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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 October 2002 (24.10.2002)

PCT

(10) International Publication Number
WO 02/084942 A1

(51) International Patent Classification[7]: H04L 9/00, G06F 11/30

(21) International Application Number: PCT/US02/12042

(22) International Filing Date: 15 April 2002 (15.04.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/283,587 13 April 2001 (13.04.2001) US

(71) Applicant: **NOKIA, INC.** [US/US]; 6000 Connection Drive, Irving, TX 75039 (US).

(72) Inventor: **SCOTT, Robert, Paxton**; 1220 N. Fair Oaks Avenue, #1311, Sunnyvale, CA 94089 (US).

(74) Agent: **BRANCH, John, W.**; Merchant & Gould P.C., P.O. Box 2903, Minneapolis, MN 55402-0903 (US).

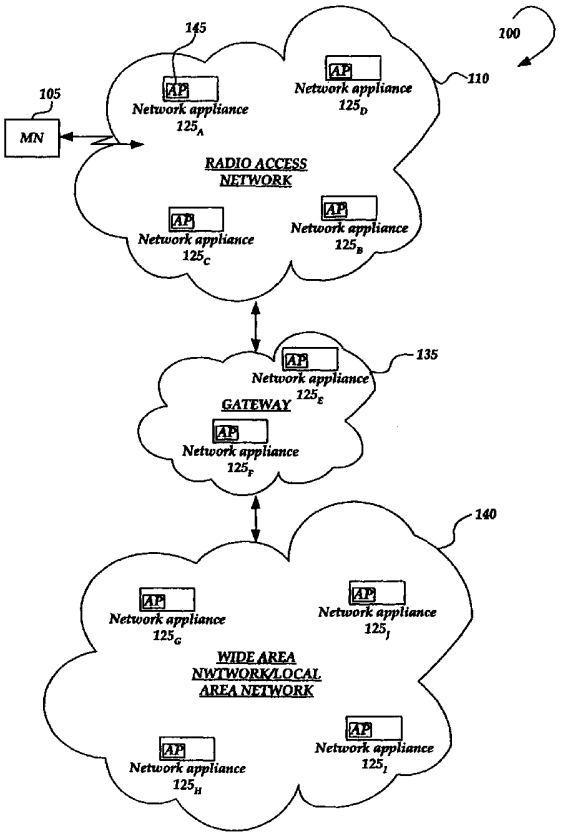
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, 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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEMS AND METHOD FOR PROTECTING NETWORK APPLIANCES AGAINST SECURITY BREACHES



(57) Abstract: The present invention is directed to a system (100) and method for protecting a network appliance (125a-j) against a security breach. The network appliance (125a-j) is protected by an appliance protector (145) component that resides within the network appliance (125a-j). The appliance protector (145) protects the network appliance (125a-j) by monitoring processes for a valid signature and terminating processes with an invalid signature.

WO 02/084942 A1

— *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.

SYSTEM AND METHOD FOR PROTECTING NETWORK APPLIANCES AGAINST SECURITY BREACHES

This application is being filed as a PCT International Patent Application in the name of Nokia Inc., a U.S. national corporation and resident, on 15 April 2002, designating all countries except the US, and claiming priority to U.S. Serial No. 60/283,587 filed 13 April 2001.

Field of the Invention

This invention relates generally to providing security to a network, and more particularly to protecting network appliances against security breaches.

Background of the Invention

In recent years, there has been a dramatic upsurge in the popularity of electronic communication in business and home applications. The number of networks and the volume of data continue to increase at a rapid rate. To cope with the ever-increasing demand for faster, more secure and more far-reaching networks, a variety of network appliances are being used to meet these demands.

As useful as they are, however, network appliances are vulnerable to hijacking or corruption. A security breach could inhibit or disrupt the intended function of a network appliance. Even worse, a security breach may disrupt an entire network in which the network appliance is installed. Network appliances do not have a readily available user interface for a system administrator to interact with it. As a result, it is difficult for a system administrator to ascertain whether a network appliance has been compromised.

Even when an interface with the network appliance is established, the active participation of a system administrator is required to adequately protect the network appliance from being invaded by unauthorized processes. Manual intervention on the part of the administrator knowledgeable in the detailed operation of the network appliance is often required to detect and repair security breaches and misappropriation of resources. It is with respect to these considerations and others that the present invention has been made.

Summary of the Invention

The present invention is directed at addressing the above-mentioned shortcomings, disadvantages and problems, and will be understood by reading and studying the following specification.

According to one aspect of the invention, a method for protecting a network appliance against a security breach on a network appliance is provided. A process executing on the network appliance is monitored for a valid signature. The current signature of the process is determined and is compared with an expected signature. If the signature is not valid, the process is terminated.

In accordance with another aspect of the invention, an encrypted response is sent to the process when the signature is valid.

In accordance with yet another aspect of the invention, the current signature is determined by sending an initiation signal and receiving the current signature from the process through a communication channel.

In accordance with still another aspect of the invention, a process associated with a process list is started and monitored for a valid signature.

In accordance with a still further aspect of the invention, a method of communicating between two processes associated with a network appliance is provided. The first process sends an initiation signal. In response to the initiation signal, the second process sends a signature to the first process.

In accordance with another aspect of the invention, a network appliance containing a computer medium encoded with components is provided. The components may be employed to implement the method described above.

Brief Description of the Drawings

FIGURE 1 shows an exemplary network system in which the invention may operate;

FIGURE 2 illustrates a schematic diagram of the various locations at which a network appliance may be coupled to a network;

FIGURE 3 illustrates a schematic diagram that shows an exemplary network appliance;

FIGURE 4 illustrates a block diagram of components of a network appliance that implement this invention;

FIGURE 5 illustrates a schematic diagram of an exemplary data store for an appliance protector;

FIGURE 6A illustrates a schematic diagram of communications between an appliance protector and an AP-aware process;

FIGURE 6B illustrates a schematic diagram of communications between an appliance protector and an AP-unaware process;

FIGURE 7 illustrates a general overview of a process that may be implemented by an appliance protector to protect a network appliance;

FIGURE 8 illustrates a block diagram of a process that may be implemented by an appliance protector to monitor an AP process for a valid signature;

FIGURE 9 illustrates a block diagram of a process that may be implemented by an appliance protector to monitor for failed AP processes;

FIGURE 10 illustrates a block diagram of a process that may be implemented by an AP-aware process to interact with an appliance protector; and

FIGURE 11 illustrates a block diagram of a process that may be implemented by an appliance protector to monitor for updates; in accordance with aspects of the invention.

Detailed Description of the Preferred Embodiment

In the following detailed description of exemplary embodiments of the invention, reference is made to the accompanied drawings, which form a part hereof, and which is shown by way of illustration, specific exemplary embodiments of which the invention may be practiced. Each embodiment is 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 other changes may be made, without departing from the spirit or 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.

Throughout the specification and claims, the following terms take the meanings explicitly associated herein, unless the context clearly dictates otherwise. The term "coupled" means either a direct connection between the items connected, or an indirect connection through one or more passive or active intermediary

devices. The term "network device" means a device that is coupled to a network. The term "network appliance" means a computing device that is coupled to a network and is designed to perform at least one function relating to the network. The term "process" means one or more tasks that may be performed by a computing device. The term "appliance protector" refers to a process that protects a network appliance against a security breach. The term "AP process" means a process that executes on a network appliance and is monitored by an appliance protector. AP process includes AP-aware process as well as AP-unaware process. AP-aware processes are processes executing on a network appliance that may directly communicate with an appliance protector. AP-unaware processes are AP processes executing on a network appliance that are not able to directly communicate with an appliance protector.

Briefly, the present invention is directed to a system and method for protecting a network appliance against a security breach. The network appliance is protected by an appliance protector component that may reside within the network appliance. The appliance protector protects the network appliance by monitoring processes for a valid signature and terminating processes with an invalid signature. The appliance protector also starts, updates, and restarts processes that execute on the network appliance.

Illustrative Operating Environment

With reference to FIGURE 1, an exemplary network system in which the invention may operate is illustrated. As shown in the figure, exemplary network system 100 includes mobile node (MN) 105, radio access network (RAN) 110, gateway 135, network appliance 125_{A-J} and wide area network (WAN)/local area network (LAN) 140.

MN 105 is coupled to RAN 110. Generally, MN 105 may include any device capable of connecting to a wireless network such as RAN 110. Such devices include cellular telephones, smart phones, pagers, radio frequency (RF) devices, infrared (IR) devices, integrated devices combining one or more of the preceding devices, and the like. MN 105 may also include other devices that have a wireless interface such as Personal Digital Assistants (PDAs), handheld computers, personal computers, multiprocessor systems, microprocessor-based or

programmable consumer electronics, network PCs, wearable computers, and the like.

RAN 110 transports information to and from devices capable of wireless communication, such as MN 105. RAN 110 may include both wireless and wired components. For example, RAN 110 may include a cellular tower that is linked to a wired telephone network. Typically, the cellular tower carries communication to and from cell phones, pagers, and other wireless devices, and the wired telephone network carries communication to regular phones, long-distance communication links, and the like. RAN 110 may include network devices, such as network appliances 125_{A-D}, as shown in the figure.

Network appliances 125_{A-D} may include computer devices such as routers, switches, hardware firewalls, content filters, file servers, network traffic load balancers, hubs, and the like. Because network appliances 125_{A-D} are coupled to a network, they are vulnerable to security breaches, such as invasion by unauthorized processes. As a security measure, an appliance protector 145 may be executing in network appliances 125_{A-D} to protect the appliances against security breaches. Appliance protector 145 will be discussed in more detail in conjunction with FIGURE 3. Briefly stated, appliance protector 145 ensures that a network appliance does not operate when a security breach is detected.

RAN 110 is coupled to WAN/LAN 140 through gateway 135. Gateway 135 routes information between RAN 110 and WAN/LAN 140. For example, a mobile node, such as MN 105, may request access to the Internet by calling a certain number or tuning to a particular frequency. Upon receipt of the request, RAN 110 is configured to pass information between MN 105 and gateway 135. Gateway 135 may translate requests from MN 105 to a specific protocol, such as hypertext transfer protocol (HTTP) messages, and then send the messages to WAN/LAN 140. Gateway 135 translates responses to such messages into a form compatible with the requesting mobile node. Gateway 135 may also transform other messages sent from MN 105 into information suitable for WAN/LAN 140, such as e-mail, audio, voice communication, contact databases, calendars, appointments, and the like. As shown in the figure, gateway 135 may include network devices, such as network appliances 125_{E-F} that may contain an appliance protector.

WAN/LAN 140 is an IP packet based backbone network that transmits information between computing devices. One example of WAN is the Internet. An example of a LAN is a network used to connect computers in an office or a home. A WAN may connect multiple LANs. As shown in the figure, WAN/LAN 140 may include network devices, such as network appliances 125_{G-J} that may also contain an appliance protector.

Communication links within LANs typically include twisted wire pair, fiber optics, or coaxial cable, while communication links between networks may utilize analog telephone lines, full or fractional dedicated digital lines including T1, T2, T3, and T4, Integrated Services Digital Networks (ISDNs), Digital Subscriber Lines (DSLs), wireless links, or other communications links.

Network system 100 may include many more components than those shown in FIGURE 1. However, the components shown are sufficient to disclose an illustrative embodiment for practicing the present invention.

The media used to transmit information in the communication links as described above illustrates one type of computer-readable media, namely communication media. Generally, computer-readable media includes any media that can be accessed by a computing device. Communication media typically embodies computer-readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism and includes any information delivery media. The term "modulated data signal" means a signal that has one or more of its characteristics set or changed in such a manner as to encode information in the signal. By way of example, communication media includes wired media such as twisted pair, coaxial cable, fiber optics, wave guides, and other wired media and wireless media such as acoustic, RF, infrared, and other wireless media.

FIGURE 2 shows a schematic diagram of exemplary locations at which a network appliance may be coupled to a network. Illustrated are network appliances 230_{A-G} that are installed at various points relative to exemplary network 210. To prevent security breaches, network appliances 230_{A-G} may be protected by appliance protector 250.

As shown in the figure, network appliances, such as network appliances 230_{A-C}, may be part of the infrastructure of network 210. According to

one embodiment, network appliances 230_{A-C} may be routers. Routers are intermediary devices on a communications network that expedite message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over available routes. Routers may be a simple computing device or a complex computing device. For example, a router may be a computer including memory, processors, and network interface units.

Network appliance 230_D is coupled to network 210 and links network 210 to other networks (not shown). Network appliance 230_D may be a router, a gateway, switch, or other device that links networks.

Network appliance 230_E connects network 210 with computer 240 and network appliance 230_F. Network appliance 230_E may be a hub, a router, a network traffic load balancer or similar device. Network appliance 230_E may also have hardware and software components that allow network appliance 230_E to service network 210, such as serving as a filter, a firewall, etc. Computer 240 may be any network device that allows direct access by a user, such as a personal computer, workstations, TV, phone, etc. Network appliances 230_{F-G} may be any network appliance at the end point of a network connection, such as a network printer, file server, etc.

FIGURE 3 illustrates a schematic diagram that shows an exemplary network appliance. Network appliance 300 may include many more components than those shown in FIGURE 3. However, the components shown are sufficient to disclose an illustrative embodiment for practicing the present invention.

As shown in FIGURE 3, network appliance 300 may be coupled to RAN 105 or WAN/LAN 140, or other communications network, via network interface unit 310. Network interface unit 310 includes the necessary circuitry and protocols for connecting network appliance 300 to RAN 105 or WAN/LAN 140. Typically, there is one network interface unit 310 provided for each network connecting to network appliance 300.

Network appliance 300 also includes processing unit 312, and a mass memory, all connected via bus 322. The mass memory generally includes RAM 316, ROM 332, and optionally, one or more permanent mass storage devices, such as hard disk drive 328, a tape drive, CD-ROM/DVD-ROM drive, and/or a floppy

disk drive. The mass memory stores operating system 320 for controlling the operation of network appliance 300. This component may comprise a general purpose operating system 320 as is known to those of ordinary skill in the art, such as UNIX, LINUX™, Microsoft WINDOWS NT®, and the like. Alternatively, the operating system may be specialized to support the specific functions of network appliance 300.

The mass memory as described above illustrates another type of computer-readable media, namely computer storage media. Computer storage media may include volatile and nonvolatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules or other data. Examples of computer storage media include RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired information and which can be accessed by a computing device.

The mass memory also stores program code and data for appliance protector 330, and other programs 334 such as programs that enable network appliance 300 to perform its functions. Appliance protector program 330 protects network appliance 300 from security breaches by starting, monitoring, restarting, terminating, and updating processes that execute on network appliance 300.

Appliance Protector

FIGURE 4 shows exemplary components of a network appliance. As illustrated, the figure shows an appliance protector (AP) 400 that interacts with data store 410, AP-aware processes 415, AP-unaware processes 420, invalid processes 425, update process 430, action and event log 435, alert notifier 440, and operating system 445.

AP 400 is a component of a network appliance, such as network appliance 300. AP 400 provides protection against security breaches by monitoring all AP processes on a network appliance for a valid signature. AP processes include AP-aware processes 415 as well as AP-unaware processes 420. According to one embodiment of the invention, AP 400 starts all AP processes on the network

appliance. In addition, AP 400 monitors for updates on its functionality as well as for updates on AP processes.

AP 400 executes at a higher priority than the other processes on a network appliance. The higher execution priority enables AP 400 to start, restart, monitor and, if necessary, terminate AP processes.

Data store 410 contains information used by AP 400. The information in data store 410 may be recorded by AP 400, update process 430, operating system 445, and other components of a network appliance. The information stored in data store 410 will be discussed in detail in conjunction with FIGURE 5. Briefly stated, the information in data store 410 includes rules for starting and interacting with AP processes that execute on a network appliance.

AP-aware processes 415 do not execute on a network appliance without an appliance protector also executing. Even if an appliance protector is executing, the survival of an AP-aware process in a network appliance depends on whether the AP-aware process has properly interacted with the appliance protector and whether it has the proper signature.

Like AP-aware processes 415, AP-unaware processes 420 are monitored by AP 400. Briefly stated, AP 400 monitors AP-unaware processes 420 to ensure that they are authorized and are properly executing (See FIGURE 6B).

Invalid processes 425 are processes that are unauthorized. An invalid process may be an AP-aware process, an AP-unaware process, or some other unauthorized process. When AP 400 determines that an invalid process is executing on a network appliance, AP 400 terminates the invalid process.

Update process 430 is a process that is used to update AP 400 or any AP process executing on a network appliance. According one embodiment of the invention, update process 430 has a higher execution priority than AP 400. Thus, when update process 430 is executing, AP 400 acts as instructed by update process 430. The procedure for updating AP 400 and AP processes will be discussed in detail in conjunction with FIGURE 11. Briefly stated, update process 430 instructs AP 400 to terminate processes that require an update, update the affected AP processes, and restart the AP processes when the update is completed.

Action and event log 435 is a data store that contains a record of events and actions taken by AP 400. The events and actions stored may include

status information relating to starting and restarting of AP processes, and information relating to the failing of AP processes, the termination of invalid processes, the updating of processes, and the like.

Alert notifier 440 sends alert notifications when a predetermined event has occurred. According to one embodiment, the notifications are sent to a system administrator. AP 400 may instruct alert notifier 440 to send an alert notification to a system administrator when a predetermined action or event has occurred.

Operating system 445 oversees operations of the network appliance. Operating system 445 may provide access to AP 400 for obtaining information about AP processes. Operating system 445 may provide process status information relating to AP processes through a process monitor.

FIGURE 5 illustrates a schematic diagram of an exemplary data store for an appliance protector, such as data store 410 shown in FIGURE 4. Data store 500 stores information that may be used by an appliance protector. As illustrated, data store 500 includes process list 510, process signatures 515, encryption data 520, starting rules 525 and updating rules 530.

Process list 510 includes AP processes that are authorized to be executing on a network appliance. AP processes listed in process list 510 are started by an appliance protector. Process list 510 may be updated by an update process, such as update process 430, as shown in FIGURE 4.

Process signatures 515 are identification data associated with AP processes. The identification data in process signatures 515 may include process identification, version information, status information, and other information related to each AP process. Status information of an AP process may include parameters related to the execution of the process, such as memory usage, run time, etc. Process signatures 515 are used to determine whether an AP process is authorized to execute on a network appliance.

Starting rules 525 are rules that instruct an appliance protector to start AP processes. The starting of AP processes will be discussed in detail in conjunction with FIGURE 8. Briefly stated, an appliance protector uses starting rules 525 to start all AP processes that are included in process list 510.

Updating rules 530 are rules that instruct an appliance protector to interact with an update process. Updating rules 530 may instruct the appliance protector to terminate itself or any one of the AP processes for updating.

Encryption data 520 enables an appliance protector to securely communicate with AP-aware processes. Encryption data 520 may include data used for encrypting information, such as public and private keys.

FIGURE 6A illustrates a schematic diagram of communications between an appliance protector and an AP-aware process. Appliance protector 600 and AP-aware process 605 interact with each other through communications that include initiation signal 610, connection 615, signature 620, encrypted response 625, and termination command 630. Appliance protector 600 monitors AP-aware process 605 for valid signature. The appliance protector may respond to AP-aware process 605 if the signature is valid or terminate AP-aware process 605 if the signature is invalid.

Initiation signal 610 initiates communication between appliance protector 600 and AP-aware process 605. Initiation signal 610 may be broadcasted to all processes executing on a network appliance. AP-aware processes may recognize and respond to initiation signal 610.

Connection 615 is a communication channel initiated by AP-aware process 605 for connecting to appliance protector 600. Connection 615 may employ any type of communication protocols, such as Transmission Control Protocol (TCP)/Internet Protocol (IP).

Signature 620 is data related to AP-aware process 605 that is sent to appliance protector 600 by AP-aware process 605. Signature 620 may include process identification, version information, status information, and other relevant data. Appliance protector 600 uses signature 620 to determine whether AP-aware process 605 is authorized to execute on the network appliance.

Encrypted response 625 is encrypted data sent to AP-aware process 605 by appliance protector 600 after signature 620 has been determined to be valid. Encrypted response is encrypted with encryption data 520. Encrypted response 625 is received and decrypted by AP-aware process 605.

Termination command 630 is a command that may be sent by appliance protector 600 to terminate AP-aware process 605. Appliance protector

may send termination command 630 to AP-aware process 605 if signature 620 has been determined to be invalid. Termination command 630 terminates AP-aware process 605.

FIGURE 6B illustrates a schematic diagram of communications between an appliance protector and an AP-unaware process. Appliance protector 600 monitors AP-unaware process 640 by obtaining signature 650 from process monitor 645. Appliance protector 600 may terminate AP-unaware process 640 if signature 650 has been determined to be invalid.

Process monitor 645 is a component of a network appliance that obtains information associated with processes executing on the network appliance. Process monitor 645 may be a part of the network appliance's operating system, such as operating system 445, or an independent process. As shown in the figure, process monitor 645 obtains signature 650 of AP-unaware process 640. Signature 650 may include process identification, version information, memory usage, run time, etc. Appliance protector 600 may obtain signature 650 from process monitor 645.

Termination command 655 may be sent by appliance protector 600 to terminate AP-unaware process 640. Appliance protector 600 may send termination command 650 to AP-unaware process 640 if signature 650 has been determined to be invalid.

FIGURE 7 illustrates a general overview of a process that may be implemented by an appliance protector to protect a network appliance, according to one embodiment of the invention. Process 700 begins at a start block and flows to block 710 where AP processes are started by the appliance protector. According to one embodiment of the invention, the appliance protector is started automatically by the operating system of a network appliance. The appliance protector starts the AP processes when it has begun executing. According to one embodiment, the appliance protector determines which AP processes to start by referring to a process list.

Moving to block 720, the AP processes are monitored by the appliance protector for a valid signature. A valid signature is a signature that matches a known signature stored in a data store associated with the appliance

protector. Depending on whether the signature is valid, the AP processes being monitored may receive an encrypted response or be terminated (See FIGURE 8).

Process 700 then flows to block 730 where the appliance protector monitors for failed AP processes. Briefly stated, the appliance protector may restart a failed AP process, record the event, and send an alert notice (See FIGURE 9).

Moving to block 740, the appliance protector monitors for updates on its functionality as well as for updates on AP processes. Briefly stated, the appliance protector interacts with an update process, which performs the update. The appliance protector may terminate processes to facilitate the updating (See FIGURE 11).

According to one embodiment of the invention, monitoring of AP processes for valid signature in block 720 and monitoring of failed AP processes in block 730 are repeated at predetermined intervals. Monitoring intervals for one process may be different than those of another process. According to another embodiment of the invention, the intervals for monitoring coincide with the clock speed of the network appliance. According to yet another embodiment of the invention, the interval for monitoring is ten times a second. The process then flows to an end block and returns to processing other actions.

FIGURE 8 illustrates a block diagram of a process 800 that may be implemented by an appliance protector to monitor an AP process for a valid signature. After a start block, process 800 flows to block 805, where a determination is made as to whether the AP process being monitored is an AP aware process or an AP unaware process. Transitioning to block 810, the appliance protector determines the current signature of the AP process being monitored. The appliance protector may determine the signature from the AP process if the AP process is an AP-aware process that is capable of presenting its signature. Alternatively, process 800 may determine the signature of the AP process from a process monitor if the AP process is either an AP-unaware process or incapable of sending its signature to the appliance protector.

Next, process 800 moves to block 820 where the appliance protector determines the expected signature for the AP process. The appliance protector may determine the expected signature from a data store associated with the appliance protector. According to one embodiment of the invention, the appliance protector

may use the process identification in the current signature to search in the data store for an expected signature with the same process identification. If the data store does not contain any expected signature with a process identification that matches the process identification in the current signature, then there is no expected signature for the AP process.

Process 800 then advances to block 830 where a determination is made as to whether the signature is valid by comparing the current signature and the expected signature. A signature is valid when the contents of the current signature and the contents of the expected signature match. If no expected signature is found, the current signature is invalid.

When the signature of the AP process is valid, process 800 moves to block 850 where an encrypted response is sent to the AP process if the AP process is an AP-aware process. The encrypted response may be created using encryption data. The encrypted response may indicate that the appliance protector validated the signature of the AP process. The encrypted response is received and decrypted by the AP-aware process. The process then flows to an end block.

When the signature of the AP-process is invalid, process 800 moves to block 840 where the appliance protector terminates the AP process. The process then flows to an end block and returns to processing other actions.

FIGURE 9 illustrates a block diagram of a process 900 that may be implemented by an appliance protector to monitor for failed AP processes. At a start block, process 900 moves to block 910 where a determination is made as to whether there are failed AP processes. When there are no failed AP processes, process 900 flows to an end block.

When there are failed AP processes, process 900 moves to block 920 where the appliance protector restarts the failed AP processes. The appliance protector may refer to rules for starting AP processes.

Process 900 then advances to block 930 where the events associated with the restarting may be logged and stored in a data store. Alert notice may also be sent to a system administrator, or some other device. The process then flows to an end block and returns to processing other actions.

FIGURE 10 illustrates a block diagram of a process 1000 that may be implemented by an AP-aware process to interact with an appliance protector. After a start block, process 1000 flows to decision block 1010.

At decision block 1010, a determination is made as to whether a successful connection to the appliance protector can be established when an AP-aware process receives an initiation signal broadcasted by the appliance protector. In one embodiment of the invention, if an AP-aware process does not receive an initiation signal after a predetermined period of time, the AP-aware process will terminate itself (Not shown). When a successful connection may not be established, the process moves to block 1030 where the AP-aware process terminates itself and the process flows to an end block.

When a connection can be established, then process 1000 advances to block 1015 where the AP-aware process establishes a connection with and sends its signature to the appliance protector. When the signature is valid, process 1000 then moves to block 1020 where the AP-aware process receives an encrypted response from the appliance protector and decrypts the response. When the signature is not valid, the AP-aware process will be terminated by the appliance protector (Not shown).

At block 1025, a determination is made as to whether the response from the appliance protector is valid. If so, process 1000 ends. If the response is not valid, then process 1000 moves to block 1030 and the AP-aware process terminates itself. The process then flows to an end block and returns to processing other actions.

FIGURE 11 illustrates a block diagram of a process 1100 that may be implemented by an appliance protector to monitor for updates. After a start block, process 1100 moves to block 1110. At block 1110, the appliance protector establishes a connection with the update process. Process 1100 then moves to block 1115 where a message about the update from the update process is received. The message may contain information on which processes are to be updated.

Next, process 1100 advances to decision block 1120 where a determination is made as to whether the update message is authenticated. When the update message is not authenticated, then process 1100 moves to block 1125 where the appliance protector will terminate the update process if authorized to do so (e.g.

having a higher priority). Then, at block 1130, the event is logged and an alert notice is sent. The process then flows to an end block.

When the update message is authenticated, process 1100 moves to block 1135 where the appliance protector determinates which AP processes will be updated. Then, at decision block 1140, a determination is made as to whether the appliance protector is to be updated. If so, then process 1100 advances to block 1145 where the appliance protector terminates all processes that are executing.

At block 1150, the update process updates the appliance protector. The update process may do so by putting updated data in a data store associated with the appliance protector. Process 1100 then moves to block 1155 where the appliance protector restarts. Then, process 1100 continues at block 1165.

Returning to decision block 1140, when the appliance protector is not to be updated, then the appliance protector also moves to 1160. At block 1160, the appliance protector terminates the AP processes that are to be updated. Then, process 1100 also continues at block 1165.

At block 1165, AP processes are updated by the update process. Process 1100 then moves to block 1170 where the AP processes terminated due to the updating are restarted by the appliance protector. The process then flows to an end block and returns to processing other actions.

The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WHAT IS CLAIMED IS:

1. A method for protecting a network appliance against a security breach, comprising:

determining when an AP process is an AP aware process;

determining when the AP process is an AP unaware process;

determining a current signature for the AP process executing on the network appliance;

determining an expected signature for the AP process;

comparing the current signature with the expected signature; and

terminating the AP process when the current signature and expected signature do not match.

2. The method in Claim 1, further comprising, sending an encrypted response to the AP aware process when the current signature and expected signature match.

3. The method in Claim 1, wherein determining the current signature further comprises:

sending an initiation signal; and

receiving the current signature from the AP process through a communication channel.

4. The method in Claim 3, wherein the communication channel uses a TCP/IP protocol.

5. The method in Claim 1, wherein determining the current signature further comprises; receiving the current signature from a process monitor when the AP process has been determined to be an AP unaware process.

6. The method in Claim 1, wherein the current signature and the expected signature comprises identification data associated with the AP process.

7. The method of Claim 6, wherein the identification data is selected from process identification, version information, memory usage, and run time data, associated with the AP process.

8. The method in Claim 1, wherein comparing the current signature with the expected signature occurs at predetermined intervals.

9. The method in Claim 8, wherein the predetermined intervals relate to a clock speed of the network appliance.

10. The method in Claim 1, further comprising determining when the process fails, and when, restarting the process.

11. The method of Claim 1, further comprising receiving an update message; and when the update message has been received: terminating the AP process; updating the AP process; and restarting the AP process.

12. A method for protecting a process on a network appliance against a security breach, comprising:

starting the process on the network appliance when the process is listed in a process list;

determining a current signature of the process;

determining an expected signature for the process;

determining when the signature is valid by comparing the current signature with the expected signature;

when the signature is not valid, terminating the process, otherwise, sending an encrypted response to the process.

13. The method of Claim 12, further comprising determining when the process fails, and when the process fails restarting the process.

14. The method of Claim 12, further comprising receiving an update message, and in response to receiving the update message updating the process.

15. The method of Claim 12, wherein updating the process further comprises:

terminating the process;

updating the process; and

restarting the updated process when the update is complete.

16. A network appliance, comprising:

a processor and a computer-readable medium;

an operating environment executing on the processor from the computer-readable medium;

a network interface unit arranged to communicate with a network;

a data store including an expected signature for a process; and

an appliance protector program executing under the control of the operating system and operative to perform actions, including: determining a current signature of the process, determining the expected signature of the process, determining when the signature is valid by comparing the current signature with the expected signature, and, when the signature is determined to not be valid, terminating the process.

17. The network appliance of Claim 16, wherein the data store further comprises a process list; and wherein the appliance protector program starts processes listed within the process list.

18. The network appliance of Claim 16, wherein the data store further comprises encryption data; and when the appliance protector program determines when the signature is valid, the appliance protector sends a response that is encrypted using the encryption data.

19. The network appliance of Claim 16, further comprising an update process; wherein the update process updates the process.

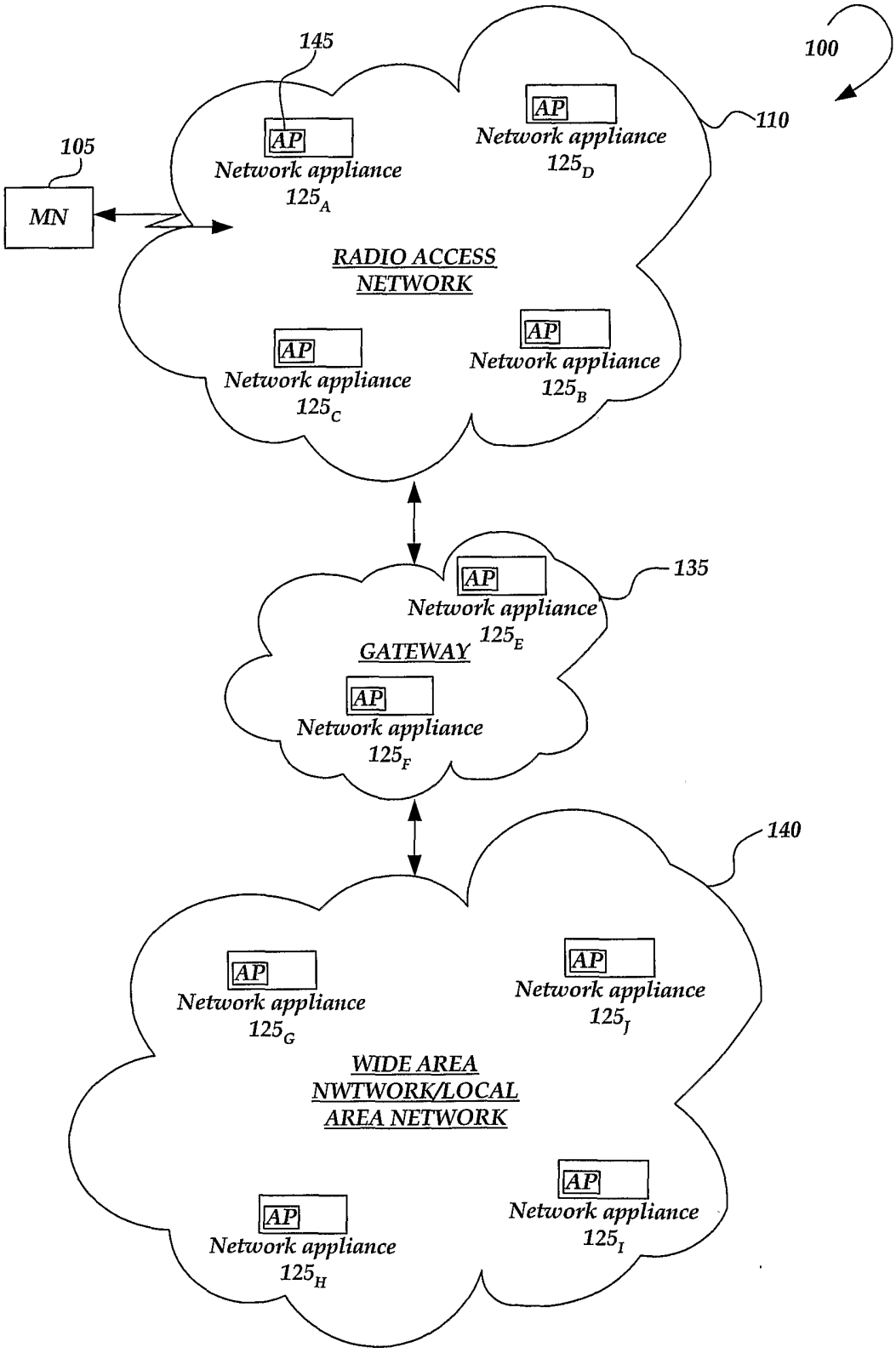

100
145
110
105
MN
AP
Network appliance
125_A
AP
Network appliance
125_D
RADIO ACCESS
NETWORK
AP
Network appliance
125_C
AP
Network appliance
125_B
135
AP
Network appliance
125_E
GATEWAY
AP
Network appliance
125_F
140
AP
Network appliance
125_G
AP
Network appliance
125_J
WIDE AREA
NWTWORK/LOCAL
AREA NETWORK
AP
Network appliance
125_H
AP
Network appliance
125_I

Fig. 1

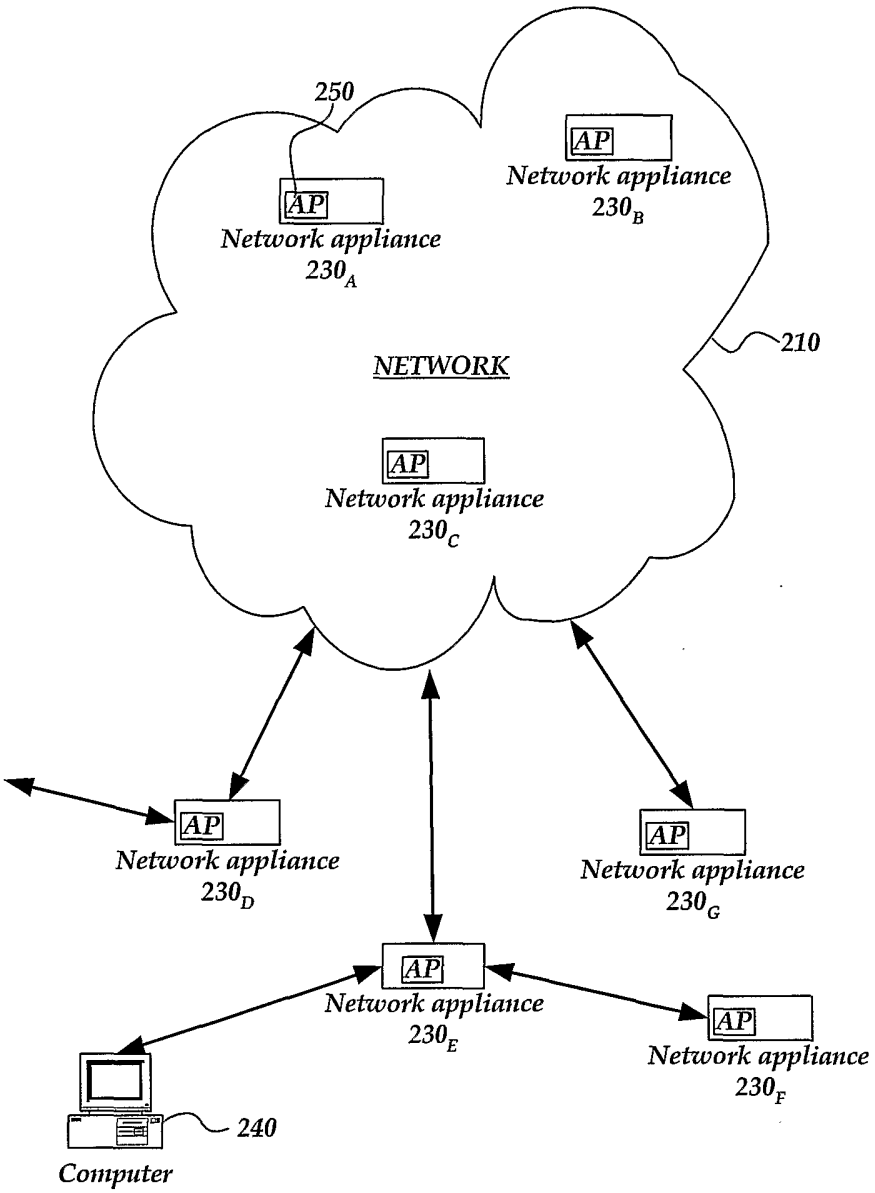

250
AP
Network appliance
230A
AP
Network appliance
230B
210
NETWORK
AP
Network appliance
230C
AP
Network appliance
230D
AP
Network appliance
230E
AP
Network appliance
230F
AP
Network appliance
230G
240
Computer

Fig. 2

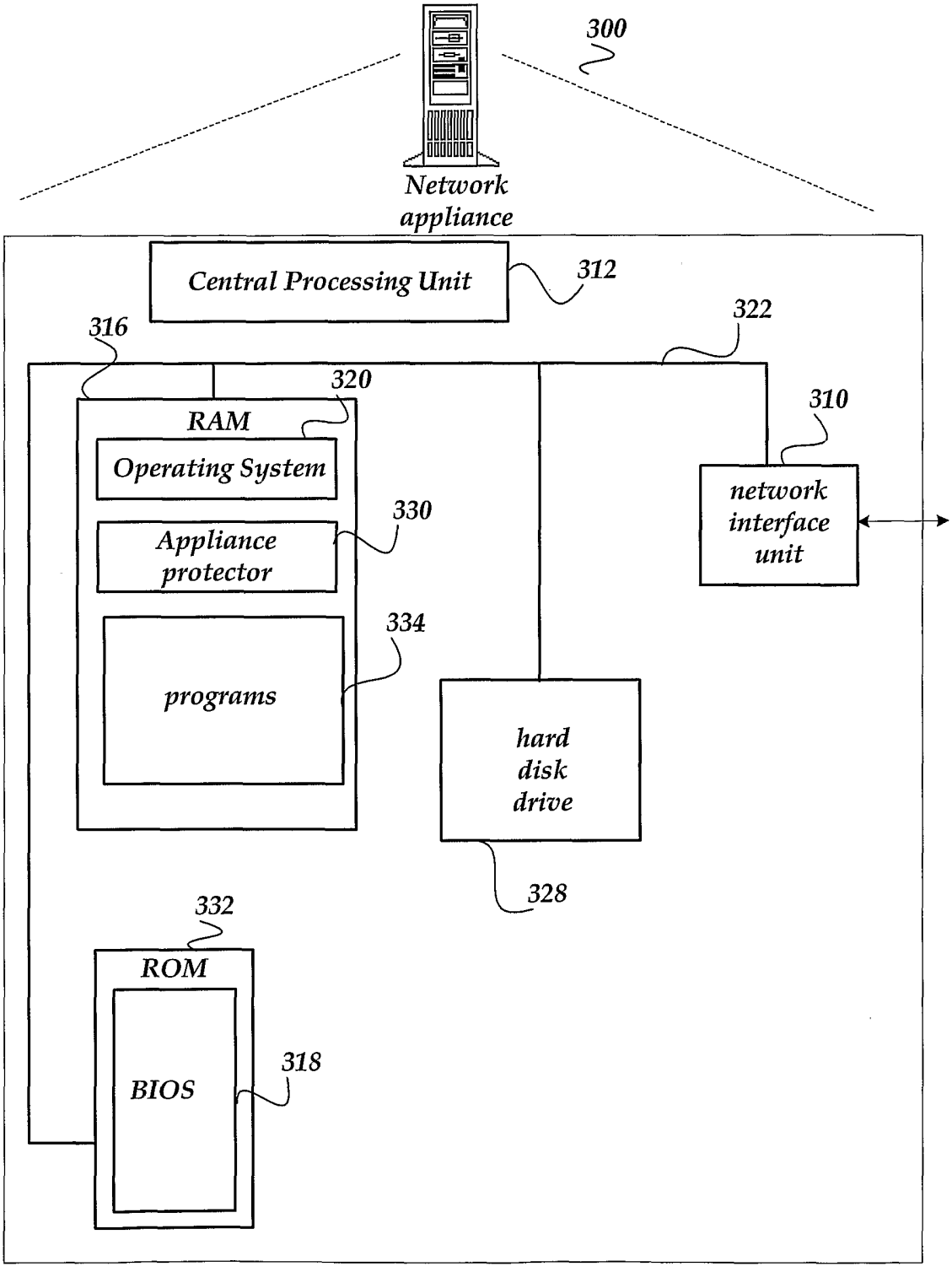

300
Network appliance
Central Processing Unit
312
316
322
320
RAM
Operating System
310
network interface unit
330
Appliance protector
334
programs
hard disk drive
328
332
ROM
BIOS
318

Fig. 3

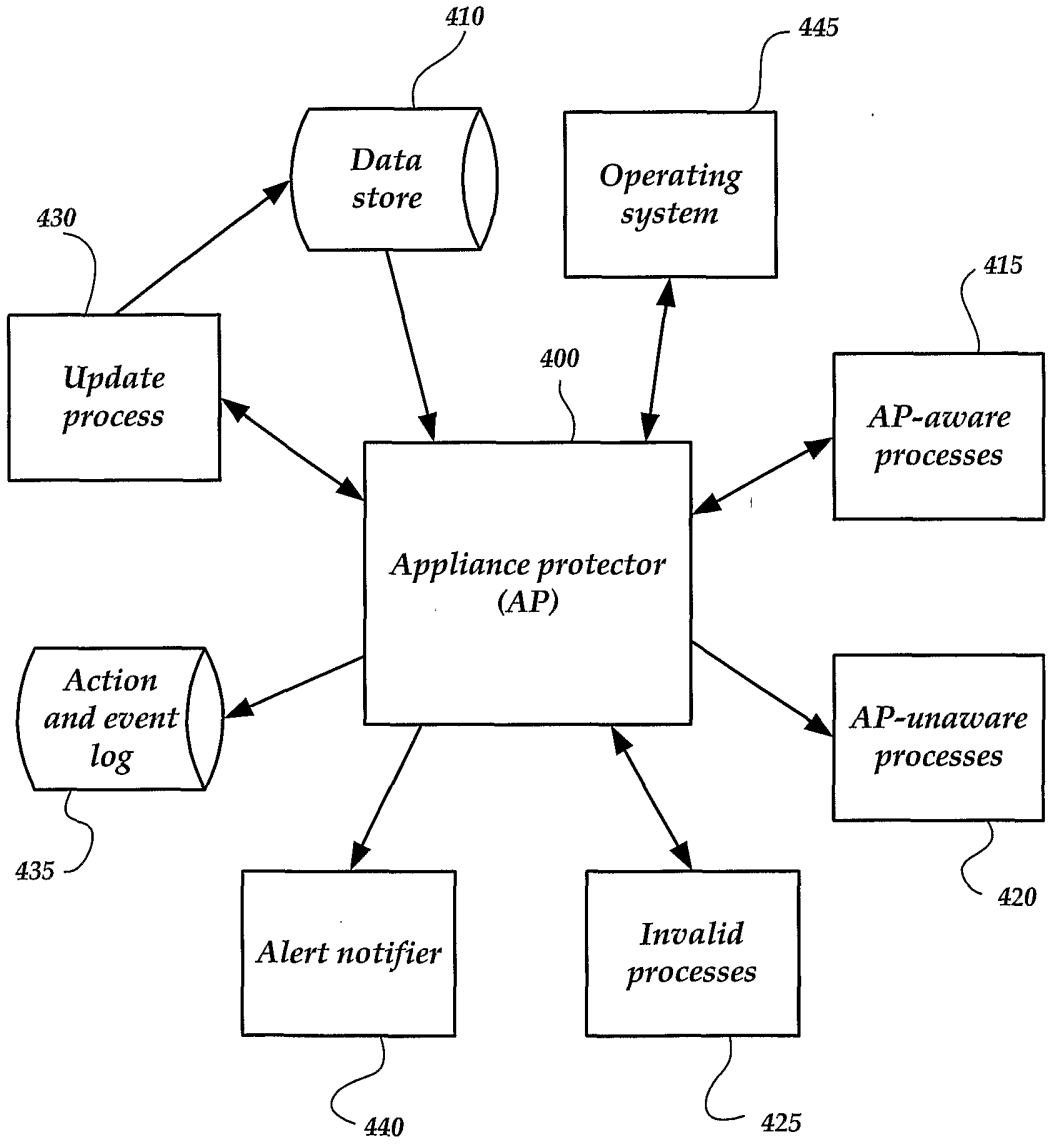

410
445
Data store
Operating system
430
415
Update process
400
AP-aware processes
Appliance protector (AP)
Action and event log
AP-unaware processes
435
420
Alert notifier
Invalid processes
440
425

Fig. 4

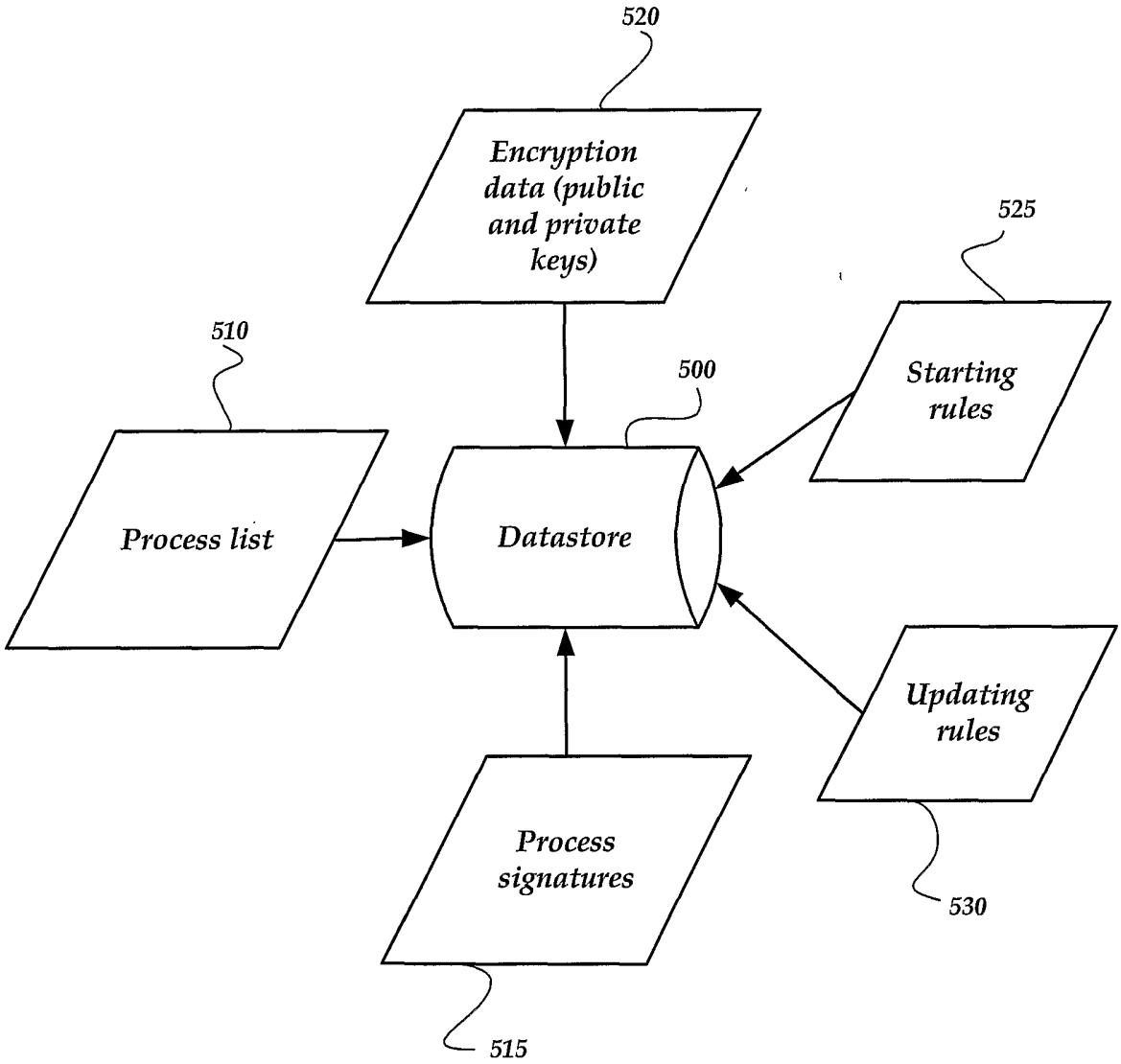

520
Encryption data (public and private keys)
525
Starting rules
510
500
Process list
Datastore
Updating rules
Process signatures
530
515

Fig. 5

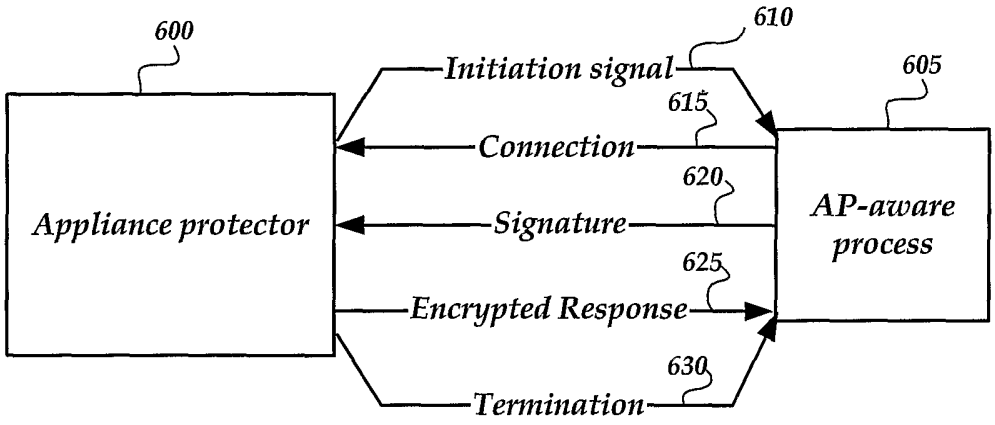

600
610
Initiation signal
605
615
Connection
620
Signature
AP-aware process
Appliance protector
625
Encrypted Response
630
Termination

Fig. 6A

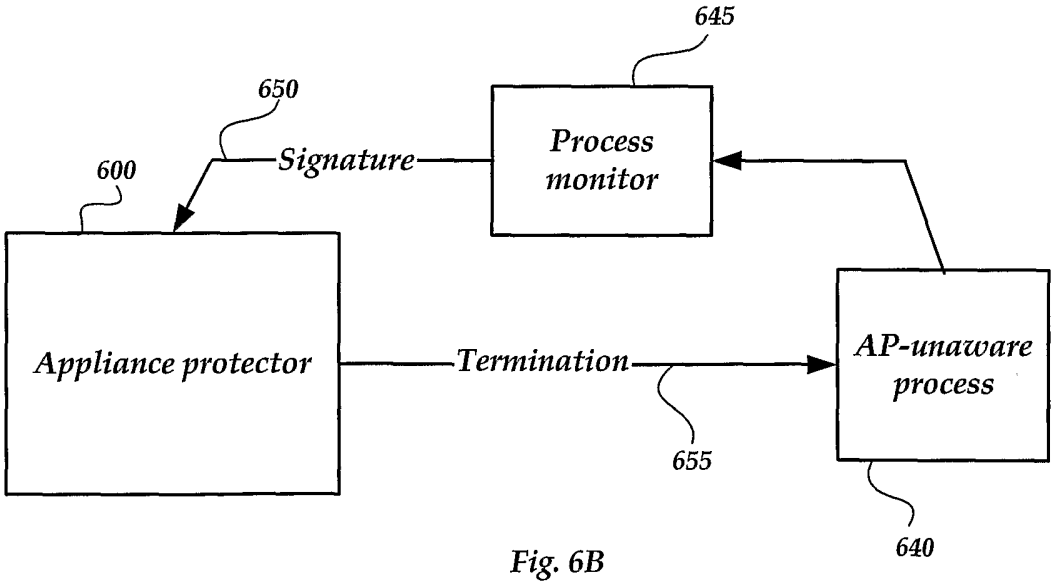

645
650
Signature
Process monitor
600
Appliance protector
Termination
AP-unaware process
655
640

Fig. 6B

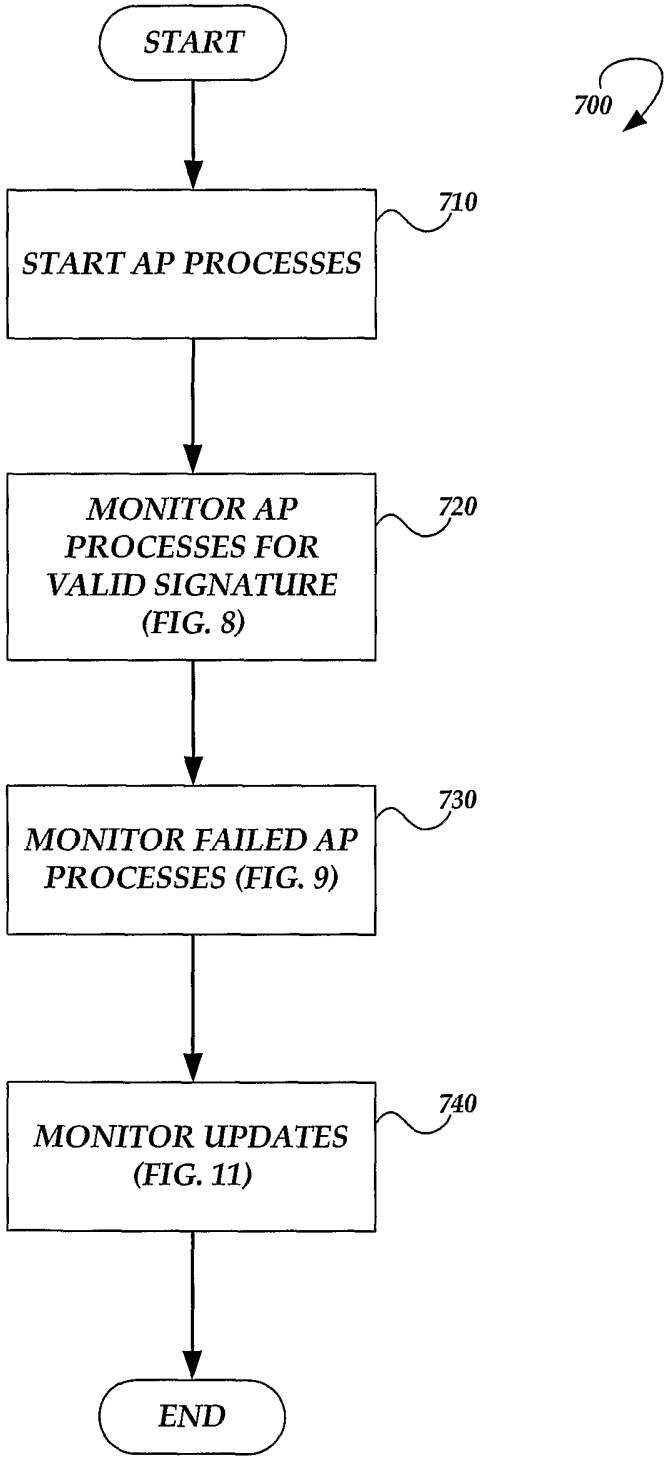

START
700
710
START AP PROCESSES
720
MONITOR AP PROCESSES FOR VALID SIGNATURE (FIG. 8)
730
MONITOR FAILED AP PROCESSES (FIG. 9)
740
MONITOR UPDATES (FIG. 11)
END

Fig. 7

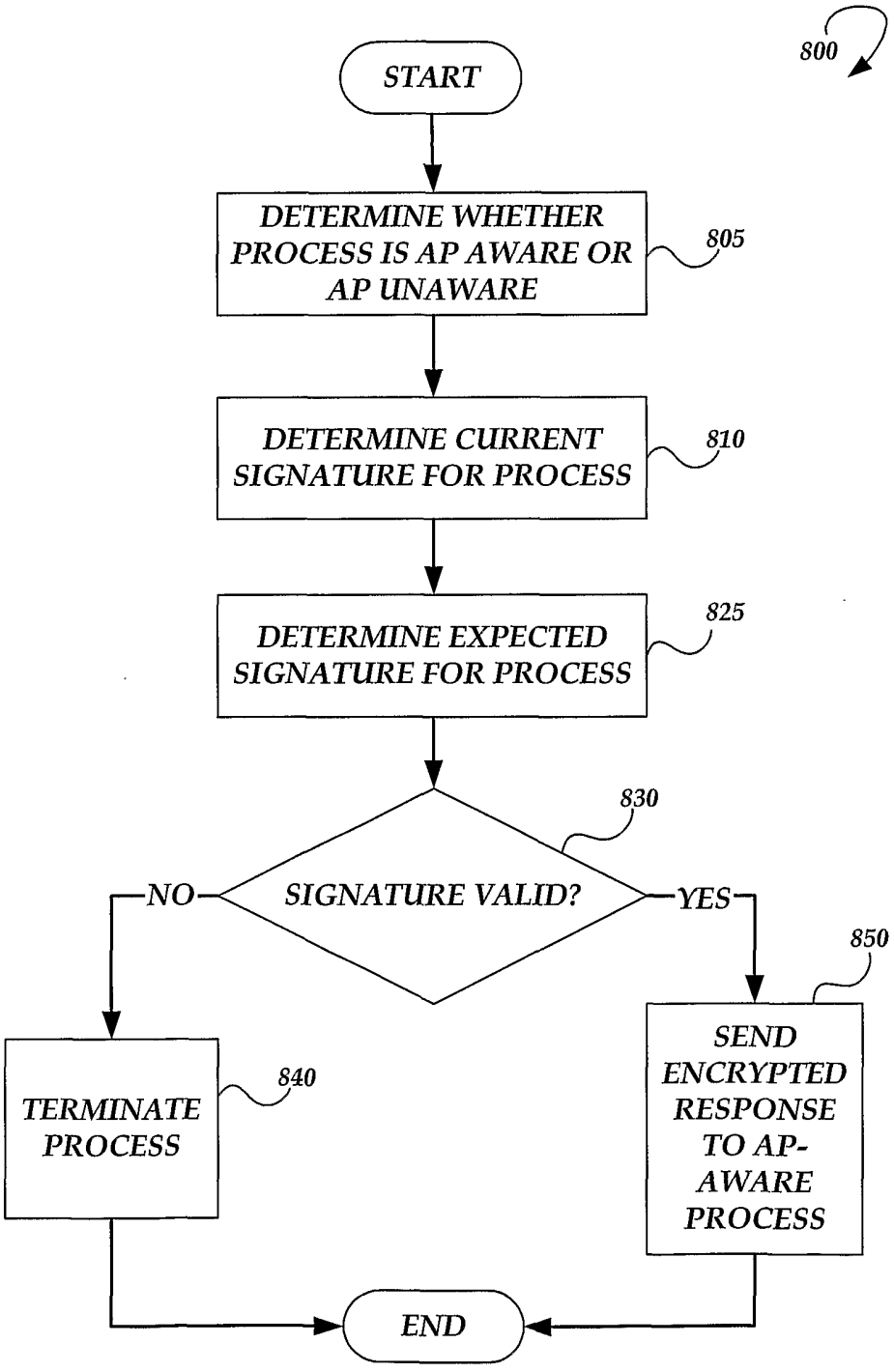

800
START
DETERMINE WHETHER PROCESS IS AP AWARE OR AP UNAWARE
805
DETERMINE CURRENT SIGNATURE FOR PROCESS
810
DETERMINE EXPECTED SIGNATURE FOR PROCESS
825
830
SIGNATURE VALID?
NO
YES
850
SEND ENCRYPTED RESPONSE TO AP-AWARE PROCESS
TERMINATE PROCESS
840
END

Fig. 8

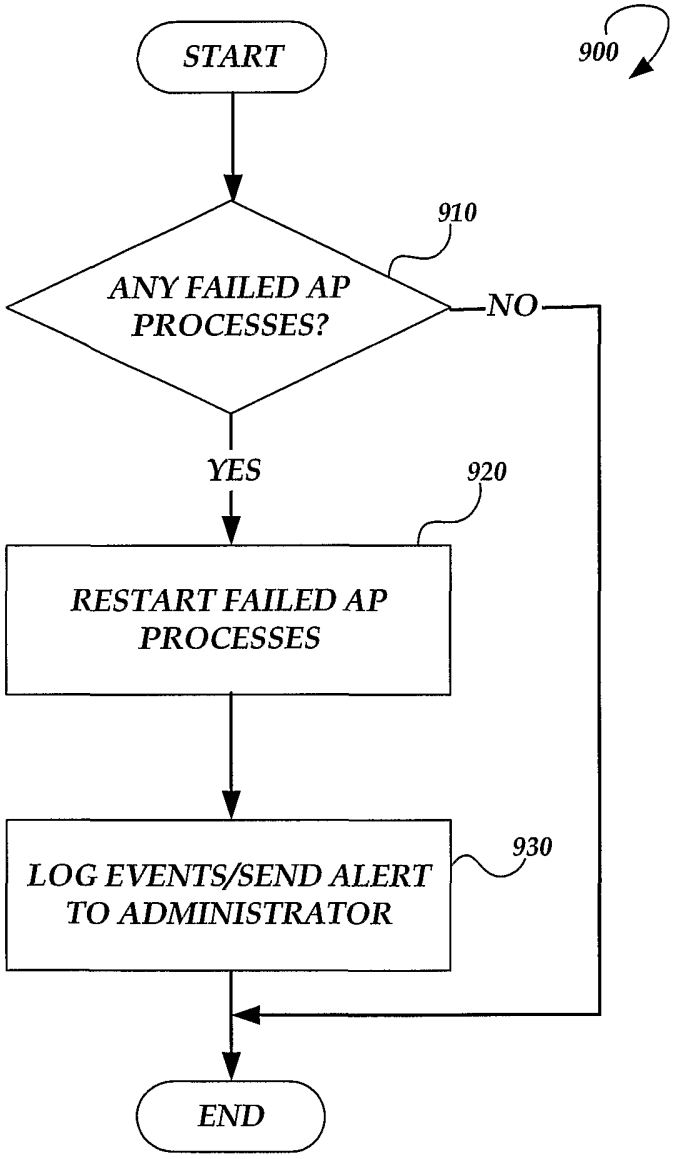

START
900
910
ANY FAILED AP PROCESSES?
NO
YES
920
RESTART FAILED AP PROCESSES
930
LOG EVENTS/SEND ALERT TO ADMINISTRATOR
END

Fig. 9

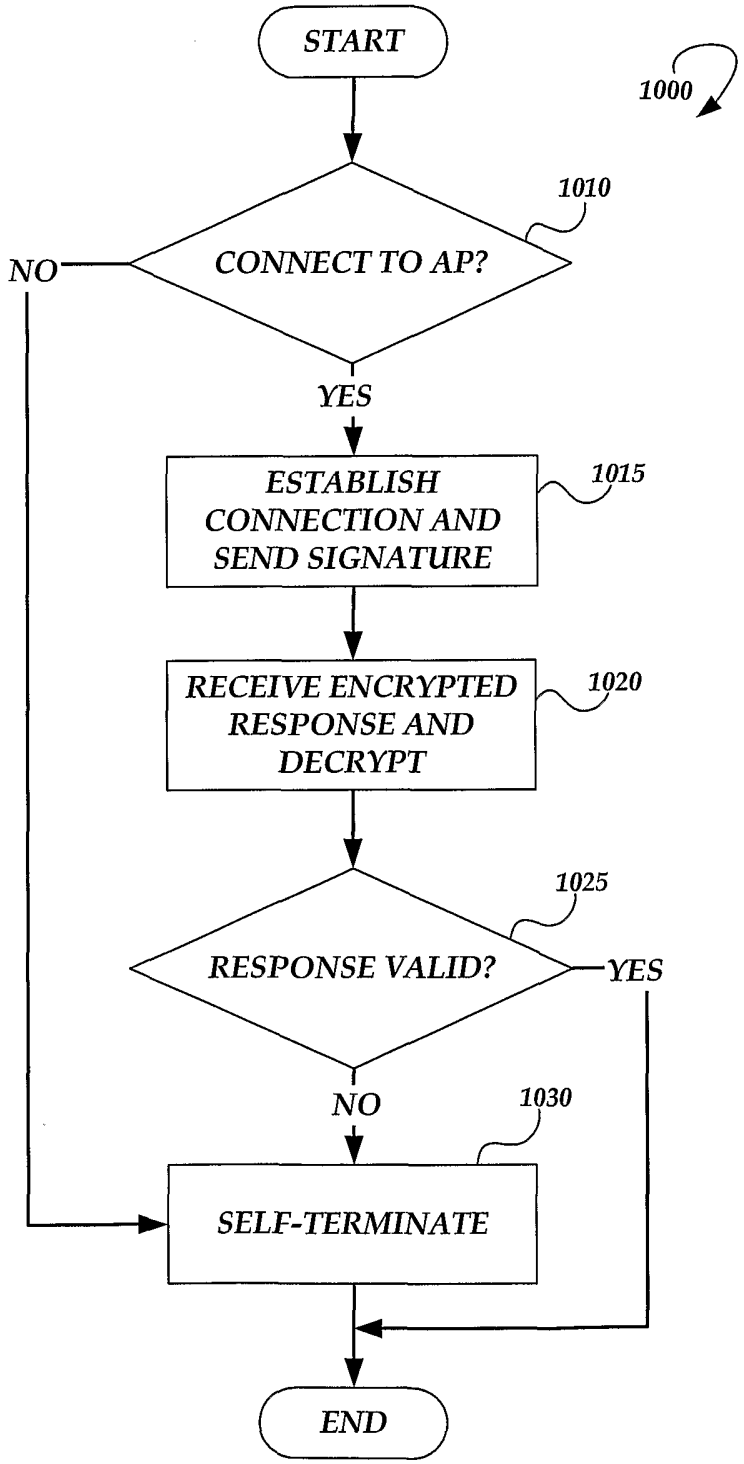

START
1000
1010
CONNECT TO AP?
NO
YES
ESTABLISH CONNECTION AND SEND SIGNATURE
1015
RECEIVE ENCRYPTED RESPONSE AND DECRYPT
1020
1025
RESPONSE VALID?
YES
NO
1030
SELF-TERMINATE
END

Fig. 10

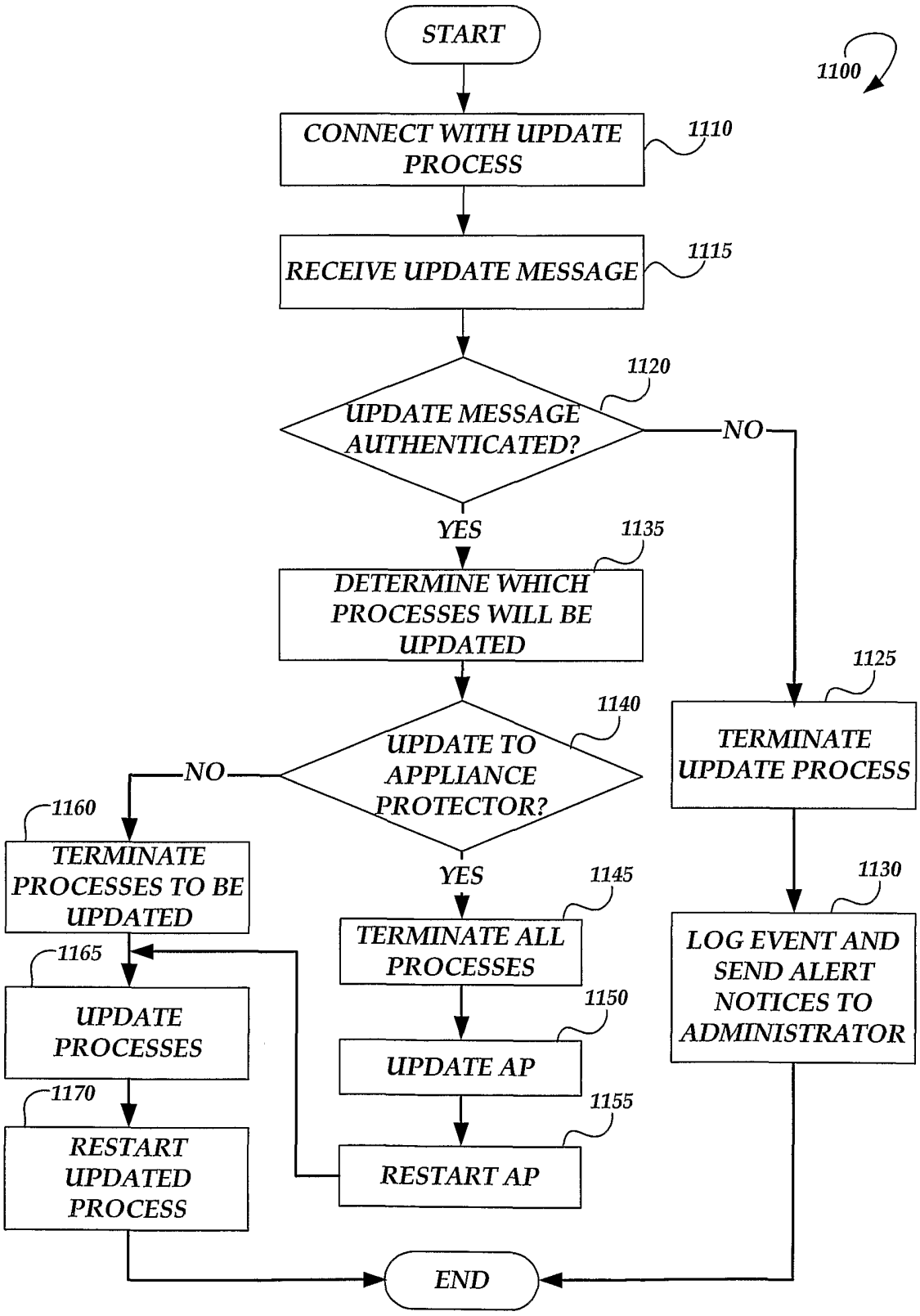

START
1100
CONNECT WITH UPDATE PROCESS
1110
RECEIVE UPDATE MESSAGE
1115
UPDATE MESSAGE AUTHENTICATED?
1120
NO
YES
DETERMINE WHICH PROCESSES WILL BE UPDATED
1135
UPDATE TO APPLIANCE PROTECTOR?
1140
NO
YES
TERMINATE UPDATE PROCESS
1125
TERMINATE PROCESSES TO BE UPDATED
1160
TERMINATE ALL PROCESSES
1145
LOG EVENT AND SEND ALERT NOTICES TO ADMINISTRATOR
1130
UPDATE PROCESSES
1165
UPDATE AP
1150
RESTART UPDATED PROCESS
1170
RESTART AP
1155
END

Fig. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/12042

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00; G06F 11/30
US CL : 713/167, 170, 187, 200, 201, 151; 380/283; 705/50, 54

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. : 713/167, 170, 187, 200, 201, 151; 380/283; 705/50, 54

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)
WEST, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,978,484 A (APPERSON et al) 02 November 1999 (02.11.1999), abstract; fig.3 and 5; col.4, lines 19-67; col. 5-7.	1-19
X	US 6,161,181 A (HAYNES, III et al) 12 December 2000 (12.12.2000), fig.1-4b and 8; col.4, lines 51-67; col.5, lines 1-48; col.6, lines 28-67; col.7-12.	1-19
X	US 6,061,794 A (ANGELO et al) 09 May 2000 (09.05.2000), fig.6a-6d; col.9, lines 47-67; col.10-12; col.13, lines 1-25.	1-19

☐ 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
22 August 2002 (22.08.2002)	12 SEP 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 Gilberto Barron Telephone No. 703-305-3900

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