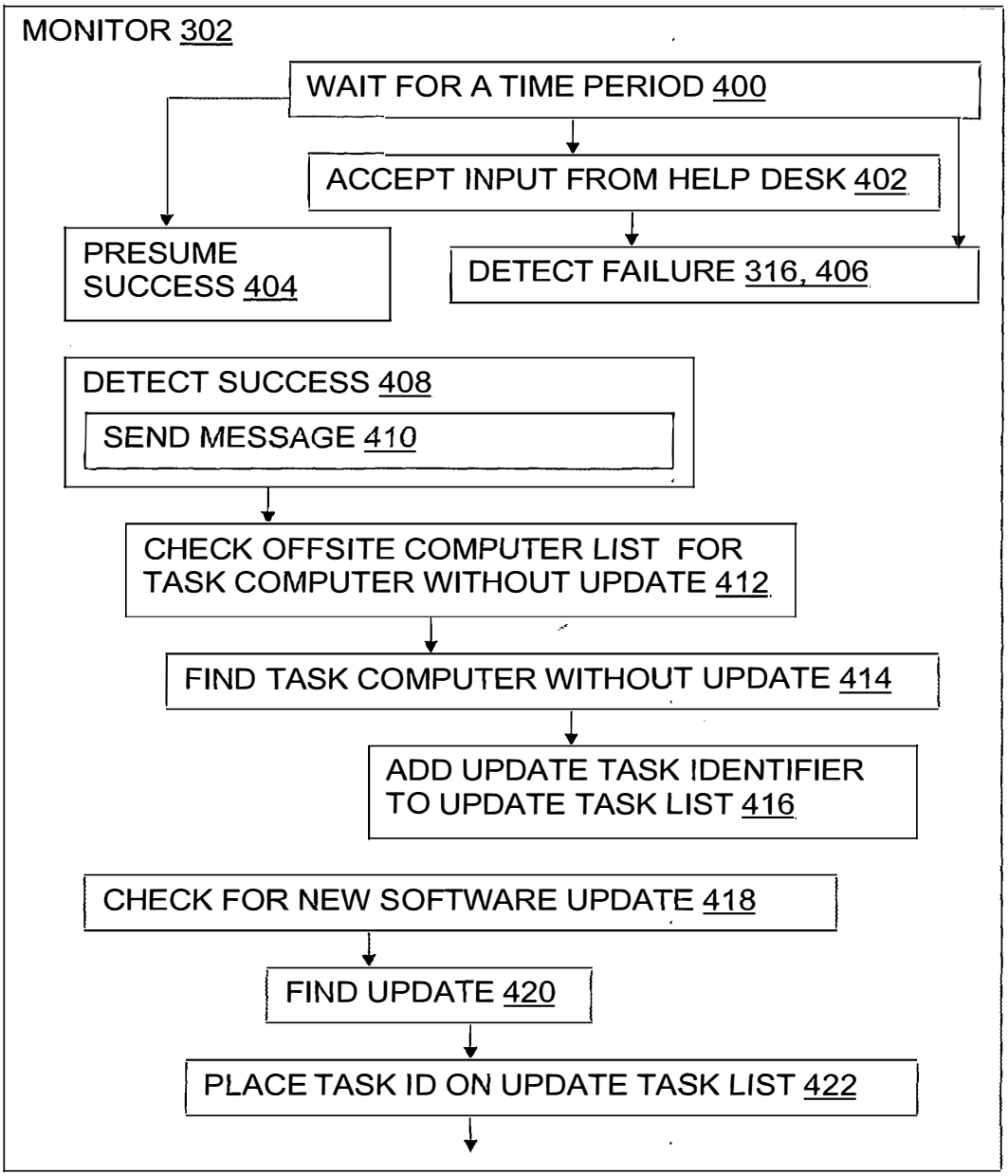

MONITOR 302
WAIT FOR A TIME PERIOD 400
ACCEPT INPUT FROM HELP DESK 402
PRESUME SUCCESS 404
DETECT FAILURE 316, 406
DETECT SUCCESS 408
SEND MESSAGE 410
CHECK OFFSITE COMPUTER LIST FOR TASK COMPUTER WITHOUT UPDATE 412
FIND TASK COMPUTER WITHOUT UPDATE 414
ADD UPDATE TASK IDENTIFIER TO UPDATE TASK LIST 416
CHECK FOR NEW SOFTWARE UPDATE 418
FIND UPDATE 420
PLACE TASK ID ON UPDATE TASK LIST 422

Fig. 4

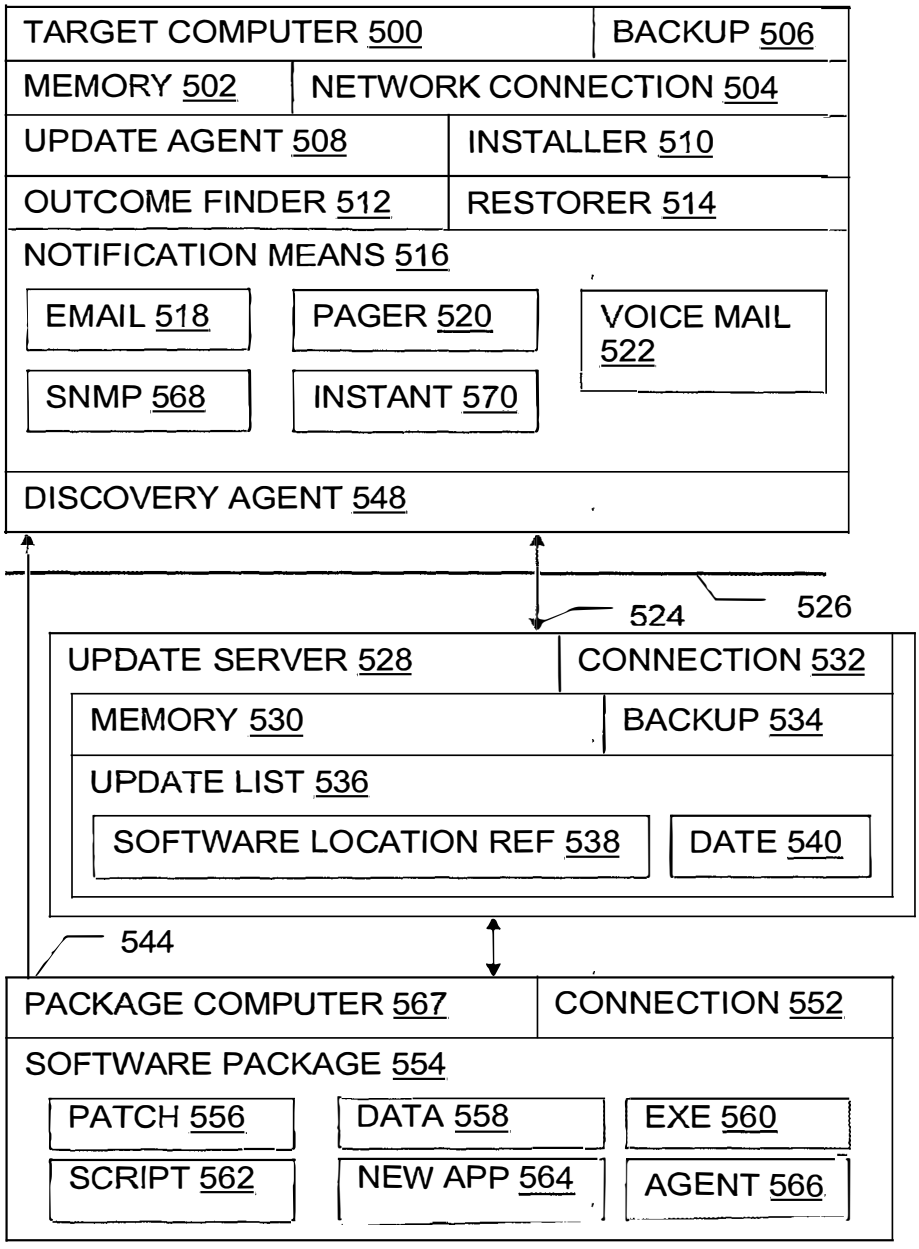

TARGET COMPUTER 500
BACKUP 506
MEMORY 502
NETWORK CONNECTION 504
UPDATE AGENT 508
INSTALLER 510
OUTCOME FINDER 512
RESTORER 514
NOTIFICATION MEANS 516
EMAIL 518
PAGER 520
VOICE MAIL 522
SNMP 568
INSTANT 570
DISCOVERY AGENT 548
524
526
UPDATE SERVER 528
CONNECTION 532
MEMORY 530
BACKUP 534
UPDATE LIST 536
SOFTWARE LOCATION REF 538
DATE 540
544
PACKAGE COMPUTER 567
CONNECTION 552
SOFTWARE PACKAGE 554
PATCH 556
DATA 558
EXE 560
SCRIPT 562
NEW APP 564
AGENT 566

Fig. 5

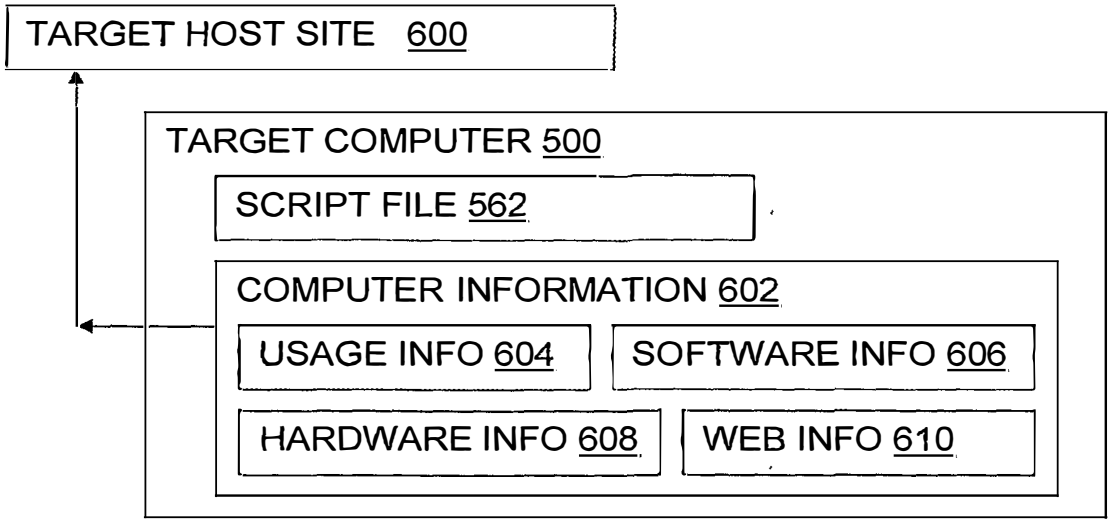

TARGET HOST SITE 600
TARGET COMPUTER 500
SCRIPT FILE 562
COMPUTER INFORMATION 602
USAGE INFO 604
SOFTWARE INFO 606
HARDWARE INFO 608
WEB INFO 610

Fig. 6

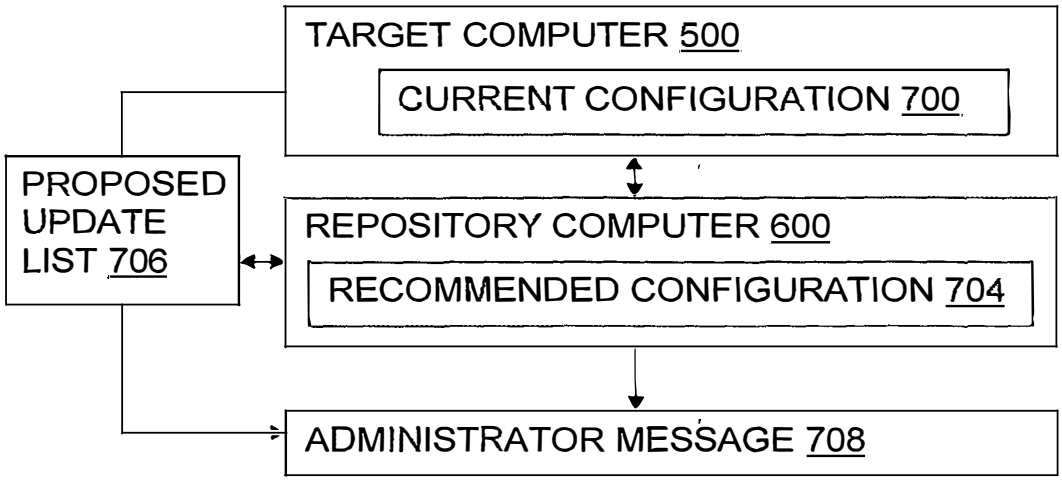

TARGET COMPUTER 500
CURRENT CONFIGURATION 700
PROPOSED UPDATE LIST 706
REPOSITORY COMPUTER 600
RECOMMENDED CONFIGURATION 704
ADMINISTRATOR MESSAGE 708

Fig. 7

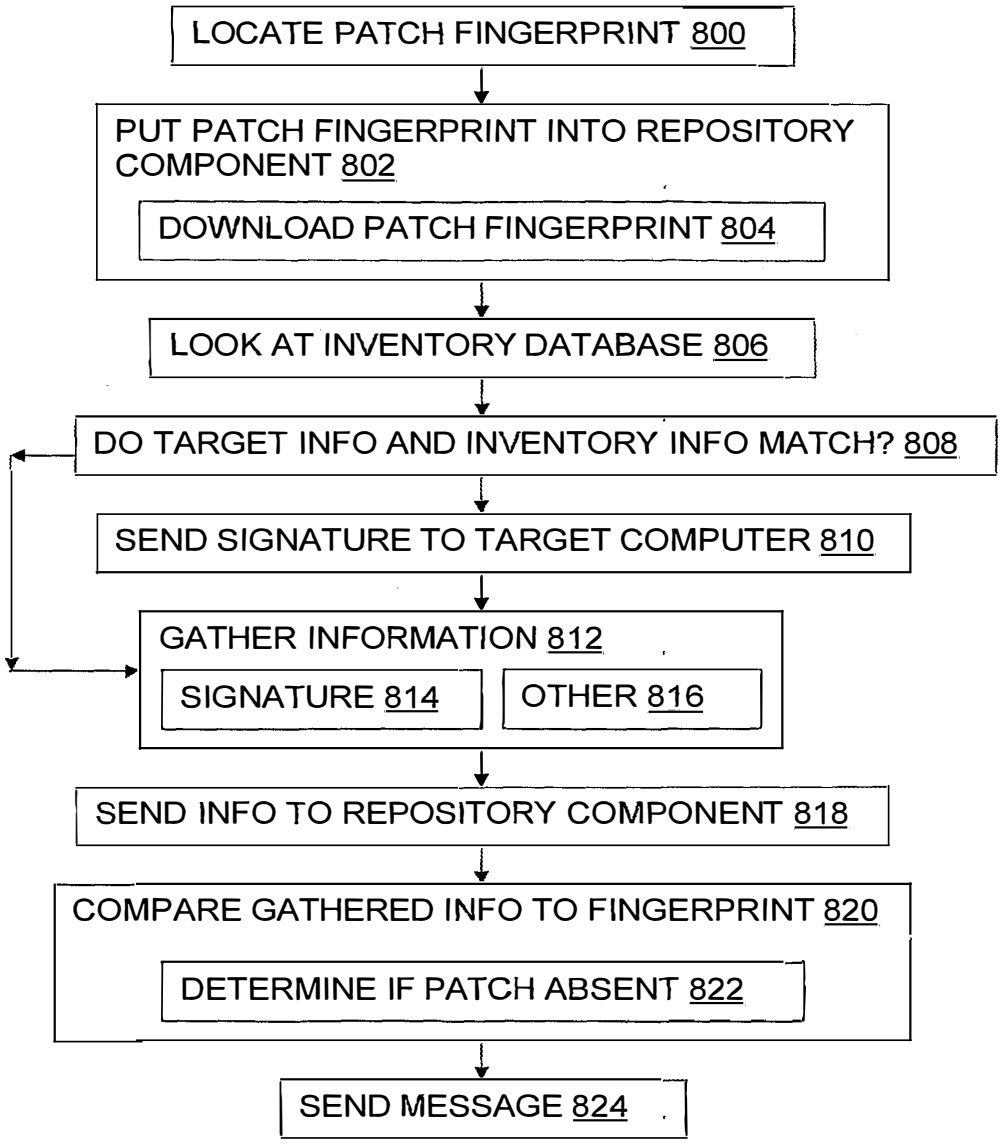

LOCATE PATCH FINGERPRINT 800
PUT PATCH FINGERPRINT INTO REPOSITORY COMPONENT 802
DOWNLOAD PATCH FINGERPRINT 804
LOOK AT INVENTORY DATABASE 806
DO TARGET INFO AND INVENTORY INFO MATCH? 808
SEND SIGNATURE TO TARGET COMPUTER 810
GATHER INFORMATION 812
SIGNATURE 814
OTHER 816
SEND INFO TO REPOSITORY COMPONENT 818
COMPARE GATHERED INFO TO FINGERPRINT 820
DETERMINE IF PATCH ABSENT 822
SEND MESSAGE 824

Fig. 8

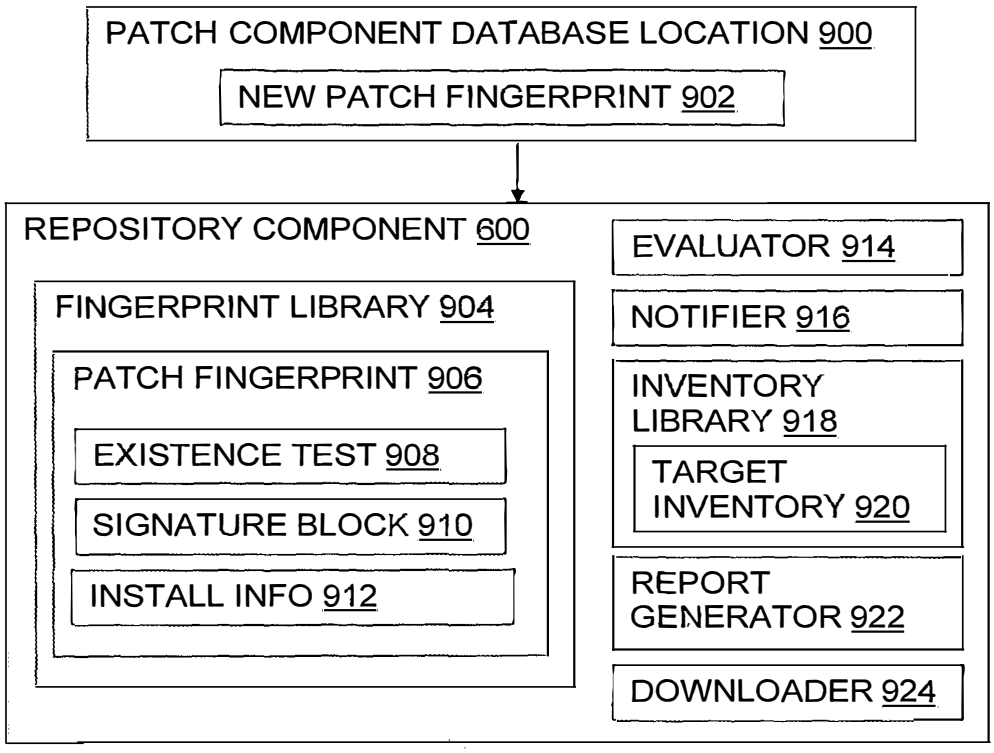

PATCH COMPONENT DATABASE LOCATION 900
NEW PATCH FINGERPRINT 902
REPOSITORY COMPONENT 600
FINGERPRINT LIBRARY 904
PATCH FINGERPRINT 906
EXISTENCE TEST 908
SIGNATURE BLOCK 910
INSTALL INFO 912
EVALUATOR 914
NOTIFIER 916
INVENTORY LIBRARY 918
TARGET INVENTORY 920
REPORT GENERATOR 922
DOWNLOADER 924

Fig. 9

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 December 2004 (29.12.2004)

PCT

(10) International Publication Number
WO 2004/114663 A1

(51) International Patent Classification[7]: H04N 7/16

(21) International Application Number:
PCT/GB2004/002570

(22) International Filing Date: 16 June 2004 (16.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0314043.1 17 June 2003 (17.06.2003) GB

(71) Applicant *(for all designated States except US)*: **IMAGINE BROADBAND LIMITED** [GB/GB]; Carmelite, 50 Victoria Embankment, Blackfriars, London EC4Y 0DX (GB).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **PATEL, Dipan**; c/o Imagine Broadband Limited, Aldwych House, 81 The Aldwych, London WC2B 4HN (GB).

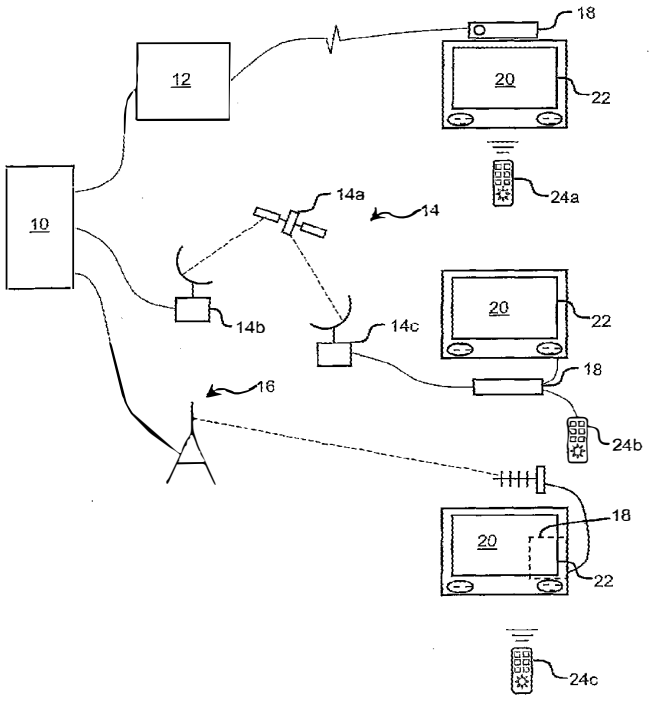
(74) Agents: **KAZI, Ilya** et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR SELECTIVELY DISTRIBUTING DATA TO A SET OF NETWORK DEVICES



(57) Abstract: A method selectively distributes data to a set of devices linked by a network, where each device has at least one unique identifier. The method comprises selecting devices to be members of the set, the set devices being selected to receive the data based on the at least one unique identifier, and distributing data to at least the selected devices, the data including at least one matching key for matching at least a portion of the unique identifier of selected devices. The unique identifier is a device hardware identifier, being a string of bits and the key correlates to at least a portion of the string of bits.

WO 2004/114663 A1

ForcePoint LLC
EX-1010-PT2
Page202

FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND SYSTEM FOR SELECTIVELY DISTRIBUTING DATA TO A SET OF NETWORK DEVICES

Technical Field

The present invention relates to a method and system for selectively distributing data to a set of network devices and will be described in relation to selectively modifying instruction code of devices of subscriber television networks. However, it will be appreciated that the invention is not limited to this particular field of use, but is also applicable to other systems of data processing equipment of which mobile telephone networks and computer networks are further non-limiting examples.

Background Art

Networks, such as subscriber television service networks, are typically controlled and run by complex computer networks, where end users access the networks' programming via "set top boxes" (STB) connected to their television, and control the programming using a remote control device. STBs may be used merely for accessing different audiovisual entertainment channels on the end user's television, or for datacasting, internet access, pay per view programs, video telephony, and so on. These STBs typically include flash memory for storing data such as software code to process information sent by the subscriber network, and to provide to the connected television a front end graphical user interface (GUI) for the user to access some functions of the software. Due to the changing and improving nature of the services provided by such networks, the STB software may be updated from time to time.

However, updating software often causes problems. For example, even though new software is thoroughly tested under workshop conditions, unforeseen problems often occur once the software is deployed to live STBs; or functionality of the software may change where end users require additional services to learn how to use the changed software. Since the updating of software is not a common event, the service network operators are typically not resourced to cope with calls from users for help with dealing with the changes or problems. For this reason, it is desirable for software updates to be deployed to a trial batch of users to detect problems before mass installation. This is often achieved in practice by using employees (and perhaps friends of employees) to trial the updated software for a

period of time to determine the software's robustness in the field. However, this may not provide a large enough or representative sample of the user base.

Furthermore, as equipment may come from a number of sources over a long period of time, there may be numerous versions of software employed by devices. It is not normally practical to maintain the complex database that would be required to track existing software versions.

Similar problems occur when rolling out computer software updates and patches for computer systems. Typical methods of providing updates and patches include using the internet or CD-ROMs distributed with trade magazines and the like.

Preferred embodiments of the present invention aim to ameliorate one or more of the problems of the prior art or to provide an alternative thereto.

Summary of the Invention

According to one aspect of the invention there is provided a method of selectively distributing data to a set of devices linked by a network, each said device having at least one unique identifier, the method comprising the steps of:

selecting devices to be members of the set, the set devices being selected to receive the data based on the at least one unique identifier; and

distributing data to at least the selected devices, the data including at least one matching key for matching at least a portion of the unique identifier of selected devices.

This method is advantageous in that the distribution of data is controllable and flexible. Preferably the data is broadcast to a plurality of the devices on the network but only selected devices selectively install the data. The data to be distributed may include updates or improvements to code for running the devices.

In a complementary method aspect, there is provided a method of selectively installing data at one of a set of devices linked by a network, each device having a unique identifier, the method comprising determining whether to install the data based on matching at least a portion of the unique identifier to at least one received matching key associated with the data.

Preferably, the unique identifier is independent of the content of the data, and most preferably is a device hardware identifier. Surprisingly, although device hardware identifiers do not have a logical connection with the decision whether or not to update software, and indeed because of this, they can provide a useful means of

selecting subsets of a population of devices.

Preferably, the set of devices comprises one of a plurality of substantially arbitrarily partitioned subsets of a population of devices. Alternatively, the set of devices may be randomly selected, or selected by one or more predetermined geographic regions common to the set devices.

Preferably, the data is instruction code, preferably a software update.

In one embodiment, the unique identifier may be a string of characters.

Preferably the identifier is a string of bits or characters, the string being preferably of a first length and the set of devices preferably determined from a shorter length subset of the string of the first length. Typically, the first length is at least about 32 bits. The shorter length subset of the string preferably has a selectable length. By using a selectable length bit string to define the set is advantageous, in that the number of matching devices to be updated can be adjusted. Alternatively the shorter length subset may be a fixed length, such as 16 bits.

Preferably, the step of installing the data is performed after performing one or more predetermined action steps on each device to determine whether or not to install the data. The step(s) may include determining whether a controller of the network has the data and whether the data includes a key or flag corresponding to the device, the key or flag preferably corresponding to the shorter length subset of the longer, first length device identifier.

The action step may be performed only when a device initialisation instruction is performed by the device, or when switching to a power on or standby state. Alternatively, the action step may be performed periodically, or at regular intervals while the device is in communication with the network, or when a user of the device performs a manual check of the network while the device is in communication with the network.

The method may include a confirmation step, after the one or more predetermined action steps, of a user of the device performing a confirmation instruction to download and run the data, if the device has been determined as a member of the set of devices.

Preferably, the one or more predetermined action steps include the steps of:

determining the version of a device data of each respective set device;

comparing the version of the device data with the version of the data to be relayed; and

determining whether or not to perform the step of downloading the data, based on the outcome of the step of comparing the versions of the device and modification data. Preferably, the predetermined action steps are performed by the device. Preferably each device is arranged to run a manual update routine for allowing the user to decide whether to download data flagged as user selectable from the networks wherein the manual update routine runs a text routine to determine whether to download data flagged as user selectable. Also preferably the test routine comprises comparing the matching key to the unique identifier.

According to a third aspect of the invention there is provided a device for running data, the device being linked to other devices by a network, the device including:

a processor;

a memory with stored data processable by the processor; and

at least one unique identifier,

wherein the data stored by the memory includes a routine for checking for update data for the device, and for selectively downloading the data based on at least a portion of the unique identifier, and at least one key associated with the update data. Preferably, the data includes the key or flag and the device selectively downloads the update data when the key correlates to the at least the portion of the unique identifier. Also preferably the unique identifier is a device hardware identifier, and is a string of bits of characters.

Preferably, the devices are set top boxes, and the network is a subscription television service. The set of devices may be selected by determining one or more channels subscribed by and common to users of the respective set devices. In this way, an operator of the subscription television service can send data to users, or subscribers of particular channel packages, such as movie channel packages, or sport channel packages. Examples of such data may include a broadcast message to the subscribers about a particular relevant event on a particular channel, or code for allowing preview access for a limited time period to another channel to which the user does not have a subscription.

Alternatively, the devices may be mobile telephones or telephone base stations and the network may be a mobile telephone network.

Alternatively, the devices may be computers and the network may be a computer network. In this embodiment, the computer network is preferably one or

more of a local area network, a wide area network or the Internet.

In another alternate arrangement, the devices may be back to base home security devices and the network may be a back to base security network.

According to a fourth aspect of the invention there is provided a system for selectively distributing data to of a set of devices linked by a network, each said device having at least one unique identifier, the system comprising:

means for selecting devices to be members of the set, the set of devices being selected to receive the data based on respective unique identifiers of the devices;

means for distributing data to at least each selected device, the data including at least one matching key for matching at least a portion of the unique identifier of selected devices; and

means for running the data on each respective selected device.

According to a fifth aspect of the invention there is provided a method of updating a device which has an update routine which checks for available updates over a network and selects available updates which are applicable to the device for download, each update having associated therewith an update condition selected from a plurality of pre-determined conditions which conditions include at least (1) at least one power change condition and (2) a user-selection condition, the device being arranged to execute a user confirmation routine on selection of an available applicable update associated with a user-selection condition, the method comprising executing a routine which performs a test to determine whether a selective update criterion is met in place of the user confirmation routine and which automatically opts to install the available applicable update if the selective update criterion is met.

This method is advantageous where an operator of the network needs to perform a "retrofit" of a new code or data routine to devices already on the network.

Preferably the device is arranged to execute the routine which performs the test to determine whether a selective update criterion is met. Also preferably performing the test comprises comparing additional update data associated with the available applicable update to device data obtained from the device, and the additional update data. Preferably the additional update data comprises matching key data and the device data comprises a unique identifier of the device. Also preferably performing the test comprises detecting at least a partial match between said matching key data and said unique identifier. The extent of match required for a positive test result may be specified in the additional updated data.

ForcePoint LLC
EX-1010-PT2
Page208

According to a sixth aspect of the invention there is provided a method of providing updated data to a population of devices, the method comprising partitioning the population of devices into subsets, making the updated data available to a first subset, and subsequently making the data available to further subsets, characterised by monitoring the response following making available to the first subset and setting the size of further subsets and/or the rate of making data available to further subsets based on the response.

The size of further subsets may be increased in the event of a low level of response.

Preferably the subsets are defined by specifying a portion of a matching key to match to a unique identifier of each device. The size of each subset may be determined by setting the length of the portion of matching key to match, wherein a shorter matching portion will match a larger number of devices.

Preferably, a longer portion of matching key is used to define a smaller first subset and a shorter portion of matching key is used to define at least one larger further subset.

Preferably, monitoring the response comprises obtaining a measure of response based on user feedback.

According to another aspect of the invention there is provided a computer program or computer program product for selectively distributing data of a set of devices of a network comprising means for performing the method aspects of the invention.

In the specification, unless otherwise stated or apparent from the context, references to STBs are intended to encompass any form of decoder which receives (preferably digital) signals from a medium (satellite, cable, DSL, terrestrial being non-limiting examples) and provides (typically analogue, but digital output is not excluded) video signals for a display device (television, plasma screen, video projector being non-limiting examples). Whilst stand-alone STBs are commonplace, the functionality of the STB may be integrated into a display device (for example a television with built in digital decoding) or other device (for example cable modem or other communication device).

Typical STBs in current use only allow of the order of about 8 megabytes for applications and only have a processor capable of the order of 100 MIPS (million instructions per second) which is an order of magnitude less than typical personal

computers. However, the architecture is applicable to other devices, such as hand-held devices (Personal Digital Assistants, or PDA being a non-limiting example), mobile devices, dedicated games or entertainment devices and even in fact to general purpose computers where it is desired to provide an efficient processing architecture.

As will be understood, the term "matching" in the context of the specification and claims is preferably to be understood as a direct match where, for a match to occur, the matching key is identical to a portion of the unique identifier.

Brief Description of the Drawings

Preferred embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a schematic overview of a system for employing the present invention;

Figure 2 is a schematic view of the architecture of a STB for employing the present invention; and

Figure 3 is flow diagram of a preferred embodiment of the present invention.

Detailed Description of the Preferred Embodiments

In the following description, an embodiment is described in the context of a device in the form of a STB for decoding video signals, which is a particularly preferred application. However, the architecture (and portions thereof) may be applied to other network systems, for devices such as mobile telephone devices, handheld devices, games platforms, general purpose computers, GPS automobile security systems, back to base building security systems, or indeed any device having a processor, memory and input and output functions.

Referring to Fig. 1, a preferred embodiment of a method, system, device and computer program or computer program product according to the invention may comprise at least one network controller in the form of a server 10 connected via a communication medium such as a digital subscriber link (DSL, or cable) headend 12, a satellite link 14, a terrestrial transmitter 16, or other communication link (not shown) to devices in the form of STBs 18. The satellite link typically includes a satellite 14a and transmitting and receiving dishes 14b and 14c respectively. The STBs 18 provide video signals to a display device such as a television 20 to be displayed on a

screen 22. The STBs 18 receive input signals, for example from an infra-red remote control 24a, a direct coupled joystick or input device 24b or, in the case of a STB 18a integrated with a television 20a, from a master control 24c for the television.

In normal use, the STB 18 decodes video signals received over the communication medium to provide video output, as is well-known in the art. The STBs normally include limited functionality for providing a graphics display, for example to display static configuration and programme menus. Alternatively, the graphics capability is made use of to provide real-time moving video (although the invention can be used to provide static video as well), for example to enable a user to play an arcade-style game.

The architecture of the STB 18 which makes this feasible will be explained with reference to Figure 2. As is well-known, a STB 18 generally has a hardware platform 26 which provides a variety of interfaces 27, including a graphics interface 28, a network interface 29, an input interface 30 and normally a sound interface (not shown). A variety of standard drivers 31 including a graphics driver 32 and input driver 34 are provided for controlling the interfaces 27. The hardware has a central processing unit (CPU) 36 and memory 38, such as flash memory or other applicable memory types, which runs the software 40, including a real time operating system (RTOS) 42.

In the preferred embodiment of the invention, each STB has a unique hardware identifier being a string of a first length in the form of at least a 32 bit linear string, resulting in a maximum of 2^{32}, or approximately 4 billion unique identifiers for the STB population.

In alternative embodiments, the unique identifier is in the form of an 8 bit x 8 bit (1 byte x 1 byte), 2 dimensional array string, or is in the form of a 64 bit linear string, each resulting in a STB population maximum of 2^{64} unique identifiers. Such a configuration would ensure no two STBs share the same unique identifier. Other embodiments of STBs may have unique identifiers with larger or smaller bit strings, or with other strings, such as alphanumeric strings. The identifier may not be truly globally unique in certain cases.

In another alternative embodiment, each STB 18 may be supplied a downloaded unique identifier, such as a subscriber number, to be written to its memory.

In yet another alternative embodiment, the unique identifier may be a whole or

part hash value of a predetermined portion of data on the STB 18. The predetermined portion of data may include user details held by the memory 38, or data relating to the user's subscription of service that they are using the STB for.

A preferred embodiment of a method according to the present invention will now be described with reference to Figures 1 to 3. The server 10 sends multiple data streams at different frequencies relating to different channels throughout the network to connected STBs. A channel may be for broadcasting audiovisual data of popular television programs, or alternatively for data streaming of teletext information, the Internet or pay-per-view programs. Typically, television programs and teletext are continuously broadcast, whereas the Internet is interactive, allowing uploading as well as downloading of data. Pay-per-view programs may be "on demand", requested by the user to be broadcast, continuously broadcast, but restricted to access by relevant subscribers.

Depending on a subscription type or level of a STB user, each respective STB contains software code to decode the data streams or channels to which the user has subscribed. In addition to subscribed channels, the Internet, etc, the server 10 may from time to time send data streams of STB data in the form of software code updates on one or more channels, where the software relates to a change in user subscription, or a change to the functionality of the STB, such as its graphical user interface. It is the method and system by which the latter data stream is transmitted which is the principal concern of the preferred embodiment of the present invention.

Prior to sending software code updates, the modification or updated code is normally tested by the network operator for robustness. Depending on the nature of the updated code, the server will roll out the code, in accordance with the preferred embodiment, to sets of subscribers over time. This has many advantages. For example, depending on the change to functionality of the STB made by the new code, network users will invariably contact the network operator with questions regarding the use of the STB. Therefore, in spreading out the roll out of updated code over time, the impact on the network operator's resources for helping the subscribers is also spread out over time, ensuring a more consistent use of such resources. Or, if there are problems with updated code, the number of updated STBs affected by the update is controlled to update a manageable portion of network subscribers. The rollout can then be stopped, and new update code repaired.

Prior to rolling out the updated code, the server 10 determines a 16-bit string

to be a flag included with the updated code, and then streams 50 the update code on a preselected channel. As illustrated in Figure 3, after occurrences of a STB trigger 52, resident software code on the STB tells the STB to run a check 54 of the server 10 to see if there are any code updates where the 16-bit string flag matches the first 16 bits of the unique identifier of the STB. If there is no match, the STB continues to function as normal. If there is a flag match, and the software code is an update of code existing on the STB 18, the STB then checks 56 whether the version of the update code is newer, older or the same as the STB's version of the existing code. If newer, the STB 18 downloads and runs the code update from a predetermined channel where the code is being constantly streamed. During or once the code has been downloaded, the version of the updated code is written to the STB memory 38. Alternatively, the code may be an initial instruction to the STB 18 that another instruction code will be available on a predetermined channel at a future predetermined time, such as a week later for example, and that the STB in question is to download and run the other instruction code from the predetermined channel at the predetermined time. Alternatively, steps 54 and 56 occur simultaneously.

There are three main triggers 52 for the STB to check the network for code updates. The first trigger is on boot or reboot of the STB 18. The second trigger is when, with the STB 18 in use, resident code on the STB 18 runs a timed routine asking the server 10 whether a code update is available containing a matching flag. The third trigger is where the user manually asks the server, via a STB GUI function or physical button on the STB 18 or remote controller 24a-c, whether a code update is available containing a matching flag.

In all the triggers 52 described above, the user may be given the option to confirm the downloading and running of the code update. Alternatively, the STB 18 will automatically download and run the code update without the user's input or knowledge. In an alternative embodiment, the code includes a secondary flag which tells the STB 18 a predetermined future time when the update code will be available for download.

Depending on the number of subscribers, approximately 1 in 65536 (2^{16}) subscribers would receive the code with the above method, due to the flag being 16-bit. This would allow the network operator to roll out new or updated code to a set, or portion, of the users, where the set is approximately 1 in 65536. Once feedback as to the success of the take-up of code of the set has been determined, the flag can be

changed to another 16-bit string to allow download and running of the code by a different set of users.

As will be appreciated by the skilled person, depending on the set size required, in alternative embodiments the flag may be larger or smaller, as required. This covers the situation where, if the unique identifier is large enough, a single STB can be targeted for downloading of code, where the flag is identical to the unique identifier of the single STB to be targeted. It also covers the situation where the flag is 1-bit, thus targeting approximately half the STB population. In the example of targeting a single STB, this may be used where only a single user requires a code update, for example should an unusual error have occurred in the download and/or running of an update code, or should that user elect to change their subscription service.

The same or shorter length subset of the string may alternatively be in the form of a string having a variable length over the period of the roll out of the new data. For example, the network operator may determine to rollout new data to a 1 in 2^{16} set of STBs, by determining a 16 bit flag. If over a predetermined time frame the network operator receives more complaints or query from STB users than it is possible for resources to effectively deal with, the operator may choose to roll out the next stage of the new data to a smaller set portion of the users, say 1 in 2^{18} users, or to delay or halt roll out. If over a predetermined time frame the network operator receives less feedback from STB users than a threshold amount, the operator may choose to roll out the next stage of the new data to a larger set portion of the users and advantageously the software automatically chooses the subset, say 1 in 2^4 users, using a 4 bit flag. This can provide effective control of network resources in dealing with rolling out of new data.

In another alternative embodiment of the invention, STBs 18 are distributed to users such that the first 16-bit string of the unique identifier is determined based on more systematically distributed data, known by the network operator to correspond to a known criteria, such as geographical region or, particularly in the example of STBs used for television subscriptions, preferred program genre. In this way code updates can be rolled out by region or by program preference. This has the advantage that regional or program specific code updates can be targeted to users who fall into appropriate regional or program specific categories.

In reality, there are already many STBs 18 in use in the market place. Many of

these have resident factory installed software code that determines when the STB will check for and download updated data or software code. The STB checks for new code on each boot, reboot/reset, or when manually requested by the user. If, on boot, etc, a newer version of code is available, a download condition is checked to see if the STB is in the correct state to download the new software. The available states for downloading, depending on the needs of the network operator, include: immediate download; on power up or next boot or reset of the STB; when the STB is put into a standby state; or when manually requested by the user.

Manual requesting of new data or software is a feature rarely used, as it is rarely related to the user as being an available feature.

This resident boot code is therefore quite limiting to the network operator who may want or need to have STB data or software updated, but will be unsure as to when the STB is likely to be booted or rebooted/reset to enable initiation of a download.

Therefore, in another embodiment of the invention, there is a method of updating a STB 18 which has an update routine which checks for available updates over the network and selects available updates which are applicable to the STB for download. Each update has associated therewith an update condition selected from a plurality of pre-determined conditions. The conditions include at least:

1. at least one power change condition
   (for example, detection of a switch to or from a standby condition or a hard power-up condition);
2. a user-selection condition; and
3. an immediate installation condition signifying that an available applicable update is to be applied without waiting for a power change condition or user selection.

The STB is arranged to execute a user confirmation routine on selection of an available applicable update associated with a user-selection condition. In this method, the STB is also arranged to execute a routine, in place of the user confirmation routine, the routine performing a test to determine whether a selective update criterion is met. Also, this routine automatically opts to install the available applicable update if the selective update criterion is met. In an alternative

embodiment, the test performing routine is arranged to revert to requesting user confirmation in the absence of data specifying the selective update criterion.

Performing the test also comprises comparing a matching key in the form of a flag associated with the available applicable update to the unique identifier of the STB in question. The extent of positive match between the flag and unique identifier is specified in the additional update data. As with previously described embodiments, the unique identifier may be 32 bits, and the flag specified may be a 16 bit flag, to be potentially matched to the first 16 bits of the unique identifier.

This embodiment can be used in conjunction with earlier described embodiments to allow for downloading of new data to a set of STBs, where the set is based on a correlation between the STBs' respective unique identifiers and a key in the new data.

It will be apparent to those skilled in the art that alternative embodiments of the invention are applicable to different types of networks. For example, the invention may be applied to a mobile telephone network. In this embodiment, the server communicates with a plurality of subscribed mobile telephones via landline telephone substations and mobile telephone tower substations. The server can then roll out updated software, code or data using a method corresponding to the method described above with respect to STBs. Similarly, each telephone would preferably have a 2-byte, or 16 bit unique identifier, and there would be three main triggers for a mobile telephone connected to the network to download data, software, etc where the triggers correspond to the three triggers described above in reference to STBs. The first trigger would be turning on the telephone, the second trigger would be a timed routine run by the telephone and the third trigger would be a manual request by the telephone user, via the user interface on the telephone.

Other embodiments suited to the use of the invention include local area computer networks (LANs); wide area computer networks (WANs); computers connected to the Internet; landline (terrestrial) video/telephones; handhelds, or personal digital assistants (PDAs); back to base alarm systems for houses and commercial properties; GPS, satellite or mobile telephone connected back to base car alarm systems, and so on.

While the present invention has been described in its preferred embodiments, it is to be understood that the words which have been used are words of description rather than limitation and that changes may be made to the invention without

departing from its scope as defined by the appended claims.

The text of the abstract filed herewith is repeated here as part of the specification.

A method selectively distributes data to a set of devices linked by a network, where each device has at least one unique identifier. The method comprises selecting devices to be members of the set, the set devices being selected to receive the data based on the at least one unique identifier, and distributing data to at least the selected devices, the data including at least one matching key for matching at least a portion of the unique identifier of selected devices. The unique identifier is a device hardware identifier, being a string of bits and the key correlates to at least a portion of the string of bits.

CLAIMS:

1. A method of selectively distributing data to a set of devices linked by a network, each said device having at least one unique identifier, the method comprising the steps of:
selecting devices to be members of the set, the set devices being selected to receive the data based on the at least one unique identifier; and
distributing data to at least the selected devices, the data including at least one matching key for matching at least a portion of the unique identifier of selected devices.

2. A method according to claim 1 wherein the data is broadcast to a plurality of the devices over the network but wherein only selected devices selectively install the data.

3. A method of selectively installing data at one of a set of devices linked by a network, each device having a unique identifier, the method comprising determining whether to install the data based on matching at least a portion of the unique identifier to at least one received matching key associated with the data.

4. The method of any preceding claim wherein the unique identifier is independent of the content of the data.

5. The method of any preceding claim wherein the unique identifier is a device hardware identifier.

6. The method of any preceding claim wherein the set of devices comprises one of a plurality of substantially arbitrarily partitioned subsets of a population of devices.

7. The method of any of claims 1 to 4 wherein the set of devices is selected by one or more predetermined geographic regions common to the set devices.

8. The method of any preceding claim wherein the data comprises instruction

code or a software update.

9. The method of any preceding claim wherein the unique identifier is a string of bits or characters.

10. The method of claim 9 wherein the unique identifier is a string of a first length and the set of devices is determined from a shorter length subset of the string of the first length.

11. The method of claim 10 wherein the first length is at least about 32 bits.

12. The method of claim 10 or 11 wherein the shorter length subset of the string is of a selectable length.

13. The method of claim 2 or any claim dependent thereon wherein the step of installing the data is performed after performing one or more predetermined action steps to determine whether or not to install the data.

14. The method of claim 13 wherein the one or more action steps include determining whether the data includes the key corresponding to the device.

15. The method of any one of claims 10 to 14 wherein the key corresponds to the shorter length subset.

16. The method of any one of claims 13 to 15 wherein the one or more action steps are performed when a device initialisation instruction is performed by the device when the device is switched to a power on state or when the device is switched to a standby state.

17. The method of any one of claims 13 to 15 wherein the one or more action steps are performed periodically or at regular intervals while the device is in communication with the network.

18. The method of any one of claims 13 to 17 wherein the one or more

predetermined action steps include the steps of:
determining the version of a device data of a set device;
comparing the version of the device data with the version of the data to be distributed; and
determining whether or not to perform the step of downloading the data to be distributed, based on the outcome of the step of comparing the versions of the device data and the data to be distributed.

19. The method of any one of claims 13 to 18 wherein the predetermined action steps are performed by the device.

20. The method of any one of the preceding claims wherein each device is arranged to run a manual update routine for allowing a user to decide whether to download data flagged as user selectable from the network, wherein the manual update routine is modified so that, in place of user decision, the routine runs a test routine to determine whether to download data flagged as user selectable.

21. The method according to claim 20 wherein the test routine comprises comparing the matching key to the unique identifier.

22. A device for running data, the device being linked to other devices by a network, the device including:
a processor;
a memory with stored data processable by the processor; and
at least one unique identifier,
wherein the data stored by the memory includes a routine for checking for update data for the device, and for selectively downloading the data based on at least a portion of the unique identifier, and at least one key associated with the update data.

23. The device of claim 22 wherein the update data includes the key and the device selectively downloads the update data when the key correlates to the at least a portion of the unique identifier.

24. The device of claim 22 or 23 wherein the unique identifier is a device hardware identifier.

25. The device of any one of claims 22 to 24 wherein the unique identifier is a string of bits or characters.

26. The device of claim 25 wherein the unique identifier is a string of a first length and the at least a portion of the unique identifier is determined from a shorter length of the first length.

27. The device of claim 26 wherein the first length is at least about 32 bits.

28. The device of claim 26 or 27 wherein the shorter length subset of the string is of a selectable length.

29. The device of any one of claims 22 to 28 wherein the device is a set top box.

30. The device of any one of claims 22 to 29 wherein the network is a subscription television service.

31. The device of any one of claims 22 to 28 wherein the devices are:
mobile telephones and the network is a mobile telephone network; or
telephone base stations and the network is a telephone network; or
computers and the network is a computer network; or
back to base home security devices and the network is a back to base security network.

32. A system for selectively distributing data to of a set of devices linked by a network, each said device having at least one unique identifier, the system comprising:
means for selecting devices to be members of the set, the set of devices being selected to receive the data based on respective unique identifiers of the devices;

means for distributing data to at least each selected device, the data including at least one matching key for matching at least a portion of the unique identifier of selected devices; and

means for running the data on each respective selected device.

33. A method of updating a device which has an update routine which checks for available updates over a network and selects available updates which are applicable to the device for download, each update having associated therewith an update condition selected from a plurality of pre-determined conditions which conditions include at least (1) at least one power change condition and (2) a user-selection condition, the device being arranged to execute a user confirmation routine on selection of an available applicable update associated with a user-selection condition, the method comprising executing a routine which performs a test to determine whether a selective update criterion is met in place of the user confirmation routine and which automatically opts to install the available applicable update if the selective update criterion is met.

34. The method of claim 33 wherein the device is arranged to execute the routine which performs the test to determine whether a selective update criterion is met.

35. The method of claim 33 or 34 wherein performing the test comprises comparing additional update data associated with the available applicable update to device data obtained from the device.

36. The method of claim 35 wherein the additional update data comprises matching key data and the device data comprises a unique identifier of the device.

37. The method of claim 36 wherein performing the test comprises detecting at least a partial match between said matching key data and said unique identifier.

38. The method of any of claims 35 to 37 wherein the extent of match required for a positive test result is specified in the additional update data.

39. The method of any of claims 33 to 38 wherein said at least one power change condition includes (a) detection of a switch to or from a standby condition and (b) a hard power-up condition.

40. The method of any of claims 33 to 39 wherein the conditions further include (3) an immediate installation condition signifying that an available applicable update is to be applied without waiting for a power change condition or user selection.

41. The method of any of claims 33 to 40 wherein the routine which performs the test is arranged to revert to requesting user confirmation in the absence of data specifying the selective update criterion.

42. A method of providing updated data to a population of devices, the method comprising partitioning the population of devices into subsets, making the updated data available to a first subset, and subsequently making the data available to further subsets, characterised by monitoring the response following making available to the first subset and setting the size of further subsets and/or the rate of making data available to further subsets based on the response.

43. The method of claim 42 wherein the size of further subsets is increased in the event of a low level of response.

44. The method of claim 42 or 43 wherein the subsets are defined by specifying a portion of a matching key to match to a unique identifier of each device.

45. The method of claim 44 wherein the size of each subset is determined by setting the length of the portion of matching key to match, wherein a shorter matching portion will match a larger number of devices.

46. The method of claim 45 wherein a longer portion of matching key is used to define a smaller first subset and a shorter portion of matching key is used to define at least one larger further subset.

47. The method of any of claims 42 to 46 wherein monitoring the response comprises obtaining a measure of response based on user feedback.

48. The method of any one of claims 1 to 20 or 33 to 47 wherein the devices are set top boxes.

49. The method of any one of claims 1 to 20 or 33 to 47 wherein the network is a subscription television service.

50. The method of claim 48 or 49 wherein the set of devices is selected by determining one or more channels subscribed by and common to users of the respective set devices.

51. The method of any one of claims 1 to 20 or 33 to 47 wherein the devices are:
mobile telephones and the network is a mobile telephone network; or
telephone base stations and the network is a telephone network; or
computers and the network is a computer network; or
back to base home security devices and the network is a back to base security network.

52. A computer program or computer program product comprising means for performing the method of any of claims 1 to 20 or 33 to 51.

53. A method of selectively distributing data to a set of devices linked by a network substantially as herein described with reference to the accompanying drawings.

54. A method of selectively installing data at one of a set of devices linked by a network substantially as herein described with reference to the accompanying drawings.

55. A device for running data substantially as herein described with reference to the accompanying drawings.

56. A system for selectively distributing data substantially as herein described with reference to the accompanying drawings.

57. A method of updating a device substantially as herein described with reference to the accompanying drawings.

58. A method of providing updated data to a population of devices substantially as herein described with reference to the accompanying drawings.

59. A computer program or a computer program product substantially as herein described with reference to the accompanying drawings.

ForcePoint LLC
EX-1010-PT2
Page225

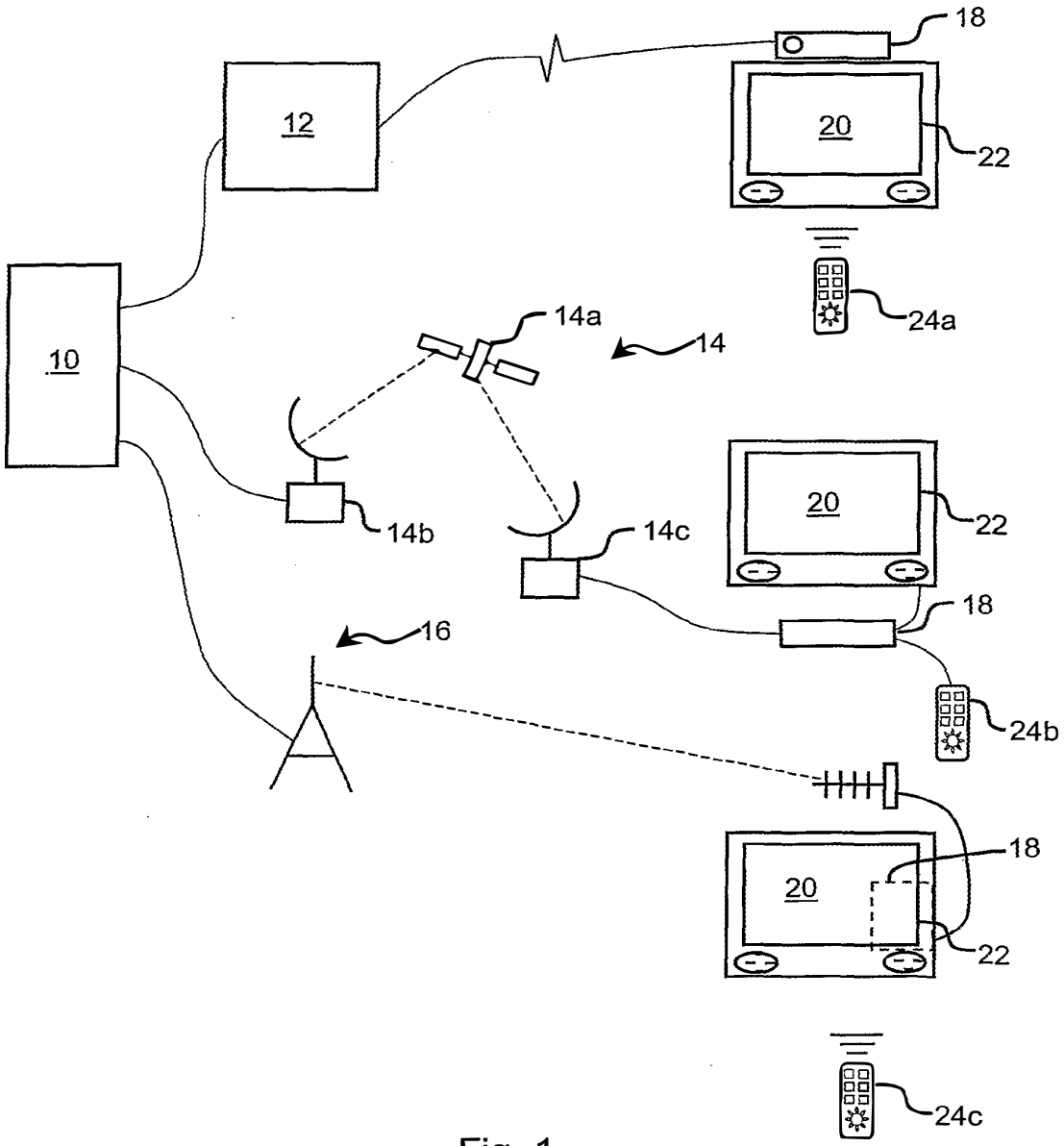


Fig. 1

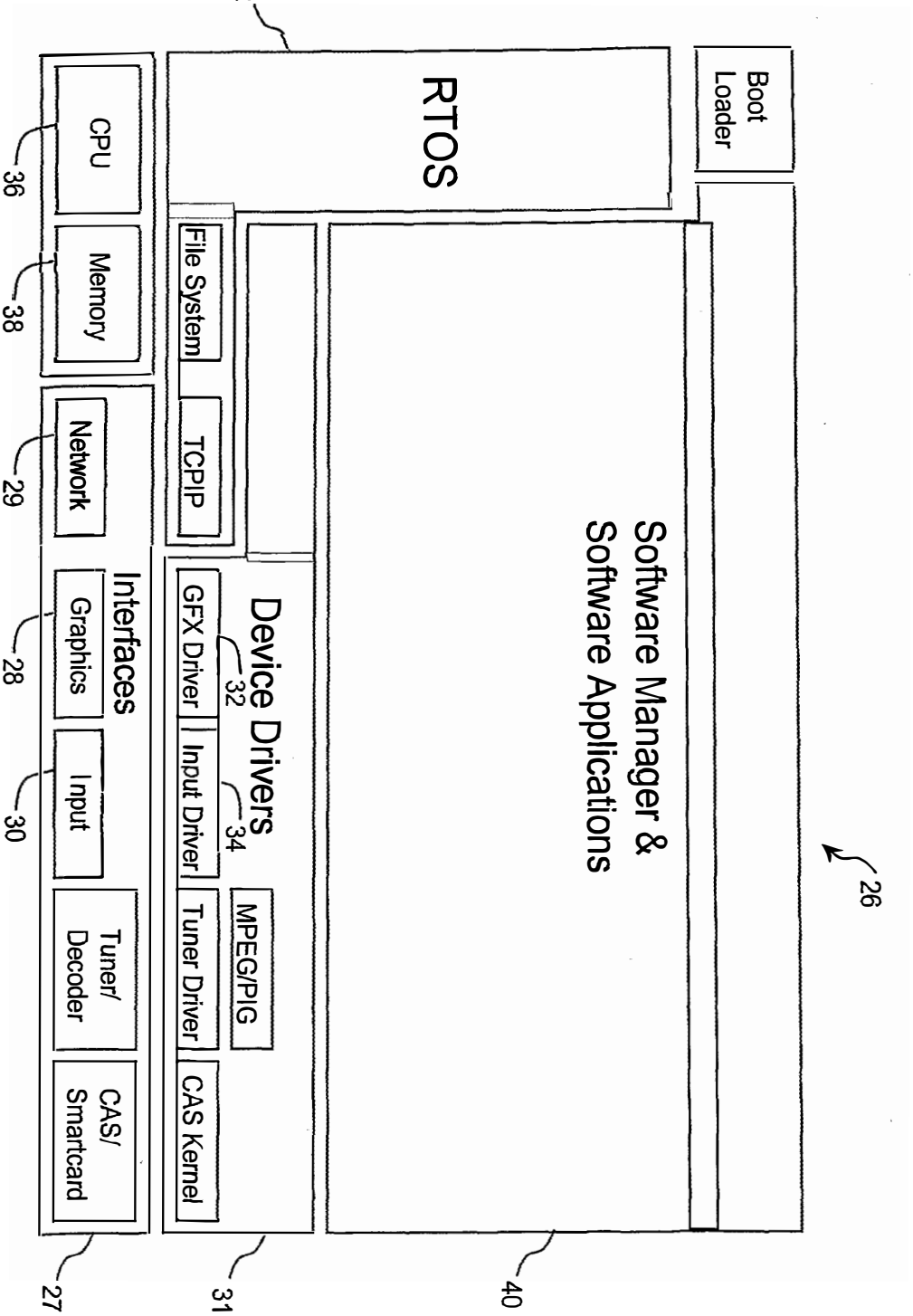

Boot Loader
RTOS
42
Software Manager & Software Applications
26
40
File System
TCPIP
Device Drivers
31
GFX Driver
32
Input Driver
34
MPEG/PIG
Tuner Driver
CAS Kernel
CPU
36
Memory
38
Network
29
Interfaces
Graphics
28
Input
30
Tuner/ Decoder
CAS/ Smartcard
27

Fig. 2

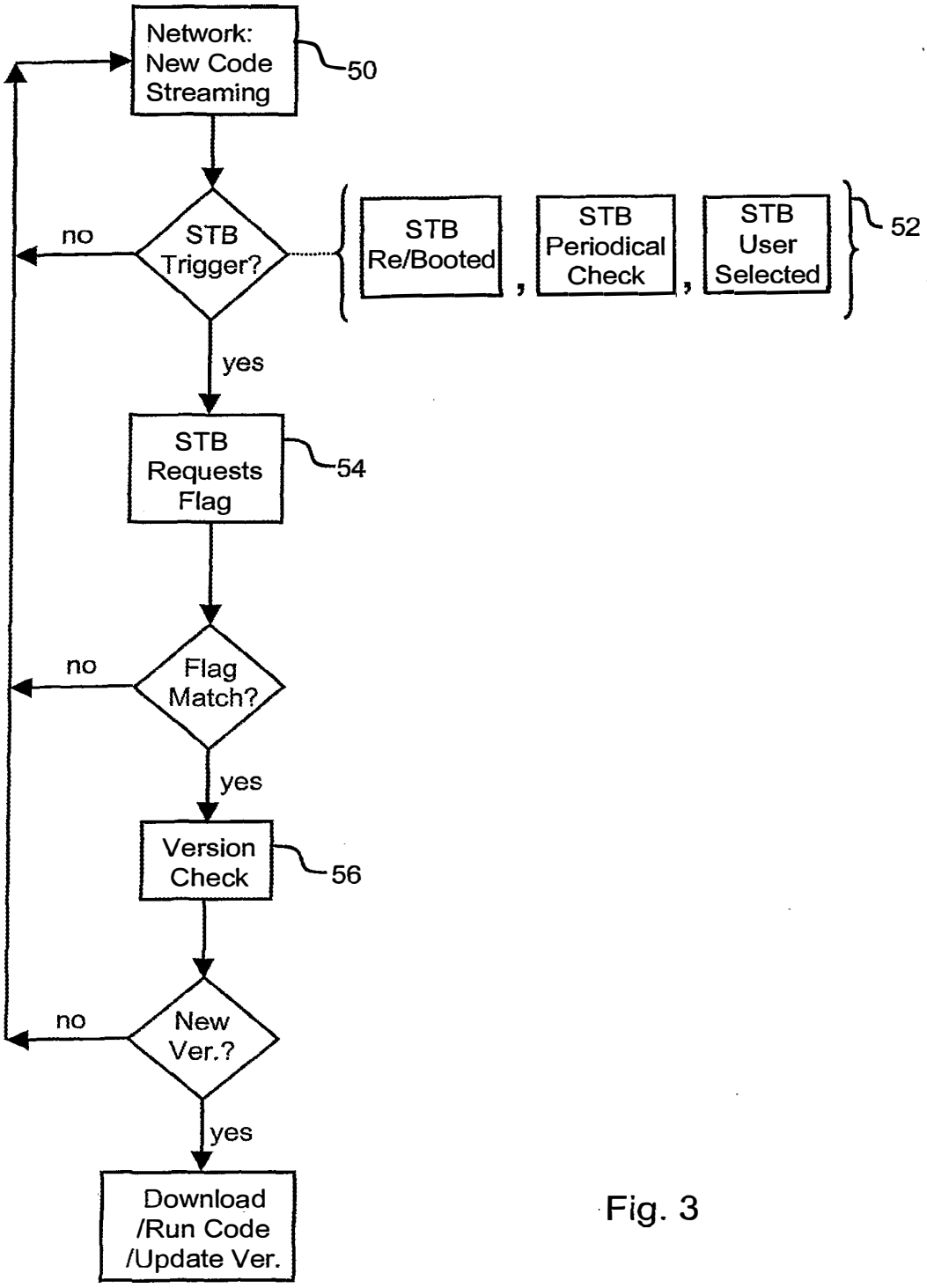

Network: New Code Streaming
50
STB Trigger?
no
yes
STB Re/Booted
STB Periodical Check
STB User Selected
52
STB Requests Flag
54
Flag Match?
no
yes
Version Check
56
New Ver.?
no
yes
Download /Run Code /Update Ver.

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB2004/002570

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00/64178 A (GEN INSTRUMENT CORP) 26 October 2000 (2000-10-26)	1-6, 8-30, 32-50, 52-59
Y	abstract page 1, line 13 - line 18 page 3, line 11 - line 17 page 3, line 23 - page 5, line 10 page 6, line 3 - page 7, line 24 page 13, line 3 - line 7 page 13, line 21 - line 28 page 16, line 19 - page 18, line 14 figures 1,3,4	7,31,51

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
2 November 2004	10/11/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ricardo, P

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB2004/002570

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 96/41472 A (KLOSTERMAN BRIAN L ; MILNES KENNETH A (US); STARSIGHT TELECAST INC (US) 19 December 1996 (1996-12-19)	7,31,51
A	page 2, line 35 - page 3, line 24 page 6, line 37 - page 8, line 3 figures 1,2 claims 1,16,26	1-6, 8-30, 32-50, 52-59
A	US 2002/083442 A1 (ELDERING CHARLES A) 27 June 2002 (2002-06-27) paragraphs '0012! - '0014! paragraphs '0028! - '0031! figure 1A	1-59
A	US 2003/041335 A1 (GAUTIER ERIC ET AL) 27 February 2003 (2003-02-27) paragraphs '0032! - '0034! paragraphs '0062!, '0063! paragraphs '0067!, '0068! figure 2	1-59

ForcePoint LLC
EX-1010-PT2
Page230

INTERNATIONAL SEARCH REPORT

tional Application No
/GB2004/002570

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0064178 A	26-10-2000	AU 4241500 A	02-11-2000
		AU 4241600 A	02-11-2000
		AU 4348600 A	02-11-2000
		AU 770984 B2	11-03-2004
		AU 4459600 A	02-11-2000
		BR 0009901 A	12-03-2002
		BR 0009902 A	12-03-2002
		BR 0009903 A	12-03-2002
		CA 2370214 A1	26-10-2000
		CA 2370764 A1	26-10-2000
		CA 2371144 A1	26-10-2000
		CA 2382509 A1	26-10-2000
		CN 1355996 T	26-06-2002
		CN 1355997 T	26-06-2002
		EP 1181824 A1	27-02-2002
		EP 1181825 A1	27-02-2002
		EP 1172005 A1	16-01-2002
		EP 1172006 A1	16-01-2002
		JP 2002542736 T	10-12-2002
		TW 480887 B	21-03-2002
		TW 472489 B	11-01-2002
		TW 503662 B	21-09-2002
		TW 472490 B	11-01-2002
		WO 0064178 A1	26-10-2000
		WO 0064179 A1	26-10-2000
		WO 0064180 A1	26-10-2000
		WO 0064181 A1	26-10-2000
		US 6718374 B1	06-04-2004
WO 9641472 A	19-12-1996	AU 714491 B2	06-01-2000
		AU 5990596 A	30-12-1996
		BR 9608610 A	25-04-2000
		CA 2223424 A1	19-12-1996
		EP 0830785 A1	25-03-1998
		JP 2001527702 T	25-12-2001
		WO 9641472 A1	19-12-1996
		US 2003167473 A1	04-09-2003
US 2002083442 A1	27-06-2002	AU 8699801 A	13-03-2002
		WO 0219581 A1	07-03-2002
		US 2002083435 A1	27-06-2002
		US 2002072966 A1	13-06-2002
		US 2002026638 A1	28-02-2002
		US 2002083444 A1	27-06-2002
		US 2002083439 A1	27-06-2002
		US 2002083443 A1	27-06-2002
		US 2002083445 A1	27-06-2002
		US 2002083441 A1	27-06-2002
		US 2001032333 A1	18-10-2001
		US 2002087975 A1	04-07-2002
		US 2002056107 A1	09-05-2002
		US 2002144263 A1	03-10-2002
US 2003041335 A1	27-02-2003	FR 2809838 A1	07-12-2001
		FR 2809839 A1	07-12-2001
		AU 3030901 A	16-07-2001
		CN 1415170 T	30-04-2003
		EP 1245116 A1	02-10-2002

ForcePoint LLC
EX-1010-PT2
Page231

INTERNATIONAL SEARCH REPORT

International Application No
GB2004/002570

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003041335 A1		WO 0150762 A1	12-07-2001
		JP 2003534676 T	18-11-2003

Form PCT/ISA/210 (patent family annex) (January 2004)

Electronic Acknowledgement Receipt

EFS ID:	27481525
Application Number:	14816931
International Application Number:	
Confirmation Number:	1044
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	127962
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012A
Receipt Date:	11-NOV-2016
Filing Date:	03-AUG-2015
Time Stamp:	07:51:11
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	Non Patent Literature	14499237_app_09-28-14.pdf	577444 ceef5ab4386d6fd22a345a9d148b9150a936eb6e	no	80

Warnings:

Information:					
2	Non Patent Literature	14499239_app_09-29-14.pdf	557462 8503777aefd4cb9141344ee35d0b6ed7c740a6ef	no	78
Warnings:					
Information:					
3	Non Patent Literature	14499241_app_09-29-14.pdf	563862 37c7a20e78cab316f1b96a4fa5687fe933e5e0e7	no	79
Warnings:					
Information:					
4	Non Patent Literature	14499241_preOA_12-15-14.pdf	101724 bc4b6ae56ff4272ac07e06fc56f6e842eaa9597b	no	3
Warnings:					
Information:					
5	Non Patent Literature	14499244_app_09-29-14.pdf	557406 83c1fbb2f820febec5c5e7a008c2a71533093e2e	no	79
Warnings:					
Information:					
6	Non Patent Literature	14499246_app_09-29-14.pdf	566764 1c91f78855a391f682ff19d1752580c92f7fd511	no	80
Warnings:					
Information:					
7	Non Patent Literature	14499250_app_09-29-14.pdf	562993 367a5b54f73ee999b3cca4d46bf8a3964caeeef7	no	79
Warnings:					
Information:					
8	Non Patent Literature	60484085_app_07-01-03.pdf	605302 c8a0dbfb37303c3afaa0891b874a42a4cde24fd0	no	37
Warnings:					
Information:					

9	Foreign Reference	FP01_EP1294128A1.pdf	5992326 615438e46215c59d0df1bd3e0329eeb9fe612880	no	57
Warnings:					
Information:					
10	Foreign Reference	FP02_JP2002366525A.pdf	1603629 40e85044017aa6d9fe3a8d7b2b282050f23140ad	no	6
Warnings:					
Information:					
11	Foreign Reference	FP03_WO0214987A2.pdf	3636571 3d492ad433f03fc19cbec97a83888ed0abc69690	no	47
Warnings:					
Information:					
12	Foreign Reference	FP04_WO03007192A1.pdf	7415215 3f587331da9b99334956ae2b7ead8b35791790d0	no	67
Warnings:					
Information:					
13	Foreign Reference	FP05_WO03029940A2.pdf	2468732 b5f8e4e14e19fab92658d4ce97adeb99792714b9	no	24
Warnings:					
Information:					
14	Foreign Reference	FP06_WO03029941A2.pdf	2381205 4e86d969dab64248536fe7d72aeee80118f9482e	no	24
Warnings:					
Information:					
15	Foreign Reference	FP07_WO2004086168.pdf	19154230 7e67dd169bcd37de99f6ee8052387043e9caec1f	no	88
Warnings:					
Information:					

16	Foreign Reference	FP08_WO2004114663.pdf	6901827 fb131e3ae4ac53d83d0afa99af57edbfa5dc25d7	no	31
Warnings:					
Information:					
17	Non Patent Literature	NPL01_60448313_prevensys_provisional.pdf	17149217 6113f53ab0cf403036a4339150e8a03f244443c6	no	141
Warnings:					
Information:					
18	Non Patent Literature	NPL02_Symantec_unveils_vulnerability_assessment_tool.pdf	1904932 e6cff707c419c919fe80182c6caae00965b9d453	no	16
Warnings:					
Information:					
19	Non Patent Literature	NPL03_SymantecIntroducesNewVulnerabilityAssessmentSolution.pdf	346170 8e3038aa72de9d06f7efbd26301f8c98f21cb13a	no	2
Warnings:					
Information:					
20	Non Patent Literature	NPL04_Enterprise-Support-Symantec-Corp-IntrotoSymantecVulnerabilityAssessment1.pdf	956297 d91e53aba6861e06de55d4b7e7b5cdd718c6519d	no	14
Warnings:					
Information:					
21	Non Patent Literature	NPL05_va-ids.pdf	1766118 9858595ca26f28f251d2e43b2a19e698eeb51ae8	no	10
Warnings:					
Information:					
22	Non Patent Literature	NPL06_IDSCorrelationofVADataandIDSAlerts_SymantecConnect.pdf	1276783 8d12f1a2680b1870fcbf1cccceb3021178764ae7	no	7
Warnings:					
Information:					

23	Non Patent Literature	NPL07_QualysIntroducesFirstNetworkVulnerabilityAssessmentPlatform.pdf	500576 cb9068b929ffb0551fcae246ea12b33a45b21e18	no	2
Warnings:					
Information:					
24	Non Patent Literature	NPL08_QualysIntroducesNewIntranetScannerAppliance.pdf	565707 f49af14b0550e425b531da1f5cd14bf8b8f89baf	no	3
Warnings:					
Information:					
25	Non Patent Literature	NPL09_bank_of_west.pdf	552061 6f8641298e397781e7449d68e4962e5bffa6a0b4	no	2
Warnings:					
Information:					
26	Non Patent Literature	NPL10_example.pdf	895103 2381d78fa2b0a6c995e08708ad0d6b9d17b22ec5	no	5
Warnings:					
Information:					
27	Non Patent Literature	NPL11_manage.pdf	957159 6d83e6918e02244b3f8192d4319fc846249ee23f	no	6
Warnings:					
Information:					
28	Non Patent Literature	NPL12_TenableNetworkSecurityInc.pdf	474211 db01ebe8234cbffea4c19750bc7b2ff41acfc6ef	no	3
Warnings:					
Information:					
29	Non Patent Literature	NPL13_screenshots.pdf	297991 ca9670115b57520ba0ec1a3deda13c0043c5fe92	no	2
Warnings:					
Information:					

30	Non Patent Literature	NPL14_SecurityProfilingNews.pdf	145137 92b8b353b2d2109d0d77a2f9ce0a5c658c792a6e	no	1
Warnings:					
Information:					
31	Non Patent Literature	NPL15_norton_ghost.pdf	20432905 c2ba68bf467e092ad16320315b2f95887372c069	no	221
Warnings:					
Information:					
32	Non Patent Literature	NPL16_ImplementationGuide.pdf	11586522 48dc882c12a82110a791c4a630ea9ff251ab37a9	no	108
Warnings:					
Information:					
33	Non Patent Literature	NPL17_LighteningSANSReview.pdf	3256219 11f12de864ff893230d617c123273161980f57ed	no	18
Warnings:					
Information:					
34	Non Patent Literature	NPL18_60441422.pdf	12161874 e4f97d333d90c60e0991d2052692000e25bd70d0	no	71
Warnings:					
Information:					
35	Non Patent Literature	NPL19_60388078.pdf	16914758 b4e3b64f7e781271b4c585921151f2f0b20333e6	no	140
Warnings:					
Information:					
36	Non Patent Literature	NPL20_60345689.pdf	3987250 11708f2be33012b53e10b981597e4d9ee0142963	no	38
Warnings:					
Information:					

37	Non Patent Literature	NPL01_CERT_Incident_Note.pdf	185520 0a8104081111ff606743c6070e7303581365bda0	no	3
Warnings:					
Information:					
38	Non Patent Literature	NPL02_StateOfThePracticeOfIntrusionDetectionTechnologies.pdf	5426831 f38c9896966f51e17e12f90501ab4bf5f256218d	no	240
Warnings:					
Information:					
39	Non Patent Literature	NPL03_ReviewSPQUERY.pdf	88355 a2bef8301740f4f993c2f0ee7e121d652edeafb5	no	2
Warnings:					
Information:					
40	Non Patent Literature	NPL04_ReadyForWindows200SP1.pdf	106377 da13948f3de77933bfd795c7038e31e4d1c346b5	no	2
Warnings:					
Information:					
41	Non Patent Literature	NPL05_UsefulSPQuery3.pdf	215429 fe48c77fd6591141ae6de59970fff8af66e095f4	no	4
Warnings:					
Information:					
42	Non Patent Literature	NPL06_SPQueryUsersManual4_2.pdf	2409396 605d2af8e96552387c28c3ba346def2ab843a473	no	58
Warnings:					
Information:					
43	Non Patent Literature	NPL07_WebConsoleCore4_0forNetware.pdf	204712 e7946526333d4bf33cd0621e51f8c2e74b79bd27	no	3
Warnings:					
Information:					

44	Non Patent Literature	NPL08_GravitixThePatchFinder.pdf	86496 114103ee5f538c53d077dfd9db8715136e6665a6	no	1
Warnings:					
Information:					
45	Non Patent Literature	NPL09_UltimateSecurityToolkit.pdf	167606 cb735cb474768ccf7dec9e7f730e906fc2aa2f85	no	3
Warnings:					
Information:					
46	Non Patent Literature	NPL10_NetworkVulnerabilityAssessmentReport.pdf	191391 664af52bb5b551978f84d2940ee933105eef57d3	no	4
Warnings:					
Information:					
47	Non Patent Literature	NPL11_HostVulnerabilitySummaryReport.pdf	400254 3ac5e50456281048de3a086593b1342285c80ffa	no	8
Warnings:					
Information:					
48	Non Patent Literature	NPL12_InternetSecuritySystems_SecuringEBusiness.pdf	138531 f70f8601c924f596c7da116d8c22a7ee37f4ade4	no	1
Warnings:					
Information:					
49	Non Patent Literature	NPL13_InternetSecuritySystems_InternetScanner.pdf	162873 d38fec614b97abb40bde245fdd4a91126089508b	no	2
Warnings:					
Information:					
50	Non Patent Literature	NPL14_ToSetupSecurePCNetwork.pdf	885114 075305249c575e2c38a511dfcca66dcf00664dea	no	15
Warnings:					
Information:					

51	Non Patent Literature	NPL15_MicrosoftSecurityGlossary.pdf	870868 4219b3e284ecc409d3189822af336dd9953b7629	no	18
Warnings:					
Information:					
52	Non Patent Literature	NPL16_60234680.pdf	3357034 57ec37e59c8dcabcb12bb1f298e8dd85c9711062	no	80
Warnings:					
Information:					
53	Non Patent Literature	NPL17_GravitixScreenshot.pdf	81589 7060cf18ce65cf47000abc27d3ab6898b0a5395a	no	1
Warnings:					
Information:					
54	Non Patent Literature	NPL18_14138014_07-10-2015.pdf	2719634 6a9eae219ac34ec4138147d2f360e1b2436ed8ce	no	58
Warnings:					
Information:					
55	Non Patent Literature	NPL19_14834102_03-24-2016.pdf	1246266 142eb82b03df01e05aac3619b911c699d323b6e7	no	36
Warnings:					
Information:					
56	Non Patent Literature	NPL20_14834102_10-7-2016.pdf	912355 59b68f24f984f30e0d2c44a60757cb43642be6f3	no	18
Warnings:					
Information:					
57	Non Patent Literature	NPL21_14816960_12-30-2015.pdf	365870 afaa0a640e2ea7e142f71aa45a737abc613b0cce	no	10
Warnings:					
Information:					

58	Non Patent Literature	NPL22_14816960_09-13-2016.pdf	565162 bae04d891cdccead0885dc8df5f0fec44dd4305d	no	12
Warnings:					
Information:					
59	Non Patent Literature	NPL23_14499234_01-19-2016.pdf	348785 feaaf670887e8096d1847df93c4314fe8c97cf15	no	5
Warnings:					
Information:					
60	Non Patent Literature	NPL24_14499234_01-29-2016.pdf	79871 c0df4a1b0b0eebf86f3fc1e7f39d8572e8444a5c	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	170990001		

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.

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. 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 contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	14/816,931	Filing Date	2015-08-03	Docket Number (if applicable)	SP1P012A	Art Unit	2438
First Named Inventor	Brett M. Oliphant			Examiner Name	Madhuri R HERZOG		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, to any international application that does not comply with the requirements of 35 U.S.C. 371, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV.

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

☐ Other _____

☒ Enclosed

☒ Amendment/Reply

☒ Information Disclosure Statement (IDS)

☐ Affidavit(s)/ Declaration(s)

☐ Other _____

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

☐ **The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.**
The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No _____

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

☐ Applicant Signature

EFS - Web 2.1.15

PTO/SB/30EFS (07-14)
Approved for use through 07/31/2016. 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 contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Patrick E. Caldwell/	Date (YYYY-MM-DD)	2016-11-10
Name	Patrick E. Caldwell, Esq.	Registration Number	44580

This collection of information is required by 37 CFR 1.114. 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.

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

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 1044
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 14/816,931	Art Unit: 2438
File Date: 2015-08-03	Docket No.: SP1P012A
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: November 10, 2016

AMENDMENT B (37 CFR 1.112) WITH RCE (37 CFR 1.114)

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

Examiner:

In response to the communication mailed 2016-08-10 (hereafter "Notice of Allowance" or "NOA"), please consider the following amendments.

ForcePoint LLC
EX-1010-PT2
Page246

Amendments to the Claims:

The listing of amended claims follows:

1. (Previously presented) An apparatus, comprising:

at least one data storage;

at least one platform communicatively coupled to the at least one data storage; and

at least one agent capable of being communicatively coupled to the at least one platform;

said at least one data storage configured to store data on a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

said at least one platform configured to:

cause display of at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allow receipt of user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability;

ForcePoint LLC
EX-1010-PT2
Page247

said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability, so that the at least one mitigation technique is capable of being applied;

said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

2. (Previously presented) The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to first user input received prior to the attack, the firewall option is capable of being applied to a plurality of different devices for preventing the at least one attack packet at any of the different devices; and the apparatus is further configured such that, in response to additional user input after the attack in connection with a particular single device of the plurality of different devices, the intrusion detection or prevention option is capable of being applied to the particular single device.

3. (Previously presented) The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to first user input prior to the attack, the intrusion detection or prevention option is capable of being applied to a plurality of different devices at the plurality of different devices; and the apparatus is further configured such that, in response to second user input after the attack in connection with a particular single device of the plurality

of different devices, the firewall option is capable of being applied to the particular single device for preventing the at least one attack packet at the particular single device.

4. (Previously presented) The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification of the operating system in connection the displaying of the at least one mitigation technique, so that, in order to avoid false positives, relevant vulnerabilities prompt mitigation technique user selection among at least two of the mitigation techniques, which involve both firewall and intrusion prevention system actions, for providing diverse mitigation options in connection with the relevant vulnerabilities.

5. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification of the operating system prior to causing the display of the at least one mitigation technique, so that which of the one or more of the mitigation techniques that is caused to be displayed is based on one or more actual vulnerabilities to which the at least one device is actually vulnerable so that only relevant one or more mitigation techniques are displayed for selection by a user for attack mitigation.

6. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the user input is capable of being received via at least one user interface of the at least one platform for different devices, for allowing different attack mitigation actions including at least one intrusion prevention action and at least one firewall action to be selectively applied to the different devices for different actual vulnerabilities determined to be actually relevant based on the identification of the operating system in connection with the different devices.

7. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a first

mitigation technique that utilizes a firewall action and a second mitigation technique that utilizes an intrusion prevention action;

8. (Original) The apparatus of Claim 7, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

9. (Original) The apparatus of Claim 7, wherein the apparatus is configured such that the at least one mitigation technique further includes a third mitigation technique that utilizes a policy compliance action, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique, the second mitigation technique, and the third mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device; only the second mitigation technique being selectively applied by the user to at least one second device; and the first mitigation technique, the second mitigation technique, and the third mitigation technique being selectively applied by the user to at least one third device.

10. (Previously presented) The apparatus of Claim 7, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from an integrated firewall/intrusion prevention system platform component of the at least one platform to firewall-supporting code of the at least one agent, and the second mitigation

technique is automatically applied utilizing a second communication from the integrated firewall/intrusion prevention system platform component of the at least one platform to intrusion prevention system-supporting code of the at least one agent, where the firewall-supporting code and the intrusion prevention system-supporting code are part of the at least one agent.

11. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the identification of the operating system is a result of a vulnerability assessment scan caused by the at least one platform.

12. (Original) The apparatus of Claim 1, wherein the at least one platform includes intrusion prevention functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality.

13. (Original) The apparatus of Claim 1, wherein the at least one platform utilizes router-based functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique.

14. (Previously presented) The apparatus of Claim 13, wherein the apparatus is configured for receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation

techniques to allow selective utilization of the router-based functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the router-based functionality and the firewall functionality.

15. (Previously presented) The apparatus of Claim 1, wherein at least one of:

said at least one data storage includes at least one database;

said at least one data storage is accessed utilizing an operation including at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said mitigation techniques include remediation techniques;

each mitigation technique has a mitigation type including the patch;

each mitigation technique has a mitigation type including the policy setting;

each mitigation technique has a mitigation type including the configuration option;

each mitigation technique is capable of mitigating the effect of the attack that takes advantage of the corresponding vulnerability, by dropping packets associated with the attack or removing the corresponding vulnerability;

said information is capable of being used to determine an intended destination of a connection request; or

said information includes a vulnerability identifier;

wherein the apparatus is operable for use with at least one network operations center (NOC) server, a data warehouse, and a software development kit (SDK) for allowing access to information associated with at least one vulnerability and at least one remediation technique; and wherein the apparatus is operable for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

16. (Previously presented) An apparatus, comprising:

at least one data storage configured to store at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; and

at least one platform communicatively coupled to the at least one data storage, the at least one platform configured to:

based on user selection, automatically apply at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type;

receive information in connection with at least one of a plurality of devices,

identify an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information, and

mitigate an effect of the attack on the at least one device that takes advantage of the at least one vulnerability, based on the automatic application of the at least two of the plurality of mitigation techniques including the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type to the at least one device;

wherein the apparatus is configured such that the at least two of the plurality of mitigation techniques are made available for the user selection, based on an identification of an operating system.

17. (Original) The apparatus of Claim 16, wherein the apparatus is configured such that the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by at least one agent that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied.

18. (Original) The apparatus of Claim 17, wherein the apparatus is configured such that the at least one agent is further capable of supporting a vulnerability assessment scan for the identification of the operating system.

19. (Original) The apparatus of Claim 16, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from the at least one platform to firewall-supporting code of at least one agent, and the second mitigation technique is automatically applied utilizing a second communication from the at least one platform to intrusion prevention system-supporting code of the at least one agent; wherein the at least one platform includes intrusion prevention functionality for supporting the first mitigation technique and firewall functionality for supporting the second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally make available for the user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are made available for the

user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user selections are capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

20. (Previously presented) An apparatus, comprising:

means for identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities associated with an operating system, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

means for:

causing display of at least two of the mitigation techniques for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allowing receipt of at least one user input in connection with one or more of the at least two mitigation techniques; and

means for applying the one or more of the at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device;

said apparatus configured such that the at least two mitigation techniques are displayed based on an identification of an operating system.

21. (Original) The apparatus of Claim 20, wherein the apparatus is configured such that the at least one first mitigation technique is automatically applied utilizing a first communication to firewall-supporting code, and the at least one second mitigation technique is automatically applied utilizing a second communication to intrusion prevention system-supporting code; wherein the apparatus includes intrusion prevention functionality for supporting the at least one first mitigation technique and firewall functionality for supporting the at least one second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by at least one component that also supports identification of attacks in connection with the at least one device, the apparatus further capable of receiving actual vulnerability information to conditionally make available for user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are made available for the user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the at least one first mitigation technique and the at least one second mitigation technique to be selectively applied to the different devices for different actual vulnerabilities, such that the different user selections are capable of resulting in: only the at least one first mitigation technique being selectively applied to at least one first device, only the at least one second mitigation technique being selectively applied to at least

one second device, and both the at least one first mitigation technique and the at least one second mitigation technique being selectively applied to at least one third device.

22. (New) The apparatus of Claim 1, wherein the apparatus is configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an application.

ForcePoint LLC
EX-1010-PT2
Page257

Remarks:

Summary

Claims 1-21 were pending.

Claims 1-22 are pending, with claims 1, 16, and 20 being independent. Claim 22 has been added. No new subject matter has been added.

Allowable Subject Matter

The Examiner is thanked for the allowable subject matter of Claims 1-21.

New Claims

The applicant brings to the Examiner's attention the subject matter of new Claim 22 below, which is added for full consideration:

> 22. The apparatus of Claim 1, wherein the apparatus is configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an application.

A notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Conclusion

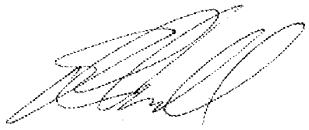
It is believed that all of the pending issues have been addressed. Claims 1-22 are in condition for allowance per the claim amendments herein.

However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, with the exception of Claim 20 (and any dependent claims), it should be noted that no claims are intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant hereby encloses the appropriate fee for the request for continued examination. Applicant does not believe that any additional fees are due. However, in the event that any

other fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-5939 (Order No. SP1P012A).

Respectfully submitted,



Dated: 10 Nov 2016

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6957348		2005-12-18	Flowers et al.	
	2	6766458		2004-07-20	Harris, et al.	
	3	6907531		2005-06-14	Dodd et al.	
	4	7178166		2007-02-13	Taylor, et al.	
	5	7185232		2007-02-27	Leavy et al.	
	6	7234163		2007-06-19	Rayes et al.	
	7	7257630		2007-08-14	Cole et al.	
	8	7331061		2008-12-02	Ramsey et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	9	7367054		2008-04-29	Soppera, Andrea	
	10	7496960		2009-02-24	Chen et al.	
	11	8250654		2012-21-08	Kennedy et al.	
	12	8266320		2012-09-11	Bell et al.	
	13	5999179		1999-12-07	Kekic, et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20020138416		2002-09-26	Lovejoy et al.	
	2	20020171546		2002-11-21	Evans et al.	
	3	20030177389		2003-09-18	Albert et al.	
	4	20030233438		2003-12-18	Hutchinson et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	5	20040148520		2004-07-29	Talpade et al.	
	6	20050193430		2005-09-01	Cohen et al.	
	7	20050216957		2005-09-29	Benzhof et al.	
	8	20060041936		2006-02-23	Anderson et al.	
	9	20080047016		2008-02-21	Spoonamore, Stephen	
	10	20080127349		2008-05-29	Ormazabal et al.	
	11	20080222724		2008-09-11	Ormazabal et al.	
	12	20090077666		2009-03-19	Chen et al.	
	13	20100218256		2010-08-26	Thomas et al.	
	14	20100241478		2010-09-23	Sahinoglu; Mehmet	
	15	20110138036		2001-06-09	Tyree, David S.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	16	20120110671		2012-05-03	Beresnevichiene et al.	
	17	20120173931		2012-07-05	Kube et al.	
	18	20120210434		2012-08-16	Curtis et al.	
	19	20130055394		2013-02-28	Beresnevichiene et al.	
	20	20140215605		2014-07-31	Decime et al.	
	21	20140331326		2014-05-06	Thakur; Satyendra	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2]	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	1	Office Action Summary in U.S. Pat. App. No. 14/138,014 dated 2/24/2015	☐
	2	Office Action Summary in U.S. Pat. App. No. 14/499,226 dated 2/20/2015	☐
	3	Office Action Summary in U.S. Pat. App. No. 14/499,227 dated 01/27/2015	☐
	4	Office Action Summary in U.S. Pat. App. No. 14/499,230 dated 01/08/2015	☐
	5	Office Action Summary in U.S. Pat. App. No. 14/499,234 dated 02/10/2015	☐
	6	Office Action Summary in U.S. Pat. App. No. 14/499,235 dated 01/21/2015	☐
	7	Office Action Summary in U.S. Pat. App. No. 14/499,237 dated 01/20/2015	☐
	8	Office Action Summary in U.S. Pat. App. No. 14/499,241 dated 3/4/2015	☐
	9	Office Action Summary in U.S. Pat. App. No. 14/499,244 dated 2/23/2015	☐
	10	Office Action Summary in U.S. Pat. App. No. 14/499,246 dated 01/28/2015	☐
	11	Office Action Summary in U.S. Pat. App. No. 14/499,250 dated 01/16/2015	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	12	Interview Summary in U.S. Pat. App. No. 14/138,014 dated 2/9/2015	☐
	13	Interview Summary in U.S. Pat. App. No. 14/138,230 dated 2/9/2015	☐
	14	Interview Summary in U.S. Pat. App. No. 14/138,246 dated 2/3/2015	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2016-11-10
Name/Print	Patrick Caldwell	Registration Number	44580

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2436

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	1	U.S. Prov. Pat. App. No. 60/484,085 filed 07/01/2003
	2	U.S. Pat. App. No. 10/882,588 filed 07/01/2004
	3	Office Action Summary in US Pat. App. No. 10/882,588 dated 05/29/2009
	4	Office Action Summary in US Pat. App. No. 10/882,588 dated 10/12/2010
	5	Office Action Summary in US Pat. App. No. 10/882,588 dated 06/12/2012
	6	Office Action Summary in US Pat. App. No. 10/882,588 dated 01/08/2010
	7	Office Action Summary in US Pat. App. No. 10/882,588 dated 04/15/2011
	8	Office Action Summary in US Pat. App. No. 10/882,588 dated 06/24/2010
	9	Office Action Summary in US Pat. App. No. 10/882,588 dated 09/26/2007
	10	Office Action Summary in US Pat. App. No. 10/882,588 dated 10/20/2011
	11	U.S. Pat. App. No. 10/882,788 filed 07/01/2004
	12	Office Action Summary in US Pat. App. No. 10/882,788 dated 12/22/2008
	13	Office Action Summary in US Pat. App. No. 10/882,788 dated 07/10/2008
	14	Office Action Summary in US Pat. App. No. 10/882,788 dated 10/04/2007
	15	U.S. Pat. App. No. 10/882,852 filed 07/01/2004
	16	Office Action Summary in US Pat. App. No. 10/882,852 dated 5/15/2013
	17	Office Action Summary in US Pat. App. No. 10/882,852 dated 6/01/2010

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2436

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	18	Office Action Summary in US Pat. App. No. 10/882,852 dated 8/14/2008
	19	Office Action Summary in US Pat. App. No. 10/882,852 dated 6/24/2009
	20	Office Action Summary in US Pat. App. No. 10/882,852 dated 11/01/2007
	21	U.S. Pat. App. No. 10/882,853 filed 07/01/2004
	22	Office Action Summary in US Pat. App. No. 10/882,853 dated 3/18/2009
	23	Office Action Summary in US Pat. App. No. 10/882,853 dated 4/30/2008
	24	Office Action Summary in US Pat. App. No. 10/882,853 dated 10/17/2008
	25	Office Action Summary in US Pat. App. No. 10/882,853 dated 10/31/2007
	26	U.S. Pat. App. No. 10/883,376 filed 07/01/2004
	27	Office Action Summary in US Pat. App. No. 10/883,376 dated 9/11/2008
	28	Office Action Summary in US Pat. App. No. 10/883,376 dated 5/06/2008
	29	U.S. Pat. App. No. 10/884,329 filed 07/01/2004
	30	Office Action Summary in US Pat. App. No. 10/884,329 dated 11/29/2007
	31	U.S. Pat. App. No. 14/138,014 filed 12/31/2013
	32	Office Action Summary in US Pat. App. No. 14/138,014 dated 8/28/2014
	33	U.S. Pat. App. No. 14/499,226 filed 9/28/2014
	34	U.S. Pat. App. No. 14/499,227 filed 9/28/2014
	35	Office Action Summary in US Pat. App. No. 14/499,227 dated 12/15/2014
	36	U.S. Pat. App. No. 14/499,230 filed 9/28/2014
	37	U.S. Pat. App. No. 14/499,234 filed 9/28/2014
	38	U.S. Pat. App. No. 14/499,235 filed 9/28/2014
	39	Office Action Summary in US Pat. App. No. 14/499,235 dated 12/15/2014
	40	U.S. Pat. App. No. 14/499,236 filed 9/28/2014
	41	Office Action Summary in US Pat. App. No. 14/499,236 dated 12/30/2014
	42	U.S. Pat. App. No. 14/499,237 filed 9/28/2014
	43	U.S. Pat. App. No. 14/499,239 filed 9/29/2014
	44	U.S. Pat. App. No. 14/499,241 filed 9/29/2014

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2436

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	45	Office Action Summary in US Pat. App. No. 14/499,241 dated 12/15/2014
	46	U.S. Pat. App. No. 14/499,244 filed 9/29/2014
	47	U.S. Pat. App. No. 14/499,246 filed 9/29/2014
	48	U.S. Pat. App. No. 14/499,250 filed 9/29/2014

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 1044
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 14/816,931	Art Unit: 2438
File Date: 2015-08-03	Docket No.: SP1P012A
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: November 10, 2016

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§ 1.56 AND 1.97(b)

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

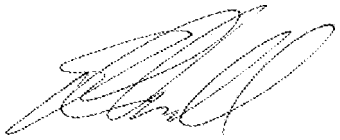
Dear Sir:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

This Information Disclosure Statement is believed to be filed within three months of the filing date of a national application other than a continued prosecution application, within three months of the date of entry of the national stage 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. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement.

Respectfully submitted,



Dated: 10 Nov 2016

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

PTO/SB/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5008814		1991-04-16	Mathur	
	2	5253932		1993-10-19	Nesovic	
	3	5335346		1994-08-02	Fabbio	
	4	5683638		1997-11-04	Crigler et al.	
	5	5765153		1998-06-09	Benantar et al.	
	6	5892903		1999-04-06	Klaus	
	7	5991881		1999-11-23	Conklin et al.	
	8	6005942		1999-12-21	Chan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	9	6044466		2000-03-28	Anand et al.	
	10	6074727		2000-06-13	Miller et al.	
	11	6131163		2000-10-10	Wiegel	
	12	6185689		2001-02-06	Todd Sr. et al.	
	13	6219786		2001-04-17	Cunningham et al.	
	14	6282546		2001-08-28	Gleichauf et al.	
	15	6298445		2001-10-02	Shostack et al.	
	16	6321334		2001-11-20	Jerger et al.	
	17	6324656		2001-11-27	Gleichauf et al.	
	18	6345361		2002-02-05	Jerger et al.	
	19	6418554		2002-07-09	Delo et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	20	6473800		2002-10-29	Jerger et al.	
	21	6526513		2003-02-25	Shrader et al.	
	22	6754896		2004-06-22	Mishra et al.	
	23	6816896		2004-11-09	Fortin et al.	
	24	6966059		2005-11-15	Shetty et al.	
	25	6990591		2006-01-24	Pearson	
	26	7000247		2006-02-14	Banzhof	
	27	7010696		2006-03-07	Cambridge et al.	
	28	7051097		2006-05-23	Pecina	
	29	7051365		2006-05-23	Bellovin	
	30	7076801		2006-07-11	Gong et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	31	7080141		2006-07-18	Baekelmans et al.	
	32	7159237		2007-01-02	Schneier et al.	
	33	7178144		2007-02-13	Melchione et al.	
	34	7216343		2007-05-08	Das et al.	
	35	7228566		2007-06-05	Caceres et al.	
	36	7240193		2007-07-03	Hatfalvi et al.	
	37	7278163		2007-10-02	Banzhof et al.	
	38	7308712		2007-12-11	Banzhof	
	39	7315801		2008-01-01	Dowd et al.	
	40	7353539		2008-04-01	Brawn et al.	
	41	7424706		2008-09-09	Ivanov et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	42	7458098		2008-11-25	Judge et al.	
	43	7509676		2009-03-24	Trueba	
	44	7519954		2009-04-14	Beddoe et al.	
	45	7519994		2009-04-14	Judge et al.	
	46	7536456		2009-05-19	Williams et al.	
	47	7624422		2009-11-24	Williams et al.	
	48	7627891		2009-12-01	Williams et al.	
	49	7673043		2010-03-02	Keir et al.	
	50	7698275		2010-04-13	O'Brien et al.	
	51	7761920		2010-07-20	Bezilla et al.	
	52	7827607		2010-11-02	Sobel et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	53	7836501		2010-11-16	Sobel et al.	
	54	7882555		2011-02-01	Ben-Itzhak	
	55	8091117		2012-01-03	Williams et al.	
	56	8135823		2012-03-13	Cole et al.	
	57	8135830		2012-03-13	McClure et al.	
	58	8181173		2012-05-15	Childress et al.	
	59	8185930		2012-05-22	Alperovitch et al.	
	60	6952779		2005-10-04	Cohen et al.	
	61	6957348		2005-10-18	Flowers et al.	
	62	7073198		2006-07-04	Flowers et al.	
	63	7181769		2007-02-20	Keanini et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	64	7249187		2007-07-24	Sobel et al.	
	65	7562388		2009-07-14	Hackenberger et al.	
	66	7574740		2009-08-11	Kennis	
	67	7594273		2009-09-22	Keanini et al.	
	68	7779468		2010-08-17	Magdych et al.	
	69	7913303		2011-03-22	Rouland et al.	
	70	7954159		2011-05-31	Hrabik et al.	
	71	8121874		2012-02-21	Guheen et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010034847	A1	2001-10-25	GaulJr. Stephen E.	

ForcePoint LLC
EX-1010-PT2
Page279

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	2	20020013811	A1	2002-01-31	Kim In-Gwang	
	3	20020026591	A1	2002-02-28	Hartley Bruce V. et al.	
	4	20020104014	A1	2002-08-01	Zobel Robert David et al.	
	5	20020112179	A1	2002-08-15	Riordan James F. et al.	
	6	20020199122	A1	2002-12-26	Davis Lauren B. et al.	
	7	20030005178	A1	2003-01-02	Hemsath David Kurt	
	8	20030014669	A1	2003-01-16	Caceres Maximiliano Gerardo et al.	
	9	20030037601	A1	2003-02-27	Mansky Paul et al.	
	10	20030061506	A1	2003-03-27	Cooper Geoffrey et al.	
	11	20030084320	A1	2003-05-01	Tarquini Richard Paul et al.	
	12	20030126472	A1	2003-07-03	Banzhof Carl E.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	13	20030135749	A1	2003-07-17	Gales George S. et al.	
	14	20030145228	A1	2003-07-31	Suuronen Janne et al.	
	15	20040030778	A1	2004-02-12	Kronenberg Sandy Craig et al.	
	16	20040054764	A1	2004-03-18	Aderton Harry et al.	
	17	20040088565	A1	2004-05-06	Norman Andrew Patrick et al.	
	18	20040103310	A1	2004-05-27	Sobel William E. et al.	
	19	20040117640	A1	2004-06-17	Chu Simon C. et al.	
	20	20040243603	A1	2004-12-02	Komatsu Masaki	
	21	20050010819	A1	2005-01-13	Williams John Leslie et al.	
	22	20050015382	A1	2005-01-20	Aaron Jeffrey A.	
	23	20050033988	A1	2005-02-10	Chandrashekhar Ganesan et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	24	20050222969	A1	2005-10-06	Yip Ying-Kin Tony et al.	
	25	20050235360	A1	2005-10-20	Pearson Sterling Michael	
	26	20060265708	A1	2006-11-23	Blanding Stephen M. et al.	
	27	20070016659	A1	2007-01-18	Peck Joseph E. et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	EP1294128	EP	A1	2003-03-19	Motoyama et al.		☐
	2	JP2002366525	JP	A	2002-12-20	Koshida et al.		☐
	3	WO0214987	WO	A2	2002-02-21	Gadish et al.		☐
	4	WO03007192	WO	A1	2003-01-23	Caceres et al.		☐
	5	WO03029940	WO	A2	2003-04-10	Singleton et al.		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	6	WO03029941	WO	A2	2003-04-10	Singleton et al.		☐
	7	WO2004086168	WO		2004-10-07	Moshir et al.		☐
	8	WO2004114663	WO		2004-12-29	Patel, Dipan		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	U.S. Provisional Application No. 60/448,313, filed February 14, 2003	☐
	2	"Symantec unveils vulnerability assessment tool," May 13, 2003, retrieved from https://web.archive.org/web/20140818164413/http://www.computerweekly.com/news/2240050753/Symantec-unveils-vulnerability-assessment-tool	☐
	3	Symantec Corporation, " Symantec Introduces New Vulnerability Assessment Solution: Symantec Vulnerability Assessment Provides Vulnerability Identification and Prioritization to Proactively Secure Systems at Risk, News Release, May 12, 2003, retrieved from http://www.symantec.com/press/2003/n030512a.html	☐
	4	"Introduction to Symantec Vulnerability Assessment 1.0," January 1, 2003, retrieved from "http://www.symantec.com/business/support/index?page=content&id=TECH111970	☐
	5	GULA, Ron, "Correlating IDS Alerts with Vulnerability Information," December 2002 (Updated January 2009), pp. 1-10, retrieved from http://docs.huihoo.com/nessus/va-ids.pdf	☐
	6	DESAI, Neil, "IDS Correlation of VA Data and IDS Alerts," June 29, 2003, retrieved from http://www.symantec.com/connect/articles/ids-correlation-va-data-and-ids-alerts	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	7	"Qualys Introduces First Network Vulnerability Assessment Platform for Managed Security and Consulting Organizations," April 10, 2001, retrieved from http://www.qualys.com/company/newsroom/news-releases/usa/2001-04-10-3/	☐
	8	"Qualys Introduces New Intranet Scanner Appliance," September 30, 2002, retrieved from http://www.qualys.com/company/newsroom/news-releases/usa/2002-09-30/	☐
	9	QUALYS "CASE STUDY: Bank of the West — Major Financial Institution Protects Information Assets Through Regular Network Vulnerability Audits," July 2005, retrieved from http://www.qualys.com/docs/bank_of_west.pdf	☐
	10	GULA, Ron, "Example Lightning Deployment Scenarios," December 2002, 5 pages, retrieved from https://web.archive.org/web/20030316012821/http://www.tenablesecurity.com/example.pdf	☐
	11	GULA, Ron, "Offering Managed Security Services with Lightning," December 2002, 6 pages, retrieved from https://web.archive.org/web/20030316085246/http://www.tenablesecurity.com/manage.pdf	☐
	12	Tenable Network Security Inc., "LIGHTNING CONSOLE," 2002, retrieved from https://web.archive.org/web/20030416093233/http://www.tenablesecurity.com/console.html	☐
	13	Tenable Network Security Inc., "Screen Shots," 2002, retrieved from https://web.archive.org/web/20030214013753/http://www.tenablesecurity.com/screenshots.html	☐
	14	SecurityProfiling, "News," July 2001, retrieved from https://web.archive.org/web/20021209114707/http://securityprofiling.com/news.htm	☐
	15	Symantec Corporation, "Norton Ghost™ User's Guide," 2002, 221 pages	☐
	16	Symantec Corporation, "Symantec™ Vulnerability Assessment Implementation Guide," Version 1.0, 2003, 108 pages	☐
	17	HUBER, Robert, "Strategies for Improving Vulnerability Assessment Effectiveness in Large Organizations," SANS Institute InfoSec Reading Room, Version 1.4b (amended August 29, 2002), GSEC Option 1, April 20, 2003, 18 pages	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	18	U.S. Provisional Application No. 60/441,422, filed January 21, 2003	☐
	19	U.S. Provisional Application No. 60/388,078, filed June 11, 2002	☐
	20	U.S. Provisional Application No. 60/345,689, filed December 31, 2001	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2016-11-10
Name/Print	Patrick Caldwell	Registration Number	44580

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	1	5,210,854	05/11/1993	Beaverton et al.			
	2	5,249,705	10/05/1993	Gates			
	3	5,253,782	10/19/1993	Gates et al.			
	4	5,272,754	12/21/1993	Boerbert			
	5	5,276,735	01/04/1994	Boebert et al.			
	6	5,361,359	11/01/1994	Tajalli et al.			
	7	5,499,297	03/12/1996	Boebert			
	8	5,502,766	03/26/1996	Boebert et al.			
	9	5,557,346	09/17/1996	Lipner et al.			
	10	5,557,765	09/17/1996	Lipner et al.			
	11	5,596,718	01/21/1997	Boebert et al.			
	12	5,612,503	03/18/1997	Sepp			
	13	5,640,454	06/17/1997	Lipner et al.			
	14	5,662,291	09/02/1997	Sepp et al.			
	15	5,696,907	12/09/1997	Tom			
	16	5,745,573	04/28/1998	Lipner et al.			
	17	5,796,836	08/18/1998	Markham			
	18	5,819,275	10/06/1998	Badger et al.			
	19	5,822,435	10/13/1998	Boebert et al.			
	20	5,831,987	11/03/1998	Spilo			
	21	5,864,683	01/26/1999	Boebert et al.			
	22	5,867,647	02/02/1999	Haigh et al.			
	23	5,913,024	06/15/1999	Green et al.			
	24	5,915,087	06/22/1999	Hammond et al.			
	25	5,918,018	06/29/1999	Gooderum et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	26	5,950,195	09/07/1999	Stockwell et al.			
	27	5,956,403	09/21/1999	Lipner et al.			
	28	5,968,133	10/19/1999	Latham et al.			
	29	5,983,350	11/09/1999	Minear et al.			
	30	5,991,406	11/23/1999	Lipner et al.			
	31	5,991,856	11/23/1999	Spilo et al.			
	32	6,003,084	12/14/1999	Green et al.			
	33	6,006,035	12/21/1999	Nabahi			
	34	6,028,514	02/22/2000	Lemelson deceased et al.			
	35	6,029,256	02/22/2000	Kouznetsov			
	36	6,035,423	03/07/2000	Hodges et al.			
	37	6,055,527	04/25/2000	Badger et al.			
	38	6,064,811	05/16/2000	Spilo et al.			
	39	6,072,942	06/06/2000	Stockwell et al.			
	40	6,084,510	07/04/2000	Lemelson et al.			
	41	6,122,657	09/19/2000	Hoffman Jr. et al.			
	42	6,134,601	10/17/2000	Spilo et al.			
	43	6,144,934	11/07/2000	Stockwell et al.			
	44	6,151,643	11/21/2000	Cheng et al.			
	45	6,173,180	01/09/2001	Hussain et al.			
	46	6,182,226	01/30/2001	Reid et al.			
	47	6,185,689	02/06/2001	Todd Sr. et al.			
	48	6,195,352	02/27/2001	Cushman et al.			
	49	6,205,552	03/20/2001	Fudge			
	50	6,208,999	03/27/2001	Spilo et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	51	6,209,101	03/27/2001	Mitchem et al.			
	52	6,219,707	04/17/2001	Gooderum et al.			
	53	6,226,372	05/01/2001	Beebe et al.			
	54	6,230,199	05/08/2001	Revashetti et al.			
	55	6,230,288	05/08/2001	Kuo et al.			
	56	6,240,531	05/29/2001	Spilo et al.			
	57	6,249,585	06/19/2001	McGrew et al.			
	58	6,266,774	07/24/2001	Sampath et al.			
	59	6,266,811	07/24/2001	Nababi			
	60	6,267,039	07/31/2001	Czarnecki			
	61	6,269,456	07/31/2001	Hodges et al.			
	62	6,272,632	08/07/2001	Carman et al.			
	63	6,275,942	08/14/2001	Bernhard et al.			
	64	6,282,546	08/28/2001	Gleichauf et al.			
	65	6,298,422	10/02/2001	Spilo et al.			
	66	6,301,658	10/09/2001	Koehler			
	67	6,301,668	10/09/2001	Gleichauf et al.			
	68	6,301,699	10/09/2001	Hollander et al.			
	69	6,314,190	11/06/2001	Zimmermann			
	70	6,321,293	11/20/2001	Fabrizio et al.			
	71	6,321,336	11/20/2001	Applegate et al.			
	72	6,324,656	11/27/2001	Gleichauf et al.			
	73	6,332,195	12/18/2001	Green et al.			
	74	6,336,186	01/01/2002	Dyksterhouse et al.			
	75	6,343,362	01/29/2002	Ptacek et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	76	6,351,794	02/26/2002	Spilo et al.			
	77	6,353,446	03/05/2002	Vaughn et al.			
	78	6,357,010	03/12/2002	Viets et al.			
	79	6,370,578	04/09/2002	Revashetti et al.			
	80	6,385,458	05/07/2002	Papadimitriou et al.			
	81	6,393,424	05/21/2002	Hallman et al.			
	82	6,402,689	06/11/2002	Scarantino et al.			
	83	6,415,321	07/02/2002	Gleichauf et al.			
	84	6,442,686	08/27/2002	McArdle et al.			
	85	6,453,347	09/17/2002	Revashetti et al.			
	86	6,453,419	09/17/2002	Flint et al.			
	87	6,457,076	09/24/2002	Cheng et al.			
	88	6,460,126	10/01/2002	Spilo et al.			
	89	6,470,384	10/22/2002	O'Brien et al.			
	90	6,477,550	11/05/2002	Balasubramaniam et al.			
	91	6,477,651	11/05/2002	Teal			
	92	6,493,756	12/10/2002	O'Brien et al.			
	93	6,496,875	12/17/2002	Cheng et al.			
	94	6,499,107	12/24/2002	Gleichauf et al.			
	95	6,499,109	12/24/2002	Balasubramaniam et al.			
	96	6,510,448	01/21/2003	Churchyard			
	97	6,513,122	01/28/2003	Magdych et al.			
	98	6,523,023	02/18/2003	Sonnenberg			
	99	6,535,227	03/18/2003	Fox et al.			
	100	6,542,943	04/01/2003	Cheng et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	101	6,546,493	04/08/2003	Magdych et al.			
	102	6,550,012	04/15/2003	Villa et al.			
	103	6,553,377	04/22/2003	Eschelbeck et al.			
	104	6,553,378	04/22/2003	Eschelbeck			
	105	6,567,808	05/20/2003	Eschelbeck et al.			
	106	6,584,504	06/24/2003	Choe			
	107	6,584,508	06/24/2003	Epstein et al.			
	108	6,587,888	07/01/2003	Chieu et al.			
	109	6,601,091	07/29/2003	Spilo			
	110	6,604,139	08/05/2003	Sajina et al.			
	111	6,608,817	08/19/2003	Ivory			
	112	6,611,869	08/26/2003	Eschelbeck et al.			
	113	6,611,925	08/26/2003	Spear			
	114	6,615,266	09/02/2003	Hoffman Jr. et al.			
	115	6,622,150	09/16/2003	Kouznetsov et al.			
	116	6,633,835	10/14/2003	Moran et al.			
	117	6,636,972	10/21/2003	Ptacek et al.			
	118	6,640,307	10/28/2003	Viets et al.			
	119	6,654,751	11/25/2003	Schmugar et al.			
	120	6,654,782	11/25/2003	O'Brien et al.			
	121	6,658,571	12/02/2003	O'Brien et al.			
	122	6,663,000	12/16/2003	Muttik et al.			
	123	6,665,269	12/16/2003	Schmitz			
	124	6,668,054	12/23/2003	Contino et al.			
	125	6,668,289	12/23/2003	Cheng et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	126	6,671,368	12/30/2003	Contino et al.			
	127	6,671,812	12/30/2003	Balasubramaniam et al.			
	128	6,674,738	01/06/2004	Yildiz et al.			
	129	6,675,042	01/06/2004	Swerdlow et al.			
	130	6,678,887	01/13/2004	Hallman et al.			
	131	6,684,329	01/27/2004	Epstein et al.			
	132	6,687,833	02/03/2004	Osborne et al.			
	133	6,693,888	02/17/2004	Cafarelli et al.			
	134	6,697,337	02/24/2004	Cafarelli et al.			
	135	6,697,870	02/24/2004	Cafarelli III et al.			
	136	6,697,950	02/24/2004	Ko			
	137	6,701,440	03/02/2004	Kim et al.			
	138	6,701,441	03/02/2004	Balasubramaniam et al.			
	139	6,704,874	03/09/2004	Porras et al.			
	140	6,707,794	03/16/2004	Leong et al.			
	141	6,708,292	03/16/2004	Mangasarian			
	142	6,711,127	03/23/2004	Gorman et al.			
	143	6,714,513	03/30/2004	Joiner et al.			
	144	6,718,469	04/06/2004	Pak et al.			
	145	6,721,847	04/13/2004	Hursey			
	146	6,725,377	04/20/2004	Kouznetsov			
	147	6,728,219	04/27/2004	Leong et al.			
	148	6,728,885	04/27/2004	Taylor et al.			
	149	6,732,157	05/04/2004	Gordon et al.			
	150	6,735,629	05/11/2004	Cafarelli III et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	151	6,735,703	05/11/2004	Kilpatrick et al.			
	152	6,742,124	05/25/2004	Kilpatrick et al.			
	153	6,742,128	05/25/2004	Joiner			
	154	6,745,192	06/01/2004	Libenzi			
	155	6,745,311	06/01/2004	Fabrizio et al.			
	156	6,748,534	06/08/2004	Gryaznov et al.			
	157	6,751,627	06/15/2004	Sternin			
	158	6,751,718	06/15/2004	Manin			
	159	6,754,488	06/22/2004	Won et al.			
	160	6,754,705	06/22/2004	Joiner et al.			
	161	6,757,727	06/29/2004	Ivory			
	162	6,757,822	06/29/2004	Feiertag et al.			
	163	6,757,830	06/29/2004	Tarbotton et al.			
	164	6,760,845	07/06/2004	Cafarelli et al.			
	165	6,763,403	07/13/2004	Cheng et al.			
	166	6,763,466	07/13/2004	Glover			
	167	6,766,458	07/20/2004	Harris et al.			
	168	6,768,721	07/27/2004	Schmitz et al.			
	169	6,768,991	07/27/2004	Hearnden			
	170	6,769,016	07/27/2004	Rothwell et al.			
	171	6,772,332	08/03/2004	Boebert et al.			
	172	6,772,334	08/03/2004	Glawitsch			
	173	6,772,345	08/03/2004	Shetty			
	174	6,775,704	08/10/2004	Watson et al.			
	175	6,775,780	08/10/2004	Muttik			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	176	6,779,033	08/17/2004	Watson et al.			
	177	6,782,421	08/24/2004	Soles et al.			
	178	6,782,527	08/24/2004	Kouznetsov et al.			
	179	6,785,237	08/31/2004	Sufleta			
	180	6,785,820	08/31/2004	Muttik et al.			
	181	6,785,821	08/31/2004	Teal			
	182	6,789,082	09/07/2004	Sternin et al.			
	183	6,789,117	09/07/2004	Joiner et al.			
	184	6,789,201	09/07/2004	Barton et al.			
	185	6,789,202	09/07/2004	Ko et al.			
	186	6,792,543	09/14/2004	Pak et al.			
	187	6,799,197	09/28/2004	Shetty et al.			
	188	6,801,756	10/05/2004	Agrawal et al.			
	189	6,801,940	10/05/2004	Moran et al.			
	190	6,802,012	10/05/2004	Smithson et al.			
	191	6,810,017	10/26/2004	Leong et al.			
	192	6,814,842	11/09/2004	Yago et al.			
	193	6,816,973	11/09/2004	Gleichauf et al.			
	194	6,823,460	11/23/2004	Hollander et al.			
	195	6,826,608	11/30/2004	Sheth et al.			
	196	6,826,698	11/30/2004	Minkin et al.			
	197	6,834,301	12/21/2004	Hanchett			
	198	6,836,860	12/28/2004	Muttik et al.			
	199	6,839,852	01/04/2005	Pantuso et al.			
	200	6,842,860	01/11/2005	Branstad et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	201	6,842,861	01/11/2005	Cox et al.			
	202	6,843,190	01/18/2005	LaPierre-McAfee			
	203	6,845,449	01/18/2005	Carman et al.			
	204	6,851,058	02/01/2005	Gartside			
	205	6,851,061	02/01/2005	Holland III et al.			
	206	6,859,793	02/22/2005	Lambiase			
	207	6,862,581	03/01/2005	Lambiase			
	208	6,868,069	03/15/2005	Knobbe et al.			
	209	6,868,413	03/15/2005	Grindrod et al.			
	210	6,871,279	03/22/2005	Sames et al.			
	211	6,874,018	03/29/2005	Wu			
	212	6,879,812	04/12/2005	Agrawal et al.			
	213	6,886,099	04/26/2005	Smithson et al.			
	214	6,892,227	05/10/2005	Elwell et al.			
	215	6,892,241	05/10/2005	Kouznetsov et al.			
	216	6,895,387	05/17/2005	Roberts et al.			
	217	6,895,513	05/17/2005	Balasubramaniam et al.			
	218	6,898,712	05/24/2005	Vignoles et al.			
	219	6,898,715	05/24/2005	Smithson et al.			
	220	6,904,521	06/07/2005	Jivsov			
	221	6,907,396	06/14/2005	Muttik et al.			
	222	6,915,426	07/05/2005	Carman et al.			
	223	6,920,493	07/19/2005	Schwab			
	224	6,920,558	07/19/2005	Sames et al.			
	225	6,922,776	07/26/2005	Cook et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	226	6,928,555	08/09/2005	Drew			
	227	6,931,540	08/16/2005	Edwards et al.			
	228	6,931,546	08/16/2005	Kouznetsov et al.			
	229	6,934,857	08/23/2005	Bartleson et al.			
	230	6,938,161	08/30/2005	Vignoles et al.			
	231	6,941,358	09/06/2005	Joiner et al.			
	232	6,944,775	09/13/2005	Barton et al.			
	233	6,947,986	09/20/2005	Huang et al.			
	234	6,950,933	09/27/2005	Cook et al.			
	235	6,950,947	09/27/2005	Purtell et al.			
	236	6,959,418	10/25/2005	Churchyard			
	237	6,961,783	11/01/2005	Cook et al.			
	238	6,963,978	11/08/2005	Muttik et al.			
	239	6,964,014	11/08/2005	Parish			
	240	6,965,928	11/15/2005	Cox et al.			
	241	6,966,059	11/15/2005	Shetty et al.			
	242	6,968,461	11/22/2005	Lucas et al.			
	243	6,970,697	11/29/2005	Kouznetsov et al.			
	244	6,970,823	11/29/2005	Yago et al.			
	245	6,971,023	11/29/2005	Makinson et al.			
	246	6,973,577	12/06/2005	Kouznetsov			
	247	6,973,578	12/06/2005	McIchione			
	248	6,976,068	12/13/2005	Kadam et al.			
	249	6,976,168	12/13/2005	Branstad et al.			
	250	6,978,454	12/20/2005	Singleton			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	251	6,980,992	12/27/2005	Hursey et al.			
	252	6,981,280	12/27/2005	Grupe			
	253	6,983,325	01/03/2006	Watson et al.			
	254	6,983,326	01/03/2006	Vigue et al.			
	255	6,983,380	01/03/2006	Ko			
	256	6,983,486	01/03/2006	Hanchett			
	257	6,986,160	01/10/2006	LeGrow			
	258	6,987,963	01/17/2006	Kouznetsov et al.			
	259	6,988,209	01/17/2006	Balasubramaniam et al.			
	260	6,993,660	01/31/2006	Libenzi et al.			
	261	7,000,247	02/14/2006	Banzhof			
	262	7,000,250	02/14/2006	Kuo et al.			
	263	7,003,561	02/21/2006	Magdych et al.			
	264	7,007,302	02/28/2006	Jagger et al.			
	265	7,010,696	03/07/2006	Cambridge et al.			
	266	7,013,330	03/14/2006	Tarbotton et al.			
	267	7,016,939	03/21/2006	Rothwell et al.			
	268	7,016,948	03/21/2006	Yildiz			
	269	7,023,861	04/04/2006	Makinson et al.			
	270	7,024,432	04/04/2006	Muttik et al.			
	271	7,024,694	04/04/2006	Ko			
	272	7,035,544	04/25/2006	Won			
	273	7,036,147	04/25/2006	Hursey			
	274	7,039,702	05/02/2006	Churchyard			
	275	7,039,721	05/02/2006	Wu et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	276	7,043,024	05/09/2006	Dinsmore et al.			
	277	7,043,634	05/09/2006	Wolff et al.			
	278	7,043,756	05/09/2006	Tsafnat et al.			
	279	7,043,758	05/09/2006	Grupe			
	280	7,047,297	05/16/2006	Huntington et al.			
	281	7,051,077	05/23/2006	Lin			
	282	7,055,036	05/30/2006	Kouznetsov et al.			
	283	7,058,975	06/06/2006	Edwards et al.			
	284	7,062,555	06/13/2006	Kouznetsov et al.			
	285	7,062,783	06/13/2006	Joiner			
	286	7,065,790	06/20/2006	Gryaznov			
	287	7,069,316	06/27/2006	Gryaznov			
	288	7,069,330	06/27/2006	McArdle et al.			
	289	7,069,581	06/27/2006	Fu et al.			
	290	7,069,594	06/27/2006	Bolin			
	291	7,076,650	07/11/2006	Sonnenberg			
	292	7,080,000	07/18/2006	Cambridge			
	293	7,080,408	07/18/2006	Pak et al.			
	294	7,085,931	08/01/2006	Smith et al.			
	295	7,085,934	08/01/2006	Edwards			
	296	7,086,050	08/01/2006	Barton et al.			
	297	7,089,259	08/08/2006	Kouznetsov et al.			
	298	7,089,302	08/08/2006	Churchyard et al.			
	299	7,093,002	08/15/2006	Wolff et al.			
	300	7,093,121	08/15/2006	Barton et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	301	7,093,292	08/15/2006	Pantuso			
	302	7,093,293	08/15/2006	Smithson et al.			
	303	7,096,368	08/22/2006	Kouznetsov et al.			
	304	7,096,500	08/22/2006	Roberts et al.			
	305	7,096,501	08/22/2006	Kouznetsov et al.			
	306	7,096,503	08/22/2006	Magdych et al.			
	307	7,107,366	09/12/2006	Cheng et al.			
	308	7,107,574	09/12/2006	Nedbal			
	309	7,107,617	09/12/2006	Hursey et al.			
	310	7,107,618	09/12/2006	Gordon et al.			
	311	7,114,183	09/26/2006	Joiner			
	312	7,114,185	09/26/2006	Moore et al.			
	313	7,117,533	10/03/2006	Libenzi			
	314	7,120,252	10/10/2006	Jones et al.			
	315	7,124,181	10/17/2006	Magdych et al.			
	316	7,134,140	11/07/2006	Fisher			
	317	7,136,487	11/14/2006	Schon et al.			
	318	7,140,042	11/21/2006	Verma			
	319	7,146,155	12/05/2006	Kouznetsov			
	320	7,146,642	12/05/2006	Magdych et al.			
	321	7,149,189	12/12/2006	Huntington et al.			
	322	7,150,042	12/12/2006	Wolff et al.			
	323	7,152,105	12/19/2006	McClure et al.			
	324	7,152,241	12/19/2006	Grupe			
	325	7,154,857	12/26/2006	Joiner et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	326	7,159,036	01/02/2007	Hinchliffe et al.			
	327	7,162,698	01/09/2007	Huntington et al.			
	328	7,171,681	01/30/2007	Duncan et al.			
	329	7,171,690	01/30/2007	Kouznetsov et al.			
	330	7,181,015	02/20/2007	Matt			
	331	7,181,506	02/20/2007	Vigue et al.			
	332	7,181,613	02/20/2007	Boebert et al.			
	333	7,185,361	02/27/2007	Ashoff et al.			
	334	7,188,367	03/06/2007	Edwards et al.			
	335	7,203,963	04/10/2007	Wu et al.			
	336	7,209,954	04/24/2007	Rothwell et al.			
	337	7,210,041	04/24/2007	Gryaznov et al.			
	338	7,210,168	04/24/2007	Hursey et al.			
	339	7,213,153	05/01/2007	Hollander et al.			
	340	7,213,260	05/01/2007	Judge			
	341	7,225,466	05/29/2007	Judge			
	342	7,228,565	06/05/2007	Wolff et al.			
	343	7,231,440	06/12/2007	Kouznetsov et al.			
	344	7,231,637	06/12/2007	McEwan			
	345	7,231,664	06/12/2007	Markham et al.			
	346	7,231,665	06/12/2007	McArdle et al.			
	347	7,234,165	06/19/2007	Hursey et al.			
	348	7,234,167	06/19/2007	Teblyashkin et al.			
	349	7,234,168	06/19/2007	Gupta et al.			
	350	7,237,008	06/26/2007	Tarbotton et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	351	7,237,122	06/26/2007	Kadam et al.			
	352	7,237,222	06/26/2007	Nedbal et al.			
	353	7,237,258	06/26/2007	Pantuso et al.			
	354	7,240,102	07/03/2007	Kouznetsov et al.			
	355	7,243,148	07/10/2007	Keir et al.			
	356	7,243,373	07/10/2007	Muttik et al.			
	357	7,251,685	07/31/2007	Yildiz			
	358	7,251,830	07/31/2007	Melchione			
	359	7,254,811	08/07/2007	Kouznetsov et al.			
	360	7,257,630	08/14/2007	Cole et al.			
	361	7,257,773	08/14/2007	Jagger et al.			
	362	7,257,842	08/14/2007	Barton et al.			
	363	7,263,561	08/28/2007	Green et al.			
	364	7,263,718	08/28/2007	O'Brien et al.			
	365	7,266,843	09/04/2007	Tarbotton et al.			
	366	7,266,844	09/04/2007	Teblyashkin et al.			
	367	7,269,649	09/11/2007	Brown et al.			
	368	7,269,851	09/11/2007	Ackroyd			
	369	7,272,724	09/18/2007	Tarbotton et al.			
	370	7,277,957	10/02/2007	Rowley et al.			
	371	7,281,267	10/09/2007	Tarbotton et al.			
	372	7,281,268	10/09/2007	Hollander et al.			
	373	7,284,267	10/16/2007	McArdle et al.			
	374	7,296,080	11/13/2007	Rowley et al.			
	375	7,299,361	11/20/2007	Kim et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	376	7,302,584	11/27/2007	Tarbotton et al.			
	377	7,302,706	11/27/2007	Hicks et al.			
	378	7,305,005	12/04/2007	Wu et al.			
	379	7,305,709	12/04/2007	Lymer et al.			
	380	7,308,702	12/11/2007	Thomsen et al.			
	381	7,308,706	12/11/2007	Markham et al.			
	382	7,308,712	12/11/2007	Banzhof			
	383	7,308,715	12/11/2007	Gupta et al.			
	384	7,310,817	12/18/2007	Hinchliffe et al.			
	385	7,310,818	12/18/2007	Parish et al.			
	386	7,315,801	01/01/2008	Dowd et al.			
	387	7,315,894	01/01/2008	Huntington et al.			
	388	7,325,252	01/29/2008	Bunker V et al.			
	389	7,328,234	02/05/2008	Nedbal et al.			
	390	7,334,222	02/19/2008	Keller			
	391	7,340,774	03/04/2008	Hursey et al.			
	392	7,340,775	03/04/2008	Tarbotton et al.			
	393	7,343,626	03/11/2008	Gallagher			
	394	7,346,781	03/18/2008	Cowie et al.			
	395	7,346,929	03/18/2008	Hammond			
	396	7,350,203	03/25/2008	Jahn			
	397	7,350,234	03/25/2008	Goseva-Popstojanova et al.			
	398	7,353,539	04/01/2008	Brawn et al.			
	399	7,359,962	04/15/2008	Willebeek-LeMair et al.			
	400	7,373,659	05/13/2008	Vignoles et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	401	7,376,842	05/20/2008	Hursey			
	402	7,380,270	05/27/2008	Tracy et al.			
	403	7,383,556	06/03/2008	Pantuso et al.			
	404	7,383,581	06/03/2008	Moore et al.			
	405	7,389,539	06/17/2008	Kouznetsov			
	406	7,391,770	06/24/2008	Taylor et al.			
	407	7,392,043	06/24/2008	Kouznetsov et al.			
	408	7,398,516	07/08/2008	Berg et al.			
	409	7,398,517	07/08/2008	Berg et al.			
	410	7,401,359	07/15/2008	Gartside et al.			
	411	7,409,593	08/05/2008	Aaron			
	412	7,409,714	08/05/2008	Gupta et al.			
	413	7,409,720	08/05/2008	Cambridge et al.			
	414	7,412,721	08/12/2008	Torii et al.			
	415	7,412,722	08/12/2008	Norris et al.			
	416	7,412,723	08/12/2008	Blake et al.			
	417	7,415,726	08/19/2008	Kelly et al.			
	418	7,418,730	08/26/2008	Chu et al.			
	419	7,418,733	08/26/2008	Connary et al.			
	420	7,418,734	08/26/2008	Berg et al.			
	421	7,418,737	08/26/2008	Grupe			
	422	7,421,266	09/02/2008	Bruestle et al.			
	423	7,421,587	09/02/2008	Cowie et al.			
	424	7,424,744	09/09/2008	Wu et al.			
	425	7,424,746	09/09/2008	Magdych et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	426	7,426,551	09/16/2008	Benzinger et al.			
	427	7,440,403	10/21/2008	Rosenfled			
	428	7,440,471	10/21/2008	Hinchliffe et al.			
	429	7,441,274	10/21/2008	Drew			
	430	7,451,488	11/11/2008	Cooper et al.			
	431	7,458,098	11/25/2008	Judge et al.			
	432	7,461,403	12/02/2008	Libenzi et al.			
	433	7,464,408	12/09/2008	Shah et al.			
	434	7,472,419	12/30/2008	Balasubramaniam et al.			
	435	7,472,421	12/30/2008	Cummins			
	436	7,480,941	01/20/2009	Balasubramaniam et al.			
	437	7,483,861	01/27/2009	Joiner et al.			
	438	7,493,659	02/17/2009	Wu et al.			
	439	7,496,043	02/24/2009	Leong et al.			
	440	7,509,681	03/24/2009	Flowers et al.			
	441	7,516,483	04/07/2009	Brennan			
	442	7,519,994	04/14/2009	Judge et al.			
	443	7,522,531	04/21/2009	Joiner et al.			
	444	7,533,272	05/12/2009	Gordon et al.			
	445	7,536,456	05/19/2009	Williams et al.			
	446	7,536,715	05/19/2009	Markham			
	447	7,540,031	05/26/2009	Kouznetsov et al.			
	448	7,543,056	06/02/2009	McClure et al.			
	449	7,543,070	06/02/2009	Watson et al.			
	450	7,543,329	06/02/2009	Viets et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	451	7,543,334	06/02/2009	Vignoles et al.			
	452	7,549,168	06/16/2009	Magdych et al.			
	453	7,552,480	06/23/2009	Voss			
	454	7,555,776	06/30/2009	Lymer et al.			
	455	7,587,759	09/08/2009	McArdle et al.			
	456	7,590,247	09/15/2009	Dinsmore et al.			
	457	7,590,725	09/15/2009	Harrison			
	458	7,590,844	09/15/2009	Sherman et al.			
	459	7,590,855	09/15/2009	Irwin			
	460	7,590,859	09/15/2009	Brennan			
	461	7,594,262	09/22/2009	Hanzlik et al.			
	462	7,603,711	10/13/2009	Scheidell			
	463	7,613,625	11/03/2009	Heinrich			
	464	7,620,816	11/17/2009	Vigue et al.			
	465	7,624,422	11/24/2009	Williams et al.			
	466	7,624,444	11/24/2009	Gupta et al.			
	467	7,624,450	11/24/2009	Lymer et al.			
	468	7,627,891	12/01/2009	Williams et al.			
	469	7,634,800	12/15/2009	Ide et al.			
	470	7,640,335	12/29/2009	Agrawal et al.			
	471	7,640,361	12/29/2009	Green et al.			
	472	7,640,586	12/29/2009	Johnson et al.			
	473	7,644,352	01/05/2010	Grupe			
	474	7,647,376	01/12/2010	Jagger et al.			
	475	7,664,845	02/16/2010	Kurtz et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	476	7,665,137	02/16/2010	Barton et al.			
	477	7,668,947	02/23/2010	Hutchinson et al.			
	478	7,669,237	02/23/2010	Shahbazi			
	479	7,673,043	03/02/2010	Keir et al.			
	480	7,673,146	03/02/2010	Wiedmann et al.			
	481	7,673,150	03/02/2010	Cox et al.			
	482	7,673,242	03/02/2010	Huntington et al.			
	483	7,673,342	03/02/2010	Hursey et al.			
	484	7,673,343	03/02/2010	Barton et al.			
	485	7,674,298	03/09/2010	Cambridge			
	486	7,681,208	03/16/2010	Pantuso et al.			
	487	7,693,742	04/06/2010	Joiner et al.			
	488	7,693,947	04/06/2010	Judge et al.			
	489	7,694,128	04/06/2010	Judge et al.			
	490	7,694,339	04/06/2010	Blake et al.			
	491	7,711,662	05/04/2010	Buscema			
	492	7,712,138	05/04/2010	Zobel et al.			
	493	7,716,719	05/11/2010	Kouznetsov et al.			
	494	7,716,742	05/11/2010	Roesch et al.			
	495	7,721,110	05/18/2010	Kouznetsov et al.			
	496	7,739,722	06/15/2010	Okajo et al.			
	497	7,757,293	07/13/2010	Caceres et al.			
	498	7,757,361	07/20/2010	Edwards et al.			
	499	7,761,605	07/20/2010	Rothwell et al.			
	500	7,770,225	08/03/2010	Hammond			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	501	7,779,466	08/17/2010	Judge et al.			
	502	7,783,545	08/24/2010	Sloan et al.			
	503	7,788,705	08/31/2010	Bruestle et al.			
	504	7,788,718	08/31/2010	Fei et al.			
	505	7,793,346	09/07/2010	Daub			
	506	7,793,348	09/07/2010	Lingafelt et al.			
	507	7,801,980	09/21/2010	Roesch et al.			
	508	7,810,091	10/05/2010	Gartside et al.			
	509	7,818,739	10/19/2010	Cox et al.			
	510	7,822,666	10/26/2010	Bursch			
	511	7,823,204	10/26/2010	Gupta et al.			
	512	7,827,607	11/02/2010	Sobel et al.			
	513	7,827,611	11/02/2010	Kouznetsov et al.			
	514	7,836,501	11/16/2010	Sobel et al.			
	515	7,840,663	11/23/2010	Hinchliffe et al.			
	516	7,841,007	11/23/2010	Currie et al.			
	517	7,845,007	11/30/2010	Kennis			
	518	7,861,285	12/28/2010	Ashoff et al.			
	519	7,861,303	12/28/2010	Kouznetsov et al.			
	520	7,865,938	01/04/2011	Shabbazi			
	521	7,865,956	01/04/2011	Cambridge et al.			
	522	7,870,203	01/11/2011	Judge et al.			
	523	7,882,555	02/01/2011	Ben-Itzhak			
	524	7,895,641	02/22/2011	Schneier et al.			
	525	7,900,254	03/01/2011	Fisher et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	526	7,903,549	03/08/2011	Judge et al.			
	527	7,904,955	03/08/2011	Bu et al.			
	528	7,917,444	03/29/2011	Bursch			
	529	7,917,647	03/29/2011	Cooper et al.			
	530	7,917,951	03/29/2011	Tarbotton et al.			
	531	7,921,459	04/05/2011	Houston et al.			
	532	7,926,113	04/12/2011	Gula et al.			
	533	7,941,855	05/10/2011	Sung et al.			
	534	7,958,554	06/07/2011	Chow et al.			
	535	7,975,296	07/05/2011	Apfelbaum et al.			
	536	7,984,511	07/19/2011	Kocher et al.			
	537	7,991,827	08/02/2011	Whitmore et al.			
	538	7,991,917	08/02/2011	Wu et al.			
	539	7,996,201	08/09/2011	Dowd et al.			
	540	7,996,902	08/09/2011	Gordon et al.			
	541	8,010,387	08/30/2011	Porter et al.			
	542	8,019,082	09/13/2011	Wiedmann et al.			
	543	8,020,211	09/13/2011	Keanini et al.			
	544	8,024,076	09/20/2011	Schlueter et al.			
	545	8,042,149	10/18/2011	Judge			
	546	8,042,178	10/18/2011	Fisher et al.			
	547	8,042,181	10/18/2011	Judge			
	548	8,051,479	11/01/2011	Bu et al.			
	549	8,068,441	11/29/2011	Wiedmann et al.			
	550	8,069,480	11/29/2011	Tarbotton et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	551	8,069,481	11/29/2011	Judge			
	552	8,074,256	12/06/2011	Valente et al.			
	553	8,074,282	12/06/2011	Lymer et al.			
	554	8,090,816	01/03/2012	Deshmukh et al.			
	555	8,091,117	01/03/2012	Williams et al.			
	556	8,099,760	01/17/2012	Cohen et al.			
	557	8,115,769	02/14/2012	Lymer et al.			
	558	8,117,273	02/14/2012	Mathur et al.			
	559	8,121,892	02/21/2012	Baggett Jr. et al.			
	560	8,122,498	02/21/2012	Gordon et al.			
	561	8,122,499	02/21/2012	Hall			
	562	8,127,359	02/28/2012	Kelekar			
	563	8,132,250	03/06/2012	Judge et al.			
	564	8,135,823	03/13/2012	Cole et al.			
	565	8,135,830	03/13/2012	McClure et al.			
	566	8,140,642	03/20/2012	Kadam et al.			
	567	8,141,157	03/20/2012	Farley et al.			
	568	8,156,483	04/10/2012	Berg et al.			
	569	8,171,551	05/01/2012	Muttik et al.			
	570	8,176,544	05/08/2012	Keanini et al.			
	571	8,176,553	05/08/2012	Magdych et al.			
	572	8,181,222	05/15/2012	Thomsen et al.			
	573	8,185,943	05/22/2012	Jagger et al.			
	574	8,219,620	07/10/2012	Hart			
	575	8,230,497	07/24/2012	Norman et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	Applicant Brett M. Oliphant	
	Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	576	8,230,502	07/24/2012	Lymer et al.			
	577	8,239,941	08/07/2012	Lymer et al.			
	578	8,256,002	08/28/2012	Chandrashekhar et al.			
	579	8,260,906	09/04/2012	Freedman			
	580	8,266,703	09/11/2012	Magdych et al.			
	581	8,291,505	10/16/2012	Hursey			
	582	8,310,955	11/13/2012	Wiedmann et al.			
	583	8,312,535	11/13/2012	Gordon et al.			
	584	8,341,693	12/25/2012	Shabbazi			
	585	8,359,650	01/22/2013	Lotem et al.			
	586	8,364,772	01/29/2013	Mathur et al.			
	587	8,380,791	02/19/2013	Gordon et al.			
	588	8,387,146	02/26/2013	Parish et al.			
	589	8,393,001	03/05/2013	Libenzi et al.			
	590	8,402,540	03/19/2013	Kapoor et al.			
	591	8,407,683	03/26/2013	Cheng et al.			
	592	8,407,798	03/26/2013	Lotem et al.			
	593	8,468,256	06/18/2013	McArdle et al.			
	594	8,490,197	07/16/2013	Herz			
	595	8,495,740	07/23/2013	Rouland et al.			
	596	8,510,839	08/13/2013	Tarbotton et al.			
	597	8,527,977	09/03/2013	Cheng et al.			
	598	8,528,042	09/03/2013	Sapp et al.			
	599	8,533,703	09/10/2013	Cheng et al.			
	600	8,539,063	09/17/2013	Sharma et al.			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	601	8,549,611	10/01/2013	Judge et al.			
	602	8,549,635	10/01/2013	Muttik et al.			
	603	8,555,344	10/08/2013	Wiedmann et al.			
	604	8,555,374	10/08/2013	Wu et al.			
	605	8,561,167	10/15/2013	Alperovitch et al.			
	606	8,561,175	10/15/2013	Williams et al.			
	607	8,578,480	11/05/2013	Judge et al.			
	608	8,615,582	12/24/2013	McClure et al.			
	609	8,621,060	12/31/2013	McClure et al.			
	610	8,621,073	12/31/2013	McClure et al.			
	611	8,621,077	12/31/2013	Hinchliffe et al.			
	612	8,627,443	01/07/2014	Jagger et al.			
	613	8,627,466	01/07/2014	Fisher et al.			
	614	8,631,124	01/14/2014	Whitmore et al.			
	615	8,631,495	01/14/2014	Judge			
	616	8,634,309	01/21/2014	O'Brien			
	617	8,656,502	02/18/2014	Gartside et al.			
	618	8,661,126	02/25/2014	Cole et al.			
	619	8,700,767	04/15/2014	Cole et al.			
	620	8,706,576	04/22/2014	Balasubramaniam et al.			
	621	8,732,835	05/20/2014	Gordon et al.			
	622	8,744,938	06/03/2014	Bursch			
	623	8,776,230	07/08/2014	Singleton			
	624	8,782,260	07/15/2014	Taylor et al.			
	625	8,789,193	07/22/2014	Kelekar			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	626	2001/0014150	08/16/2001	Beebe Todd et al.			
	627	2001/0027388	10/04/2001	Beverina Anthony et al.			
	628	2001/0027389	10/04/2001	Beverina Anthony et al.			
	629	2001/0028268	10/11/2001	Shuler Robert L. JR.			
	630	2001/0028269	10/11/2001	Shuler Robert L. JR.			
	631	2001/0034847	10/25/2001	GaulJr. Stephen E.			
	632	2001/0042004	11/15/2001	Taub Herman P.			
	633	2001/0043778	11/22/2001	Griffis Jeffrey A. et al.			
	634	2002/0026591	02/28/2002	Hartley Bruce V. et al.			
	635	2002/0032860	03/14/2002	Wheeler Anne McAfee et al.			
	636	2002/0042687	04/11/2002	Tracy Richard P. et al.			
	637	2002/0042877	04/11/2002	Wheeler Anne Mcafee et al.			
	638	2002/0069035	06/06/2002	Tracy Richard P. et al.			
	639	2002/0078381	06/20/2002	Farley Timothy P. et al.			
	640	2002/0092924	07/18/2002	Ingham John W. JR. et al.			
	641	2002/0104014	08/01/2002	Zobel Robert David et al.			
	642	2002/0109963	08/15/2002	Aoki Russell S. et al.			
	643	2002/0112179	08/15/2002	Riordan James F. et al.			
	644	2002/0116631	08/22/2002	Torii Satoru et al.			
	645	2002/0120558	08/29/2002	Reid William Joseph			
	646	2002/0137991	09/26/2002	Scarantino Charles W. et al.			
	647	2002/0147803	10/10/2002	Dodd Timothy David et al.			
	648	2002/0150866	10/17/2002	Perry John S. et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	649	2002/0178383	11/28/2002	Hrabik Michael et al.			
	650	2002/0199122	12/26/2002	Davis Lauren B. et al.			
	651	2003/0014669	01/16/2003	Caceres Maximiliano Gerardo et al.			
	652	2003/0023873	01/30/2003	Ben-Itzhak Yuval			
	653	2003/0028803	02/06/2003	Bunker Nelson Waldo V et al.			
	654	2003/0033542	02/13/2003	Goseva-Popstojanova Katerina et al.			
	655	2003/0037258	02/20/2003	Koren Izchak			
	656	2003/0046128	03/06/2003	Heinrich Nicolas			
	657	2003/0050718	03/13/2003	Tracy Richard P. et al.			
	658	2003/0051163	03/13/2003	Bidaud Olivier			
	659	2003/0056116	03/20/2003	Bunker Nelson Waldo V et al.			
	660	2003/0065945	04/03/2003	Lingafelt Charles Steven et al.			
	661	2003/0070003	04/10/2003	Chong Chee-Yee et al.			
	662	2003/0083831	05/01/2003	Agrawal Dakshi et al.			
	663	2003/0091951	05/15/2003	Guilmette Dennis L. et al.			
	664	2003/0097228	05/22/2003	Satya Akella V. S.et al.			
	665	2003/0126472	07/03/2003	Banzhof Carl E.			
	666	2003/0135749	07/17/2003	Gales George S. et al.			
	667	2003/0140249	07/24/2003	Taninaka Yoshihito et al.			
	668	2003/0140250	07/24/2003	Taninaka Yoshihito et al.			
	669	2003/0154269	08/14/2003	Nyanchama Matunda G. et al.			
	670	2003/0159060	08/21/2003	Gales George S. et al.			
	671	2003/0159063	08/21/2003	Apfelbaum Larry et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	672	2003/0188194	10/02/2003	Currie David et al.			
	673	2003/0195569	10/16/2003	Swerdlow Charles D. et al.			
	674	2003/0195861	10/16/2003	McClure Stuart C. et al.			
	675	2003/0202663	10/30/2003	Hollis Robert L. et al.			
	676	2003/0204632	10/30/2003	Willebeek-LeMair Marc et al.			
	677	2003/0204719	10/30/2003	Ben-Itzhak Yuval			
	678	2003/0204728	10/30/2003	Irwin Victoria Lynn			
	679	2003/0212779	11/13/2003	Boyter Brian A. et al.			
	680	2003/0212909	11/13/2003	Chandrashekhar Uma et al.			
	681	2003/0217039	11/20/2003	Kurtz George R. et al.			
	682	2003/0233438	12/18/2003	Hutchinson Robin et al.			
	683	2004/0006704	01/08/2004	Dahlstrom Dale A. et al.			
	684	2004/0015338	01/22/2004	Lawrence William Richard et al.			
	685	2004/0015728	01/22/2004	Cole David M. et al.			
	686	2004/0015737	01/22/2004	Martin Robert J. et al.			
	687	2004/0019803	01/29/2004	Jahn Alfred			
	688	2004/0021889	02/05/2004	McAfee David A. et al.			
	689	2004/0022359	02/05/2004	Acharya Kishore et al.			
	690	2004/0024781	02/05/2004	Youd David W.			
	691	2004/0044912	03/04/2004	Connary Iven et al.			
	692	2004/0049372	03/11/2004	Keller Alexander			
	693	2004/0064722	04/01/2004	Neelay Dinesh et al.			
	694	2004/0064726	04/01/2004	Girouard Mario			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	695	2004/0071081	04/15/2004	Rosenfled Amir			
	696	2004/0073800	04/15/2004	Shah Paragi et al.			
	697	2004/0078384	04/22/2004	Keir Robin M. et al.			
	698	2004/0088564	05/06/2004	Norman Andrew Patrick			
	699	2004/0088565	05/06/2004	Norman Andrew Patrick et al.			
	700	2004/0088581	05/06/2004	Brawn John Melvin et al.			
	701	2004/0098623	05/20/2004	Scheidell Michael			
	702	2004/0102922	05/27/2004	Tracy Richard P. et al.			
	703	2004/0102923	05/27/2004	Tracy Richard P. et al.			
	704	2004/0103431	05/27/2004	Davenport H. Edward et al.			
	705	2004/0106955	06/03/2004	Swerdlow Charles D. et al.			
	706	2004/0117624	06/17/2004	Brandt David D. et al.			
	707	2004/0117640	06/17/2004	Chu Simon C. et al.			
	708	2004/0128529	07/01/2004	Blake Kenneth W. et al.			
	709	2004/0128530	07/01/2004	Isenberg Henri J.			
	710	2004/0128543	07/01/2004	Blake Kenneth W. et al.			
	711	2004/0153171	08/05/2004	Brandt David D. et al.			
	712	2004/0158545	08/12/2004	Turgeon Andre			
	713	2004/0172550	09/02/2004	Sai Kousetsu			
	714	2004/0181787	09/16/2004	Wickham Robert T. et al.			
	715	2004/0192204	09/30/2004	Periyalwar Shalini et al.			
	716	2004/0193918	09/30/2004	Green Kenneth et al.			
	717	2004/0210653	10/21/2004	Kanoor Madhu et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	718	2004/0215972	10/28/2004	Sung Andrew H. et al.			
	719	2004/0215978	10/28/2004	Okajo Sumitaka et al.			
	720	2004/0221176	11/04/2004	Cole Eric B.			
	721	2004/0250115	12/09/2004	Gemmel James Dal et al.			
	722	2004/0250128	12/09/2004	Bush Stephen F. et al.			
	723	2004/0259640	12/23/2004	Gentles Thomas A. et al.			
	724	2004/0268322	12/30/2004	Chow Stanley T. et al.			
	725	2005/0005169	01/06/2005	Kelekar Samir Gurunath			
	726	2005/0007743	01/13/2005	Eckblad Michael Z. et al.			
	727	2005/0010821	01/13/2005	Cooper Geoffrey et al.			
	728	2005/0015382	01/20/2005	Aaron Jeffrey A.			
	729	2005/0015667	01/20/2005	Aaron Jeffrey A.			
	730	2005/0022028	01/27/2005	Hall Aron			
	731	2005/0049962	03/03/2005	Porter Keith Alan et al.			
	732	2005/0091542	04/28/2005	Banzhof Carl E.			
	733	2005/0114186	05/26/2005	Heinrich Nicolas			
	734	2005/0160286	07/21/2005	Currie David et al.			
	735	2005/0177752	08/11/2005	Hollander Yona et al.			
	736	2005/0195975	09/08/2005	Kawakita Kevin			
	737	2005/0240756	10/27/2005	Mayer Yaron			
	738	2006/0004614	01/05/2006	Hutchinson Robin et al.			
	739	2006/0030972	02/09/2006	Schlueter Robert et al.			
	740	2006/0031938	02/09/2006	Choi Unho			
	741	2006/0069912	03/30/2006	Zheng Yuliang et al.			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	742	2006/0070129	03/30/2006	Sobel William E. et al.			
	743	2006/0130139	06/15/2006	Sobel William E. et al.			
	744	2006/0156407	07/13/2006	Cummins Fred A.			
	745	2006/0168660	07/27/2006	Edwards Jonathan et al.			
	746	2006/0179325	08/10/2006	Debiez Jacques			
	747	2006/0230006	10/12/2006	Buscema Massimo			
	748	2006/0265746	11/23/2006	Farley Timothy P. et al.			
	749	2006/0272011	11/30/2006	Ide Curtis E. et al.			
	750	2006/0293942	12/28/2006	Chaddha Parmeet S. et al.			
	751	2008/0005555	01/03/2008	Lotem Amnon et al.			
	752	2008/0052054	02/28/2008	Beverina Anthony et al.			
	753	2008/0060075	03/06/2008	Cox Brian R. et al.			
	754	2008/0216173	09/04/2008	Hammond Nicolas J.			
	755	2008/0222731	09/11/2008	Dowd Alan et al.			
	756	2008/0263525	10/23/2008	BERG Ryan James et al.			
	757	2008/0263668	10/23/2008	Chu Simon C. et al.			
	758	2008/0271151	10/30/2008	Blake Kenneth W. et al.			
	759	2009/0320138	12/24/2009	Keanini Timothy D. et al.			
	760	2009/0328213	12/31/2009	Blake Kenneth W. et al.			
	761	2010/0083382	04/01/2010	Farley Timothy P. et al.			
	762	2010/0100961	04/22/2010	Scheidell Michael			
	763	2011/0131644	06/02/2011	Keanini Timothy D. et al.			
	764	2011/0162049	06/30/2011	Shahbazi Majid			

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Brett M. Oliphant	
(37 CFR §1.98(b))		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	765	2011/0173342	07/14/2011	Cooper Geoffrey et al.			
	766	2011/0173677	07/14/2011	Tarbotton Lee Codel Lawson et al.			
	767	2011/0214179	09/01/2011	CHOW Stanley T. et al.			
	768	2011/0214185	09/01/2011	Parish Sandy et al.			
	769	2011/0258315	10/20/2011	Whitmore Brent S. et al.			
	770	2011/0258694	10/20/2011	Wu Handong et al.			
	771	2012/0017278	01/19/2012	Fisher Lee Adam et al.			
	772	2012/0030766	02/02/2012	Tarbotton Lee Codel Lawson et al.			
	773	2012/0084867	04/05/2012	Baggett JR. Charlie C. et al.			
	774	2012/0102570	04/26/2012	Herz Frederick S.M.			
	775	2012/0144476	06/07/2012	McClure Stuart C. et al.			
	776	2012/0144493	06/07/2012	Cole David M. et al.			
	777	2012/0144494	06/07/2012	Cole David M. et al.			
	778	2012/0151594	06/14/2012	McClure Stuart C. et al.			
	779	2012/0151595	06/14/2012	McClure Stuart C. et al.			
	780	2012/0151596	06/14/2012	McClure Stuart C. et al.			
	781	2012/0185549	07/19/2012	Hart Matthew Thomas			
	782	2012/0185550	07/19/2012	Hart Matthew Thomas			
	783	2012/0185551	07/19/2012	HART Matthew Thomas			
	784	2012/0192262	07/26/2012	Jagger Luke D. et al.			
	785	2012/0192279	07/26/2012	Muttik Igor Garrievich et al.			
	786	2012/0204265	08/09/2012	Judge Paul			

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Brett M. Oliphant	
		Filing Date 08/03/2015	Group Art Unit 2438

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	787	2012/0271890	10/25/2012	Judge Paul et al.			
	788	2012/0317627	12/13/2012	Chandrashekhar Uma et al.			
	789	2013/0031265	01/31/2013	Freedman Jerome N.			
	790	2013/0031635	01/31/2013	Lotem Amnon et al.			
	791	2013/0167240	06/27/2013	Kelekar Samir Gurunath			
	792	2013/0246620	09/19/2013	Rothwell Anton C. et al.			
	793	2013/0275999	10/17/2013	Gordon Bryson P. et al.			
	794	2013/0312101	11/21/2013	Lotem Amnon et al.			

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	1	CERT Incident Note IN-2000-07, "Exploitation of Hidden File Extensions", July 27, 2000, at CERT.org, pp. 1-3
	2	Julia Allen et al., "State of the Practice of Intrusion Detection Technologies," January 2000, Networked Systems Survivability Program, cover page - page 220 and report documentation page
	3	"Review SPQUERY", in Network Computing, November 2000, www.networkcomputer.co.uk/back_iss/prod_update/reviews/spquery4.1.htm
	4	Business Wire, "Ready for Windows 2000 Service Pack 1? St. Bernard Software's SPQuery 4.0 is Here Just Time," August 2, 2000, pp. 1-2, www.findarticles.com/p/articles/mi_m0EIN/is_August_2/ai_63819686/print

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Form (PTO-1449)

Form PTO-1449 (Modified) U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. SP1P0012A	Application No. 14/816,931
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	Applicant Brett M. Oliphant	
	Filing Date 08/03/2015	Group Art Unit 2438

Other Documents (include Author, Title, Date, and Place of Publication)		
Examiner Initial	Desig. ID	Document
	5	Mark Joseph Edwards, "Useful SPQuery 3.0 automates finding, installing hotfixes," in InfoWorld, June 21, 1999, www.infoworld.com/cgi-bin/displayArchive.pl?/99/25/c04-25.46.htm
	6	SPQuery User's Manual, Version 4.2, pp. 1-58
	7	WebConsole Core 4.0 for NetWare, archived May 11, 2000, pp. 1-3 http://web.archive.org/web/20000511133746/www.patchlink.com/products/wcnw_product...
	8	PatchLink, Gravitix The Patch Finder, archived August 15, 2000, http://web.archive.org/web/20000815094824//www.patchlink.com/products/gravitix.asp
	9	Steve Manzuik , "Ultimate Security Toolkit", InstantDoc #9202, May 16, 2000, pp. 1-3 http://web.archive.org/web/2001160751/www.ntsecurity.net/Articles/Index.cfm?ArticleId=9202&SearchString=cyber
	10	"Network Vulnerability Assessment Report," April 19, 2000, pp. 1-4, http://web.archive.org/web/20000917072109/documents.iss.net/literature/InternetScanner/reports/Line_Mgmt_Vulnerability_Assessment_Report.pdf
	11	"Host Vulnerability Summary Report," April 19, 2000, pp. 1-8, http://web.archive.org/web/20000917072216/documents.iss.net/literature/InternetScanner/reports/Technician_Host_Vulnerability_Summary_Report.pdf
	12	Internet Security Systems, Inc.: Securing E-Business, ISS SAFEsuite products, Security Assessment: Internet Scanner, archived August 20, 2000 http://web.archive.org/web/20000820203428/www.iss.net/securing_e-business/security_pr...
	13	"Internet Security Systems; Internet Scanner", archived June 6, 2001, pp. 1-2 http://web.archive.org/web/2001060422406/documents.iss.net/literature/InternetScanner/is_ps.pdf
	14	"To Setup Secure PC Network:", archived August 16, 2000, pp. 1-15 http://web.archive.org/web/20000816192628/www.citadel.com/downloads/SPC+readme.txt
	15	"Microsoft Security Glossary", published October 29, 2002, updated December 19, 2005, pp. 1-18, www.microsoft.com/security/glossary.mspx
	16	U.S. Provisional Application No. 60/234,680, filed September 22, 2000
	17	Gravitix Screenshot, July 24, 2000
	18	Notice of Allowance in U.S. Pat. Appl. No. 14/138,014 dated 07-10-2015
	19	Office Action Summary in U.S. Pat. Appl. No. 14/834,102 dated 03-24-2016
	20	Notice of Allowance in U.S. Pat. Appl. No. 14/834,102 dated 10-7-2016
	21	Office Action Summary in U.S. Pat. Appl. No. 14/816,960 dated 12-30-2015
	22	Notice of Allowance in U.S. Pat. Appl. No. 14/816,960 dated 09-13-2016
	23	Notice of Allowance in U.S. Pat. Appl. No. 14/499,234 dated 01-19-2016
	24	Notice of Allowance in U.S. Pat. Appl. No. 14/499,234 dated 01-29-2016

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

Form (PTO-1449)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 1044
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 14/816,931	Art Unit: 2438
File Date: 2015-08-03	Docket No.: SP1P012A
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: November 10, 2016

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§ 1.56 AND 1.97(b)

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

Dear Sir:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

One or more related patents (e.g. US8266699, US8984644, US9100431, US9117069, US9118708, and US9225686) are the subject of pending litigation (EDTX 6:16-cv-01016, EDTX 6:16-cv-01165). No invalidity contentions have been provided in such litigation. This Information Disclosure Statement is believed to be filed within three months of the filing date of a national application other than a continued prosecution application, within three months of the date of entry of the national stage 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. Accordingly, it is believed that no fees are due in connection with the filing of this Information Disclosure Statement.

Respectfully submitted,



Dated: 10 Nov 2016

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Patrick E. Caldwell, Esq.
Reg. No. 44,580

Electronic Patent Application Fee Transmittal

Application Number:	14816931
Filing Date:	03-Aug-2015
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012A

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 1st Request	2801	1	600	600
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt	
EFS ID:	27481033
Application Number:	14816931
International Application Number:	
Confirmation Number:	1044
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	127962
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012A
Receipt Date:	10-NOV-2016
Filing Date:	03-AUG-2015
Time Stamp:	21:06:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$600
RAM confirmation Number	111416INTEFSW21080700
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	SP1P012A_SB30-RCE_vF_10-Nov-2016.pdf	39472 e7d731d9d78ac3996b3256073076ea656ee4dbca	no	3
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Amendment Submitted/Entered with Filing of CPA/RCE	SP1P012A_Resp-RCE_vF_10-Nov-2016.pdf	101137 2cf89f60632dda82fac02b362d8805f32bd6d102	no	14
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	SP1P012A_IDS_1_vF_10-Nov-2016.pdf	39051 59e683baa5915f447a4ce5881c18c05147c35dc2	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Information Disclosure Statement (IDS) Form (SB08)	SP1P012A_IDS_2_vF_10-Nov-2016.pdf	55953 5760ed5232fe929b1993c22ee856e225f13aeae5	no	8
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Information Disclosure Statement (IDS) Form (SB08)	SP1P012A_IDS_3_vF_10-Nov-2016.pdf	36739 50c585dfc0abd69e0cdd01d88285654c1562d8a9	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					

6	Transmittal Letter	SP1P012A_IDS_3_XMTL_vF_10-Nov-2016.pdf	50199 c98b57ecf2fb8e5083d394906da04c65ab52c42b	no	2
Warnings:					
Information:					
7	Information Disclosure Statement (IDS) Form (SB08)	SP1P012A_IDS_4_vF_10-Nov-2016.pdf	91927 509778d3257dddb004778403351e9c41b7662f5f	no	15
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
8	Information Disclosure Statement (IDS) Form (SB08)	SP1P012A_IDS_5_vF_10-Nov-2016.pdf	267955 f24fbd20a9f2037039379701b88746f7cc5f1533	no	34
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
9	Transmittal Letter	SP1P012A_IDS_5_XMTL_vF_10-Nov-2016.pdf	51123 604234b68623db2e6b41fd0384ada534cc714ff2	no	2
Warnings:					
Information:					
10	Fee Worksheet (SB06)	fee-info.pdf	30677 09aa5c4e863c48f0ee8d8c57065498e2b7c3a387	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	764233		

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/08a (01-10)
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 contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(**Not for submission under 37 CFR 1.99)**

Application Number	14816931
Filing Date	2015-08-03
First Named Inventor	Brett M. Oliphant
Art Unit	2438
Examiner Name	Madhuri R HERZOG
Attorney Docket Number	SP1P0012A

U.S.PATENTS

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

	1	Office Action Summary in U.S. Pat. App. No. 14/499,226 dated 5/19/2015	☐
	2	Office Action Summary in US Pat. App. No. 14/499,236 dated 05/06/2015	☐
	3	Office Action Summary in U.S. Pat. App. No. 14/499,239 dated 6/18/2015	☐
	4	Office Action Summary in U.S. Pat. App. No. 14/499,246 dated 03/30/2015	☐
	5	Office Action Summary in U.S. Pat. App. No. 14/499,246 dated 04/28/2015	☐
	6	Office Action Summary in U.S. Pat. App. No. 14/499,250 dated 05/13/2015	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

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

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**		
	Application Number	14816931
	Filing Date	2015-08-03
	First Named Inventor	Brett M. Oliphant
	Art Unit	2438
	Examiner Name	Madhuri R HERZOG
	Attorney Docket Number	SP1P0012A

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Patrick Caldwell/	Date (YYYY-MM-DD)	2016-11-10
Name/Print	Patrick Caldwell	Registration Number	44580

This collection of information is required by 37 CFR 1.97 and 1.98. 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 1 hour 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 04/21/2017

JOLSEN SALE #00000001 Mailroom Dt: 11/10/2016 505939 14816931
01 FC : 2202 40.00 DA

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025



Courtesy Reminder for
Application Serial No: 14/816,931

Attorney Docket No: SP1P012A
Customer Number: 127962
Date of Electronic Notification: 08/10/2016

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

eofficeaction@appcoll.com
pcaldwell@thecaldwellfirm.com

To view your correspondence online or update your email addresses, please visit us anytime at **https://sportal.uspto.gov/secure/myportal/privatepair.** If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

UNITED STATES PATENT AND TRADEMARK OFFICE

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

NOTICE OF ALLOWANCE AND FEE(S) DUE

127962 7590 08/10/2016

Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

EXAMINER	
HERZOG, MADHURI R	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 08/10/2016

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A	1044

TITLE OF INVENTION: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	11/10/2016

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 ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

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.

ForcePoint LLC
EX-1010-PT2
Page336

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)

127962 7590 08/10/2016
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

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.
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A	1044

TITLE OF INVENTION: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	11/10/2016

EXAMINER	ART UNIT	CLASS-SUBCLASS
HERZOG, MADHURI R	2438	726-025000

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 credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

PTOL-85 Part B (10-13) Approved for use through 10/31/2013. OMB 0651-0033 U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

ForcePoint LLC
EX-1010-PT2
Page337

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.
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A	1044

127962 7590 08/10/2016

Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

EXAMINER	
HERZOG, MADHURI R	
ART UNIT	PAPER NUMBER
2438	

DATE MAILED: 08/10/2016

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

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.

ForcePoint LLC
EX-1010-PT2
Page338

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B 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.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 14/816,931	Applicant(s) OLIPHANT ET AL.	
	Examiner MADHURI HERZOG	Art Unit 2438	AIA (First Inventor to File) Status No

-- 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 *06/28/2016*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-21*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   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.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ 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. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/MADHURI HERZOG/
Primary Examiner, Art Unit 2438

ForcePoint LLC
EX-1010-PT2
Page340

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.

3. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.

4. Claims 1-21 have been examined and are pending.

Terminal Disclaimer

5. The terminal disclaimer filed on 06/28/2016 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of U.S Patent No. 9100431 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

6. Claims 1-21 are allowed over prior art of record.

Response to Arguments

7. Applicant's arguments, see pages 13-14 of the Remarks, filed on 06/28/2016, have been fully considered and are persuasive.

Examiner's Statement of Reasons for Allowance

8. The following is an examiner's statement of reasons for allowance:

Independent claims 1, 16 and 20 are allowed for reasons presented by the applicant in pages 13-14 of the Remarks. Claims 2-15, 17-19 and 21 depend on one of the above mentioned independent claims and are therefore allowed by virtue of their dependencies.

Prior art of record Brawn teaches: a management system stores various remediation techniques corresponding to various vulnerabilities. The management system transmits an interrogation program to the client that attempts to exploit a known vulnerability present in the software of the client, determines whether the vulnerability is exploited and transmits a remediation program if the vulnerability is exploited. Prior art Banzhof1 teaches: Constructing remediation signatures such as patches or fixes to remediate a vulnerability. IT or security personnel select which remediation signatures to deploy to client computers. Prior art of record Banzhof2 teaches displaying vulnerabilities to an administrator.

However, Brawn, Banzhof1 and Banzhof2 fail to teach "said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system", i.e., the prior arts fail to teach identifying a remediation technique based on the operating system.

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

ITS4 : A Static Vulnerability Scanner for C and C++ Code by Viega et al: We describe ITS4, a tool for statically scanning security-critical C source code for vulnerabilities. Compared to other approaches, our scanning technique stakes out a new middle ground between accuracy and efficiency. This method is efficient enough to offer real-time feedback to developers during coding while producing few false negatives.

An automated approach for identifying potential vulnerabilities in software by Ghosh et al: The paper presents results from analyzing the vulnerability of security-critical software applications to malicious threats and anomalous events using an automated fault injection analysis approach. The work is based on the well understood premise that a large proportion of security violations result from errors in software source code and configuration. The methodology employs software fault injection to force anomalous program states during the execution of software and observes their corresponding effects on system security. If insecure behaviour is detected, the

perturbed location that resulted in the violation is isolated for further analysis and possibly retrofitting with fault tolerant mechanisms.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on M-F from 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/MADHURI HERZOG/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/816,931	Applicant(s)/Patent Under Reexamination OLIPHANT ET AL.	
	Examiner MADHURI HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US 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	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Ghosh, Anup K., Tom O'Connor, and Gary McGraw. "An automated approach for identifying potential vulnerabilities in software." Security and Privacy, 1998. Proceedings. 1998 IEEE Symposium on. IEEE, 1998.
	V	Viega, John, et al. "ITS4: A static vulnerability scanner for C and C++ code." Computer Security Applications, 2000. ACSAC'00. 16th Annual Conference. IEEE, 2000.
	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.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	Art Unit
	MADHURI HERZOG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 63/02all, 63/14all	7/20/2016	M.H
G06F 21/5all	7/20/2016	M.H

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	1, 11-14, 22-25	7/20/2016	M.H
713	187-188	7/20/2016	M.H

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search, Assignee search	7/20/2016	M.H
East search	7/20/2016	M.H
Google Scholar search	7/20/2016	M.H
search terms: determine, detect, resolve, find, discover, uncover, identify, check, scan, examine, vulnerability, application, administer, implement, install, deploy, distribute, send, transmit, transfer, forward, mitigate, remediate, user, client, customer, subscriber, select, choose, pick, choice, input, specific, particular, distinct, different, explicit, individual, unique, operating, system	7/20/2016	M.H

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/MADHURI HERZOG/ Primary Examiner.Art Unit 2438

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	1, 11-14, 22-25 with search terms: determine, detect, resolve, find, discover, uncover, identify, check, scan, examine, vulnerability, application, administer, implement, install, deploy, distribute, send, transmit, transfer, forward, mitigate, remediate, user, client, customer, subscriber, select, choose, pick, choice, input, specific, particular, distinct, different, explicit, individual, unique, operating, system	7/20/2016	M.H
713	187-188 with the above search terms	7/20/2016	M.H
H04L	63/02all, 63/14all with the above search terms	7/20/2016	M.H
G06F	21/5all with the above search terms	7/20/2016	M.H

	/MADHURI HERZOG/ Primary Examiner.Art Unit 2438

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. 1044

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/816,931	08/03/2015 RULE	726	2438	SP1P012A

APPLICANTS
SecurityProfiling, LLC, Garland, TX;

INVENTORS
Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

**** CONTINUING DATA ***************************
This application is a CON of 14/499,230 09/28/2014 PAT 9100431
which is a CIP of 14/138,014 12/21/2013 PAT 9117069
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/18/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /MADHURI R HERZOG/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		TX	12	21	3

ADDRESS
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025
UNITED STATES

TITLE
COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

FILING FEE RECEIVED		
840	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

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	**Art Unit**
	MADHURI HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/22/2015	07/20/2016							
1	1	✓	=							
2	2	✓	=							
3	3	✓	=							
4	4	✓	=							
5	5	✓	=							
6	6	✓	=							
7	7	✓	=							
8	8	✓	=							
9	9	✓	=							
10	10	✓	=							
11	11	✓	=							
12	12	✓	=							
13	13	✓	=							
14	14	✓	=							
15	15	✓	=							
16	16	✓	=							
17	17	✓	=							
18	18	✓	=							
19	19	✓	=							
20	20	✓	=							
21	21	✓	=							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S13	1038	(determin$6 or detect$4 or resolv$4 or find$4 or discover$4 or uncover$4 or identiy$4 or identification or check$4 or scan$4 or examin$6) with vulnerabilit$4 and (application or apply$4 or administer$5 or implenat$6 or deploy$4 or install$6 or distribu$4 or send$4 or transmi$6 or transfer$4 or forward$4) with (mitigat$4 or remediat$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 14:51
S14	5455	(726/1,11-14,22-25.ccls. or 713/187-188.ccls.) and S13	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 14:51
S15	1	S14 and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) near5 (signature or technique or method or type or category or class or group or kind or fingerprint or variety or classification) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 14:52
S16	505	(H04L63/02$ or H04L63/14$ or G06F21/5$).cpc. and S14	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 14:52
S17	1	S16 and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) near5 (signature or technique or method or type or category or class or group or kind or fingerprint or variety or classification) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 14:53
S18	173	S13 and (user or client or customer or subscriber) with (select$4 or choos$4 or pick$4 or choice or input$4) with (mitigat$4 or remediat$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 15:05
S19	5	S18 and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4 or pick$4 or choice) with (mitigat$4 or remediat$4) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 15:08

S20	5	(H04L63/02$ or H04L63/14$ or G06F21/5$).cpc. and S19	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 15:09
S21	4	(726/1,11-14,22-25.ccls. or 713/187-188.ccls.) and S19	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2016/07/19 15:09

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S22	1	(H04L63/02$ or H04L63/14$ or G06F21/5$).cpc. and ((determin$6 or detect$4 or resolv$4 or find$4 or discover$4 or uncover$4 or identiy$4 or identification or check$4 or scan$4 or examin$6) with vulnerabilit$4 and (application or apply$4 or administer$5 or implenat$6 or deploy$4 or install$6 or distribu$4 or send$4 or transmi$6 or transfer$4 or forward$4) with (mitigat$4 or remediat$4) and (user or client or customer or subscriber) with (select$4 or choos$4 or pick$4 or choice or input$4) with (mitigat$4 or remediat$4) and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4 or pick$4 or choice) with (mitigat$4 or remediat$4) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system).clm.	USPAT	ADJ	ON	2016/07/19 15:11
S23	0	(726/1,11-14,22-25.ccls. or 713/187-188.ccls.) and ((determin$6 or detect$4 or resolv$4 or find$4 or discover$4 or uncover$4 or identiy$4 or identification or check$4 or scan$4 or examin$6) with vulnerabilit$4 and (application or apply$4 or administer$5 or implenat$6 or deploy$4 or install$6 or distribu$4 or send$4 or transmi$6 or transfer$4 or forward$4) with (mitigat$4 or remediat$4) and (user or client or customer or subscriber) with (select$4 or choos$4 or pick$4 or choice or input$4) with (mitigat$4 or remediat$4) and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4 or pick$4 or choice) with (mitigat$4 or remediat$4) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system).clm.	USPAT	ADJ	ON	2016/07/19 15:11
S24	1	(726/1,11-14,22-25.ccls. or 713/187-188.ccls.) and ((determin$6 or detect$4 or resolv$4 or find$4 or discover$4 or uncover$4 or identiy$4 or identification or check$4 or scan$4 or examin$6) with vulnerabilit$4 and (application or apply$4 or administer$5 or implenat$6 or deploy$4 or install$6 or distribu$4 or send$4 or transmi$6 or transfer$4 or forward$4) with (mitigat$4 or remediat$4) and (user or client or customer or subscriber) with (select$4 or	USPAT	ADJ	ON	2016/07/19 15:17

		choos$4 or pick$4 or choice or input$4) with (mitigat$4 or remediat$4) and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4 or pick$4 or choice) with (mitigat$4 or remediat$4) with operating near5 system).clm.				
S25	6	(H04L63/02$ or H04L63/14$ or G06F21/5$).cpc. and ((determin$6 or detect$4 or resolv$4 or find$4 or discover$4 or uncover$4 or identiy$4 or identification or check$4 or scan$4 or examin$6) with vulnerabilit$4 and (application or apply$4 or administer$5 or implenat$6 or deploy$4 or install$6 or distribu$4 or send$4 or transmi$6 or transfer$4 or forward$4) with (mitigat$4 or remediat$4) and (user or client or customer or subscriber) with (select$4 or choos$4 or pick$4 or choice or input$4) with (mitigat$4 or remediat$4) and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4 or pick$4 or choice) with (mitigat$4 or remediat$4) with operating near5 system).clm.	USPAT	ADJ	ON	2016/07/19 15:18

7/ 20/ 2016 10:03:50 AM
C:\ Users\ mherzog\ Documents\ EAST\ Workspaces\ App14816931.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	**Art Unit**
	MADHURI HERZOG	2438

CPC						
Symbol					**Type**	**Version**
H04L		63	/	1433	F	2013-01-01
H04L		63	/	1441	I	2013-01-01
G06F		21	/	577	I	2013-01-01
G06F		21	/	55	I	2013-01-01
H04L		63	/	14	I	2013-01-01
G06F		21	/	554	I	2013-01-01
H04L		63	/	1408	I	2013-01-01
H04L		63	/	02	I	2013-01-01
G06F		21	/	50	I	2013-01-01
H04L		63	/	0263	A	2013-01-01
H04L		63	/	1416	I	2013-01-01
H04L		63	/	20	I	2013-01-01
G06F		21	/	57	I	2013-01-01
H04L		63	/	0227	I	2013-01-01
H04L		63	/	145	I	2013-01-01

CPC Combination Sets							
Symbol				**Type**	**Set**	**Ranking**	**Version**
			/				
			/				

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	21	
/MADHURI HERZOG/ Primary Examiner.Art Unit 2438	07/20/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	**Art Unit**
	MADHURI HERZOG	2438

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	25	H	0	4	L	29 / 00 (2006.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	13	22	26	24	
713	187	188			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	21	
/MADHURI HERZOG/ Primary Examiner.Art Unit 2438	07/20/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	**Art Unit**
	MADHURI HERZOG	2438

☐ 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	Final	Original
1	1	17	17												
2	2	18	18												
3	3	19	19												
4	4	20	20												
5	5	21	21												
6	6														
7	7														
8	8														
9	9														
10	10														
11	11														
12	12														
13	13														
14	14														
15	15														
16	16														

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	21	
/MADHURI HERZOG/ Primary Examiner.Art Unit 2438	07/20/2016	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

ForcePoint LLC
EX-1010-PT2
Page355

Doc Code: DIST.E.FILE **Document Description: Electronic Terminal Disclaimer - Filed**	PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce

Electronic Petition Request	**TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT**
Application Number	14816931
Filing Date	03-Aug-2015
First Named Inventor	Brett Oliphant
Attorney Docket Number	SP1P012A
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action

☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.

Owner	Percent Interest
SecurityProfiling, LLC	100%

The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)

9100431

as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:
- expires for failure to pay a maintenance fee;
- is held unenforceable;
- is found invalid by a court of competent jurisdiction;
- is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321;
- has all claims canceled by a reexamination certificate;
- is reissued; or
- is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

◉ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.

○	I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

Applicant claims the following fee status:

◉ Small Entity

○ Micro Entity

○ Regular Undiscounted

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.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

◉ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application

Registration Number 44580

○ A sole inventor

○ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application

○ A joint inventor; all of whom are signing this request

Signature	/Patrick E. Caldwell/
Name	Patrick E. Caldwell

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Electronic Patent Application Fee Transmittal

Application Number:	14816931
Filing Date:	03-Aug-2015
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012A

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Statutory or Terminal Disclaimer	2814	1	160	160
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**160**

Doc Code: DISQ.E.FILE
Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 14816931

Filing Date: 03-Aug-2015

Applicant/Patent under Reexamination: Oliphant et al.

Electronic Terminal Disclaimer filed on June 28, 2016

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt	
EFS ID:	26203786
Application Number:	14816931
International Application Number:	
Confirmation Number:	1044
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	127962
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012A
Receipt Date:	28-JUN-2016
Filing Date:	03-AUG-2015
Time Stamp:	22:30:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$160
RAM confirmation Number	062916INTEFSW22303800
Deposit Account	0581
Authorized User	Patrick Caldwell
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Electronic Terminal Disclaimer-Filed	eTerminal-Disclaimer.pdf	33373 c013318c065cf6d1752ae16899deb498a4b01da9	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30663 daa23cf1a43e00099b60b3ec342ff8894b6d9268	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	64036		

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.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Confirmation No.: 1044
Brett M. Oliphant	Examiner: Madhuri R HERZOG
Application No.: 14/816,931	Art Unit: 2438
File Date: 2015-08-03	Docket No.: SP1P012A
Title: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: Jun 28, 2016

AMENDMENT A

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

Examiner:

In response to the communication mailed 2015-12-28 (hereafter "Non Final Office Action" or "NFOA"), please consider the following amendments believed to place the claims in condition for allowance.

ForcePoint LLC
EX-1010-PT2
Page363

Amendments to the Claims:

The listing of amended claims follows:

1. (Currently Amended) An apparatus, comprising:

at least one data storage;

at least one platform communicatively coupled to the at least one data storage; and

at least one agent capable of being communicatively coupled to the at least one platform;

said at least one data storage configured to store data on a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

said at least one platform configured to:

cause display of at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allow receipt of user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability;

said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability, so that the at least one mitigation technique is capable of being applied;

said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

2. (Currently Amended) The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to first user input received prior to the attack, the firewall option is capable of being applied to a plurality of different devices for preventing the at least one attack packet at any of the different devices; and the apparatus is further configured such that, in response to additional user input after the attack in connection with a particular single device of the plurality of different devices, the intrusion detection or prevention option is capable of being applied to the particular single device.

3. (Currently Amended) The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to first user input prior to the attack, the intrusion detection or prevention option is capable of being applied to a plurality of different devices at the plurality of different devices; and the apparatus is further configured such that, in response to second user input after the attack in connection with a particular single device of the plurality

of different devices, the firewall option is capable of being applied to the particular single device for preventing the at least one attack packet at the particular single device.

4. (Currently Amended) The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification of the operating system in connection ~~with the accessing for~~ the displaying of the at least one mitigation technique, so that, in order to avoid false positives, relevant vulnerabilities prompt mitigation technique user selection among at least two of the mitigation techniques, which involve both firewall and intrusion prevention system actions, for providing diverse mitigation options in connection with the relevant vulnerabilities.

5. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification of the operating system prior to causing the display of the at least one mitigation technique, so that which of the one or more of the mitigation techniques that is caused to be displayed is based on one or more actual vulnerabilities to which the at least one device is actually vulnerable so that only relevant one or more mitigation techniques are displayed for selection by a user for attack mitigation.

6. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the user input is capable of being received via at least one user interface of the at least one platform for different devices, for allowing different attack mitigation actions including at least one intrusion prevention action and at least one firewall action to be selectively applied to the different devices for different actual vulnerabilities determined to be actually relevant based on the identification of the operating system in connection with the different devices.

7. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a first

mitigation technique that utilizes a firewall action and a second mitigation technique that utilizes an intrusion prevention action;

8. (Original) The apparatus of Claim 7, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

9. (Original) The apparatus of Claim 7, wherein the apparatus is configured such that the at least one mitigation technique further includes a third mitigation technique that utilizes a policy compliance action, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique, the second mitigation technique, and the third mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device; only the second mitigation technique being selectively applied by the user to at least one second device; and the first mitigation technique, the second mitigation technique, and the third mitigation technique being selectively applied by the user to at least one third device.

10. (Currently Amended) The apparatus of Claim 7, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from an integrated firewall/intrusion prevention system platform component of the at least one platform to firewall-supporting code of the at least one agent, and the second mitigation

technique is automatically applied utilizing a second communication from the integrated firewall/intrusion prevention system platform component of the at least one platform to intrusion prevention system-supporting code of the at least one agent, where the firewall-supporting code and the intrusion prevention system-supporting code are part of the at least one agent.

11. (Original) The apparatus of Claim 1, wherein the apparatus is configured such that the identification of the operating system is a result of a vulnerability assessment scan caused by the at least one platform.

12. (Original) The apparatus of Claim 1, wherein the at least one platform includes intrusion prevention functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality.

13. (Original) The apparatus of Claim 1, wherein the at least one platform utilizes router-based functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique.

14. (Currently Amended) The apparatus of Claim 13, wherein the apparatus is configured ~~such that the system is capable of~~for receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the

plurality of mitigation techniques to allow selective utilization of the router-based functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the router-based functionality and the firewall functionality.

15. (Currently Amended) The apparatus of Claim 1, wherein at least one of:

said at least one data storage includes at least one database;

said at least one data storage is accessed [[by]]utilizing an operation including at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said mitigation techniques include remediation techniques;

each mitigation technique has a mitigation type including the patch;

each mitigation technique has a mitigation type including the policy setting;

each mitigation technique has a mitigation type including the configuration option;

each mitigation technique is capable of mitigating the effect of the attack that takes advantage of the corresponding vulnerability, by dropping packets associated with the attack or removing the corresponding vulnerability;

said information is capable of being used to determine an intended destination of a connection request; or

said information includes a vulnerability identifier;

wherein the apparatus is operable for use with at least one network operations center (NOC) server, a data warehouse, and [[an]]a software development kit (SDK) for allowing access to information associated with at least one vulnerability and at least one remediation technique; and wherein the apparatus is operable for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

16. (Currently Amended) An apparatus, comprising:

at least one data storage configured to store at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; and

at least one platform communicatively coupled to the at least one data storage, the at least one platform configured to:

based on user selection, automatically apply at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type ~~to the at least one device~~;

receive information in connection with at least one of a plurality of devices,

identify an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information, and

mitigate an effect of the attack on the at least one device that takes advantage of the at least one vulnerability, based on the automatic application of the at least two of the plurality of mitigation techniques including the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type to the at least one device;

wherein the apparatus is configured such that the at least two of the plurality of mitigation techniques are made available for the user selection, based on an identification of an operating system.

17. (Original) The apparatus of Claim 16, wherein the apparatus is configured such that the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by at least one agent that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied.

18. (Original) The apparatus of Claim 17, wherein the apparatus is configured such that the at least one agent is further capable of supporting a vulnerability assessment scan for the identification of the operating system.

19. (Original) The apparatus of Claim 16, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from the at least one platform to firewall-supporting code of at least one agent, and the second mitigation technique is automatically applied utilizing a second communication from the at least one platform to intrusion prevention system-supporting code of the at least one agent; wherein the at least one platform includes intrusion prevention functionality for supporting the first mitigation technique and firewall functionality for supporting the second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally make available for the user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and

the firewall functionality, so that only relevant mitigation techniques are made available for the user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user selections are capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

20. (Currently Amended) An apparatus, comprising:

means for identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities associated with an operating system, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

means for:

causing display of at least two of the mitigation techniques for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allowing receipt of at least one user input in connection with one or more of the at least two mitigation techniques; and

means for ~~automatically~~applying the one or more of the at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device;

said apparatus configured such that the at least two mitigation techniques are displayed based on an identification of an operating system.

21. (Original) The apparatus of Claim 20, wherein the apparatus is configured such that the at least one first mitigation technique is automatically applied utilizing a first communication to firewall-supporting code, and the at least one second mitigation technique is automatically applied utilizing a second communication to intrusion prevention system-supporting code; wherein the apparatus includes intrusion prevention functionality for supporting the at least one first mitigation technique and firewall functionality for supporting the at least one second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by at least one component that also supports identification of attacks in connection with the at least one device, the apparatus further capable of receiving actual vulnerability information to conditionally make available for user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are made available for the user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the at least one first mitigation technique and the at least one second mitigation technique to be selectively applied to the different devices for

different actual vulnerabilities, such that the different user selections are capable of resulting in: only the at least one first mitigation technique being selectively applied to at least one first device, only the at least one second mitigation technique being selectively applied to at least one second device, and both the at least one first mitigation technique and the at least one second mitigation technique being selectively applied to at least one third device.

Remarks:

The Examiner has acknowledged applicants' claim to priority as a continuation of parent application 14/499,230, now U.S Patent No. 9,100,431. Applicant emphasizes that the full priority chain is set forth below (as set forth in the current application):

> "This application is a continuation of U.S. application Ser. No. 14/499,230 filed Sep. 28, 2014 which, in turn, is a continuation-in-part of U.S. application Ser. No. 14/138,014 filed Dec. 21, 2013, now U.S. Pat. No. 9,100,431, which, in turn, is a continuation of U.S. application Ser. No. 10/882,852 filed Jul. 1, 2004 which, in turn, claims priority to U.S. App. No. 60/484,085 filed Jul. 1, 2003, which are all incorporated herein by reference in their entirety for all purposes."

Claims 1-21 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 9,100,431. A terminal disclaimer is submitted herewith for overcoming such rejection.

Claims 1-21 of this application is patentably indistinct from claims 1-21 of Application No. 14/816,960. Applicant respectfully disagrees with this rejection, and asserts that such rejection is further deemed moot in view of the amendments made to the above claims and the claims of Application No. 14/816,960.

Claim 15 is objected to because of informalities. Applicant respectfully asserts that such objection is rendered moot in view of the clarifications made to the claims hereinabove.

Claims 1, 15 and 16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter regarded as the invention. Applicant respectfully disagrees. Further, as for Claims 1, 15

and 16, such rejection is deemed moot in view of the clarification made hereinabove to the claims.

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Still yet, nothing in this reply should be construed as intention to concede any issue with regard to any claim, except as specifically stated in this reply. Finally, with the exception of Claim 20 (and any dependent claims), it should be noted that no claims are intended to be construed under 35 U.S.C. 112, paragraph 6.

Applicant hereby requests an extension of time to respond and encloses the appropriate fee. Applicant does not believe that any additional fees are due. However, in the event that any other fees are due, the Director is hereby authorized to charge any required fees due (other than issue fees), and to credit any overpayment made, in connection with the filing of this paper to Deposit Account No. 50-5939 (Order No. SP1P012A).

Respectfully submitted,



Dated: 28 Jun 2016

Patrick E. Caldwell, Esq.
Reg. No. 44,580

The Caldwell Firm, LLC
PO Box 59655
Dallas, Texas 75229-0655
Telephone: (214) 734-2313
pcaldwell@thecaldwellfirm.com

Electronic Patent Application Fee Transmittal

Application Number:	14816931
Filing Date:	03-Aug-2015
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Patrick Edgar Caldwell
Attorney Docket Number:	SP1P012A

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
			Total in USD ($)	**700**

Electronic Acknowledgement Receipt	
EFS ID:	26203853
Application Number:	14816931
International Application Number:	
Confirmation Number:	1044
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	127962
Filer:	Patrick Edgar Caldwell
Filer Authorized By:	
Attorney Docket Number:	SP1P012A
Receipt Date:	28-JUN-2016
Filing Date:	03-AUG-2015
Time Stamp:	22:07:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$700
RAM confirmation Number	062916INTEFSW22082700
Deposit Account	0581
Authorized User	Patrick Caldwell
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	SP1P012A_OA_Resp_vF_28-Jun-2016.pdf	100740 e4bfe0cb55d5ed1acfc7ffeb18e8392c7538b72d	no	14
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30878 fbee2dfff3c7d137dbea8e1d96485738eee99bcb	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	131618		

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/06 (09-11)
Approved for use through 1/31/2014. 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 14/816,931	Filing Date 08/03/2015	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	x $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	x $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 06/28/2016	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 21	Minus	** 21	= 0	x $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	x $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	x $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	x $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					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.

LIE
ERIC DANTZLER

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 f

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
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A

CONFIRMATION NO. 1044

127962
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

PUBLICATION NOTICE

OC000000080339786

Title:COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Publication No.US-2016-0036852-A1
Publication Date:02/04/2016

NOTICE OF PUBLICATION OF APPLICATION

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

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

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

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

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

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

ForcePoint LLC
EX-1010-PT2
Page382

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.
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A	1044

127962 7590 12/28/2015

Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

EXAMINER
HERZOG, MADHURI R

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
12/28/2015	PAPER

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

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

Office Action Summary	Application No. 14/816,931	Applicant(s) OLIPHANT ET AL.	
	Examiner MADHURI HERZOG	Art Unit 2438	AIA (First Inventor to File) Status No

-- 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* MONTHS 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 *08/03/2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ 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*

5)☒ Claim(s) *1-21* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-21* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *08/03/2015* 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).

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).

Certified copies:

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)).

** 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) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. Claims 1-21 have been examined.

Priority

3. Acknowledgement is made of the applicants' claim to priority as a continuation of parent application 14/499230, now U.S Patent No. 9100431.

Double Patenting

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

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the reference application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(l)(1) - 706.02(l)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/forms/. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to http://www.uspto.gov/patents/process/file/efs/guidance/eTD-info-l.jsp.

5. Claims 1-21 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 9100431. Although the claims at issue are not identical, they are not patentably distinct from each other because:

Claim 1 of the instant application: 1. An apparatus, comprising: at least one data storage; at least one platform communicatively coupled to the at least one data storage;

and at least one agent capable of being communicatively coupled to the at least one platform; said at least one data storage configured to store data on a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where: each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; said at least one platform configured to: cause display of at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and allow receipt of user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability; said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability; said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

Is analogous to:

Claim 1 of U.S. Patent No. 9100431: 1. A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising: code for: accessing at least one data storage identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, such that: each mitigation technique is capable of mitigating an effect of

an attack that takes advantage of a corresponding vulnerability, and each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; code for: displaying at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and receiving user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability; and code for: receiving information in connection with at least one of a plurality of devices, and identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability, based on the information; wherein the computer program product is operable such that, as a result of the user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability, the identified attack is prevented from taking advantage of the at least one vulnerability; wherein the computer program product is operable such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

Similarly, the rest of the independent and dependent claims of the instant application are analogous to the rest of the independent and dependent claims of U.S. Patent No. 9100431.

6. Claims 1-21 of this application is patentably indistinct from claims 1-21 of Application No. 14/816931. Pursuant to 37 CFR 1.78(f) or pre-AIA 37 CFR 1.78(b), when two or more applications filed by the same applicant contain patentably indistinct claims, elimination of such claims from all but one application may be required in the absence of good and sufficient reason for their retention during pendency in more than one application. Applicant is required to either cancel the patentably indistinct claims from all but one application or maintain a clear line of demarcation between the applications. See MPEP § 822.

Claim Objections

7. Claim 15 is objected to because of the following informalities: Claim 15 recites: NOC server, SDK. Full form of the acronyms should be recited. Appropriate correction is required.

Claim Rejections - 35 USC § 112

8. The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1, 15 and 16 are rejected under 35 U.S.C. 112(b) or 35 U.S.C. 112 (pre-AIA), second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA

the applicant regards as the invention. Claim 1 recites the limitation: “said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability”. It is unclear how this limitation is related to the rest of the claim. Is the agent configured to identify an attack so that a corresponding mitigation technique can be applied?

10. Claim 15 recites the limitation: “said at least one data storage is accessed by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith”. It is unclear what the data storage is being accessed by. Or is the limitation supposed to recite: said at least one data storage is accessed ***for*** at least one of?

11. Claim 16 recites: “mitigate an effect of the attack on the at least one device that takes advantage of the at least one vulnerability, based on the application”. It is unclear what "based on the application" refers to.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

US 7278163 to Banzhof et al: A system and method for assessing risks to computer network is provided. The system includes a first module assesses a human factor related to a risk to the computer network. A second module assesses a remediation to the computer network.

US 20030126472 to Banzhof et al: A system and process for addressing computer security vulnerabilities. The system and process generally comprise aggregating vulnerability information on a plurality of computer vulnerabilities; constructing a remediation database of said plurality of computer vulnerabilities; constructing a remediation signature to address the computer vulnerabilities; and deploying said remediation signature to a client computer.

US 20040088581 to Brawn et al: A method of identifying a software vulnerability in computer systems in a computer network includes a multiple level scanning process controlled from a management system connected to the network.

US 20030195861 to McClure et al: A system and method provide comprehensive and highly automated testing of vulnerabilities to intrusion on a target network, including identification of operating system, identification of target network topology and target computers, identification of open target ports, assessment of vulnerabilities on target ports, active assessment of vulnerabilities based on information acquired from target computers, quantitative assessment of target network security and vulnerability, and hierarchical graphical representation of the target network, target computers, and vulnerabilities in a test report.

US 20060101517 to Banzhof et al: A remediation server, downloadable software and an associated method for protecting a computer network from vulnerabilities.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MADHURI HERZOG whose telephone number is (571)270-3359. The examiner can normally be reached on M-F from 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on 571-272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/MADHURI HERZOG/
Primary Examiner, Art Unit 2438

Notice of References Cited	Application/Control No. 14/816,931	Applicant(s)/Patent Under Reexamination OLIPHANT ET AL.	
	Examiner MADHURI HERZOG	Art Unit 2438	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2003/0126472 A1	07-2003	Banzhof, Carl E.	G06F21/577	726/25
*	B	US-2003/0195861 A1	10-2003	McClure, Stuart C.	H04L41/12	1/1
*	C	US-2004/0088581 A1	05-2004	Brawn, John Melvin	H04L63/1433	726/25
*	D	US-2006/0101517 A1	05-2006	Banzhof; Carl E.	G06F21/577	726/25
*	E	US-7,278,163 B2	10-2007	Banzhof; Carl E.	G06F21/577	705/38
	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	CPC 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.

ForcePoint LLC
EX-1010-PT2
Page393

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. 1044

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
14/816,931	08/03/2015 RULE	726	2438	SP1P012A

APPLICANTS
SecurityProfiling, LLC, Garland, TX;

INVENTORS
Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

**** CONTINUING DATA **************************
This application is a CON of 14/499,230 09/28/2014 PAT 9100431
which is a CIP of 14/138,014 12/21/2013 PAT 9117069
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

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

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/18/2015

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /MADHURI R HERZOG/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		TX	12	21	3

ADDRESS
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025
UNITED STATES

TITLE
COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

FILING FEE RECEIVED		
840	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

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	Art Unit
	MADHURI HERZOG	2438

CPC- SEARCHED		
Symbol	Date	Examiner
H04L 63/02all, 63/14all	12/22/2015	M.H
G06F 21/5all	12/22/2015	M.H

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
726	1, 11-14, 22-25	12/22/2015	M.H
713	187-188	12/22/2015	M.H

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor search, Assignee search	12/22/2015	M.H
East search	12/22/2015	M.H

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

	/MADHURI HERZOG/ Primary Examiner.Art Unit 2438

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	14816931	OLIPHANT ET AL.
	Examiner	**Art Unit**
	MADHURI HERZOG	2438

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	12/22/2015								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								

ForcePoint LLC
EX-1010-PT2
Page396

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	17	(identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/22 09:18
S1	2	"14499230"	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 15:27
S2	890	("20010014150" | "20010027388" | "20010027389" | "20010028268" | "20010028269" | "20010034847" | "20010042004" | "20010043778" | "20020013811" | "20020026591" | "20020032860" | "20020042687" | "20020042877" | "20020069035" | "20020078381" | "20020092924" | "20020104014" | "20020109963" | "20020112179" | "20020116631" | "20020120558" | "20020137991" | "20020138416" | "20020147803" | "20020150866" | "20020171546" | "20020178383" | "20020199122" | "20030005178" | "20030014669" | "20030023873" | "20030028803" | "20030033542" | "20030037258" | "20030037601" | "20030046128" | "20030050718" | "20030051163" | "20030056116" | "20030061506" | "20030065945" | "20030070003" | "20030083831" | "20030084320" | "20030091951" | "20030097228" | "20030126472" | "20030135749" | "20030140249" | "20030140250" | "20030145228" | "20030154269" | "20030159060" | "20030159063" | "20030177389" | "20030188194" | "20030195569" | "20030195861" | "20030202663" | "20030204632" | "20030204719" | "20030204728" | "20030212779" | "20030212909" | "20030217039" | "20030233438" | "20040006704" | "20040015338" | "20040015728" | "20040015737" | "20040019803" | "20040021889" | "20040022359" | "20040024781" | "20040030778" | "20040044912" | "20040049372" | "20040054764" | "20040064722" | "20040064726" |	US-PGPUB; USPAT; USOCR	ADJ	ON	2015/12/21 15:27

		"20040071081" | "20040073800" | "20040078384" | "20040088564" | "20040088565" | "20040088581" | "20040098623" | "20040102922" | "20040102923" | "20040103310" | "20040103431" | "20040106955" | "20040117624").PN. OR ("20040117640" | "20040128529" | "20040128530" | "20040128543" | "20040148520" | "20040153171" | "20040158545" | "20040172550" | "20040181787" | "20040192204" | "20040193918" | "20040210653" | "20040215972" | "20040215978" | "20040221176" | "20040243603" | "20040250115" | "20040250128" | "20040259640" | "20040268322" | "20050005169" | "20050007743" | "20050010819" | "20050010821" | "20050015382" | "20050015667" | "20050022028" | "20050033988" | "20050049962" | "20050091542" | "20050114186" | "20050160286" | "20050177752" | "20050193430" | "20050195975" | "20050216957" | "20050222969" | "20050235360" | "20050240756" | "20060004614" | "20060030972" | "20060031938" | "20060041936" | "20060069912" | "20060070129" | "20060101517" | "20060130139" | "20060156407" | "20060168660" | "20060179325" | "20060230006" | "20060265708" | "20060265746" | "20060272011" | "20060293942" | "20070016659" | "20080005555" | "20080047016" | "20080052054" | "20080060075" | "20080127349" | "20080216173" | "20080222724" | "20080222731" | "20080263525" | "20080263668" | "20080271151" | "20090077666" | "20090320138" | "20090328213" | "20100083382" | "20100100961" | "20100218256" | "20100241478" | "20110131644" | "20110138036" | "20110162049" | "20110173342" | "20110173677" | "20110214179" | "20110214185" | "20110258315" | "20110258694" | "20120017278" | "20120030766" | "20120084867" | "20120102570" | "20120110671" | "20120144476" | "20120144493" | "20120144494" | "20120151594" | "20120151595").PN. OR ("20120151596" | "20120173931" | "20120185549" | "20120185550" | "20120185551" | "20120192262" | "20120192279" | "20120204265" | "20120210434" | "20120271890" | "20120317627" | "20130031265" | "20130031635" | "20130055394" | "20130167240" | "20130246620" | "20130275999" | "20130312101" | "20140215605" | "20140331326" | "5008814" | "5210854" | "5249705" |				

"5253782" | "5253932" | "5272754" |
"5276735" | "5335346" | "5361359" |
"5499297" | "5502766" | "5557346" |
"5557765" | "5596718" | "5612503" |
"5640454" | "5662291" | "5683638" |
"5696907" | "5745573" | "5765153" |
"5796836" | "5819275" | "5822435" |
"5831987" | "5864683" | "5867647" |
"5892903" | "5913024" | "5915087" |
"5918018" | "5950195" | "5956403" |
"5968133" | "5983350" | "5991406" |
"5991856" | "5991881" | "5999179" |
"6003084" | "6005942" | "6006035" |
"6028514" | "6029256" | "6035423" |
"6044466" | "6055527" | "6064811" |
"6072942" | "6074727" | "6084510" |
"6122657" | "6131163" | "6134601" |
"6144934" | "6151643" | "6173180" |
"6182226" | "6185689" | "6195352" |
"6205552" | "6208999" | "6209101" |
"6219707" | "6219786" | "6226372" |
"6230199" | "6230288" | "6240531" |
"6249585" | "6266774" | "6266811" |
"6267039" | "6269456" | "6272632" |
"6275942" | "6282546" | "6298422" |
"6298445" | "6301658" | "6301668" |
"6301699" | "6314190" | "6321293" |
"6321334" | "6321336" | "6324656" |
"6332195" | "6336186" | "6343362" |
"6345361" | "6351794" | "6353446" |
"6357010" | "6370578" | "6385458" |
"6393424" | "6402689").PN. OR
("6415321" | "6418554" | "6442686" |
"6453347" | "6453419" | "6457076" |
"6460126" | "6470384" | "6473800" |
"6477550" | "6477651" | "6493756" |
"6496875" | "6499107" | "6499109" |
"6510448" | "6513122" | "6523023" |
"6526513" | "6535227" | "6542943" |
"6546493" | "6550012" | "6553377" |
"6553378" | "6567808" | "6584504" |
"6584508" | "6587888" | "6601091" |
"6604139" | "6608817" | "6611869" |
"6611925" | "6615266" | "6622150" |
"6633835" | "6636972" | "6640307" |
"6654751" | "6654782" | "6658571" |
"6663000" | "6665269" | "6668054" |
"6668289" | "6671368" | "6671812" |
"6674738" | "6675042" | "6678887" |
"6684329" | "6687833" | "6693888" |
"6697337" | "6697870" | "6697950" |
"6701440" | "6701441" | "6704874" |
"6707794" | "6708292" | "6711127" |
"6714513" | "6718469" | "6721847" |
"6725377" | "6728219" | "6728885" |
"6732157" | "6735629" | "6735703" |
"6742124" | "6742128" | "6745192" |
"6745311" | "6748534" | "6751627" |
"6751718" | "6754488" | "6754705" |
"6754896" | "6757727" | "6757822" |
"6757830" | "6760845" | "6763403" |
"6763466" | "6766458" | "6768721" |
"6768991" | "6769016" | "6772332" |
"6772334" | "6772345" | "6775704" |

		"6775780" | "6779033" | "6782421" | "6782527" | "6785237" | "6785820" | "6785821" | "6789082" | "6789117" | "6789201" | "6789202" | "6792543" | "6799197" | "6801756" | "6801940" | "6802012" | "6810017" | "6814842" | "6816896" | "6816973" | "6823460" | "6826608" | "6826698" | "6834301" | "6836860" | "6839852" | "6842860" | "6842861" | "6843190").PN. OR ("6845449" | "6851058" | "6851061" | "6859793" | "6862581" | "6868069" | "6868413" | "6871279" | "6874018" | "6879812" | "6886099" | "6892227" | "6892241" | "6895387" | "6895513" | "6898712" | "6898715" | "6904521" | "6907396" | "6907531" | "6915426" | "6920493" | "6920558" | "6922776" | "6928555" | "6931540" | "6931546" | "6934857" | "6938161" | "6941358" | "6944775" | "6947986" | "6950933" | "6950947" | "6952779" | "6957348" | "6959418" | "6961783" | "6963978" | "6964014" | "6965928" | "6966059" | "6968461" | "6970697" | "6970823" | "6971023" | "6973577" | "6973578" | "6976068" | "6976168" | "6978454" | "6980992" | "6981280" | "6983325" | "6983326" | "6983380" | "6983486" | "6986160" | "6987963" | "6988209" | "6990591" | "6993660" | "7000247" | "7000250" | "7003561" | "7007302" | "7010696" | "7013330" | "7016939" | "7016948" | "7023861" | "7024432" | "7024694" | "7035544" | "7036147" | "7039702" | "7039721" | "7043024" | "7043634" | "7043756" | "7043758" | "7047297" | "7051077" | "7051097" | "7051365" | "7055036" | "7058975" | "7062555" | "7062783" | "7065790" | "7069316" | "7069330" | "7069581" | "7069594" | "7073198" | "7076650" | "7076801" | "7080000" | "7080141" | "7080408" | "7085931" | "7085934" | "7086050" | "7089259" | "7089302" | "7093002" | "7093121" | "7093292" | "7093293" | "7096368" | "7096500" | "7096501" | "7096503" | "7107366" | "7107574" | "7107617" | "7107618" | "7114183" | "7114185" | "7117533" | "7120252" | "7124181" | "7134140" | "7136487" | "7140042").PN. OR ("7146155" | "7146642" | "7149189" | "7150042" | "7152105" | "7152241" | "7154857" | "7159036" | "7159237" | "7162698" | "7171681" | "7171690" | "7178144" | "7178166" | "7181015" | "7181506" | "7181613" | "7181769" | "7185232" | "7185361" | "7188367" | "7203963" | "7209954" | "7210041" | "7210168" | "7213153" | "7213260" | "7216343" | "7225466" | "7228565" | "7228566" | "7231440" | "7231637" | "7231664" | "7231665" | "7234163" |				

		"7234165"	"7234167"	"7234168"						
		"7237008"	"7237122"	"7237222"						
		"7237258"	"7240102"	"7240193"						
		"7243148"	"7243373"	"7249187"						
		"7251685"	"7251830"	"7254811"						
		"7257630"	"7257773"	"7257842"						
		"7263561"	"7263718"	"7266843"						
		"7266844"	"7269649"	"7269851"						
		"7272724"	"7277957"	"7278163"						
		"7281267"	"7281268"	"7284267"						
		"7296080"	"7299361"	"7302584"						
		"7302706"	"7305005"	"7305709"						
		"7308702"	"7308706"	"7308712"						
		"7308715"	"7310817"	"7310818"						
		"7315801"	"7315894"	"7325252"						
		"7328234"	"7331061"	"7334222"						
		"7340774"	"7340775"	"7343626"						
		"7346781"	"7346929"	"7350203"						
		"7350234"	"7353539"	"7359962"						
		"7367054"	"7373659"	"7376842"						
		"7380270"	"7383556"	"7383581"						
		"7389539"	"7391770"	"7392043"						
		"7398516"	"7398517"	"7401359"						
		"7409593"	"7409714"	"7409720"						
		"7412721"	"7412722"	"7412723"						
		"7415726"	"7418730"	"7418733"						
		"7418734"	"7418737"	"7421266"						
		"7421587"	"7424706"	"7424744"						
		"7424746"	"7426551"	"7440403"						
		"7440471"	"7441274").PN. OR							
		("7451488"	"7458098"	"7461403"						
		"7464408"	"7472419"	"7472421"						
		"7480941"	"7483861"	"7493659"						
		"7496043"	"7496960"	"7509676"						
		"7509681"	"7516483"	"7519954"						
		"7519994"	"7522531"	"7533272"						
		"7536456"	"7536715"	"7540031"						
		"7543056"	"7543070"	"7543329"						
		"7543334"	"7549168"	"7552480"						
		"7555776"	"7562388"	"7574740"						
		"7587759"	"7590247"	"7590725"						
		"7590844"	"7590855"	"7590859"						
		"7594262"	"7594273"	"7603711"						
		"7613625"	"7620816"	"7624422"						
		"7624444"	"7624450"	"7627891"						
		"7634800"	"7640335"	"7640361"						
		"7640586"	"7644352"	"7647376"						
		"7664845"	"7665137"	"7668947"						
		"7669237"	"7673043"	"7673146"						
		"7673150"	"7673242"	"7673342"						
		"7673343"	"7674298"	"7681208"						
		"7693742"	"7693947"	"7694128"						
		"7694339"	"7698275"	"7711662"						
		"7712138"	"7716719"	"7716742"						
		"7721110"	"7739722"	"7757293"						
		"7757361"	"7761605"	"7761920"						
		"7770225"	"7779466"	"7779468"						
		"7783545"	"7788705"	"7788718"						
		"7793346"	"7793348"	"7801980"						
		"7810091"	"7818739"	"7822666"						
		"7823204"	"7827607"	"7827611"						
		"7836501"	"7840663"	"7841007"						
		"7845007"	"7861285"	"7861303"						
		"7865938"	"7865956"	"7870203"						

		"7882555" | "7895641" | "7900254" | "7903549" | "7904955" | "7913303" | "7917444" | "7917647" | "7917951" | "7921459" | "7926113" | "7941855" | "7954159" | "7958554" | "7975296" | "7984511" | "7991827" | "7991917" | "7996201" | "7996902" | "8010387" | "8019082" | "8020211").PN. OR ("8024076" | "8042149" | "8042178" | "8042181" | "8051479" | "8068441" | "8069480" | "8069481" | "8074256" | "8074282" | "8090816" | "8091117" | "8099760" | "8115769" | "8117273" | "8121874" | "8121892" | "8122498" | "8122499" | "8127359" | "8132250" | "8135823" | "8135830" | "8140642" | "8141157" | "8156483" | "8171551" | "8176544" | "8176553" | "8181173" | "8181222" | "8185930" | "8185943" | "8219620" | "8230497" | "8230502" | "8239941" | "8250654" | "8256002" | "8260906" | "8266320" | "8266703" | "8291505" | "8310955" | "8312535" | "8341693" | "8359650" | "8364772" | "8380791" | "8387146" | "8393001" | "8402540" | "8407683" | "8407798" | "8468256" | "8490197" | "8495740" | "8510839" | "8527977" | "8533703" | "8539063" | "8549611" | "8549635" | "8555344" | "8555374" | "8561167" | "8561175" | "8578480" | "8615582" | "8621060" | "8621073" | "8621077" | "8627443" | "8627466" | "8631124" | "8631495" | "8634309" | "8656502" | "8661126" | "8700767" | "8706576" | "8732835" | "8744938" | "8776230" | "8782260" | "8789193").PN. OR ("9100431").URPN.				
S3	908	(determin$6 or detect$4 or resolv$4 or find$4 or discover$4 or uncover$4 or identiy$4 or identification or check$4 or scan$4 or examin$6) with vulnerabilit$4 and (application or apply$4 or administer$5 or implenat$6 or deploy$4 or install$6 or distribu$4 or send$4 or transmi$6 or transfer$4 or forward$4) with (mitigat$4 or remediat$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 16:36
S4	1	S3 and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) near5 (signature or technique or method or type or category or class or group or kind or fingerprint or variety or classification) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 16:39
S7	491	(726/1,11-14,22-25.ccls. or 713/187-188.ccls.) and S3	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 16:44
S8	1	S7 and (identify$4 or identification or	US-	ADJ	ON	2015/12/21

		recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) near5 (signature or technique or method or type or category or class or group or kind or fingerprint or variety or classification) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	PGPUB; USPAT; EPO; JPO; DERWENT			16:44
S9	611	(H04L63/02$ or H04L63/14$ or G06F21/5$).cpc. and S3	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 16:48
S10	1	S9 and (identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) near5 (signature or technique or method or type or category or class or group or kind or fingerprint or variety or classification) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 16:48
S11	4	(identify$4 or identification or recogni$5 or determin$5 or discover$4 or choos$4 or select$4) with (mitigat$4 or remediat$4) near5 (signature or technique or method or type or category or class or group or kind or fingerprint or variety or classification) with (specific$4 or particular$4 or distinct$4 or differ$4 or explicit$4 or individual$4 or unique$4) near5 operating near5 system	US-PGPUB; USPAT; EPO; JPO; DERWENT	ADJ	ON	2015/12/21 17:03

EAST Search History (Interference)

<This search history is empty>

12/22/2015 11:58:09 AM
C:\Users\mherzog\Documents\EAST\Workspaces\App14816931.wsp

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/816,931	08/03/2015	2431	840	SP1P012A	21	3

CONFIRMATION NO. 1044

UPDATED FILING RECEIPT

127962
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

OC000000078288139

Date Mailed: 10/26/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. 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 submit a written request for a Filing Receipt Correction. 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**

Inventor(s)

Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

Applicant(s)

SecurityProfiling, LLC, Garland, TX;

Power of Attorney: The patent practitioners associated with Customer Number 127962

Domestic Priority data as claimed by applicant

This application is a CON of 14/499,230 09/28/2014 PAT 9100431
which is a CIP of 14/138,014 12/21/2013 PAT 9117069
which is a CON of 10/882,852 07/01/2004 ABN
which claims benefit of 60/484,085 07/01/2003

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 08/18/2015
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/816,931**
Projected Publication Date: 02/04/2016
Non-Publication Request: No
Early Publication Request: No
**** SMALL ENTITY ****

ForcePoint LLC
EX-1010-PT2
Page404

Title

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

ForcePoint LLC
EX-1010-PT2
Page405

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

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

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/816,931

APPLICATION AS FILED - PART I

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), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	* 1	x 40 =	40	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	770		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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 found in the appropriate box in column 1.

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 1044
Brett M. Oliphant	Examiner:
Application No.: 14/816,931	Art Unit: 2431
Filed: 08-03-2015	Atty. Docket No.: SP1P012A
For: COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Date: 10/19/2015

RESPONSE TO NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

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

Sir:

In response to the Notice to File Missing Parts of NonProvisional Application, mailed Aug 19, 2015, Applicant submits a properly executed inventor's declaration for John P. Blignaut along with payment of $70 for deficient fees.

Respectfully submitted,

/Brian Owens/

Brian Owens
Reg. No. 55,517
469-277-0934

SUPPLEMENTAL APPLICATION DATA SHEET

In re application of: Brett M. Oliphant Application No.: 14/816,931 Filed: 08-03-2015 For: : COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	Confirmation No.: 1044 Examiner: Art Unit: 2431 Atty. Docket No.: SP1P012A Date: 10/19/2015

Please correct the Application Data Sheet as follows:

DOMESTIC PRIORITY INFORMATION

Application Number::	Continuity Type::	Prior Application Number::	Filing Date::
	Continuation of	14/499,230	09-28-2014
~~14/499,237~~ 14/499,230	Continuation in part of	14/138,014	12-21-2013
14/138,014	Continuation of	10/882,852	07-01-2004
10/882,852	Claims benefit of provisional	60/484,085	07-01-2003

SIGNATURE:
A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature: /Brian Owens/ **Date: October 19, 2015**
Name: Brian Owens
Registration No.: 55,517

ForcePoint LLC
EX-1010-PT2
Page409

Electronic Patent Application Fee Transmittal

Application Number:	14816931
Filing Date:	03-Aug-2015
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Brian Dean Owens
Attorney Docket Number:	SP1P012A

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late Filing Fee for Oath or Declaration	2051	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**70**

Electronic Acknowledgement Receipt	
EFS ID:	23828631
Application Number:	14816931
International Application Number:	
Confirmation Number:	1044
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	127962
Filer:	Brian Dean Owens
Filer Authorized By:	
Attorney Docket Number:	SP1P012A
Receipt Date:	19-OCT-2015
Filing Date:	03-AUG-2015
Time Stamp:	19:22:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$70
RAM confirmation Number	6288
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Oath or Declaration filed	SP1P012_Declaration_Blignaut.pdf	67224 d426537329f64ba6e8812eeb494c46fb6451460	no	1
Warnings:					
Information:					
2	Miscellaneous Incoming Letter	SP1P012A_Missing_Parts_10_19_15.pdf	91877 0e08cff7668780317c0dcf1c9d23c876dc061747	no	1
Warnings:					
Information:					
3	Application Data Sheet	SP1P012A_supp_ADS_10-19-15.pdf	104279 853138837910 29fe23e77f9bfc24ca8df31a680c	no	1
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
4	Fee Worksheet (SB06)	fee-info.pdf	30618 8651f53048373 16e6743a3aa03f559420558fda5	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	293998		

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.

Attorney Docket No.: SP1P0012

COMBINED DECLARATION (37 C.F.R. 1.63) AND ASSIGNMENT FOR UTILITY APPLICATION USING AN APPLICATION DATA SHEET (37 C.F.R. 1.76)

Title of Invention: **COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION**

As the below named inventor, I hereby declare that:

This declaration is directed to the attached application, or (if following box is checked)
☐ United States application or PCT international application number _____, filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby state that I have reviewed and understand the contents of the above-identified application, including the claims.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, CFR § 1.56.

Whereas, I the undersigned inventor have invented certain new and useful improvements as set forth in the above-identified patent application and further identified by the Attorney Docket Number provided above in the header of this document.

For good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, I the undersigned inventor hereby:

1) Sell(s), assign(s) and transfer(s) to SecurityProfiling, LLC, a Texas limited liability company having a place of business at 1919 S Shiloh Rd. Garland, TX 75042, (hereinafter referred to as ("ASSIGNEE"), the entire right title and interest in any and all improvements and inventions disclosed in, application(s) based upon, and Patent(s) (including foreign patents) granted upon the information which is disclosed in the above referenced application.

2) Authorize and request the Commissioner of Patents to issue any and all Letters Patents resulting from said application or any division(s), continuation(s), substitutes(s) or reissue(s) thereof to the ASSIGNEE.

3) Agree to execute all papers and documents and, entirely at the ASSIGNEE's expense, perform any acts which are reasonably necessary in connection with the prosecution of said application, as well as any derivative and applications thereof, foreign applications based thereon, and/or the enforcement of patents resulting from such applications.

4) Agree that the terms, covenants and conditions of this assignment shall inure to the benefit of the Assignee, its successors, assigns and other legal representative, and shall be binding upon the inventor(s), as well as the inventor's heirs, legal representatives and assigns.

5) Warrant and represent that I have not entered, and will not enter into any assignment, contract, or understanding that conflicts with this assignment.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

Signed on the date indicated beside my signature.

Legal Name of Inventor: John P. Blignaut

Signature: _____ Date: 9.24.14

ForcePoint LLC
EX-1010-PT2
Page415

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
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A

CONFIRMATION NO. 1044

127962
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

FORMALITIES LETTER

OC000000076940187

Date Mailed: 08/19/2015

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing.

Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items 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).

- Surcharge as set forth in 37 CFR 1.16(f) must be submitted.
  The surcharge is due for any one of:
  - late submission of the basic filing fee, search fee, or examination fee,
  - late submission of inventor's oath or declaration,
  - filing an application that does not contain at least one claim on filing, or
  - submission of an application filed by reference to a previously filed application.

SUMMARY OF FEES DUE:

The fee(s) required within **TWO MONTHS** from the date of this Notice to avoid abandonment is/are itemized below. Small entity discount is in effect. If applicant is qualified for micro entity status, an acceptable Certification of Micro Entity Status must be submitted to establish micro entity status. (See 37 CFR 1.29 and forms PTO/SB/15A and 15B.)

- $ **70** surcharge.
- $(**0**) previous unapplied payment amount.
- $ **70** TOTAL FEE BALANCE DUE.

Items Required To Avoid Processing Delays:

Applicant is notified that the above-identified application contains the deficiencies noted below. No period for reply is set forth in this notice for correction of these deficiencies. However, if a deficiency relates to the inventor's oath or declaration, the applicant must file an oath or declaration in compliance with 37 CFR 1.63, or a substitute statement in compliance with 37 CFR 1.64, executed by or with respect to each actual inventor no later than the expiration of the time period set in the "Notice of Allowability" to avoid abandonment. See 37 CFR 1.53(f).

- A properly executed inventor's oath or declaration has not been received for the following inventor(s):

ForcePoint LLC
EX-1010-PT2
Page416

John P. Blignaut

Replies must be received in the USPTO within the set time period or must include a proper Certificate of Mailing or Transmission under 37 CFR 1.8 with a mailing or transmission date within the set time period. For more information and a suggested format, see Form PTO/SB/92 and MPEP 512.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web, including a copy of this Notice and selecting the document description "Applicant response to Pre-Exam Formalities Notice". https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

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

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

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**.

/atesfaye/

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	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
14/816,931	08/03/2015	2431	770	SP1P012A	21	3

CONFIRMATION NO. 1044

127962
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025

FILING RECEIPT

OC000000078940186

Date Mailed: 08/19/2015

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. 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 submit a written request for a Filing Receipt Correction. 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**

Inventor(s)

Brett M. Oliphant, Plano, TX;
John P. Blignaut, West Lafayette, IN;

Applicant(s)

SecurityProfiling, LLC, Garland, TX;

Power of Attorney: The patent practitioners associated with Customer Number 127962

Domestic Priority data as claimed by applicant

This application is a CON of 14/499,230 09/28/2014 PAT 9100431

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.) - None.
Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

If Required, Foreign Filing License Granted: 08/18/2015

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 14/816,931**

Projected Publication Date: 03/31/2016

Non-Publication Request: No

Early Publication Request: No
**** SMALL ENTITY ****

ForcePoint LLC
EX-1010-PT2
Page418

Title

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

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

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

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

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

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

ForcePoint LLC
EX-1010-PT2
Page419

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

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

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

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

NOT GRANTED

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

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit http://www.SelectUSA.gov or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 14/816,931

APPLICATION AS FILED - PART I

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), (b), or (c))	N/A	N/A	N/A	70		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	300		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	360		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	21 minus 20 =	* 1	x 40 =	40	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 210 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	770		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							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 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 NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
14/816,931	08/03/2015	Brett M. Oliphant	SP1P012A

CONFIRMATION NO. 1044

IMPROPER CFR REQUEST

127962
Brian Owens, Esq.
3712 Kimble Dr
Plano, TX 75025



Date Mailed: 08/19/2015

RESPONSE TO REQUEST FOR CORRECTED FILING RECEIPT

Continuity, Priority Claims, Petitions, and Non-Publication Requests

In response to your request for a corrected Filing Receipt, the Office is unable to comply with your request because:

- One or more of the benefit claims under 35 U.S.C. § 120 cannot be included on the Filing Receipt since applicant did not specify whether the application is a continuation, divisional or continuation-in-part of the prior application. Applicant must submit a new application data sheet (ADS) that sets forth the relationship, and the ADS must be accompanied by a petition under 37 CFR 1.78 if filed after the time period set forth in 37 CFR 1.78.

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**.

/bcao/

ForcePoint LLC
EX-1010-PT2
Page422

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	
Filing Date	08-03-2015
First Named Inventor	Brett M. Oliphant
Title	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
Art Unit	
Examiner Name	
Attorney Docket Number	SP1P012A

SIGNATURE of Applicant or Patent Practitioner

Signature	/Brian Owens/	Date (Optional)	
Name	Brian Owens	Registration Number	55,517
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☑ *Total of 2 forms are submitted.

This collection of information is required by 37 CFR 1.131, 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

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
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

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/82A.)

☑ I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above: 127962

OR

☐ I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above 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 Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

SecurityProfiling, LLC

☐ Inventor or Joint Inventor (title not required below)

☐ Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

☑ Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

☐ Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	/John Blignaut/	Date (Optional)	
Name	John Blignaut		
Title	Member - SecurityProfiling, LLC		

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ Total of forms are submitted.

This collection of information is required by 37 CFR 1.131, 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

COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a continuation of U.S. App. No.: 14/499,230 filed September 28, 2014 which, in turn, is a continuation-in-part of U.S. App. No.: 14/138,014 filed December 21, 2013, now U.S. Pat. No.: 9,100,431, which, in turn, is a continuation of U.S. App. No.: 10/882,852 filed July 1, 2004 which, in turn, claims priority to U.S. App. No.: 60/484,085 filed July 1, 2003, which are all incorporated herein by reference in their entirety for all purposes.

FIELD OF THE INVENTION

[0002] The present invention relates to computer systems, and more particularly to management of security of computing and network devices that are connected to other such devices.

SUMMARY

[0003] A system, method, and computer program product are provided for a database associating a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities. Each of the device vulnerabilities is associated with at least one remediation technique. Each remediation technique associated with a particular device vulnerability remediates that particular vulnerability. Further, each remediation technique has a remediation type are selected from the type group consisting of patch, policy setting, and configuration option. Still yet, a first one of the device vulnerabilities is associated with at least two alternative remediation techniques.

ForcePoint LLC
EX-1010-PT2
Page425

BRIEF DESCRIPTION OF THE DRAWINGS

[0004] FIG. 1 is a block diagram of a networked system of computers in one embodiment of the present invention.

[0005] FIG. 2 is a block diagram showing components of several computing devices in the system of FIG. 1.

[0006] FIGS. 3 and 4 trace signals that travel through the system of FIGS. 1 and 2 and the present invention is applied to them.

[0007] FIG. 5A is a flow chart of a filtering proxy method according to one embodiment of the present invention.

[0008] FIG. 5B and 6 illustrate a platform, in accordance with possible embodiments.

[0009] FIG. 7 illustrates an intelligent IDS, in accordance with one embodiment.

[0010] FIG. 8 illustrates an update system, in accordance with one embodiment.

[0011] FIG. 9 shows a configured network, in accordance with one embodiment.

[0012] FIG. 10 shows policy compliance and enforcement, in accordance with one embodiment.

[0013] FIG. 11 illustrates an intelligent IPS, in accordance with one embodiment.

[0014] FIG. 12 illustrates an SDK function call flow, in accordance with one embodiment.

DETAILED DESCRIPTION

GLOSSARY

[0015] data warehouse = a component that contains vulnerabilities and updates for devices that operate on at least one network

ForcePoint LLC
EX-1010-PT2
Page426

[0016] NOC server = network operations center server that periodically synchronize latest vulnerability and update data with other servers.

[0017] SDK = software development kit that allows programmers to develop security applications that access data collected in a database

[0018] CM application = change management application that controls documentation and logging of change.

[0019] For the purpose of promoting an understanding of the principles of the present invention, reference will now be made to the embodiment illustrated in the drawings and specific language will be used to describe the same. It will, nevertheless, be understood that no limitation of the scope of the invention is thereby intended; any alterations and further modifications of the described or illustrated embodiments, and any further applications of the principles of the invention as illustrated therein are contemplated as would normally occur to one skilled in the art to which the invention relates.

[0020] Generally, the present invention in one embodiment operates in the context of a network as shown in FIG. 1. System 100 includes a vulnerability and remediation database 110 connected by Internet 120 to subnet 130. In this exemplary embodiment, firewall 131 serves as the gateway between Internet 120 and the rest of subnet 130. Router 133 directs connections between computers 137 and each other and other devices on Internet 120. Server 135 collects certain information and provides certain data services that will be discussed in further detail herein.

[0021] In particular, security server 135 includes processor 142, and memory 144 encoded with programming instructions executable by processor 142 to perform several important security-related functions. For example, security server 135 collects data from devices 131, 133, 137, and 139, including the software installed on those devices, their configuration and policy settings, and patches that have been installed. Security server 135 also obtains from vulnerability and remediation database 110 a regularly updated list of security vulnerabilities in software for a wide variety of operating systems, and even in the operating systems themselves. Security server 135 also downloads a regularly updated list of remediation techniques that can be applied to

ForcePoint LLC
EX-1010-PT2
Page427

protect a device from damage due to those vulnerabilities. In one embodiment, each vulnerability in remediation database 110 is identified by a vulnerability identifier, and the vulnerability identifier can be used to retrieve remediation information from database 110 (and from database 146, discussed below in relation to FIG. 2).

[0022] In one embodiment, computers 137 and 139 each comprise a processor 152, 162, memory 154, 164, and storage 156, 166. Computer 137 executes a client-side program (stored in storage 156, loaded into memory 154, and executed by processor 152) that maintains an up-to-date collection of information regarding the operating system, service pack (if applicable), software, and patches installed on computer 137, and the policies and configuration data (including configuration files, and elements that may be contained in files, such as *.ini and *.conf files and registry information, for example), and communicates that information on a substantially real-time basis to security server 135. In an alternative embodiment, the collection of information is not retained on computer 137, but is only communicated once to security server 135, then is updated in real time as changes to that collection occur.

[0023] Computer 139 stores, loads, and executes a similar software program that communicates configuration information pertaining to computer 139 to security server 135, also substantially in real time. Changes to the configuration registry in computer 139 are monitored, and selected changes are communicated to security server 135 so that relevant information is always available. Security server 135 may connect directly to and request software installation status and configuration information from firewall 131 and router 133, for embodiments wherein firewall 131 and router 133 do not have a software program executing on them to communicate this information directly.

[0024] This collection of information is made available at security server 135, and combined with the vulnerability and remediation data from source 110. The advanced functionality of system 100 is thereby enabled as discussed further herein.

[0025] Turning to FIG. 2, one sees additional details and components of the devices in subnet 130. Computers 137 and 139 are traditional client or server machines, each having a processor 152, 162, memory 154, 164, and storage 156, 166. Firewall 131 and router 133 also have processors 172, 182 and storage 174, 184, respectively, as is known in the art. In this embodiment, devices 137 and 139 each execute a client-side program that continuously monitors

ForcePoint LLC
EX-1010-PT2
Page428

the software installation and configuration status for that device. Changes to that status are communicated in substantially real time to security server 135, which continuously maintains the information in database 146. Security server 135 connects directly to firewall 131 and router 133 to obtain software installation and configuration status for those devices in the absence of a client-side program running thereon.

[0026] Processors 142, 152, 162 may each be comprised of one or more components configured as a single unit. Alternatively, when of a multi-component form, processor 142, 152, 162 may each have one or more components located remotely relative to the others. One or more components of processor 142, 152, 162 may be of the electronic variety defining digital circuitry, analog circuitry, or both. In one embodiment, processor 142, 152, 162 are of a conventional, integrated circuit microprocessor arrangement, such as one or more PENTIUM 4 or XEON processors from INTEL Corporation of 2200 Mission College Boulevard, Santa Clara, Calif., 95052, USA, or ATHLON XP processors from Advanced Micro Devices, One AMD Place, Sunnyvale, Calif., 94088, USA.

[0027] Memories 144, 154, 164 may include one or more types of solid-state electronic memory, magnetic memory, or optical memory, just to name a few. By way of non-limiting example, memory 40b may include solid-state electronic Random Access Memory (RAM), Sequentially Accessible Memory (SAM) (such as the First-In, First-Out (FIFO) variety or the Last-In First-Out (LIFO) variety), Programmable Read Only Memory (PROM), Electrically Programmable Read Only Memory (EPROM), or Electrically Erasable Programmable Read Only Memory (EEPROM); an optical disc memory (such as a DVD or CD ROM); a magnetically encoded hard drive, floppy disk, tape, or cartridge media; or a combination of any of these memory types. Also, memories 144, 154, 164 may be volatile, nonvolatile, or a hybrid combination of volatile and nonvolatile varieties.

[0028] In this exemplary embodiment, storage 146, 156, 166 comprises one or more of the memory types just given for memories 144, 154, 164, preferably selected from the non-volatile types.

[0029] This collection of information is used by system 100 in a wide variety of ways. With reference to FIG. 3, assume for example that a connection request 211 arrives at firewall 131 requesting that data be transferred to computer 137. The payload of request 211 is, in this

example, a probe request for a worm that takes advantage of a particular security vulnerability in a certain computer operating system. Based on characteristics of the connection request 211, firewall 131 sends a query 213 to security server 135. Query 213 includes information that security server 135 uses to determine (1) the intended destination of connection request 211, and (2) some characterization of the payload of connection request 211, such as a vulnerability identifier. Security server 135 uses this information to determine whether connection request 211 is attempting to take advantage of a particular known vulnerability of destination machine 137, and uses information from database 146 (see FIG. 2) to determine whether the destination computer 137 has the vulnerable software installed, and whether the vulnerability has been patched on computer 137, or whether computer 137 has been configured so as to be invulnerable to a particular attack.

[0030] Security server 135 sends result signal 217 back to firewall 131 with an indication of whether the connection request should be granted or rejected. If it is to be granted, firewall 131 passes the request to router 133 as request 219, and router 133 relays the request as request 221 to computer 137, as is understood in the art. If, on the other hand, signal 217 indicates that connection request 211 is to be rejected, firewall 133 drops or rejects the connection request 211 as is understood in the art.

[0031] Analogous operation can protect computers within subnet 130 from compromised devices within subnet 130 as well. For example, FIG. 4 illustrates subnet 130 with computer 137 compromised. Under the control of a virus or worm, for example, computer 137 sends connection attempt 231 to router 133 in an attempt to probe or take advantage of a potential vulnerability in computer 139. On receiving connection request 231, router 133 sends relevant information about request 231 in a query 233 to security server 135. Similarly to the operation discussed above in relation to FIG. 3, security server 135 determines whether connection request 231 poses any threat, and in particular any threat to software on computer 139. If so, security server 135 determines whether the vulnerability has been patched, and if not, it determines whether computer 139 has been otherwise configured to avoid damage due to that vulnerability. Security server 135 replies with signal 235 to query 233 with that answer. Router 133 uses response 235 to determine whether to allow the connection attempt.

ForcePoint LLC
EX-1010-PT2
Page430

[0032] In some embodiments, upon a determination by security server 135 that a connection attempt or other attack has occurred against a computer that is vulnerable (based on its current software, patch, policy, and configuration status), security server 135 selects one or more remediation techniques from database 146 that remediate the particular vulnerability. Based on a prioritization previously selected by an administrator or the system designer, the remediation technique(s) are applied (1) to the machine that was attacked, (2) to all devices subject to the same vulnerability (based on their real-time software, patch, policy, and configuration status), or (3) to all devices to which the selected remediation can be applied.

[0033] In various embodiments, remediation techniques include the closing of open ports on the device; installation of a patch that is known to correct the vulnerability; changing the device's configuration; stopping, disabling, or removing services; setting or modifying policies; and the like. Furthermore, in various embodiments, events and actions are logged (preferably in a non-volatile medium) for later analysis and review by system administrators. In these embodiments, the log also stores information describing whether the target device was vulnerable to the attack.

[0034] A real-time status database according to the present invention has many other applications as well. In some embodiments, the database 146 is made available to an administrative console running on security server 135 or other administrative terminal. When a vulnerability is newly discovered in software that exists in subnet 130, administrators can immediately see whether any devices in subnet 130 are vulnerable to it, and if so, which ones. If a means of remediation of the vulnerability is known, the remediation can be selectively applied to only those devices subject to the vulnerability.

[0035] In some embodiments, the database 146 is integrated into another device, such as firewall 131 or router 133, or an individual device on the network. While some of these embodiments might avoid some failures due to network instability, they substantially increase the complexity of the device itself. For this reason, as well as the complexity of maintaining security database functions when integrated with other functions, the network-attached device embodiment described above in relation to FIGS. 1-4 is one possible embodiment.

[0036] In one embodiment, a software development kit (SDK) allows programmers to develop security applications that access the data collected in database 146. The applications developed with the SDK access information using a defined application programming interface

ForcePoint LLC
EX-1010-PT2
Page431

(API) to retrieve vulnerability, remediation, and device status information available to the system. The applications then make security-related determinations and are enabled to take certain actions based on the available data.

[0037] In these exemplary systems, "configuration information" for each device may take the form of initialization files (often named *.ini or *.conf), configuration registry (such as, the Windows Registry on Microsoft WINDOWS operating systems), or configuration data held in volatile or non-volatile memory. Such configuration information often determines what and how data is accepted from other devices, sent to other devices, processed, stored, or otherwise handled, and in many cases determines what routines and sub-routines are executed in a particular application or operating system.

[0038] In one embodiment, security information management system is provided, wherein a database of potential vulnerabilities is maintained, along with data describing remediation techniques (patches, policy settings, and configuration options) available to protect against them. At least one vulnerability is associated in the database with multiple available remediation techniques. In one embodiment, the system presents a user with the list of remediation techniques available to protect against a known vulnerability, accepts the user's selection from the list, and executes the selected technique. In other embodiments, the system uses a predetermined prioritization schedule to automatically select among the available remediation techniques, then automatically executes the selected technique.

[0039] One embodiment of the present invention is a database of information about a plurality of devices, updated in real-time and used by an application to make a security-related decision. The database stores data indicating the installed operating system(s), installed software, patches that have been applied, system policies that are in place, and configuration information for each device. The database answers queries by one or more devices or applications attached by a network to facilitate security-related decision making. In one form of this embodiment, a firewall or router handles a connection request or maintenance of a connection based on the configuration information stored in the database that relates to one or both of the devices involved in the transmission.

[0040] In one embodiment, database 146 includes vulnerability and remediation information such that, for at least one vulnerability, multiple methods of remediating the vulnerability are

ForcePoint LLC
EX-1010-PT2
Page432

specified. When the system has occasion to implement or offer remediation of a vulnerability, all known alternatives are presented that are relevant to the device or machine's particular configuration or setup. For example, when a vulnerability of a device is presented to an administrator, the administrator is given a choice among the plurality of remediation options to remediate the vulnerability. In some embodiments, the administrator can select a preferred type of remediation that will be applied if available and a fallback type. For example, an administrator may select application of a policy setting over installation of a software patch, so that the risk of disruption of critical business systems is minimized.

[0041] In other embodiments, an administrator or other user is presented with a set of user interface elements that identify multiple options for remediating and identifying the vulnerability. The administrator or user selects the method to be used, and that remediation is applied to the vulnerable device(s).

[0042] FIG. 5A is a flow chart of a filtering proxy method according to one embodiment of the present invention.

[0043] In use, a database maintains security status information on each device in a network, based on whether the device's operating system, software, and patches are installed and configured to meet a baseline level of security. A network gateway proxy blocks connection attempts from devices for which the database indicates a substandard security status, but allows connections from other devices to pass normally. The database is preferably updated on a substantially real-time basis by client-side software run by each device in the network.

[0044] Another form of the present embodiment includes a connection proxy that filters connections originating within the network. In particular, one embodiment employs a proxy that denies connection attempts originating with devices in the network when the originating device has a status, reflected in the database, that fails to meet predetermined security characteristics in terms of installed operating system and software, patch levels, and system policy and configuration registry information.

[0045] In this embodiment, router 133 serves as a connection proxy for devices and subnet 130, as will be understood by those skilled in the art. In addition to basic proxy functionality, however, router 133 accesses database 146 on security server 135 via the SDK at each connection attempt. If, for example, device 137 attempts to connect to any device where the

ForcePoint LLC
EX-1010-PT2
Page433

connection must pass through the proxy server (router 133 in this example), such as a device on Internet 120, router 133 checks the security status of device 137 in database 146, using the real-time status therein to determine whether device 137 complies with one or more predetermined security policies. If it does, router 133 allows the connection to be made. If it does not, router 133 prevents the connection, preferably redirecting the connection to a diagnostic page that explains why the connection is not being made.

[0046] This system is illustrated by method 200 in FIG. 5A. Method 200 begins with start point 201. The proxy (router 133 in the above example) receives a connection request at block 203, then retrieves the security status of the source device at block 205. This preferably uses the real-time updated status information from database 146 (see FIG. 2) at decision block 207. If the security status indicates that the source device complies with the predetermined security policy, the proxy allows the connection at block 209. If not, the proxy refuses the connection at block 211 and redirects the connection to an explanation message (such as a locally generated web page or other message source) at block 213. In either case, method 200 ends at end point 219.

[0047] In possible embodiments, the determination and decision at block 207 apply a comprehensive minimum policy set that protects other devices in subnet 130 (see FIG. 1) from viruses, trojans, worms, and other malware that might be inadvertently and/or carelessly acquired due to the requested connection.

[0048] In another embodiment, a security information management system is provided, wherein client-side devices preferably collect and monitor information describing the operating system, software, and patches installed on the device(s), as well as configuration thereof. A database of this information is maintained, along with data describing vulnerabilities of available software and associated remediation techniques available for it. The system exposes an API to support security-related decisions by other applications. For example, an intrusion detection system (IDS) accesses the database to determine whether an actual threat exists and should be (or has been) blocked.

[0049] In another form of this embodiment, client software runs on each monitored device and reports configuration information to the database, so that the database has substantially real-time-current information.

ForcePoint LLC
EX-1010-PT2
Page434

[0050] The present embodiment of the present invention advantageously acquires the real-time status information from each client using client-side software. In this manner, a resource burden of monitoring is spread among the devices being monitored, and uses far fewer network resources in the process.

[0051] In these exemplary systems, "configuration information" for each device may take the form of initialization files (often named *.ini or *.conf), configuration registry (such as the Windows Registry on Microsoft Windows operating systems), or configuration data held in volatile or non-volatile memory. Such configuration information often determines what and how data is accepted from other devices, sent to other devices, processed, stored, or otherwise handled, and in many cases determines what routines and sub-routines are executed in a particular application or operating system.

[0052] In one embodiment, a system maintains a database of vulnerabilities and associated remediation techniques. The remediation techniques include software patches, policy settings or changes, and registry settings or changes. This multi-faceted provides novel flexibility in management of security issues, and convenience for security administrators in both determining available options and selecting remediation steps for vulnerable systems.

[0053] In another embodiment of the present invention, patches, policy changes, software updates, and configuration changes are rolled out to devices on a network using a staged roll-out technique. In this technique, the change is applied to a selected device or set of devices identified by an administrator. After a predetermined amount of time passes, unless the administrator has canceled the roll-out, the change is applied to an additional group of devices on the network. Third- and fourth-tier groups may also be identified by the administrator, where implementation of the remediation or upgrade is automatically effected in subsequent stages a predetermined amount of time after the preceding stage roll-out. Thus, if no failures are noted following a more limited roll-out (on a first set of devices), then the remediation or upgrade is automatically applied to other devices. If, on the other hand, an error or failure is observed, the subsequent roll-out can be canceled so that further failures and problems are avoided.

[0054] FIG. 5B and 6 illustrate a platform, in accordance with possible embodiments.

[0055] In one possible embodiment, provided is a platform and underlying back end that includes a logic engine and vulnerability data warehouse. It may easily integrate with and enable

ForcePoint LLC
EX-1010-PT2
Page435

network security products such as IDS, scanners, or firewalls to intelligently reference and share the same vulnerability data set, and independently provide complete vulnerability remediation (patching) functionalities such as that provided by the patch management and vulnerability remediation application. Thereby, the technology may improve system accuracy and efficiencies, minimize false positives and false negatives, and provide policy compliance and enforcement capabilities.

[0056] The latest network compromises are combining qualities of viruses, worms, and denial of service attacks into new blended attacks. Additionally, blended attacks may now utilize metamorphic or polymorphic abilities to change their signatures to avoid detection. To mitigate these new risks, organizations are now deploying a multi-tiered network defense strategy comprised of a variety of network security components layered at the perimeter and to internal network machines and devices. The security components are managed separately, and possibly their data is ported into a Security Information Management System (SIMS) correlation engine.

[0057] However, network security components and correlation engines rely on signatures or anomalies, producing an ever-increasing quantity of data, including false positive, benign, and erroneous events. They also lack the intelligence to identify, reference, or remediate the vulnerabilities targeted by the attack. Furthermore, the time and cost to acquire, manage, and maintain these numerous network security components is overwhelming the end user. Therefore, more sophisticated technology is provided to resolve these performance and management issues.

[0058] In one embodiment, technology may be provided that addresses these requirements by making each security component smarter and provides managers with remote remediation options. Thereby, improving system performance and streamlining management processes.

[0059] In one embodiment, an intelligent integration platform and SDK are provided to meet the above requirements.

[0060] In one embodiment, security products are enhanced and system intelligence may be provided. The same vulnerability data warehouse information is shared with the products so that more intelligent actions may then be taken to mitigate complex threats.

[0061] One embodiment cross-references the threat's identifier with the target's configuration. The threat's CVE ID, or other identifier, and the destination IP address are fed

into the logic engine where it cross-references the threat with the machine's existing OS, application, and patch configuration profile. An answer is returned accurately indicating if the machine is vulnerable.

[0062] In one embodiment, network vulnerabilities are identified. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

[0063] One embodiment proactively remediates the vulnerability. Once a vulnerability is identified, a remediation function may be provided that may remotely and automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

[0064] Examples of Anti-Vulnerability applications that may be integrated into network security products for enterprise and small office home office (SOHO) networks when integrated with one embodiment, via the SDK, will be described.

[0065] In one embodiment, update or patch deployment are provided, which remotely remediate network vulnerabilities and provide policy compliance and enforcement capabilities. And, for the consumer market, it may additionally support non-security related updates such as application version, performance, and bug-fix upgrades.

[0066] In one embodiment, an IDS may be provided that accurately determines if the targeted machine is actually vulnerable to an attack; virtually eliminates false positives and false negatives; and adds vulnerability remediation and policy compliance and enforcement functionalities.

[0067] In one embodiment, a scanner may be provided that virtually eliminates false positive and false negatives, and adds vulnerability remediation and policy compliance and enforcement functionalities.

[0068] In one embodiment, a firewall may be provided that virtually eliminates false positive and false negatives, preventing the security system from denying valid traffic to the organization – self-inflicted denial of service attacks - and adds vulnerability remediation, and policy compliance and enforcement functionalities.

[0069] In one embodiment, vulnerability management may be provided, as set forth above.

ForcePoint LLC
EX-1010-PT2
Page437

[0070] In one embodiment, multiple products are provided including an IDS, scanner, and firewall. Each may communicate with the same back-end data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats.

[0071] In one embodiment, change management may be provided, which may automatically create a change request in the system, specifying what update/patch is applicable to what system or groups of systems by vulnerability. After approval of the request, they may automatically deploy and install the update/patch. Finally, they may also verify correct operation after installation and automatically provide all necessary documentation and logging required.

[0072] Lastly, the platform may also provide product upgrades and signature updates to each of these various security products.

[0073] The platform is comprised of the following software components: SDK, client agent, logic engine, and data warehouse stored on a dedicated on-site server. Network operations center (NOC) Servers periodically synchronize the customers' servers with the latest vulnerability and update data. See FIG. 5B.

[0074] The same client agent and on-site server support all security applications that are integrated onto the platform, thereby providing the added anti-vulnerability functionalities presented in the previous section.

[0075] There are two system requirements: TCP/IP connectivity, and supported network machines and devices. In one embodiment, platforms supported are set forth below in Table 1.

Table 1

All Windows Operating Systems and their applications
All UNIX variants
Cisco routers and firewalls
Toshiba network devices
Netgear network devices
Linksys network devices, including wireless access points

ForcePoint LLC
EX-1010-PT2
Page438

[0076] Platform support is scalable to any network size or architecture; consumer, small office home office (SOHO), enterprise, and distributed networks.

[0077] In one embodiment, technology may be provided that includes a backend platform that includes a logic engine and vulnerability data warehouse. It may easily integrate with and enable network security products such as IDS, scanners, or firewalls to intelligently reference and share the same vulnerability data set, and independently provide complete vulnerability remediation (patching) functionalities such as that provided by the patch management and vulnerability remediation application, update application and the intelligent IDS. Thereby, the technology may improve system accuracy and efficiencies, minimize false positives and false negatives, and provide policy compliance and enforcement capabilities.

[0078] As shown in FIG. 5B, the technology may meet market requirements, presented in the next section.

[0079] For example, networks are probed at an ever-increasing frequency for vulnerabilities, which may be exploited with compromise attacks. To protect the network, administrators have traditionally set up perimeter defense strategies.

[0080] These strategies generally call for network managers to lock down core servers, and monitor/scan/filter all incoming and outgoing traffic at the network perimeter with several network security products such as antivirus and firewalls to identify and attempt to neutralize hackers and malicious code. In the past, these strategies worked well, however new threats are becoming more complex.

[0081] The latest malicious code may combine qualities of viruses, worms, and direct compromise attacks into new blended attacks. Virus payloads are becoming more complex and by using metamorphic or polymorphic abilities, viruses are able to change their signatures to avoid the fingerprint-type filtering that most applications employ.

[0082] To mitigate these new risks, organizations deploy a multi-tiered network defense strategy comprised of a variety of additional network security products layered at the perimeter and to internal network machines and devices. Such network security products include antivirus, firewall, scanners, and network and host based intrusion detection systems.

ForcePoint LLC
EX-1010-PT2
Page439

[0083] Each of these systems is based on specific signatures, rules, or anomalies of each attack and their variants, and do not identify and remediate the specific network vulnerabilities the attack is targeting. So each attack, and its variants, must be identified and analyzed, a signature prepared, then finally deployed to each point product on each customer's network. This process is uncoordinated among multiple disparate systems, and creates an ever-increasing number of signatures producing more and more attack alerts requiring immediate attention – many of which are erroneous. The security components are managed separately, and possibly their data is ported into a security information management system (SIMS) correlation engine.

[0084] Additionally, to proactively remediate the vulnerabilities the malicious code is targeting, administrators quickly and diligently update or "patch" each network machine and device, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives may require higher standards of network security and integrity to protect consumer privacy, and they are documented with change tracking and audit trail reports.

[0085] Therefore, it is increasingly difficult and costly to effectively mitigate new threats and manage numerous systems — particularly in an environment of rising security standards and policy compliance requirements.

[0086] Thus, the multi-tiered network defense strategy is falling short primarily for four reasons. First, there is an inability of multi-tiered network security products to communicate and share information necessary to mitigate blended threats, and minimize false positives and false negatives. The vulnerabilities targeted by malicious code are not accurately identified nor proactively remediated. The associated excessive aggregate cost of ownership of multiple systems. The excessive administrative burden and cost of managing and maintaining multiple systems.

[0087] Hence, there is a need to integrate systems, share information intelligently to better defend against blended threats, reduce management and cost requirements, and automate vulnerability identification and remediation functionalities, as presented in the high-level requirements.

ForcePoint LLC
EX-1010-PT2
Page440

[0088] In one embodiment, technology is provided to meet the following market requirements: integrate network security products to share information; provide system intelligence; and remediate network vulnerabilities.

[0089] In one embodiment, technology may integrate with and enable network security products to intelligently reference and share information from the same vulnerability data set, provide vulnerability identification and remediation functionalities, and efficiently meet policy compliance and enforcement requirements.

[0090] In one embodiment, the platform is a complimentary network security technology. When integrated into the defense strategy, it adds intelligence that more accurately and efficiently mitigates blended threats and offloads the time-consuming functions that burden network administrators.

[0091] In one embodiment, the platform enables network security products to share information via its proprietary logic engine to automatically cross-reference the threat identifier with the targeted machine's configuration to determine if it is actually vulnerable to that threat. Previously separate and uncoordinated processes are now more intelligent and automated, resulting in improved system accuracy and efficiency. Therefore the need to layer more and more point products and add a SIMS is reduced, in-turn decreasing the amount of data – particularly erroneous data – to manage. Subsequently, the costs to acquire, operate, and manage the additional multiple point products, and the need to implement a SIMS, are also reduced.

[0092] In one embodiment, the platform may also remotely and proactively remediate vulnerabilities by first determining which updates are needed and compatible with each machine or device, taking into account the OS, applications, or firmware installed. Then, the updates may be deployed, installed, and validated. Thereby, policy compliance is effectively and efficiently enforced, and documented.

[0093] In one embodiment, the present technology fulfills market requirements noted in the previous section. For example, it may integrate network security products and provides system intelligence. The same vulnerability data warehouse information is shared with all products so that more intelligent actions may then be taken to mitigate complex threats.

ForcePoint LLC
EX-1010-PT2
Page441

[0094] Still yet, it may cross-reference the threat's identifier with the target's configuration. The threat's CVE ID, or other identifier, and the destination IP address are fed into the logic engine where it cross-references the threat with the machine's existing OS, application, and patch configuration profile. An answer is returned accurately indicating if the machine is vulnerable. Thereby, minimizes erroneous, benign, and false positive data produced by each security product.

[0095] One embodiment identifies network vulnerabilities. The platform may independently identify which network machines and devices have vulnerabilities by querying a client agent, or a device's OS or firmware directly.

[0096] One embodiment proactively remediates the vulnerability. Once a vulnerability is identified, a remediation function may be provided that may remotely and automatically deploy the appropriate update to each machine or device, install it, and document it with change tracking and audit trail reports.

[0097] Various possible benefits include blended attacks being more effectively mitigated and the overwhelming management and maintenance burden on administrators to purchase, operate, and maintain multiple network security products being reduced, while increasing productivity, reducing costs, and more effectively and efficiently meeting policy compliance and enforcement requirements.

[0098] Table 2 illustrates a plurality of end user details.

Table 2

- Supplements existing technology to better defend against blended attacks
- Intelligently accesses the vulnerability data warehouse, and remediates vulnerabilities.
- Offers policy compliance and enforcement functionality
- Vulnerabilities may be automatically remediated, verified and documented, therefore enforcing compliance.
- No additional software or hardware implementation costs

- Anti-Vulnerability functionalities may be integrated into existing product platforms.
- Reduces cost of ownership of multi network security products
- Shared vulnerability data sets and added vulnerability remediation functionalities may reduce the number of network security products needed to adequately attain defense strategy requirements.
- Reduces management and maintenance costs
- Increased accuracy of vulnerability identification, remediation and policy enforcement, and reduction of false positives, false negatives and denial of service (DoS), significantly reduces management time and costs.
- Manage more machines and devices on the network through one portal
- Vulnerability remediation and policy compliance and enforcement may be integrated with existing security network security products, and their respective interfaces.
- Minimize end user education/ absorption costs
- Anti-Vulnerability applications are transparently integrated, retaining pre-existing architecture, processes, and interfaces. Therefore, the end user experience remains the same, or improved with simplified or automated processes.
- User experience remains the same – additional time or costs to understand and execute new technologies are minimized
- Anti-Vulnerability applications may be integrated transparently and seamlessly, and the pre-existing operational processes and user interfaces are virtually unchanged.
- Supports both the enterprise and SOHO networks
- Data warehouse contains vulnerabilities and updates for many machines and devices that operate on both enterprise and SOHO networks.
- Applications presented hereinafter

ForcePoint LLC
EX-1010-PT2
Page443

[0099] Examples of applications that may be made available for enterprise and small office home office (SOHO) networks when integrated with Anti-Vulnerability technology via the SDK will now be set forth.

[00100] In one embodiment, update or patch deployment is provided. In one embodiment, a patch management and vulnerability remediation solution is provided. The technology enables products to add accurate vulnerability identification, remediation, verification, and policy compliance functions. With such technology, products may gain intelligence, accuracy and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks. And, for the consumer market, it may additionally support non-security related updates such as application version, performance, and bug-fix updates for widely distributed programs, which may optimize system performance and enhance the consumer experience.

[00101] In one embodiment, an IDS is provided. IDS products attempt to identify malicious code by signatures at both the network and host client level. While they may be able to identify malicious code by CVE ID or other identifier, and targeted machines by IP address, but they generally do not have the intelligence to determine if the any of the machines on the network are susceptible to that attack, or with finer granularity, if any machine has a specific vulnerability to that specific attack, or if the targeted vulnerability has already been patched. For example, if the malicious code has been written as a Windows based attack targeting a Windows vulnerability, is the Destination IP actually running Windows, or a UNIX variant? And, if Windows, is it vulnerable to the attack, or has it already been patched? IDS do not have the intelligence to answer these questions, and incident alerts are generated indiscriminately. Lastly, even if the targeted machine is vulnerable - it remains unremediated – an IDS does not have the capability to remediate it.

[00102] With the present embodiment, a product architect can integrate functionalities listed in the previous section to enable the IDS to access the Anti-Vulnerability logic engine and platform. It may then have the intelligence to determine if any machine on the network is susceptible to the attack, remediate the vulnerability, mitigate the attack, and verify policy compliance. Now, if no machines were susceptible to the attack, it is identified as an event but

ForcePoint LLC
EX-1010-PT2
Page444

not an incident, no further data or alert is generated, and a management response is not required. Integrated products may gain intelligence, accuracy, and efficiency, eliminate false positives and false negatives, and ensure policy compliance, thereby saving the organization time and money. Such functionalities and benefits are available for both the enterprise and SOHO networks.

[00103] In one embodiment, scanners may be provided. Vulnerability scanners assess each machine on the network for vulnerabilities, and create lists of potential vulnerabilities to the system managers. The lists commonly contain many false positives and false negatives, burdening the system and managers with inaccuracies.

[00104] With the present embodiment, a product architect can integrate functionalities listed in the previous section to enable the scanner to access the logic engine and platform, and then have the intelligence to determine if the machine has actual vulnerabilities, remediate them, and verify policy compliance. Integrated products may gain intelligence, accuracy, and efficiency, eliminated false positives and false negatives, and ensured policy compliance, thereby saving the organization time and money.

[00105] In one embodiment, a firewall may be provided. "Smart" firewalls are based in part on signatures and other similar functionalities as the IDS products described above.

[00106] With the present embodiment, the firewall can determine whether an attack is valid or a false positive, thereby preventing the security system from denying valid traffic to the organization – self-inflicted DoS attacks. Such functionalities and benefits may be available for both the enterprise and SOHO networks.

[00107] In one embodiment, vulnerability management may be provided. Vulnerability management products enable managers to set policy and identify potential network vulnerabilities. They typically do not accurately identify each vulnerability on each network machine and device, nor remediate each vulnerability, meeting policy compliance enforcement requirements.

[00108] The present embodiment offers similar functionalities and benefits as the patch deployment products described above. In short, it enables products to add accurate vulnerability identification, remediation, verification, and policy compliance and enforcement. Such functionalities and benefits are available for both the enterprise and SOHO networks.

ForcePoint LLC
EX-1010-PT2
Page445

[00109] To this end, multiple products may be provided: IDS, scanner, firewall, and vulnerability management. Each product functions as the individual products noted above. Each may be deployed and operated on the network in a multi-tiered network defense strategy. They may be disparate system, and their signatures and update deployment schedules may vary. Therefore, the probability of mitigating a new and complex threat decreases, while management requirements and cost increases.

[00110] In one embodiment, they each may communicate with the same backend data warehouse, sharing the same vulnerability information, attaining intelligence and more accurate information about the target and its vulnerabilities, thereby more effectively mitigating complex threats. It may also enable the products to add accurate vulnerability identification, remediation, verification, and policy compliance and enforcement functionalities.

[00111] In one embodiment, change management (CM) may be provided. Existing CM applications control the documentation and logging of change throughout the enterprise. These applications ensure that an organization maintains consistent records of what happened and when. Currently administrators must independently recognize that a security patch/update must be deployed to a computer or group of computers.

[00112] The user enters the request in the system, through the pipelined process of change management the request would be approved, the patch/update would be manually installed by a user, then documented in the change management software that the process has been completed. While CM software assists in documentation, very little if any assistance may be provided to identify the patches/updates needed, nor verifying correct function after the update/patch is installed.

[00113] With the current possible embodiment, change management integration may greatly streamline this process further reducing total cost of ownership, ease of use, and a higher standard of documentation. The products may then automatically create a change request in the system, specifying what update/patch is applicable to what system or groups of systems by vulnerability. After approval of the request, they may automatically deploy and install the update/patch. Finally, they may also verify correct operation after installation and automatically provide all necessary documentation and logging required.

ForcePoint LLC
EX-1010-PT2
Page446

[00114] Lastly, one possible embodiment may also provide product upgrades and signature updates to each of these various security products - including all of the technology benefits such as ensuring compliance of signature versions, logging, reporting, and verification of installation.

[00115] Thus, one possible embodiment includes an intelligent platform that may supplement any existing defense strategy. Once integrated with the technology, security products may share the same vulnerability data set to improve automation and accuracy – increasing efficiencies and minimizing false positives and false negatives. It also enables remote identification, management, and remediation of network vulnerabilities, and provides update deployment, validation, and reporting capabilities. Thereby, the technology improves network security and integrity, mitigation of blended threats, while increasing productivity, reducing total cost ownership, and more effectively and efficiently attaining policy compliance and enforcement requirements.

[00116] One embodiment provides IDS intelligence, accuracy and remote patching functions - IDS data output integrated with the aforementioned platform via the SDK. The platform's underlying backend including a logic engine and vulnerability data warehouse provides the added functions and performance.

[00117] Conventional IDS produce an ever-increasing quantity of alert data, including erroneous and false positive data. They also lack the intelligence to identify or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintaining conventional IDS is overwhelming the end user.

[00118] Therefore, a more sophisticated, intelligent technology is provided to resolve these issues. In one embodiment, an intelligent IDS is provided to meet market requirements. The alert data output from a distribution of Snort is integrated with the platform via the SDK, which may add the following functions.

[00119] In one embodiment, it cross-references the threat's identifier with the target's configuration. The CVE ID, or other identifier, and the Destination IP address are fed into the logic engine where it cross-references the threat with the machine's configuration profile.

[00120] In one embodiment, it virtually eliminates false positives and false negatives. The backend accurately determines in real time if the targeted machine is susceptible to the attack.

ForcePoint LLC
EX-1010-PT2
Page447

And, if the machine is not susceptible, it is filtered and reported back as an event and not an incident. No further data or alert is generated, and a management response is not required.

[00121] In one embodiment, it remotely remediates the vulnerability. When a machine is identified as vulnerable to an attack, an incident, a remediation function may be provided to the administrator to remotely deploy the appropriate update to the machine or device, install it, verifies the files and hashes, and document it with change tracking and audit trail reports.

[00122] Table 3 sets forth a plurality of features.

Table 3

Supports Windows and UNIX variants
Determines if targeted machine is vulnerable to an attack in real time
Filters out erroneous, benign and false positive alerts
Remotely patches targeted vulnerabilities in one click
Installs in minutes

[00123] To this end, erroneous, benign, and false positive data is filtered out, and incidents may be remotely remediated. Therefore, complex threats are more effectively and efficiently mitigated. Correspondingly, the management and maintenance burden on administrators is reduced, saving time and effort.

[00124] FIG. 7 illustrates an intelligent IDS, in accordance with one embodiment. As shown in 701, the on-site server periodically initiates communication with the NOC servers. In 702, updates are pulled from the NOC servers to the on-site server. In 703a, a sensor monitors and processes network traffic, and sends real time alert data to the on-site server where it cross-references the data with the backend. In 703b, centralized IDS console filters alerts; separating events from incidents. It also offers administrators remote patching function. In 704, agents are deployed to each client, accurately identifying which OS, apps, and updates are installed. In 705, the logic engine automatically determines which updates are needed to remediate the targeted

ForcePoint LLC
EX-1010-PT2
Page448

machine. As shown in 706, appropriate updates are remotely deployed, installed, and validated on each client.

[00125] In one embodiment, the intelligent patch management and vulnerability remediation application automatically updates computer OS and application vulnerabilities before they can be exploited by hackers and viruses.

[00126] Networks are probed at an ever-increasing frequency for vulnerabilities, which may be exploited with directed compromise attacks. To protect the network, administrators must diligently update or "patch" server and workstation vulnerabilities, which is a time-consuming and costly process. Further compounding the burden on administrators, best practice and government compliance directives now require higher standards of network security to protect consumer privacy and proprietary data, which must be documented with change tracking and audit trail reports. Therefore, fully automated technology is provided to resolve these issues.

[00127] In one embodiment, a intelligent application called SysUpdate — the first technology to fully automate the updating and reporting processes, as described below.

[00128] In terms of function, one possible embodiment automatically researches updates. In collaboration with software development companies, it receives updates and their respective compatibility and installation guidelines, which are thoroughly reviewed and tested in a lab for system compatibility and stability. One embodiment automatically and securely downloads, and archives, all updates. Once the updates and guidelines are thoroughly reviewed and tested, they are automatically downloaded to each customer's on-site server, verified with MD5 hashes, and archived in a self-populating patch repository database.

[00129] One possible embodiment automatically determines the update and dependency requirements for all computers on a network, based on their individual operating systems, applications, and previously installed updates. The logic engine automatically matches the tested updates and their guidelines across each computer's configuration profile.

[00130] One possible embodiment remotely, securely, and automatically deploys updates to each computer and device. Updates may be tested on a test group, and then queued for release to each computer on the network, consistently in accordance with the policy determined by the network administrator.

ForcePoint LLC
EX-1010-PT2
Page449

[00131] One possible embodiment automatically verifies the updates are installed and running correctly. Each computer's client agent installs the updates, and verifies the files and hashes.

[00132] One possible embodiment automatically generates change tracking and audit trail reports. Change tracking and audit trail reports may be selected and printed from the management console reporting modules. Additionally, application license audit reports may be generated, which lists software installed on each machine, by license key.

[00133] Table 4 illustrates possible features in one embodiment.

Table 4

Supports Windows, UNIX variants, and network devices
Supports non-Microsoft applications
Logic engine provides system intelligence
Files verified with SHA1 or MD5 hashes
MMC snap-in console with Crystal Reports
AES encryption

[00134] FIG. 8 illustrates an update system, in accordance with one embodiment.

As shown in 801, the on-site server periodically initiates communication with the off-site NOC servers. In 802, updates are pulled from the NOC servers to the on-site server. In 803, the centralized MMC snap-in console offers flexible security policy options and comprehensive reporting capabilities. In 804. agents accurately identifies OS, apps, and updates installed on each client by file versions and hashes. In 805, logic engine automatically determines which updates are needed on each client, taking into account OS, app, and update dependencies. In 806, appropriate updates are automatically deployed, installed, and validated on each client.

[00135] In one embodiment, a secure computer log management application is provided with fully automated archiving, querying, and reporting options.

ForcePoint LLC
EX-1010-PT2
Page450

[00136] Best practice directives and government compliancy regulations now require administrators to archive log events over an extended period of time, and extensively document log and audit trail reports. With existing tools, these are time-consuming processes. Furthermore, existing tools transfer logs in clear text and are subject to malicious manipulation, and logs may be lost since few utilize guaranteed delivery protocols. Therefore, the integrity and security of the log data is not assured. In the event of an internal or external compromise, logs may be deleted, manipulated, or the network flooded with decoy log data.

[00137] The present possible embodiment automatically and continuously transfers logs from each computer into a self-configuring, self-populating, maintenance-free database where they may be archived for years on end. The transfer process utilizes AES encryption for authentication between the client and server, and a guarantee delivery protocol — ensuring no data is compromised or lost. Flexible cross-correlation queries may be run from a single, remote viewer console, and the data is then automatically formatted into reports.

[00138] In one embodiment, cross-correlation query type descriptions are provided. Such embodiment may provide the following three flexible cross-correlation queries in Table 5, which provide increasing detail and breadth of filtering/sorting capabilities, respectively.

Table 5

General Queries – This is the default query. It filters or sorts the logs of any one computer, by any one of the three log types.

Specific Queries – Detailed queries across all machines, and all log types.

Advanced Queries – Query across any combination of machines, by any combination of sources, events, and log types, over any period of time.

[00139] In one embodiment, features shown in Table 6 may be provided.

Table 6

- Continuously pulls all logs into a central database, which may be archived for years on end
- AES encryption and a guarantee delivery protocol ensure logs are not compromised or lost
- Queries may be across any computer, for any log type, over any time frame
- Automatically generates event log reports — ideal for documenting audit and compliance requirements
- Easy download installation

[00140] In one embodiment, automated reports may be provided. Query data is automatically formatted into professional reports Also, a separate reporting interface is available to generate general, machine, and user statistics. The present embodiment quickly and easily fulfills best practice and government compliance requirements for log event archiving and reporting.

[00141] FIG. 9 shows a configured network, in accordance with one embodiment.

[00142] As shown in 901, the server component automatically configures the application, and the database and communicates with the client agents. In 902, client agents are deployed, which then identifies, manages, and continuously transfers all logs to the server. In 903, all client log data may be automatically archived the self-populating database, for years on end. In 904, from the centralized viewer, general, specific, or advanced cross-correlation queries may be run. See Table 7. Query and statistics data is automatically formatted into professional reports to easily document audit and compliance requirements.

Table 7

Filter/Sort By:	**General**	**Specific**	**Advanced**

# of Computers	Any One	Any One	Any
# of Log Types	Any One	All	Any
Period of Time	Last or All	Last or All	Any
# of Event Detail Fields *	By ID Only	Any One	Any

* Defined as Time/Date Written, UserID, ComputerID, EventID, Source, Type, and Category

[00143] One possible embodiment provides best practice security policy templates to proactively and remotely manage and enforce enterprise security compliance policies.

[00144] Best practice and government compliance directives require higher standards of network security to protect consumer privacy and proprietary data, which must be consistently enforced, and documented with change tracking and audit trail reports for compliance verification. Therefore, a fully automated technology is provided to resolve these issues.

[00145] One embodiment offers an intelligent application to manage and enforce security policies — the first technology to fully automate the policy configuration, enforcement, and reporting processes, as described below.

[00146] In one embodiment, centralized, remote management is provided. The policy compliance and enforcement module is managed via the centralized management console - in MMC format, and automates the deployment, assessment, and enforcement of the policy chosen.

[00147] One embodiment provides standardized policies selected from many standardized policy templates recommended by NSA, SANS, US Navy, and ISO 17799, or custom policy options to formulate policies that meet the individual needs of any organization.

[00148] One possible embodiment automatically determines out-of-compliance parameters for all computers and devices on a network. Based on each client's individual policy parameter settings and configuration profile, the system's logic engine automatically reports back each client's out-of-compliance parameters.

[00149] In one embodiment, it remotely, securely, and automatically enforces policy to each computer or device. Policy changes may be automatically enforced to each computer or device

individually, or by group, consistently in accordance with the policy selected by the network administrator. Policy configuration profiles are transmitted between client agent and server in an AES encrypted format for security and privacy. Policy options may be rolled back with one-click.

[00150] Automatically generates change tracking and audit trail reports. Change tracking and audit trail reports may be selected and printed from the Management Console's Reporting Center. Table 8 sets forth some possible features.

Table 8

Supports Windows, UNIX variants, and network devices
Supports NSA, SANS, Navy, ISO 17799 and other standardized policies
Logic engine provides system intelligence
One-click policy rollback
Automatically generates change tracking and audit trail reports

[00151] FIG. 10 shows policy compliance and enforcement, in accordance with one embodiment.

[00152] As shown in 1001, the on-site server periodically initiates communication with the off-site NOC servers. In 1002, templates, rules, and updates are pulled from the NOC servers to the on-site server. In 1003, a centralized management console offers flexible security policy templates, options, and comprehensive reporting capabilities. In 1004, agents are automatically deployed to each client, accurately identifying which policy parameters, OS, apps, and updates are applied or installed. In 1005, a logic engine automatically determines which clients are out of compliance. In 1006, appropriate policy changes are automatically enforced on each client.

[00153] In one embodiment an intelligent IPS may be provided that provides intelligence, accuracy, real-time prevention, and remote patching functions. In one embodiment, it accurately identifies and prevents malicious code from reaching their destination at the in-line IPS Sensor. Thereafter, a security officer may remotely patch the targeted vulnerability.

ForcePoint LLC
EX-1010-PT2
Page454

[00154] Conventional IDS/IPS produce an ever-increasing quantity of alert data, including erroneous and false positive data. They also lack the intelligence to identify or remediate the vulnerabilities targeted by the attack. Furthermore, the cost of the acquiring, managing, and maintaining conventional IPS is overwhelming the end user.

[00155] Therefore, a more sophisticated, intelligent technology is provided to resolve these issues, by offering an intelligent IPS to meet market requirements. The alert data output from a standard distribution of Snort is integrated with the platform via the SDK which accurately identifies attacks, and the attack is terminated at the in-line sensor – as described in the following functions.

[00156] One embodiment cross-references the threat's identifier with the target's configuration. The in-line Sensor monitors and processes traffic and sends alert data to the on-site server where its logic engine queries the backend in real-time to determine if the destination IP is vulnerable to the attack.

[00157] One possible embodiment provides enhanced flex response. If the destination IP is vulnerable to the attack, the in-line Sensor is commanded to immediately drop the exploit packets – preventing the attack. Further, it remotely remediates the vulnerability. When a machine is identified as vulnerable to an attack, an incident, a remediation function is also provided to the administrator to remotely deploy the appropriate update to the machine or device, install it, verifies the files and hashes, and documents it with change tracking and audit trail reports.

[00158] In one embodiment, attacks are accurately identified and mitigated before they reach their targets, and targeted vulnerabilities may be remotely remediated. Therefore, complex threats are more effectively and efficiently mitigated. Correspondingly, the management and maintenance burden on administrators is reduced, saving time and effort.

[00159] Table 9 illustrates some possible features.

Table 9

Supports Windows and UNIX variants

ForcePoint LLC
EX-1010-PT2
Page455

Determines in real-time if targeted machine is vulnerable to an attack, virtually eliminating false positives

in-line Sensor flex response terminates the attack

Remotely patches targeted vulnerabilities in one click

Installs in minutes

[00160] FIG. 11 illustrates an intelligent IPS, in accordance with one embodiment.

[00161] As shown in 1101, the on-site server periodically initiates communication with the NOC servers. In 1102, updates are pulled from the NOC servers to the on-site server.

[00162] In 1103a, an IPS in-line sensor monitors and processes network traffic, and sends real time alert data to the on-site server where it cross-references the data with the backend. In 1103b, if the destination IP is vulnerable to the attack, the in-line Sensor is commanded in real-time to drop the malicious packets. As shown in 1104, agents are deployed to each client, accurately identifying which OS, apps, and updates are installed. In 1105, the logic engine automatically determines which updates are needed to remediate the targeted machine, and may be remotely deployed from the IPS console. In 1106, appropriate updates are remotely deployed, installed, and validated on each client.

[00163] In one embodiment, an anti-vulnerability SDK is provided. The SDK was designed to be a simple integration pathway to the Anti-Vulnerability platform backend. The SDK is documented and deliverable. The SDK is compatible with many different programming languages such as C, C++, VB, Java, and others.

[00164] The technology is sophisticated, yet all of the details of managing the communications are implemented in the library, requiring the developer to only learn a simple function calls as detailed hereinafter. A product architect chooses the functionality desired, inserts the provided functionality SDK code into the product code. The SDK code may then query – via the logic engine – the data warehouse, and in turn may return an answer to the point product. The architect can then show the results in any format desired in the product's interface. Full vulnerability remediation and policy compliance and enforcement functionalities may be integrated as well.

[00165] FIG. 12 illustrates an SDK function call flow, in accordance with one embodiment.

[00166] Hence, the SDK serves as the architect's tool belt or building blocks needed to quickly and transparently access the Anti-Vulnerability backend and seamlessly integrate the desired functionality into the product without changing or complicating the end user experience.

[00167] Furthermore, the SDK enables system architects to use the Anti-Vulnerability platform to integrate multiple security products and functionalities. Products may then share the same vulnerability data set, improve system automation and accuracy – increasing efficiencies and minimizing false positives and false negatives, and coordinate policy compliance and enforcement functionalities.

[00168] Anti-Vulnerability functions that are accessible via the SDK. The functions are presented in groups, as follows in Table 10.

Table 10

Session Management
Group Management Functions
Client Management Functions
Patch Management Functions
Polling Functions
User Management Functions
Miscellaneous Functions
Policy Compliance Functions
Session Management Functions

[00169] Table 11 sets forth Session Management Functions

Table 11

ForcePoint LLC
EX-1010-PT2
Page457

OpenSession – Parameters: HOST name or IP address, LOGIN and PASSWORD for host
Returns: new SESSION Description: This function opens a new session to the OnSite Server
CloseSession – Parameters: SESSION to close
Returns: None Description: Closes a session that is no longer needed
IsSessionGood – Parameters: SESSION to test
Returns: TRUE or FALSE Description: returns TRUE if the session is still valid FALSE if it is not
SUGetLastError – Parameters: None
Returns: Error code of last error in the thread Description: Returns the error code of the last SDK error to occur in this thread
SUSetLastError – Parameters: ERROR code to set
Returns: None Description: Sets the error code for the thread to be returned by SUGetLastError
GetSDKVersion – Parameters: None
Returns: a WORD containing the version of the SDK Description: the MSB of the returned value is the major version number, the LSB is the minor version number
Ping – Parameters: SESSION to use, VALUE to ping with
Returns: VALUE on success 0 on failure Description: attempts to pass VALUE to the OnSite Server, which should pass it back.

[00170] Table 12 sets forth Group Management Functions.

Table 12

CreateGroup – Parameters: Group NAME and Description
Returns: GROUP that was just created or 0 on failure

Description: This function creates a new group with the provided name and Description
GetGroups – Parameters: None
Returns: A LIST of GROUPs. Description: This function Returns a list of all configured groups.
GetGroupsEx – Parameters: None
Returns: A LIST of GROUPINFO structures Description: This function Returns a list of all configured groups' information
DeleteGroup – Parameters: GROUP to be deleted.
Returns: Success or failure Description: This function permanently removes a group.
EditGroup – Parameters: GROUP to be edited, GROUPINFO to be applied
Returns: Success or failure Description: This function changes a GROUP's information
GetGroupPolicyOSCategories – Parameters: GROUP to get information about
Returns: A LIST of OPERATINGSYSYTEMCATEGORYs that have group policies configured Description: This function retrieves a list of operating system categories that have group policies configured
GetGroupPolicyOSSubCategories – Parameters: GROUP to get information about, OPERATINGSYSTEMCATEGORY to get sub category information about
Returns: A LIST of OPERATINGSYSTEMSUBCATEGORYs Description: This function retrieves a list of operating system sub-categories of OPERATINGSYSTEMCATEGORY that have policies for the GROUP
GetGroupPolicyInfo – Parameters: GROUPPOLICY to get information about, GROUPPOLICYINFO pointer to receive the information
Returns: Success or Failure Description: This function fills the passed GROUPPOLICYINFO structure with the information for the GROUPPOLICY
GetGroupPolicyInfoByOSCat – Parameters: GROUP to get information about, OPERATINGSYSTEMCATEGORY to get the policy for, GROUPPOLICYINFO

pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for a policy for the OPERATINGSYSTEMCATEGORY in the GROUP
GetGroupPolicyInfoByOSSubCat – Parameters: GROUP to get information about, OPERATINGSYSTEMSUBCATEGORY to get the policy for, GROUPPOLICYINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for a policy for the OPERATINGSYSTEMSUBCATEGORY in the GROUP
DeleteGroupPolicy – Parameters: GROUPPOLICY to delete
Returns: Success or failure Description: This function permanently deletes the GROUPPOLICY
EditGroupPolicy – Parameters: GROUPPOLICYINFO with new information
Returns: Success or failure Description: This function updates the group policy (contained in GROUPPOLICYINFO) with the information in GROUPPOLICYINFO
AddGroupPolicy – Parameters: GROUP to add the policy to, GROUPPOLICYINFO containg the policy information
Returns: Success or Failure Description: This function creates a new group policy and applies it to the GROUP
GetClientsInGroup – Parameters: GROUP to retrieve the clients from
Returns: LIST of CLIENTs belonging to the group Description: This function retrieves a list of clients that are members of a specific group
GetClientsInGroupEx – Parameters: GROUP to retrieve the clients from
Returns: LIST of CLIENTINFOs for clients belonging to the group Description: This function Returns a list of CLIENTINFO structures containing information for the clients that belong to this group
AddClientToGroup – Parameters: CLIENT to add to a group, GROUP to add the client to.

Returns: Success or failure Description: This function adds a client to a group
RemoveClientFromGroup – Parameters: CLIENT to remove from group, GROUP to remove the client from
Returns: Success or failure. Description: This function removes a client from a group.
MoveClientToGroup – Parameters: CLIENT to move, GROUP to move client to
Returns: Success or Failure Description: This function moves CLIENT to GROUP
GetUngroupedClients -- Parameters: None
Returns: LIST of ungrouped clients Description: This function Returns a LIST of the clients that do not belong to any group
GetUngroupedClientsEx – Parameters: None
Returns: LIST of CLIENTINFO structures Description: This function Returns a LIST of CLIENTINFO structures for the clients that do not belong to any group
GetGroupInfo – Parameters: GROUP to get information about, GROUPINFO pointer to receive the information
Returns: Success or failure Description: This function retrieves the information for the GROUP

[00171] Table 13 sets forth Client Management Functions.

Table 13

GetClientInstalledSoftware – Parameters: CLIENT to get information about
Returns: LIST of SOFTWARE installed on the client Description: This function retrieves a list of the software that has been detected on the

client
GetClientInstalledSoftwareEx – Parameters: CLIENT to get information about
Returns: LIST of SOFTWAREINFO for software installed on the client Description: This function returns a LIST of SOFTWAREINFO structures describing the software detected on the client
GetClientInstalledPatches – Parameters: CLIENT to get information from.
Returns: LIST of PATCHes corresponding to the installed patches on the client Description: This function retrieves a list of patches that were verified as installed on the last polling
GetClientInstalledPatchesEx – Parameters: CLIENT to get information from
Returns: LIST of PATCHINFO structures corresponding to the installed patches on the client Description: This function retrieves a LIST of PATCHINFO structures for patches that were verified as installed on the last polling
GetClientPendingPatches – Parameters: CLIENT to get information from.
Returns: LIST of PATCHes corresponding to the pending patches for the client Description: This function returns a list of patches that the client needs (according to group policy) as of the last polling.
GetClientPendingPatchesEx – Parameters: CLIENT to get information from
Returns: A LIST of PATCHINFO structures corresponding to the pending patches for the client Description: This function returns a LIST of PATCHINFO structures for patches that the client needs (according to group policy) as of the last polling.
GetClientPendingServicePack – Parameters: CLIENT to get information from
Returns: SERVICEPACK if a service pack is pending or 0 if not Description: This function returns a SERVICEPACK if there is a service pack pending for the client (according to group policy) as of the last polling. If there is no service pack pending it returns 0
GetClientPendingSoftware – Parameters: CLIENT to get information from
Returns: LIST of SOFTWARE that is pending

Description: This function returns a list of software that is pending for the client (according to group policy) as of the last polling
GetClientLogs - Parameters: CLIENT to get information from
Returns: LIST of LOGs for the client. Description: This function returns a list of logs for a particular client.
GetClientLogsEx – Parameters: CLIENT to get information from
Returns: LIST of LOGINFO structures Description: This function returns a list of LOGINFO structures containing log entries for a particular client.
DeleteClient – Parameters: CLIENT to delete.
Returns: Success or failure. Description: This function removes all information pertaining to this client from the SysUpdate database.
GetClientOS – Parameters: CLIENT to get information from
Returns: OPERATINGSYSTEM installed on client Description: This function returns the OPERATINGSYSTEM installed on the client
GetClientServicePack – Parameters: CLIENT to get information from
Returns: SERVICEPACK installed on client or 0 Description: This function returns the service pack installed on the client or 0 if the client does not have a service pack installed, or if service packs are not applicable to the client's platform
GetClientInfo – Parameters: CLIENT to get information from CLIENTINFO pointer to receive the information
Returns: Success or failure Description: This function fills the passed CLIENTINFO structure with information pertaining to the passed CLIENT
GetClientFromIP – Parameters: IP address of client
Returns: CLIENT that corresponds to the passed IP address Description: This function maps IP addresses to clients

[00172] Table 14 sets forth Patch Management Functions.

Table 14

GetPatchInfo – Parameters: PATCH to get information about, PATCHINFO pointer to receive information
Returns: Success or failure Description: This function fills the passed patch info structure with information about the passed patch
InstallPatchForClient – Parameters: CLIENT to install the patch on, PATCH to install
Returns: Success or failure Description: This function deploys the patch to the client. Installation proceeds asynchronously
InstallPatchForGroup – Parameters: GROUP to install the patch on, PATCH to install
Returns: Success or failure Description: This function deploys the patch to all clients in the group
InstallAllPendingForClient – Parameters: CLIENT to install patches on
Returns: Success or failure Description: This function deploys all pending patches for a client to the client
InstallAllPendingForGroup – Parameters: GROUP to install patches on
Returns: Success or failure Description: This function deploys all pending patches to all clients in a group
RejectPatchForClient – Parameters: CLIENT to reject patch for, PATCH to reject
Returns: Success or failure Description: This function rejects a patch for a client. This patch will not be queued down or installed
RejectPatchForGroup – Parameters: GROUP to reject patch for, PATCH to reject
Returns: Success or failure Description: This function rejects a patch for every client in a group. This patch will not be queued down or installed
RequeuePatchForClient – Parameters: CLIENT to requeue the patch for, PATCH to requeue

ForcePoint LLC
EX-1010-PT2
Page464

Returns: Success or failure Description: This function requeues a previously rejected patch for a client
RequeuePatchForGroup – Parameters: GROUP to requeue the patch for, PATCH to requeue
Returns: Success or failure Description: This function requeues a previously rejected patch for every client in a group
RemovePatchFromClient – Parameters: CLIENT to remove patch from, PATCH to remove
Returns: Success or failure Description: This function will uninstall a patch from a client
RemovePatchFromGroup – Parameters: GROUP to remove patch from, PATCH to remove
Returns: Success or failure Description: This function will uninstall a patch for every client in a group
InstallServicePackForClient – Parameters: CLIENT to install service pack on, SERVICEPACK to install on client
Returns: Success or failure Description: This function will install a service pack on a client
InstallServicePackForGroup – Parameters: GROUP to install service pack on, SERVICEPACK to install
Returns: Success or failure Description: This function will install a service pack on every client in a group
InstallSoftwareForClient – Parameters: CLIENT to install software update on, SOFTWARE to install
Returns: Success or failure Description: This function will install a software update on a client
InstallSoftwareForGroup – Parameters: GROUP to install software update on, SOFTWARE to install
Returns: Success or failure Description: This function will install a software update on every client in a group.
GetCveIDsFromPatch – Parameters: PATCH to get CveIDs from
Returns: A LIST of CVEIDs

Description: This function returns a list of CVEIDs the correspond to the PATCH

[00173] Table 15 sets forth Polling Functions.

Table 15

PollClient – Parameters: CLIENT to poll
Returns: Success or failure. Description: This function causes a client to be polled by the OnSite Server immediately.
PollGroup – Parameters: GROUP to poll
Returns: Success or failure. Description: This function causes all the clients in a particular group to be polled immediately.
PollAll – Parameters: NONE
Returns: Success or failure. Description: This function causes all clients to be polled immediately.

[00174] Table 16 sets forth User Management Functions.

Table 16

GetUsers – Parameters: None
Returns: A LIST of USERs Description: This function returns a list of all users for the system
GetUserInfo – Parameters: USER to get information about, USERINFO pointer to receive the information
Returns: Success or failure Description: This function populates the passed USERINFO structure with information

about the passed USER
GetUserGroupPrivileges – Parameters: USER to get information about
Returns: A LIST of USERGROUPPRIVILEGEs Description: This function returns a LIST of USERGROUPPRIVILEGES representing the privileges that a particular user has
GetUserGroupPrivilegesEx – Parameters: USER to get information about
Returns: A LIST of USERGROUPPRIVILEGEINFO structures Description: This function returns a LIST of USERGROUPPRIVILEGEINFO structures representing the privileges that a particular user has
GetUserGroupPrivilegeInfo – Parameters: USERGROUPPRIVILEGE to get information about, USERGROUPPRIVILEGEINFO pointer to receive information
Returns: Success or failure Description: This function populates the passed USERGROUPPRIVILEGEINFO structure with the details of the particular privilege
GetUserGroupPrivilegeInfoByGroup – Parameters: USER to get information about, GROUP to get information for, USERGROUPPRIVILEGEINFO pointer to populate
Returns: Success or Failure Description: This function populates the passed USERGROUPPRIVILEGEINFO structure with the detailed information regarding the permissions that the passed user has on the passed group
AddUserGroupPrivilege – Parameters: USERGROUPPRIVILEGEINFO structure to add
Returns: Success or failure Description: This function adds a USERGROUPPRIVILEGE
EditUserGroupPrivilege – Parameters: USERGROUPPRIVILEGEINFO with new values
Returns: Success or failure Description: This function edits the USERGROUPPRIVILEGEINFO structure passed in, assign it the new values
DeleteUserGroupPrivilege – Parameters: USERGROUPPRIVILEGE to delete
Returns: Success or failure Description: This function deletes the passed USERGROUPPRIVILEGE from the

system
AddUser – Parameters: USERNAME, PASSWORD, and USERTYPE
Returns: USER representing the user that was just created Description: This function creates a new user with the provided username, password, and type, and returns a USER representing the new user or 0 in the case of an error
DeleteUser – Parameters: USER to delete
Returns: Success or failure Description: This function permanently deletes the USER from the system along with any privileges the user may have had
ChangeUserPassword – Parameters: USER to change password for, new PASSWORD
Returns: Success or failure Description: This function changes the password for a user
ChangeUserRole – Parameters: USER to change role, ROLE to change to
Returns: Success or failure Description: This Function changes a user's role
GetUserFromName – Parameters: USERNAME
Returns: USER corresponding to the passed user name Description: This function provides a mapping from user names to USERs

[00175] Table 17 sets forth Miscellaneous Functions.

Table 17

CreateList – Parameters: None
Returns: A new, empty, LIST Description: This functions creates a new LIST that is initially empty
GetListItemEx – Parameters: LIST to retrieve item from, INDEX of item to retrieve, VOID pointer to receive item
Returns: Success or failure

Description: This function populates the memory pointed to by VOID with the contents of the LIST item at INDEX
GetListSize – Parameters: LIST to get the size of
Returns: the size of the LIST Description: This function returns the number of elements currently in the list
AddItemToList – pointer to LIST to add the item to, LONG item to add
Returns: None Description: This function adds an "item" (such as a GROUP or a CLIENT) to a LIST
AddClientInfoExToList – See AddItemToList
AddGroupInfoToList – See AddItemToList
AddPatchInfoExToList – See AddItemToList
AddSoftwareInfoToList – See AddItemToList
AddSoftwareCategoryInfoToList – See AddItemToList
AddUserGroupPrivilegeInfoExToList – See AddItemToList
RemoveItemFromList – Parameters: pointer to LIST to remove the item from, INDEX of item to remove
Returns: None Description: This function removes the item at INDEX from the LIST
FreeList – LIST to deallocate
Returns: None Description: This function deallocates the resources used by LIST
GetSoftwareInfo – Parameters: SOFTWARE to get information for, SOFTWAREINFO pointer to hold the information
Returns: Success or failure Description: This function populates the SOFTWAREINFO structure pointed at with information regarding the SOFTWARE
GetLogInfo – Parameters: LOG to get information about, LOGINFO pointer to contain the information
Returns: Success or failure Description: This function populates the LOGINFO structure pointed at with

information regarding the LOG
GetSoftwareCategories – Parameters: None
Returns: A LIST of SOFTWARECATEGORYs Description: This function returns a LIST of SOFTWARECATEGORYs
GetSoftwareCategoriesEx – Parameters: None
Returns: A LIST of SOFTWARECATEGORYINFO structures Description: This function returns LIST of SOFTWARECATEGORYINFO structures for every software category known on the system
GetSoftwareCategoriesForOperatingSystemCategory – Parameters: an OPERATINGSYSTEMCATEGORY to get information for
Returns: A LIST of SOFTWARECATEGORYs Description: This function returns a LIST of software categories for the passed operating system category.
GetSoftwareCategoriesForOperatingSystemCategoryEx – As above only, returning the appropriate "info" structures in the list
GetSoftwareCategoryInfo – Parameters: SOFTWARECATEGORY to get information for, SOFTWARECATEGORYIFNO pointer to contain the information Returns: Success or failure

[00176] Table 18 sets forth Policy Compliance Functions.

[00177] These functions are provided in a separate source tree (policy tree) for the Policy Compliance and Enforcement module. Function include: Password/system access policies, log configurations, audit settings, user/group privilege rights, general service settings, service permissions, registry values, registry permissions, file permissions. It can also perform deltas on and get information about: groups, users, services, and all the "Run" registry keys.

[00178] The function calls are being integrated into the live production tree and subject to change.

Table 18

GetPolicyItemInfo – As GetOperatingSystemInfo for POLICYITEM and POLICYITEMINFO

InstallPolicyItemForClient – As InstallPatchForClient for POLICYITEM
InstallPolicyItemForGroup – As InstallPatchForGroup for POLICYITEM
InstallAllPendingPolicyItemsForClient – As InstallAllPendingPatchesForClient for POLICYITEM
InstallAllPendingPolicyItemsForGroup – As InstallAllPendingPatchesForGroup for POLICYITEM
RemovePolicyItemFromClient – As RemovePatchForClient for POLICYITEM
RemovePolicyItemFromGroup – As RemovePatchFromGroup for POLICYITEM

[00179] All publications, prior applications, and other documents cited herein are hereby incorporated by reference in their entirety as if each had been individually incorporated by reference and fully set forth.

[00180] While the invention has been illustrated and described in detail in the drawings and foregoing description, the same is to be considered as illustrative and not restrictive in character, it being understood that only the preferred embodiments have been shown and described and that all changes and modifications that would occur to one skilled in the relevant art are desired to be protected.

ForcePoint LLC
EX-1010-PT2
Page471

CLAIMS

What is claimed is:

1. An apparatus, comprising:

at least one data storage;

at least one platform communicatively coupled to the at least one data storage; and

at least one agent capable of being communicatively coupled to the at least one platform;

said at least one data storage configured to store data on a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

said at least one platform configured to:

cause display of at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allow receipt of user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability;

ForcePoint LLC
EX-1010-PT2
Page472

said at least one agent configured to identify information in connection with at least one of a plurality of devices for use in identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability;

said apparatus configured such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system.

2. The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to user input received prior to the attack, the firewall option is capable of being applied to a plurality of different devices for preventing the at least one attack packet at any of the different devices; and the apparatus is further configured such that, in response to additional user input after the attack in connection with a particular single device of the plurality of different devices, the intrusion detection or prevention option is capable of being applied to the particular single device.

3. The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a firewall option for preventing at least one attack packet of the attack by terminating or dropping the same, and an intrusion detection or prevention option; the apparatus is further configured such that, in response to user input prior to the attack, the intrusion detection or prevention option is capable of being applied to a plurality of different devices at the plurality of different devices; and the apparatus is further configured such that, in response to user input after the attack in connection with a particular single device of the plurality of different devices, the firewall option is capable of being applied to the particular single device for preventing the at least one attack packet at the particular single device.

4. The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification

ForcePoint LLC
EX-1010-PT2
Page473

of the operating system in connection with the accessing for the displaying of the at least one mitigation technique, so that, in order to avoid false positives, relevant vulnerabilities prompt mitigation technique user selection among at least two of the mitigation techniques, which involve both firewall and intrusion prevention system actions, for providing diverse mitigation options in connection with the relevant vulnerabilities.

5. The apparatus of Claim 1, wherein the apparatus is configured such that the one or more of the plurality of mitigation techniques is capable of being identified based on the identification of the operating system prior to causing the display of the at least one mitigation technique, so that which of the one or more of the mitigation techniques that is caused to be displayed is based on one or more actual vulnerabilities to which the at least one device is actually vulnerable so that only relevant one or more mitigation techniques are displayed for selection by a user for attack mitigation.

6. The apparatus of Claim 1, wherein the apparatus is configured such that the user input is capable of being received via at least one user interface of the at least one platform for different devices, for allowing different attack mitigation actions including at least one intrusion prevention action and at least one firewall action to be selectively applied to the different devices for different actual vulnerabilities determined to be actually relevant based on the identification of the operating system in connection with the different devices.

7. The apparatus of Claim 1, wherein the apparatus is configured such that the at least one mitigation technique includes at least two mitigation techniques including a first mitigation technique that utilizes a firewall action and a second mitigation technique that utilizes an intrusion prevention action;

8. The apparatus of Claim 7, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first

mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

9. The apparatus of Claim 7, wherein the apparatus is configured such that the at least one mitigation technique further includes a third mitigation technique that utilizes a policy compliance action, wherein the apparatus is configured such that different user input is capable of being received via the at least one platform for different devices, for allowing different mitigation techniques including the first mitigation technique, the second mitigation technique, and the third mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user input is capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device; only the second mitigation technique being selectively applied by the user to at least one second device; and the first mitigation technique, the second mitigation technique, and the third mitigation technique being selectively applied by the user to at least one third device.

10. The apparatus of Claim 7, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from an integrated firewall/intrusion prevention system platform component of the at least one platform to firewall-supporting code of the at least one agent, and the second mitigation technique is automatically applied utilizing a second communication from the integrated firewall/intrusion prevention system platform component of the at least one platform to intrusion prevention system-supporting code of the at least one agent, where the firewall-supporting code and the system-supporting code are part of the at least one agent.

11. The apparatus of Claim 1, wherein the apparatus is configured such that the identification of the operating system is a result of a vulnerability assessment scan caused by the at least one platform.

12. The apparatus of Claim 1, wherein the at least one platform includes intrusion prevention functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality.

13. The apparatus of Claim 1, wherein the at least one platform utilizes router-based functionality for supporting a first mitigation technique and firewall functionality for supporting a second mitigation technique.

14. The apparatus of Claim 13, wherein the apparatus is configured such that the system is capable of receiving actual vulnerability information to conditionally display, as a function of an existence of one or more actual vulnerabilities, one or more of the plurality of mitigation techniques to allow selective utilization of the router-based functionality and the firewall functionality, so that only relevant mitigation techniques are displayed for selection to reduce false positives in connection with both the router-based functionality and the firewall functionality.

15. The apparatus of Claim 1, wherein at least one of:

said at least one data storage includes at least one database;

said at least one data storage is accessed by at least one of: receiving at least one update therefrom; pulling at least one update therefrom, communicating therewith, or synchronizing therewith;

said mitigation techniques include remediation techniques;

each mitigation technique has a mitigation type including the patch;

each mitigation technique has a mitigation type including the policy setting;

each mitigation technique has a mitigation type including the configuration option;
each mitigation technique is capable of mitigating the effect of the attack that takes advantage of the corresponding vulnerability, by dropping packets associated with the attack or removing the corresponding vulnerability;
said information is capable of being used to determine an intended destination of a connection request; or
said information includes a vulnerability identifier;
wherein the apparatus is operable for use with at least one NOC server, a data warehouse, and an SDK for allowing access to information associated with at least one vulnerability and at least one remediation technique; and wherein the apparatus is operable for determining which devices have vulnerabilities by directly querying a firmware or operating system of the devices.

16. An apparatus, comprising:

at least one data storage configured to store at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option; and

at least one platform communicatively coupled to the at least one data storage, the at least one platform configured to:

based on user selection, automatically apply at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation

ForcePoint LLC
EX-1010-PT2
Page477

type and at least one second mitigation technique of a second mitigation type to the at least one device;

receive information in connection with at least one of a plurality of devices,

identify an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information, and

mitigate an effect of the attack on the at least one device that takes advantage of the at least one vulnerability, based on the application;

wherein the apparatus is configured such that the at least two of the plurality of mitigation techniques are made available for the user selection, based on an identification of an operating system.

17. The apparatus of Claim 16, wherein the apparatus is configured such that the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by at least one agent that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied.

18. The apparatus of Claim 17, wherein the apparatus is configured such that the at least one agent is further capable of supporting a vulnerability assessment scan for the identification of the operating system.

19. The apparatus of Claim 16, wherein the apparatus is configured such that the first mitigation technique is automatically applied utilizing a first communication from the at least one platform to firewall-supporting code of at least one agent, and the second mitigation technique is automatically applied utilizing a second communication from the at least one platform to intrusion prevention system-supporting code of the at least one agent; wherein the at

ForcePoint LLC
EX-1010-PT2
Page478

least one platform includes intrusion prevention functionality for supporting the first mitigation technique and firewall functionality for supporting the second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by the at least one agent that also supports the identification of the attack in connection with the at least one device, the at least one platform further capable of receiving actual vulnerability information to conditionally make available for the user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the plurality of mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are made available for the user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the first mitigation technique and the second mitigation technique to be selectively applied by a user to the different devices for different actual vulnerabilities, such that the different user selections are capable of resulting in: only the first mitigation technique being selectively applied by the user to at least one first device, only the second mitigation technique being selectively applied by the user to at least one second device, and both the first mitigation technique and the second mitigation technique being selectively applied by the user to at least one third device.

20. An apparatus, comprising:

means for identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities associated with an operating system, where:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

means for:

ForcePoint LLC
EX-1010-PT2
Page479

causing display of at least two of the mitigation techniques for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

allowing receipt of at least one user input in connection with one or more of the at least two mitigation techniques; and

means for automatically applying the one or more of the at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device;

said apparatus configured such that the at least two mitigation techniques are displayed based on an identification of an operating system.

21. The apparatus of Claim 20, wherein the apparatus is configured such that the at least one first mitigation technique is automatically applied utilizing a first communication to firewall-supporting code, and the at least one second mitigation technique is automatically applied utilizing a second communication to intrusion prevention system-supporting code; wherein the apparatus includes intrusion prevention functionality for supporting the at least one first mitigation technique and firewall functionality for supporting the at least one second mitigation technique, such that the intrusion prevention functionality and the firewall functionality are both supported by at least one component that also supports identification of attacks in connection with the at least one device, the apparatus further capable of receiving actual vulnerability information to conditionally make available for user selection, as a function of an existence of one or more actual vulnerabilities, the at least two of the mitigation techniques to allow selective utilization of the intrusion prevention functionality and the firewall functionality, so that only relevant mitigation techniques are made available for the user selection to reduce false positives in connection with both the intrusion prevention functionality and the firewall functionality; wherein the apparatus is further configured such that different user selections are capable of being received for different devices, for allowing different mitigation techniques including the at

least one first mitigation technique and the at least one second mitigation technique to be selectively applied to the different devices for different actual vulnerabilities, such that the different user selections are capable of resulting in: only the at least one first mitigation technique being selectively applied to at least one first device, only the at least one second mitigation technique being selectively applied to at least one second device, and both the at least one first mitigation technique and the at least one second mitigation technique being selectively applied to at least one third device.

ForcePoint LLC
EX-1010-PT2
Page481

ABSTRACT

A system, method, and computer program product are provided for a database associating a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities. Each of the device vulnerabilities is associated with at least one remediation technique. Each remediation technique associated with a particular device vulnerability remediates that particular vulnerability. Further, each remediation technique has a remediation type are selected from the type group consisting of patch, policy setting, and configuration option. Still yet, a first one of the device vulnerabilities is associated with at least two alternative remediation techniques.

ForcePoint LLC
EX-1010-PT2
Page482

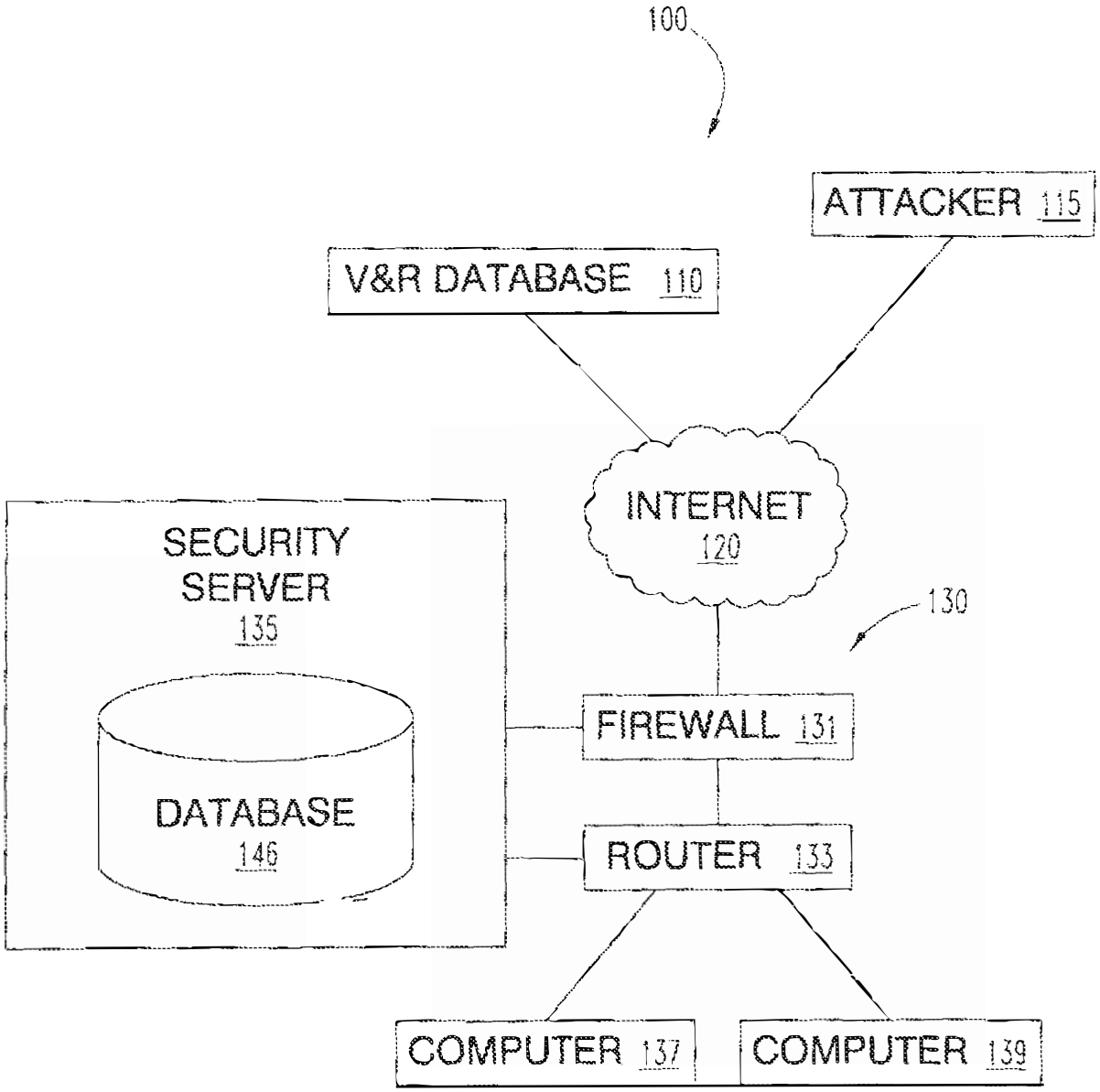

100
ATTACKER 115
V&R DATABASE 110
INTERNET 120
130
SECURITY SERVER 135
DATABASE 146
FIREWALL 131
ROUTER 133
COMPUTER 137
COMPUTER 139

FIG. 1

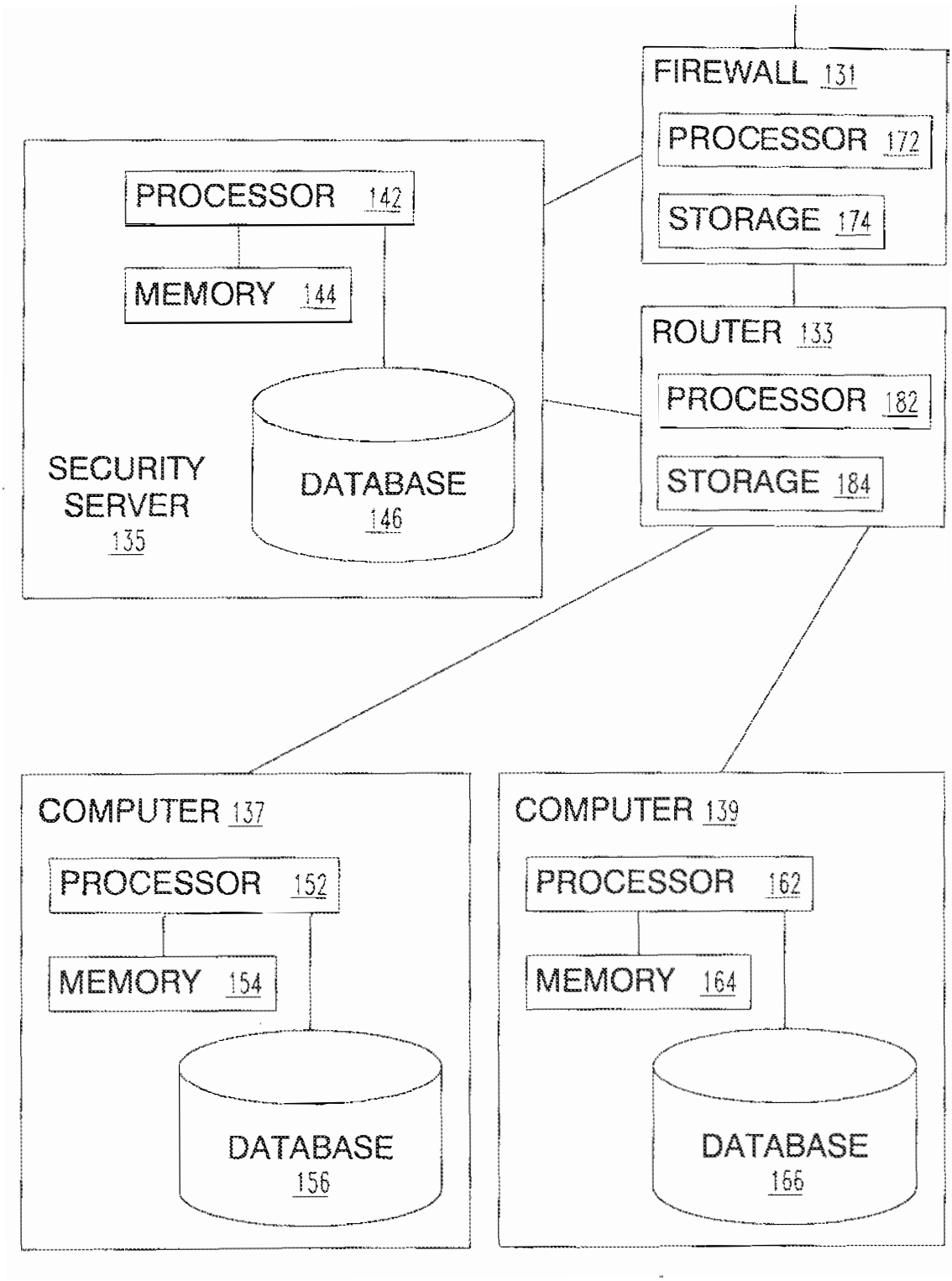

FIREWALL 131
PROCESSOR 172
STORAGE 174
PROCESSOR 142
MEMORY 144
ROUTER 133
PROCESSOR 182
STORAGE 184
DATABASE
146
SECURITY
SERVER
135
COMPUTER 137
PROCESSOR 152
MEMORY 154
DATABASE
156
COMPUTER 139
PROCESSOR 162
MEMORY 164
DATABASE
166

FIG. 2

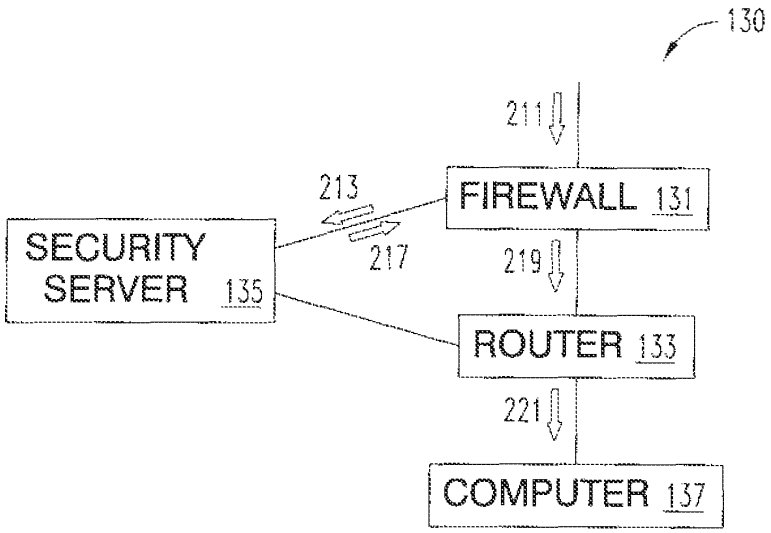

130
211
FIREWALL 131
213
217
SECURITY SERVER 135
219
ROUTER 133
221
COMPUTER 137

FIG. 3

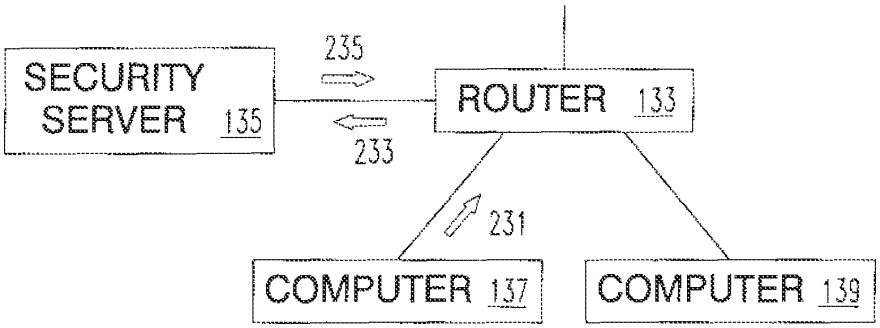

SECURITY SERVER 135
235
233
ROUTER 133
231
COMPUTER 137
COMPUTER 139

FIG. 4

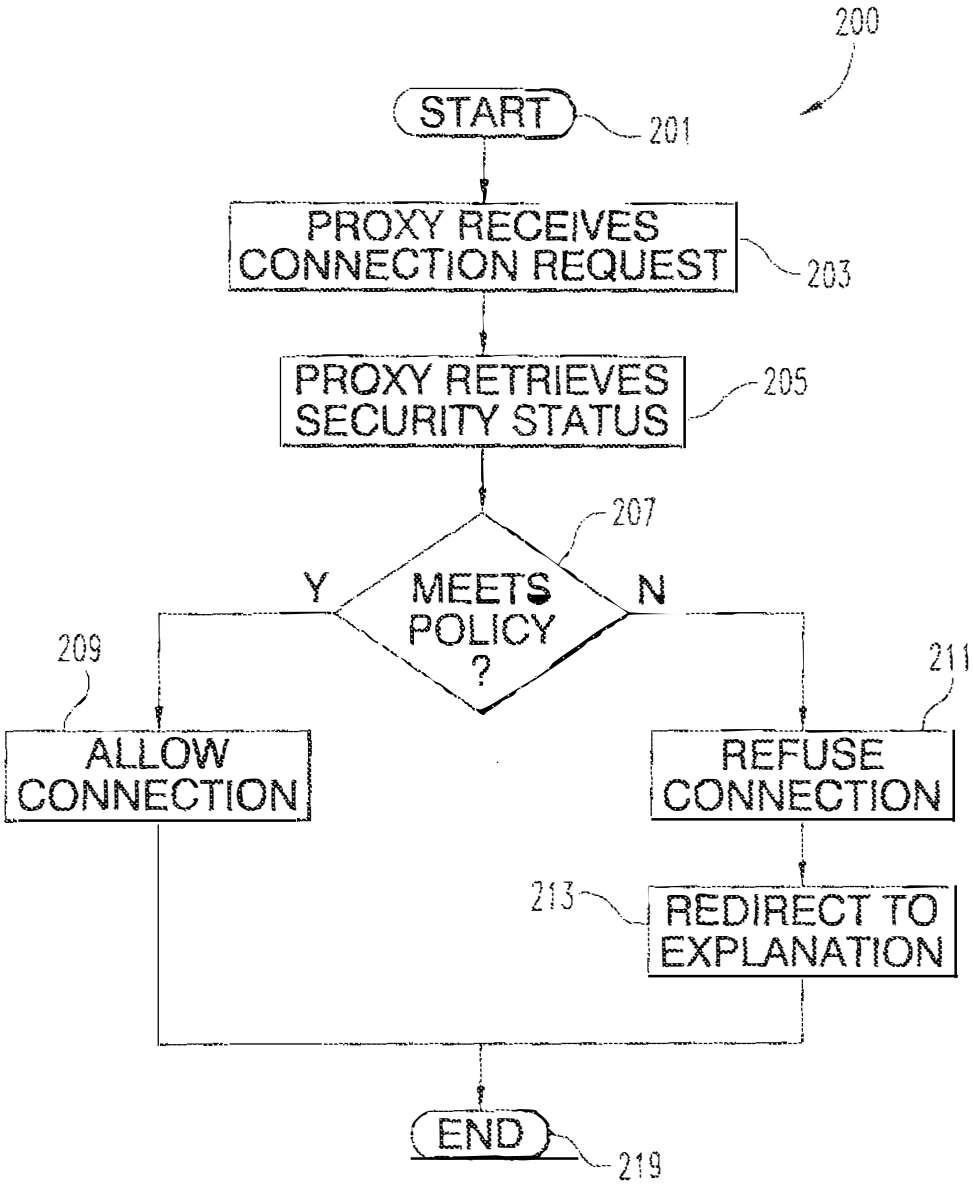

200
START
201
PROXY RECEIVES CONNECTION REQUEST
203
PROXY RETRIEVES SECURITY STATUS
205
207
MEETS POLICY ?
Y
N
209
ALLOW CONNECTION
211
REFUSE CONNECTION
213
REDIRECT TO EXPLANATION
END
219

FIG. 5A

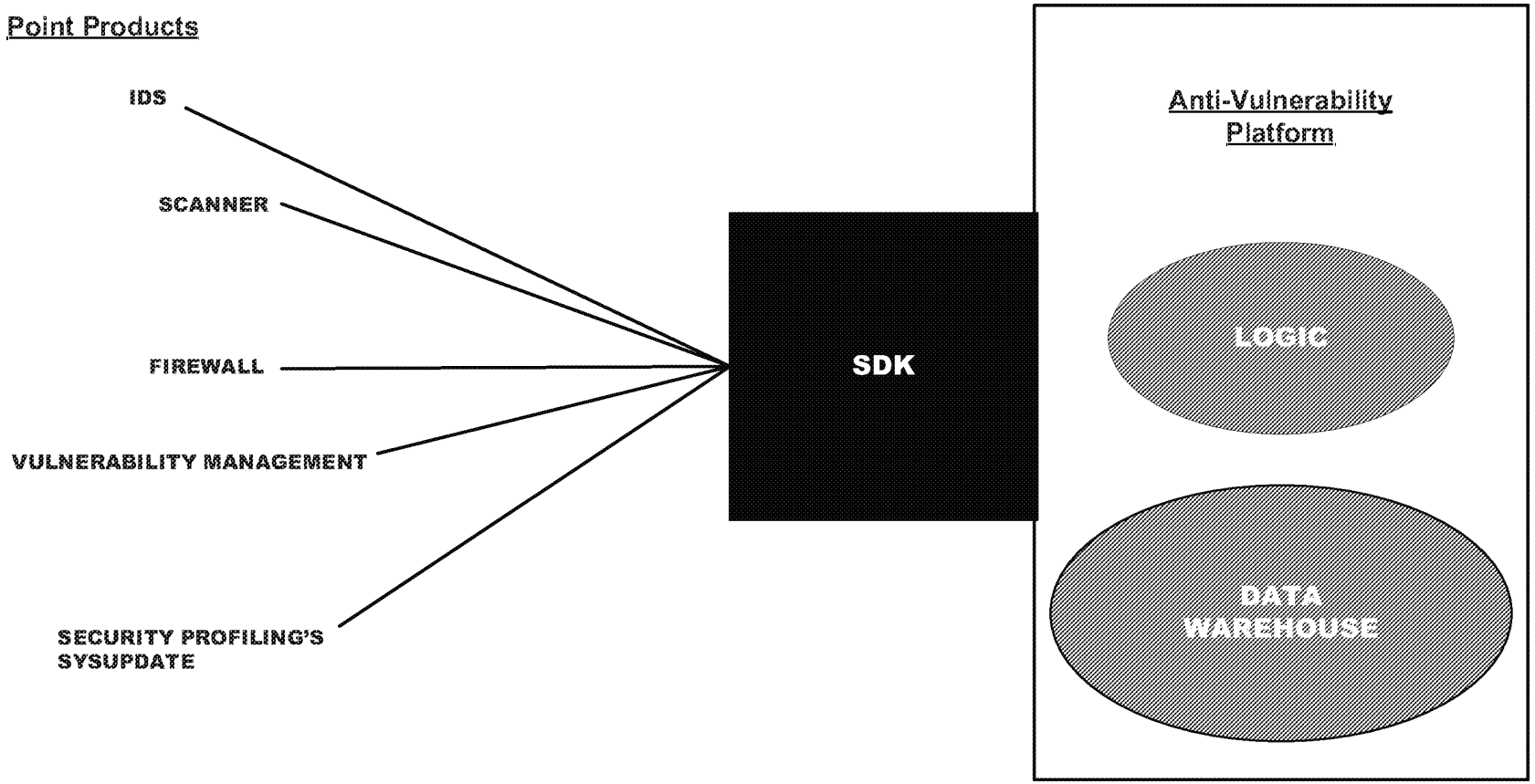


FIG. 5B

ForcePoint LLC
EX-1010-PT2
Page487

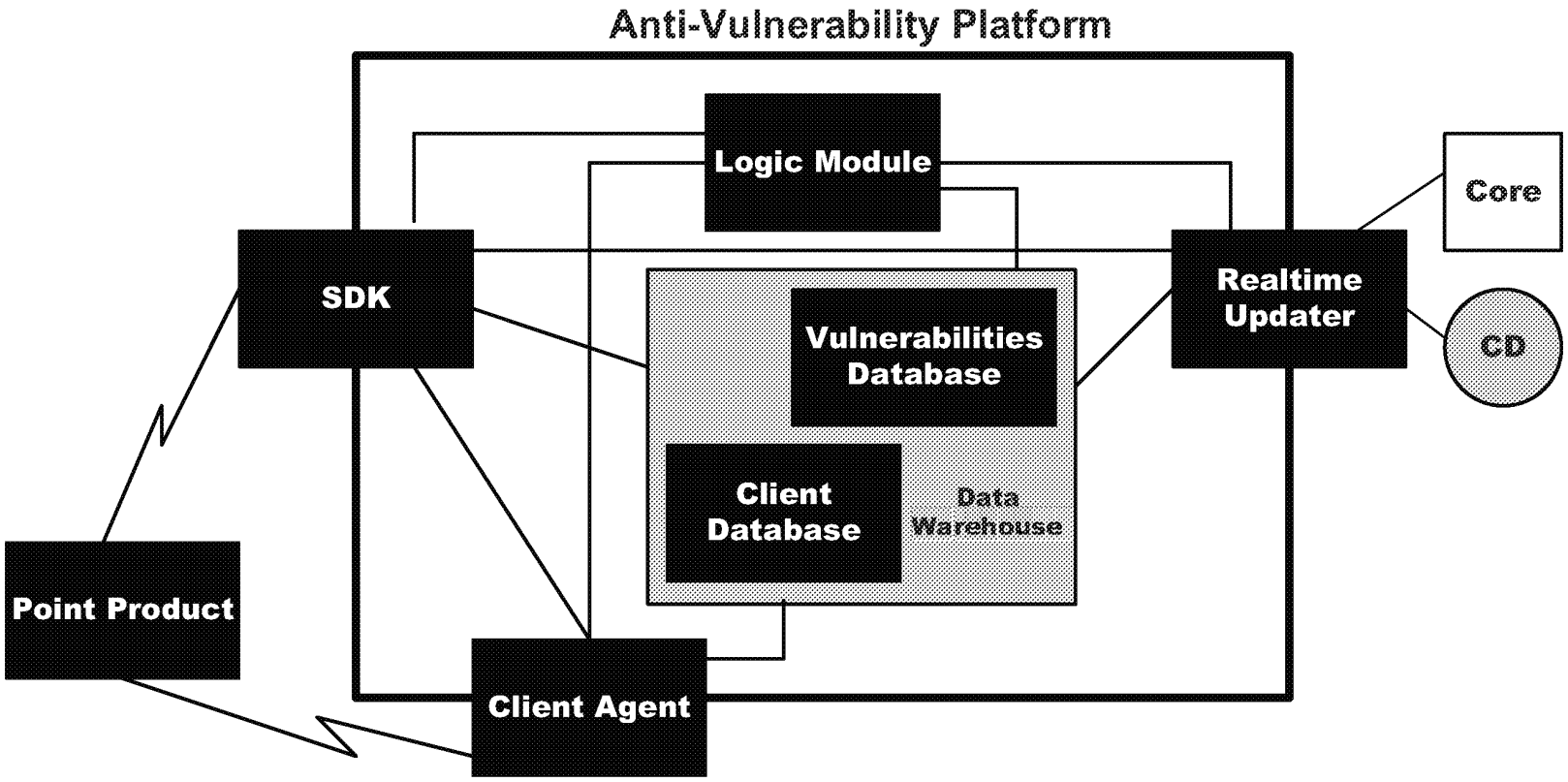


FIG. 6

ForcePoint LLC
EX-1010-PT2
Page488

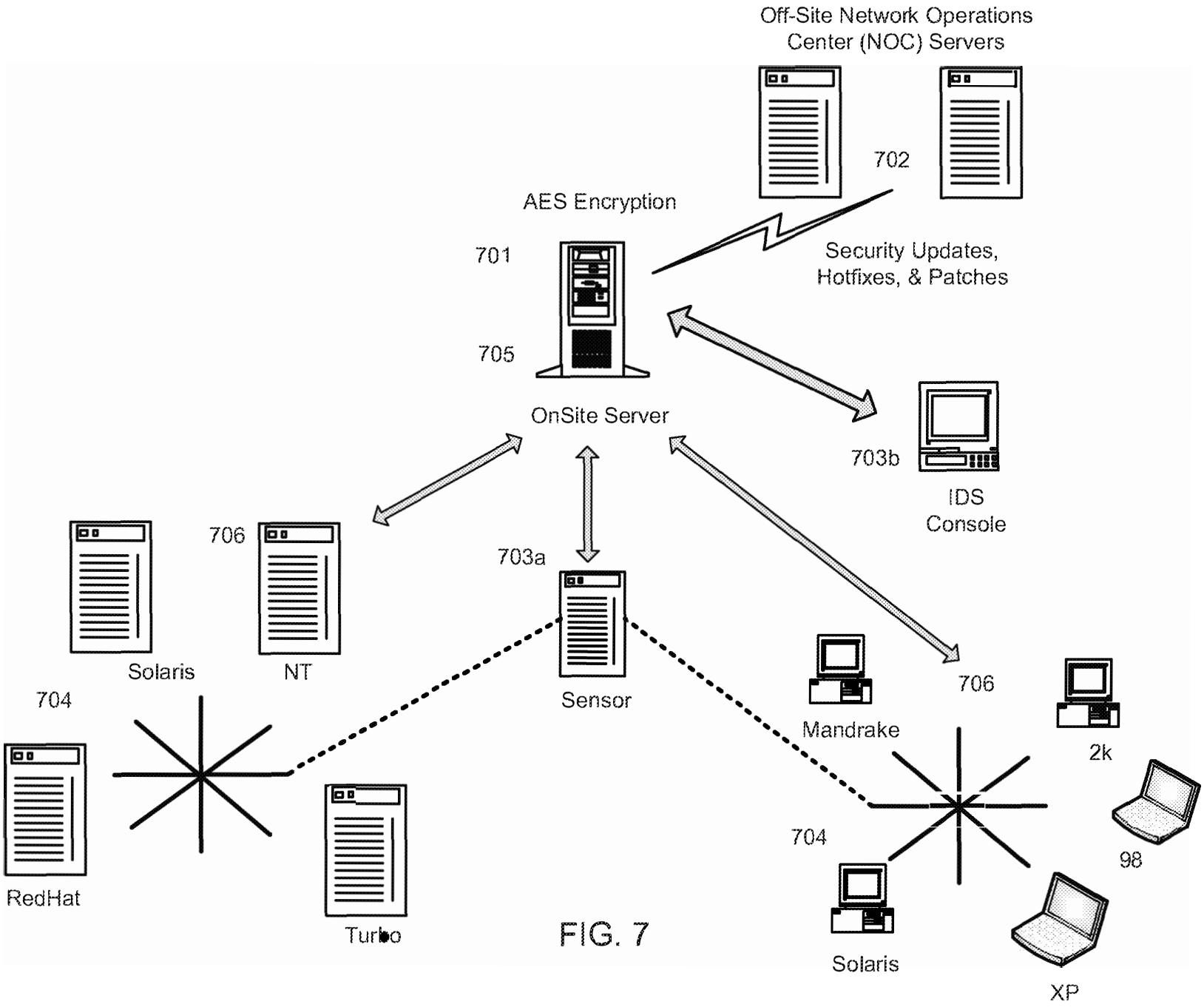


FIG. 7

ForcePoint LLC
EX-1010-PT2
Page489

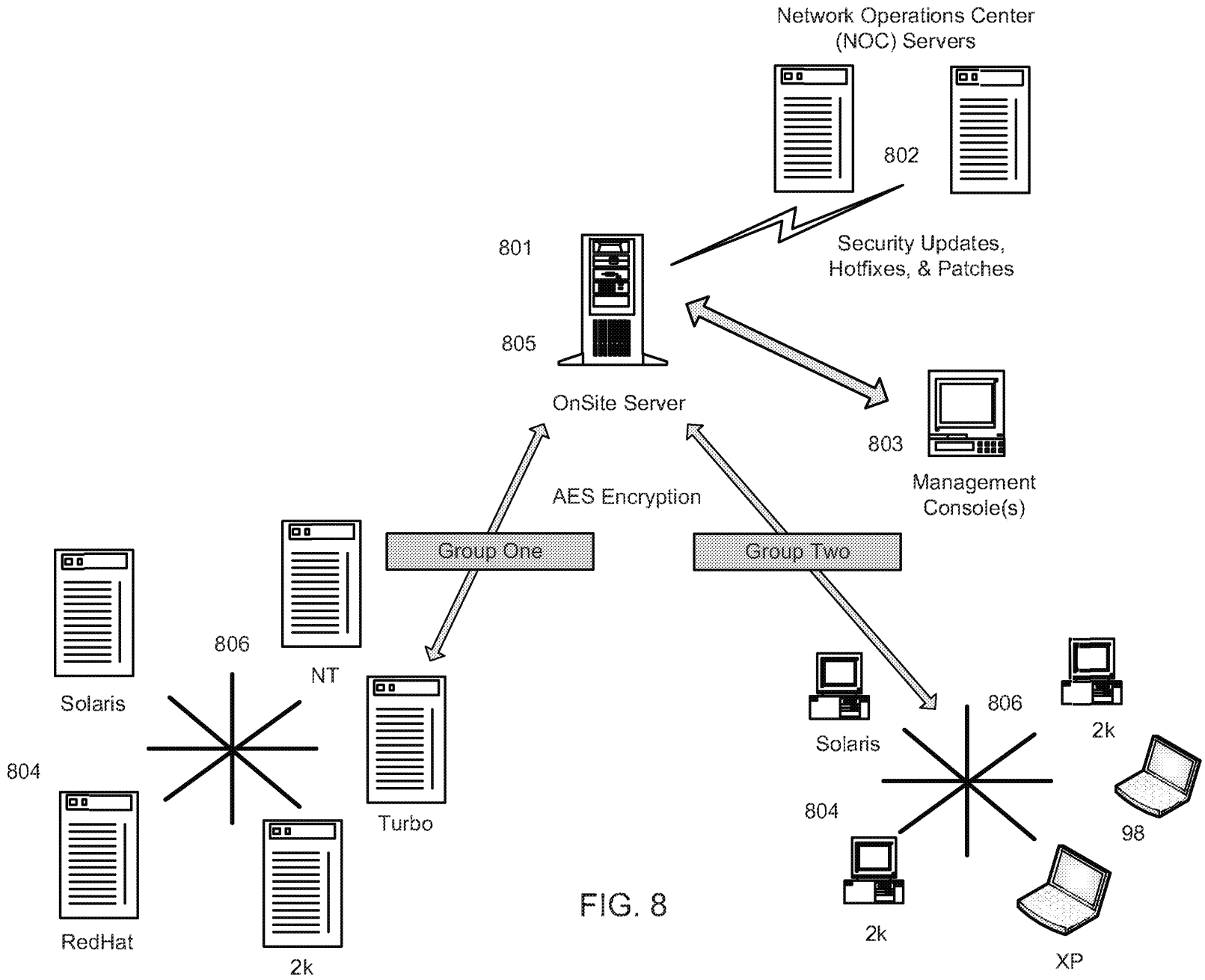


FIG. 8

ForcePoint LLC
EX-1010-PT2
Page490

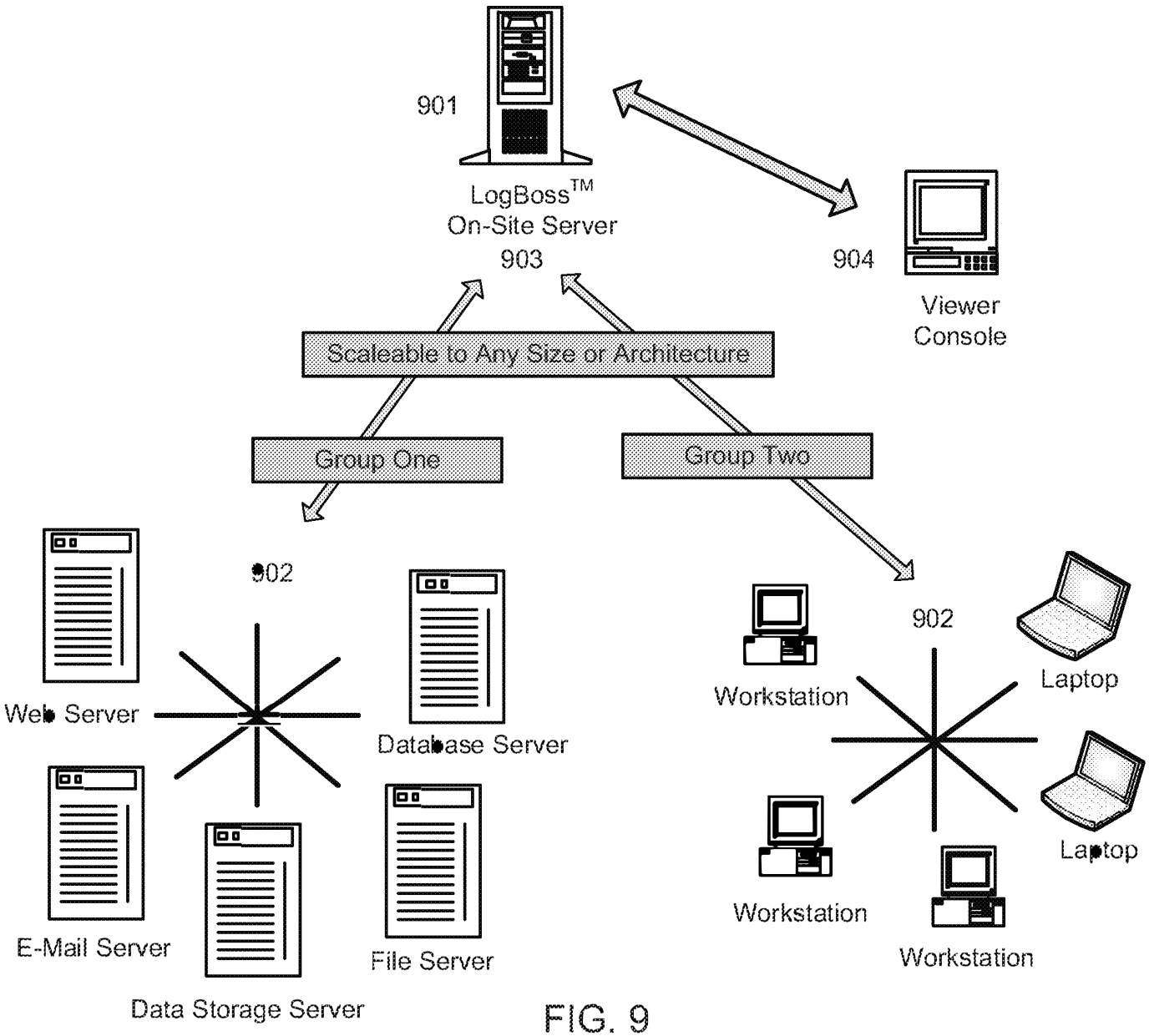


FIG. 9

ForcePoint LLC
EX-1010-PT2
Page491

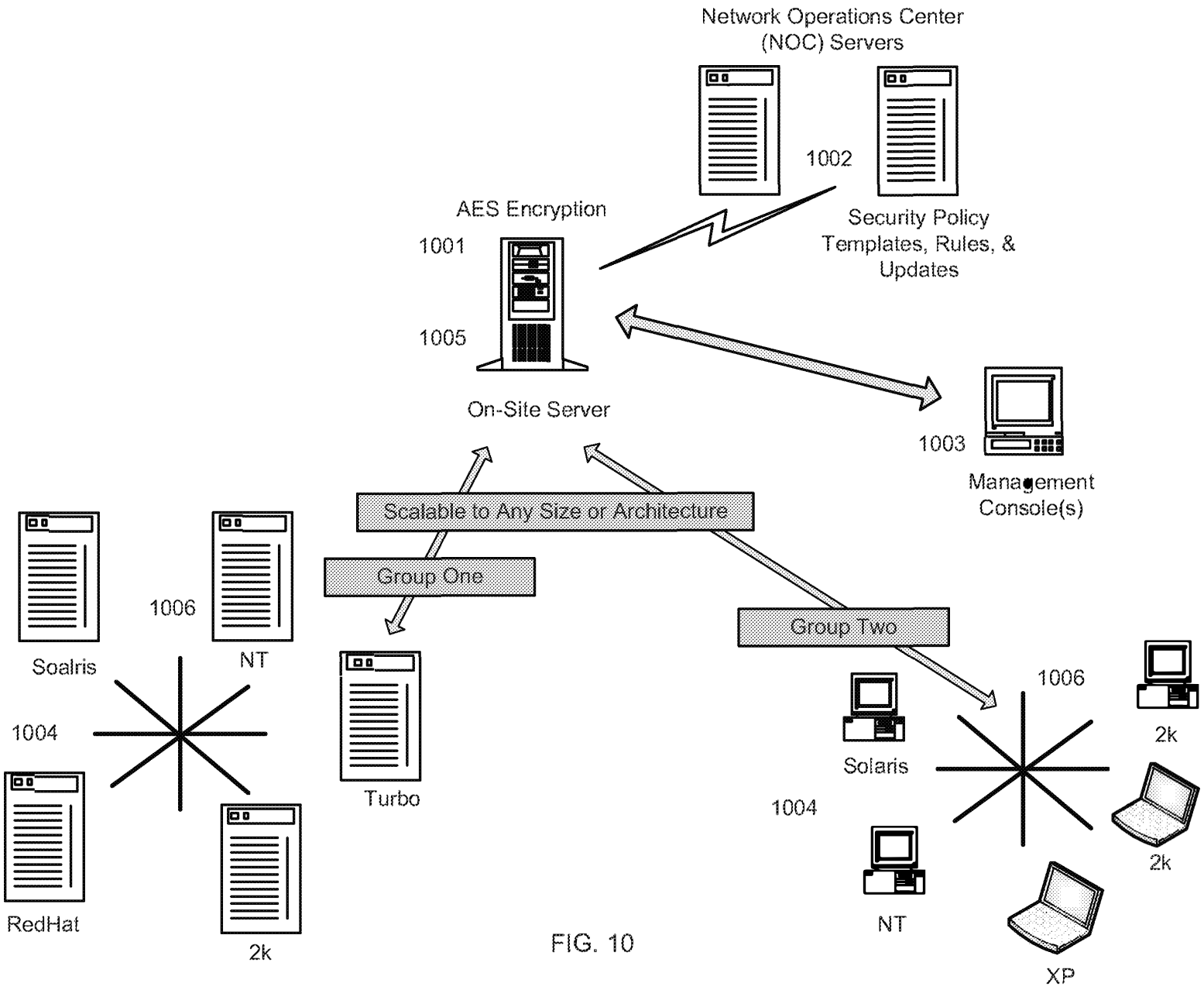


FIG. 10

ForcePoint LLC
EX-1010-PT2
Page492

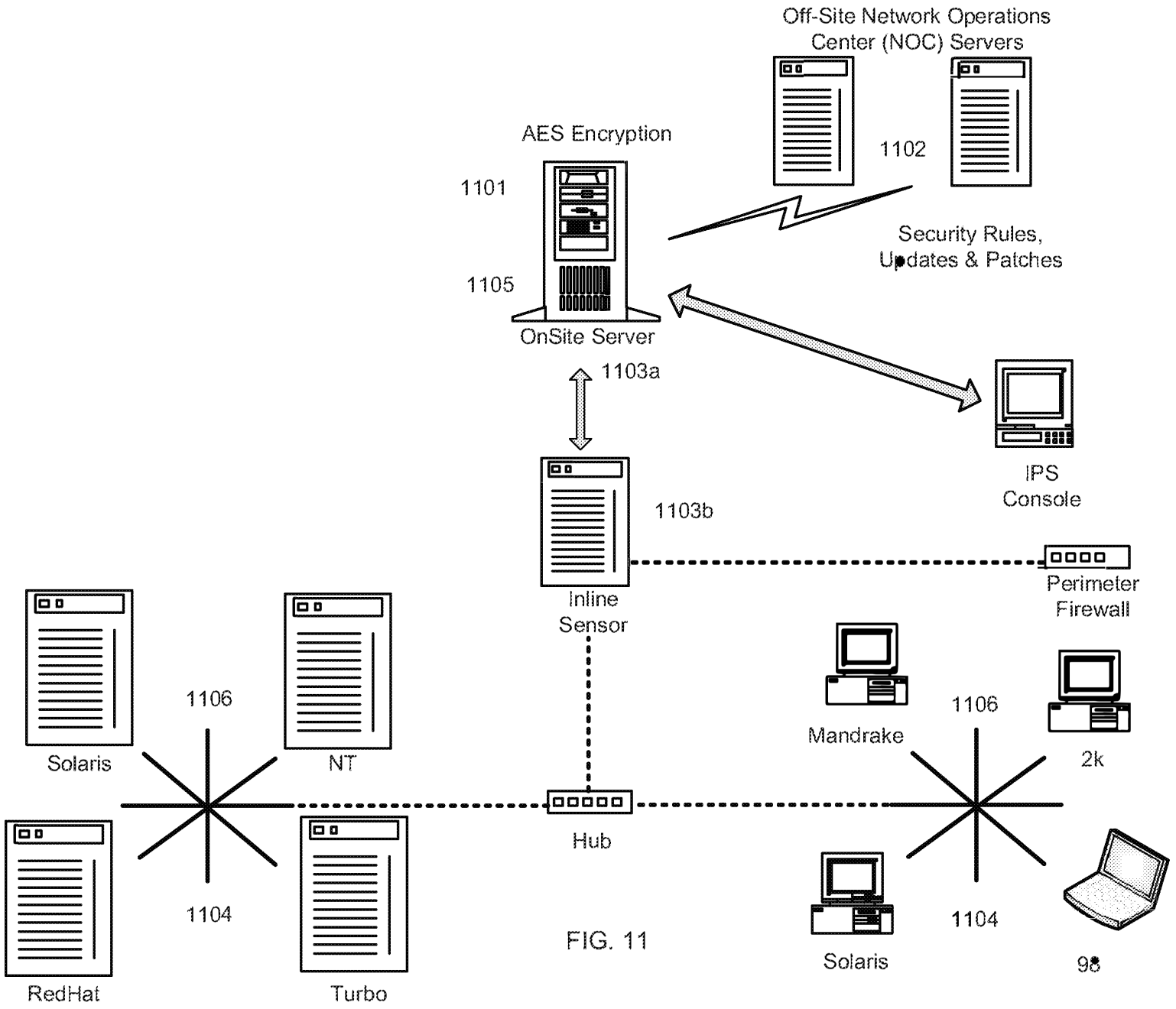


FIG. 11

ForcePoint LLC
EX-1010-PT2
Page493

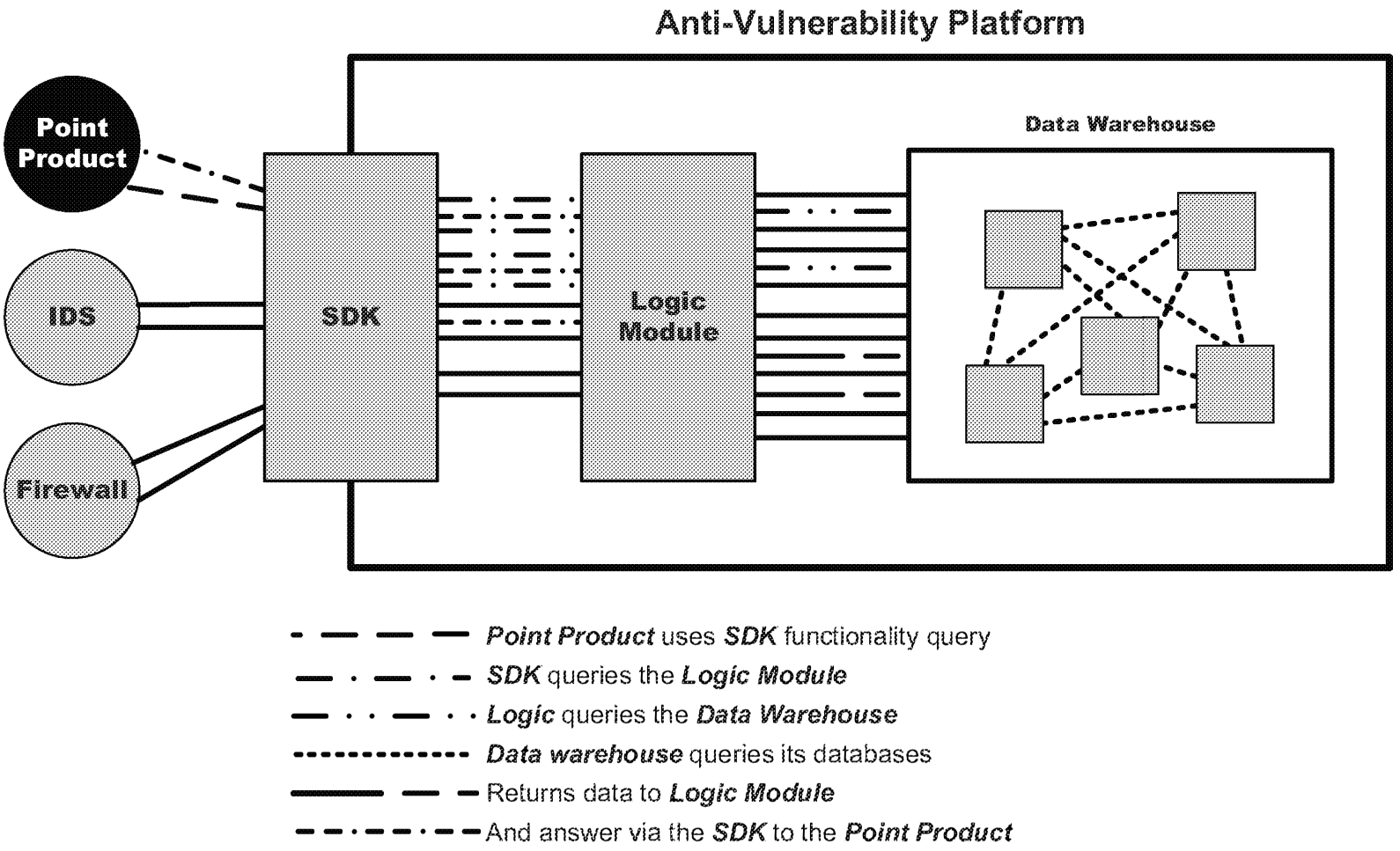


FIG. 12

ForcePoint LLC
EX-1010-PT2
Page494

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Filer:	Brian Dean Owens
Attorney Docket Number:	SP1P012A

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	70	70
Utility Search Fee	2111	1	300	300
Utility Examination Fee	2311	1	360	360
Pages:				
Claims:				
Claims in excess of 20	2202	1	40	40
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**770**

Electronic Acknowledgement Receipt	
EFS ID:	23101485
Application Number:	14816931
International Application Number:	
Confirmation Number:	1044
Title of Invention:	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION
First Named Inventor/Applicant Name:	Brett M. Oliphant
Customer Number:	127962
Filer:	Brian Dean Owens
Filer Authorized By:	
Attorney Docket Number:	SP1P012A
Receipt Date:	03-AUG-2015
Filing Date:	
Time Stamp:	18:09:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	$770
RAM confirmation Number	5253
Deposit Account	
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	SP1P012A_ADS.pdf	1561493 32626e38525a871c6c6597d9d61bc269f544d693	no	7
Warnings:					
Information:					
2	Oath or Declaration filed	SP1P012A_Declaration.pdf	64525 7ccca72d2590448880e70107bcb4d2ad48a9a7d8	no	1
Warnings:					
Information:					
3	Power of Attorney	SP1P012A_POA.pdf	218503 cd0bfa7f7f5483c306adc456b205cd1799c34b61	no	2
Warnings:					
Information:					
4	Specification	SP1P012A_Application.pdf	484437 e801f646ecfaa03a94315734080bf75202843c03	no	58
Warnings:					
Information:					
5	Drawings-only black and white line drawings	SP1P012A_Figures.pdf	171020 fac4cd4b0352133a88169c22b813039d26414655	no	12
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	36607 2d822b07c809099b44600280c8cc06c1ecfb5075	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2536585		

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/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012A
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Inventor Information:

Inventor 1 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	Brett	M.	Oliphant	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Plano	State/Province	TX	Country of Residence i	US

Mailing Address of Inventor:

Address 1	SecurityProfiling, LLC
Address 2	1919 S Shiloh Rd.

City	Garland	State/Province	TX
Postal Code	75042	Country i	US

Inventor 2 Remove

Legal Name

Prefix	Given Name	Middle Name	Family Name	Suffix
	John	P.	Blignaut	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	West Lafayette	State/Province	IN	Country of Residence i	US

Mailing Address of Inventor:

Address 1	SecurityProfiling, LLC
Address 2	1919 S Shiloh Rd.

City	Garland	State/Province	TX
Postal Code	75042	Country i	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012A
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

☐ **An Address is being provided for the correspondence Information of this application.**			
Customer Number	127962		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION		
Attorney Docket Number	SP1P012A	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Total Number of Drawing Sheets (if any)		**Suggested Figure for Publication (if any)**	

Filing By Reference :

Only complete this section when filing an application by reference under 35 U.S.C. 111(c) and 37 CFR 1.57(a). Do not complete this section if application papers including a specification and any drawings are being filed. Any domestic benefit or foreign priority information must be provided in the appropriate section(s) below (i.e., "Domestic Benefit/National Stage Information" and "Foreign Priority Information").

For the purposes of a filing date under 37 CFR 1.53(b), the description and any drawings of the present application are replaced by this reference to the previously filed application, subject to conditions and requirements of 37 CFR 1.57(a).

Application number of the previously filed application	Filing date (YYYY-MM-DD)	Intellectual Property Authority or Country

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☐ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Either enter Customer Number or complete the Representative Name section below. If both sections are completed the customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)
Customer Number	127962		

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012A
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78.
When referring to the current application, please leave the application number blank.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	Continuation of	14499230	2014-09-28
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14499237	Continuation in part of	14138014	2013-12-21
Prior Application Status	Abandoned		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
14138014	Continuation of	10882852	2004-07-01
Prior Application Status	Expired		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
10882852	Claims benefit of provisional	60484085	2003-07-01

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim priority to a foreign application. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(d). When priority is claimed to a foreign application that is eligible for retrieval under the priority document exchange program (PDX) [i] the information will be used by the Office to automatically attempt retrieval pursuant to 37 CFR 1.55(h)(1) and (2). Under the PDX program, applicant bears the ultimate responsibility for ensuring that a copy of the foreign application is received by the Office from the participating foreign intellectual property office, or a certified copy of the foreign priority application is filed, within the time period specified in 37 CFR 1.55(g)(1).

Remove

Application Number	Country [i]	Filing Date (YYYY-MM-DD)	Access Code[i] (if applicable)

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012A
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications

☐ This application (1) claims priority to or the benefit of an application filed before March 16, 2013 and (2) also contains, or contained at any time, a claim to a claimed invention that has an effective filing date on or after March 16, 2013.
NOTE: By providing this statement under 37 CFR 1.55 or 1.78, this application, with a filing date on or after March 16, 2013, will be examined under the first inventor to file provisions of the AIA.

Authorization to Permit Access:

☐ Authorization to Permit Access to the Instant Application by the Participating Offices

If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the instant patent application is filed access to the instant patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the instant patent application is filed to have access to the instant patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the instant patent application with respect to: 1) the instant patent application-as-filed; 2) any foreign application to which the instant patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the instant patent application; and 3) any U.S. application-as-filed from which benefit is sought in the instant patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing this Authorization.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012A
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Applicant 1 Remove

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

Clear

◉ Assignee	○ Legal Representative under 35 U.S.C. 117	○ Joint Inventor
○ Person to whom the inventor is obligated to assign.	○ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name	SecurityProfiling, LLC		
Mailing Address Information:			
Address 1	1919 S Shiloh Rd.		
Address 2			
City	Garland	**State/Province**	TX
Country i	US	Postal Code	75042
Phone Number		Fax Number	
Email Address			

Additional Applicant Data may be generated within this form by selecting the Add button. Add

Assignee Information including Non-Applicant Assignee Information:

Providing assignment information in this section does not subsitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Assignee 1

Complete this section if assignee information, including non-applicant assignee information, is desired to be included on the patent application publication . An assignee-applicant identified in the "Applicant Information" section will appear on the patent application publication as an applicant. For an assignee-applicant, complete this section only if identification as an assignee is also desired on the patent application publication.

Remove

If the Assignee or Non-Applicant Assignee is an Organization check here. ☐

PTO/AIA/14 (12-13)
Approved for use through 01/31/2014. 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 contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	SP1P012A
	Application Number	
Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION	

Prefix	**Given Name**	Middle Name	**Family Name**	Suffix

Mailing Address Information For Assignee including Non-Applicant Assignee:

Address 1			
Address 2			
City		**State/Province**	
Country i		Postal Code	
Phone Number		Fax Number	
Email Address			

Additional Assignee or Non-Applicant Assignee Data may be generated within this form by selecting the Add button. Add

Signature:

Remove

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications

Signature	/Brian Owens/			Date (YYYY-MM-DD)	2015-08-03
First Name	Brian	Last Name	Owens	Registration Number	55517

Additional Signature may be generated within this form by selecting the Add button. Add

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/AIA/01 (06-12)
Approved for use through 01/31/2014. 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.

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76)

Title of Invention	COMPUTER PROGRAM PRODUCT AND APPARATUS FOR MULTI-PATH REMEDIATION

As the below named inventor, I hereby declare that:

This declaration is directed to:

- [■] The attached application, or
- [ ] United States application or PCT international application number _____

  filed on _____.

The above-identified application was made or authorized to be made by me.

I believe that I am the original inventor or an original joint inventor of a claimed invention in the application.

I hereby acknowledge that any willful false statement made in this declaration is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.

WARNING:

Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available.

LEGAL NAME OF INVENTOR

Inventor: Brett M. Oliphant Date (Optional) :_____

Signature: _____

Note: An application data sheet (PTO/SB/14 or equivalent), including naming the entire inventive entity, must accompany this form or must have been previously filed. Use an additional PTO/AIA/01 form for each additional inventor.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 1 minute 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.

SCORE Placeholder Sheet for IFW Content

Application Number: 14816931 Document Date: 08/03/2015

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings – Other than Black and White Line Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions below.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface.
- Other USPTO employees can bookmark the current SCORE URL (http://Score.uspto.gov/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces.

Form Revision Date: September 30, 2013