



US 20080276302A1

(19) **United States**  
(12) **Patent Application Publication**  
**Touboul**

(10) **Pub. No.: US 2008/0276302 A1**  
(43) **Pub. Date: Nov. 6, 2008**

(54) **SYSTEM AND METHOD FOR PROVIDING DATA AND DEVICE SECURITY BETWEEN EXTERNAL AND HOST DEVICES**

(60) Provisional application No. 60/893,109, filed on Mar. 5, 2007, provisional application No. 60/750,326, filed on Dec. 13, 2005.

(75) Inventor: **Shlomo Touboul, Kefar Haim (IL)**

Correspondence Address:  
**THELEN REID BROWN RAYSMAN & STEINER LLP**  
**P.O. Box 640640**  
**SAN JOSE, CA 95164-0640 (US)**

(73) Assignee: **YOGGIE SECURITY SYSTEMS LTD., Beit Halevy (IL)**

(21) Appl. No.: **12/042,938**

(22) Filed: **Mar. 5, 2008**

**Related U.S. Application Data**

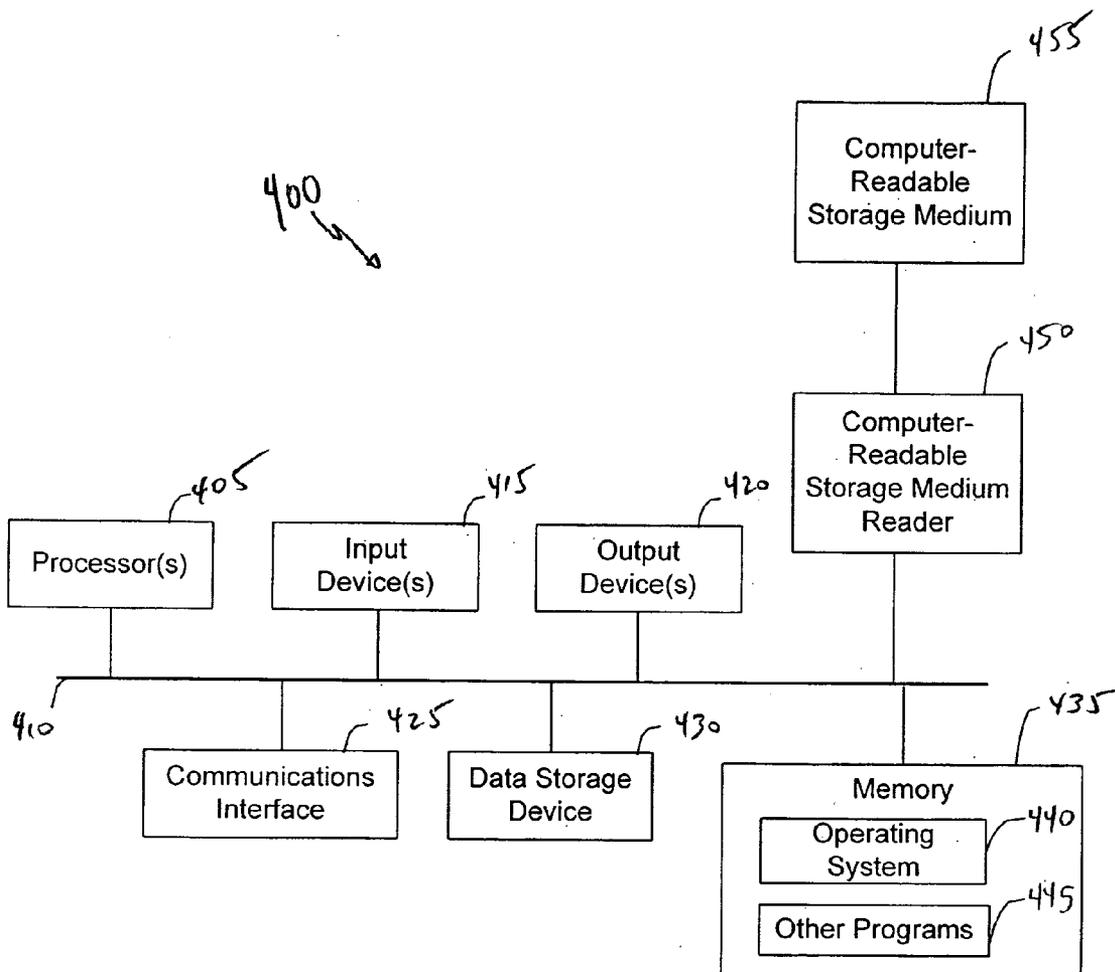
(63) Continuation-in-part of application No. 11/376,919, filed on Mar. 15, 2006.

**Publication Classification**

(51) **Int. Cl.**  
**G06F 15/16** (2006.01)  
(52) **U.S. Cl.** ..... **726/3**

(57) **ABSTRACT**

A secure data exchange system comprising a security device including a first external device plug, and a security engine operative to enforce a security policy on data transfer requests received from the host; an external device including a second external device plug; and a host including a first external device port operative to communicatively couple with the first external device plug, a second external device port operative to communicatively couple with the second external device plug, and a driver, e.g., a redirect driver, operative to transfer a data transfer request to the security device before executing the data transfer request.



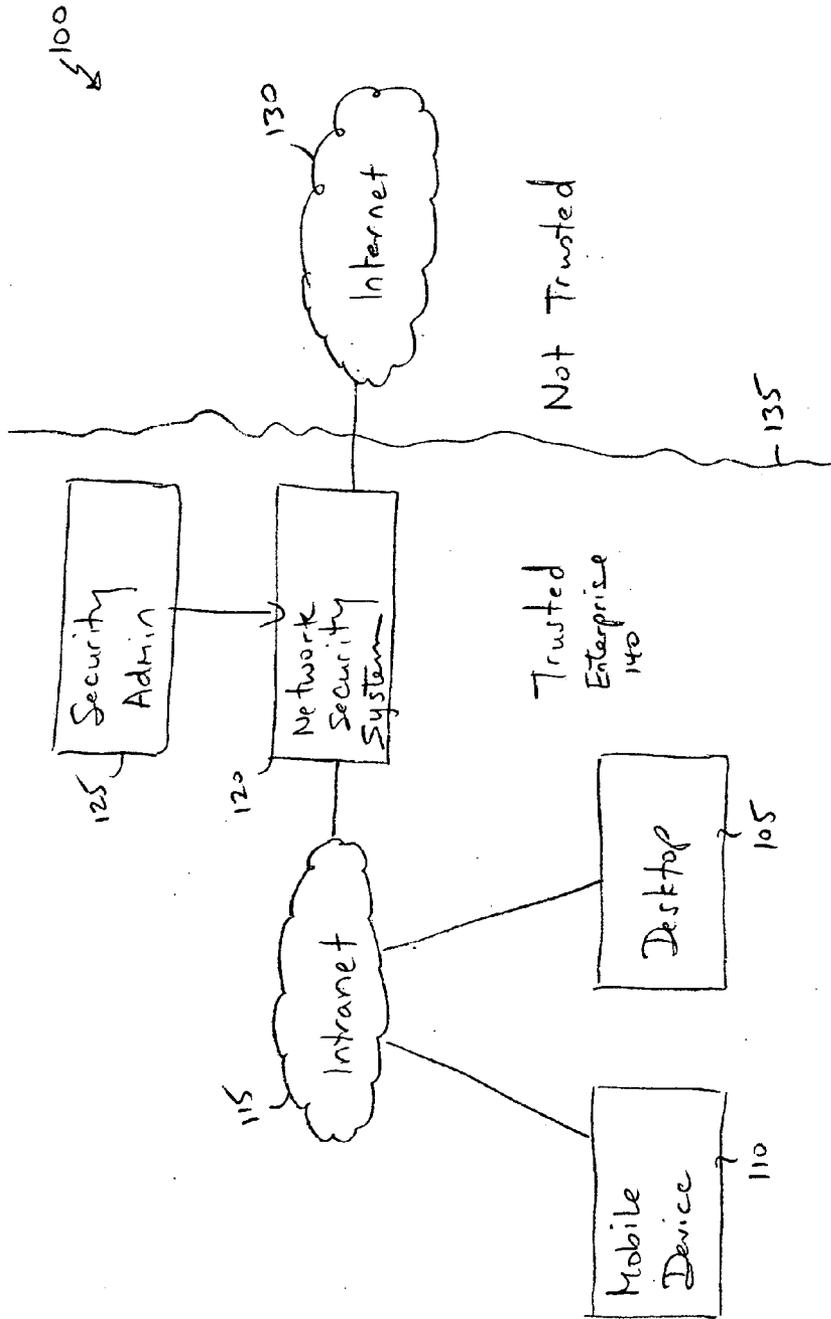


FIG. 1  
(prior art)

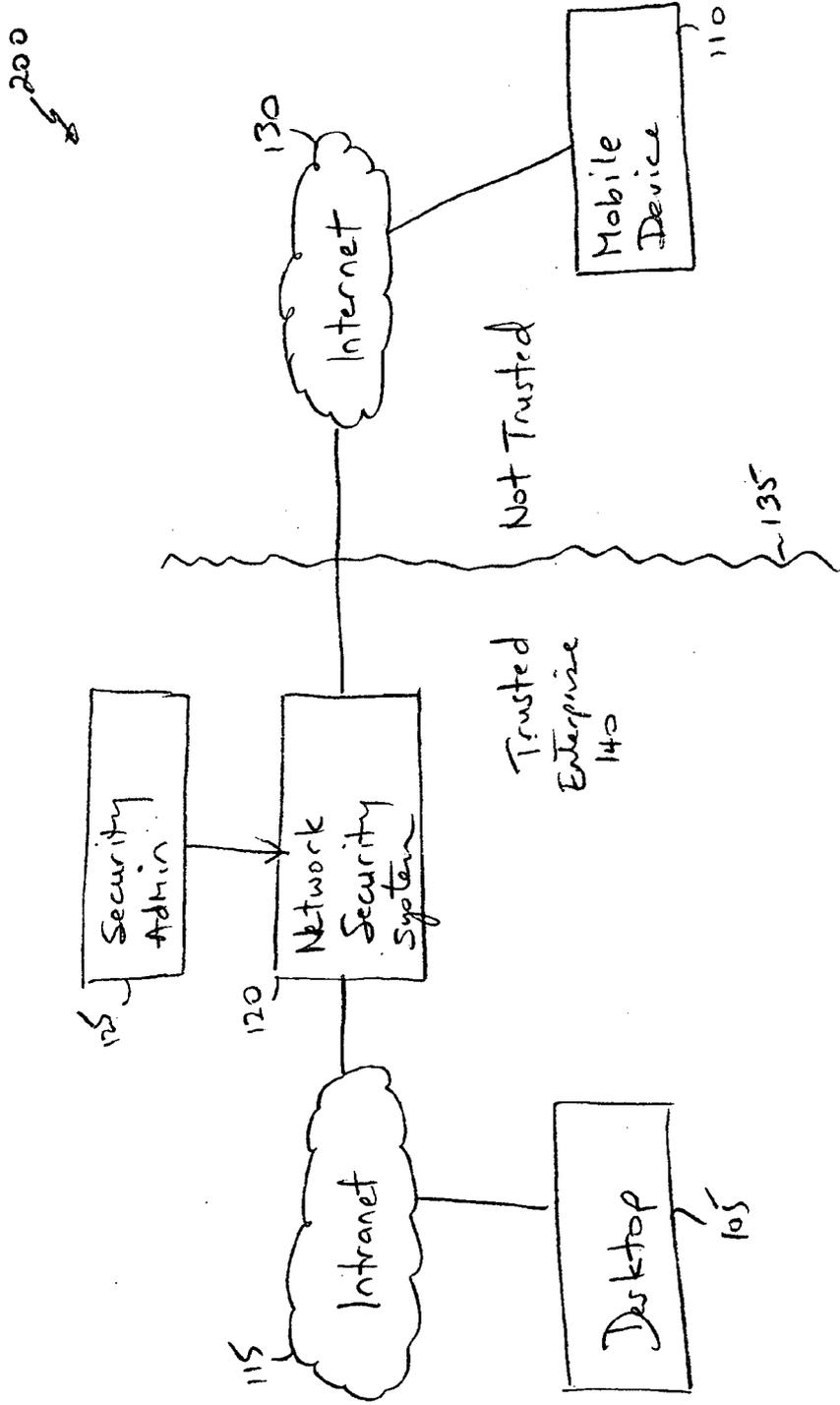


FIG. 2  
(prior art)

300

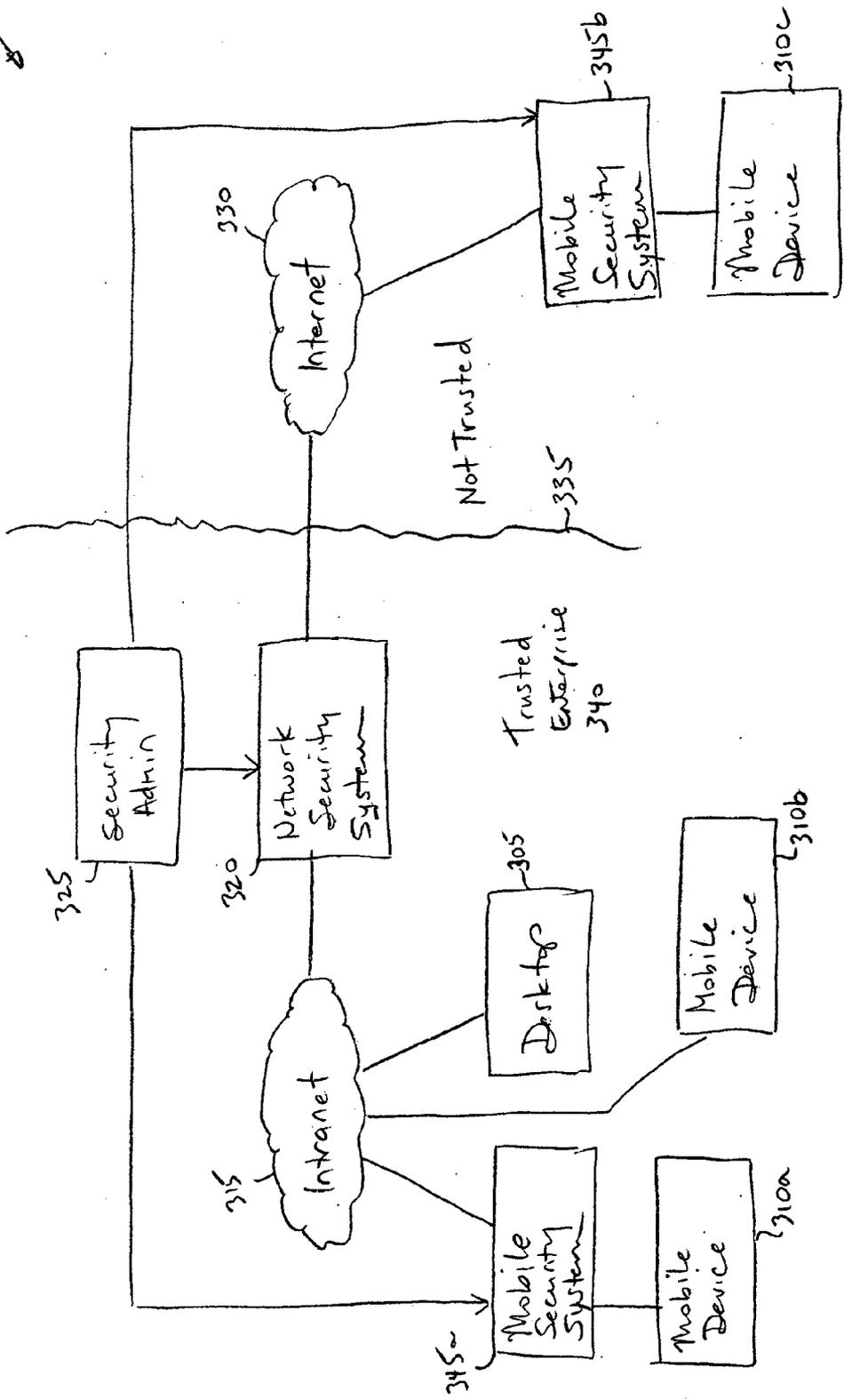


FIG. 3

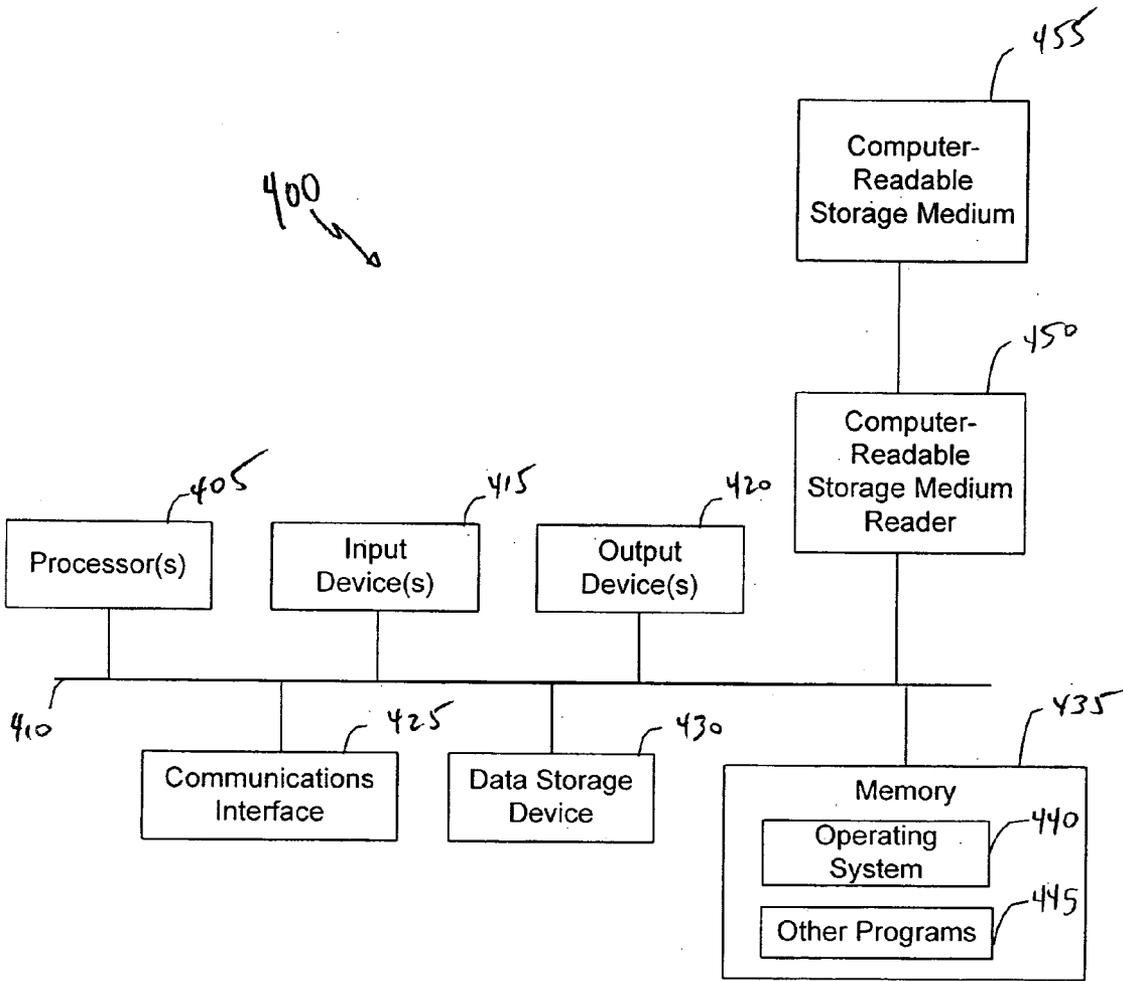


FIG. 4

345  
↙

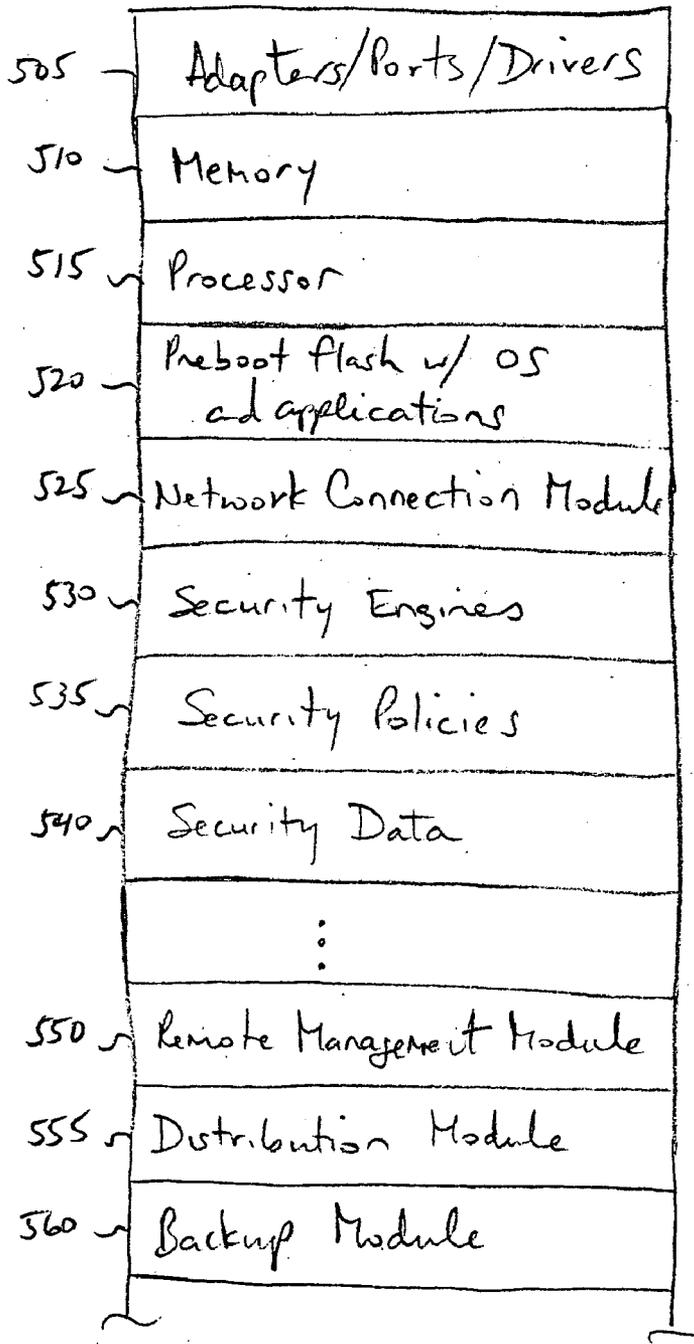


FIG. 5

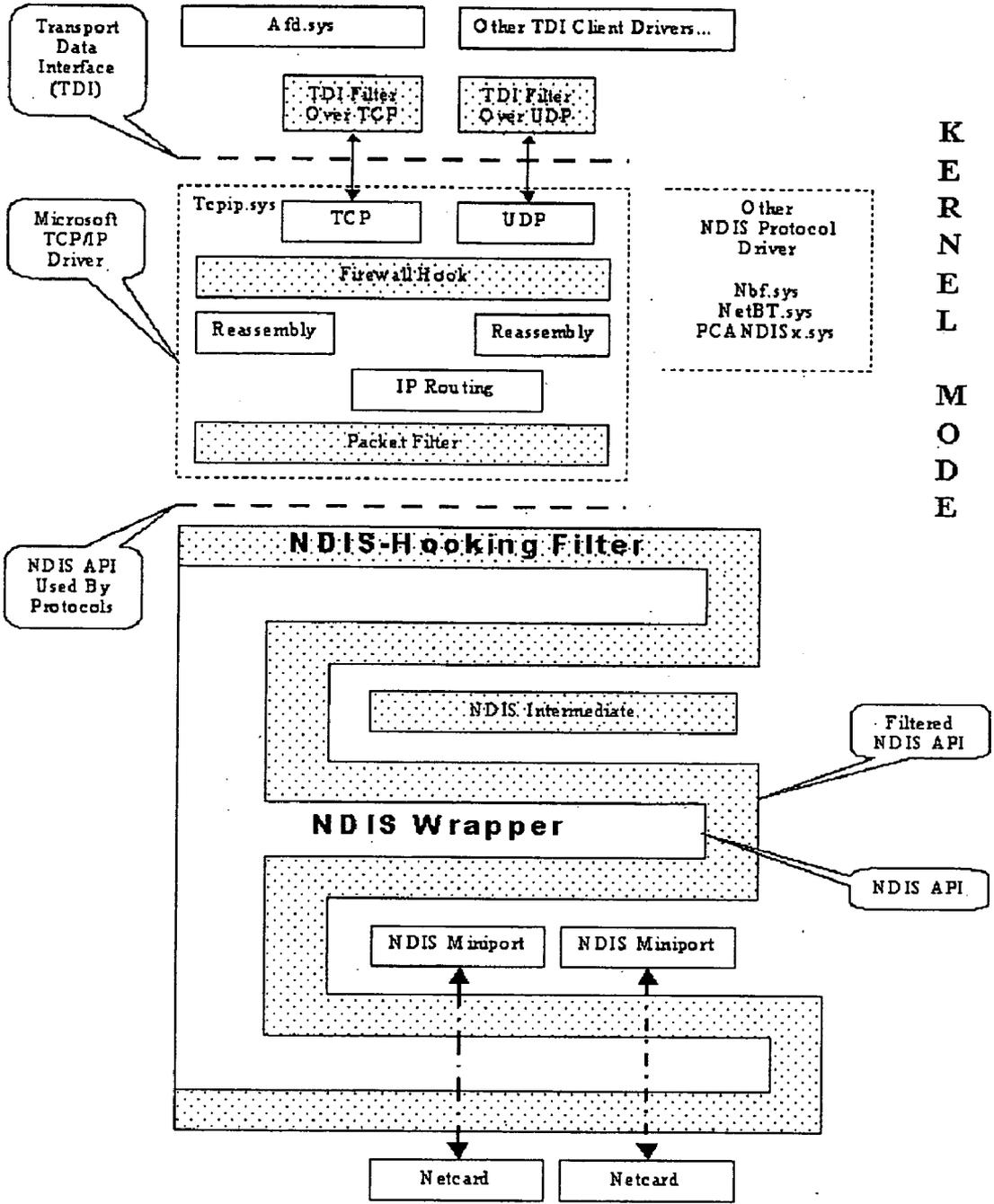


FIG. 6

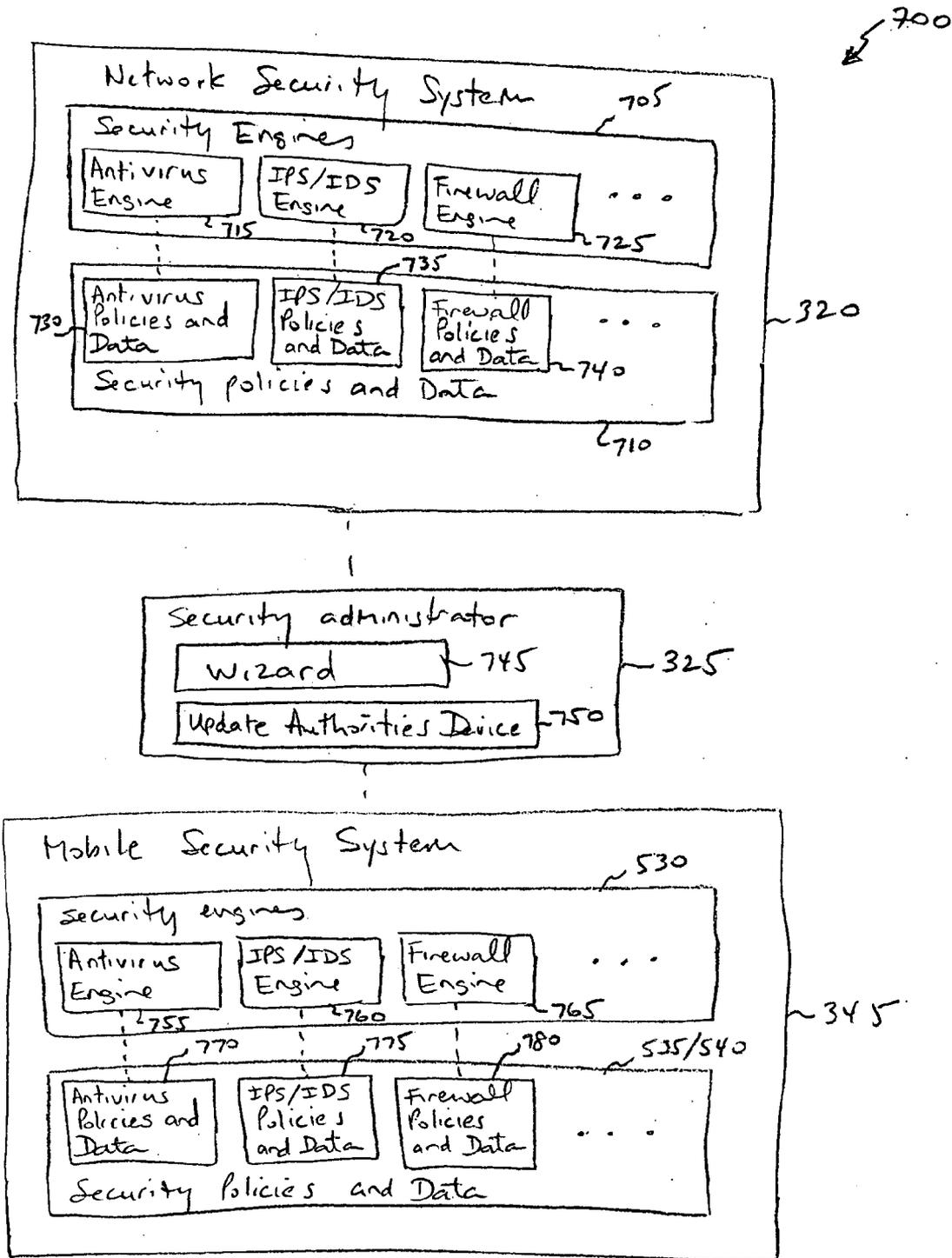


FIG. 7

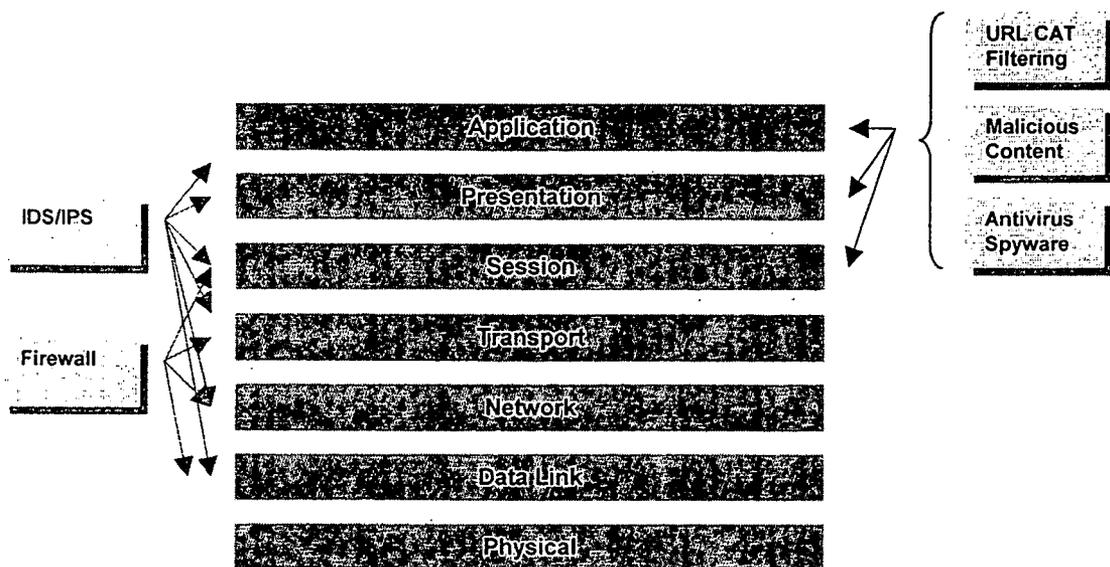


FIG. 8

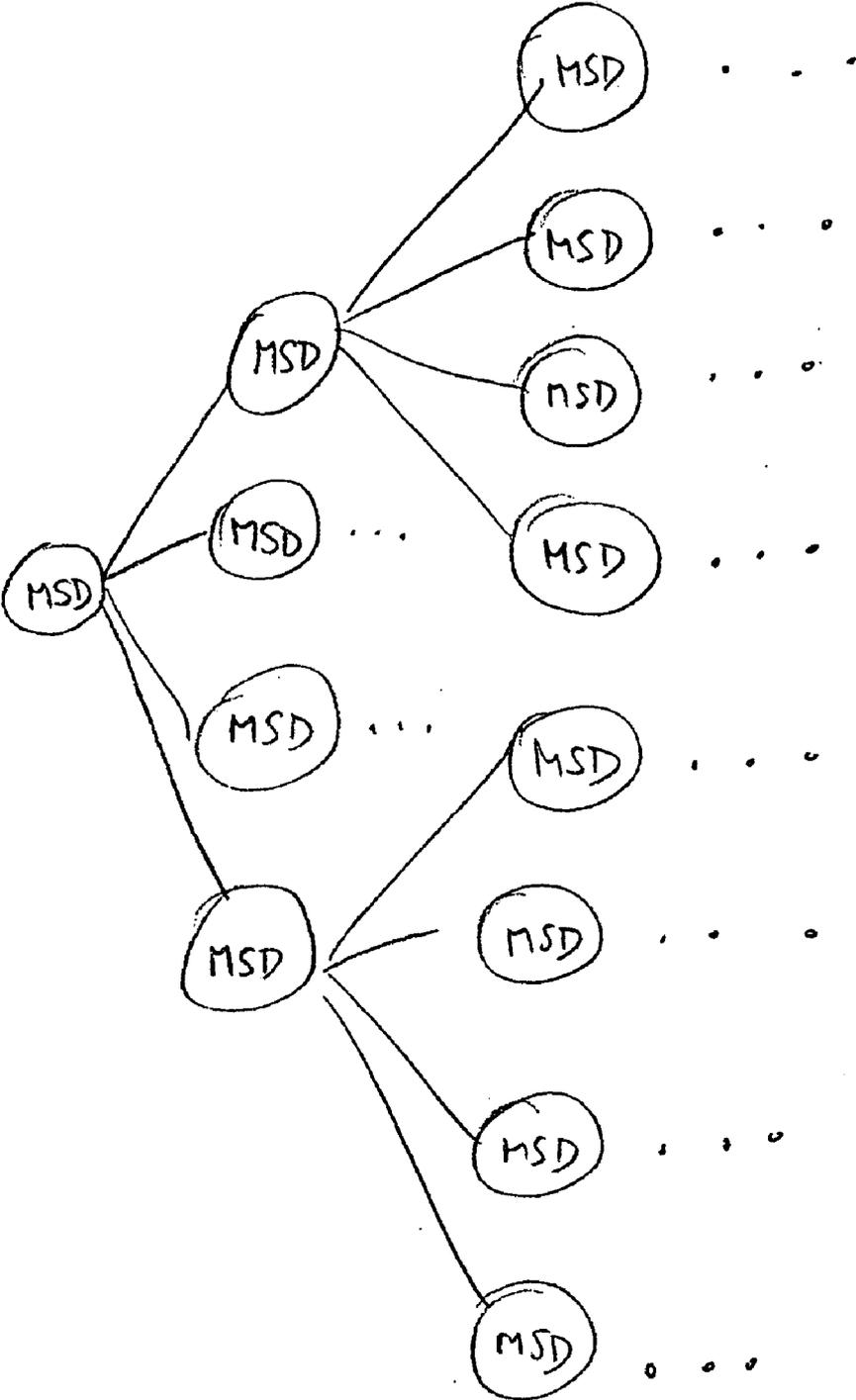
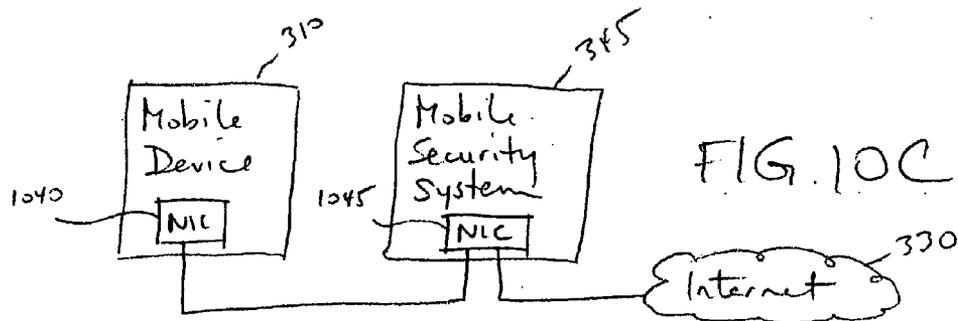
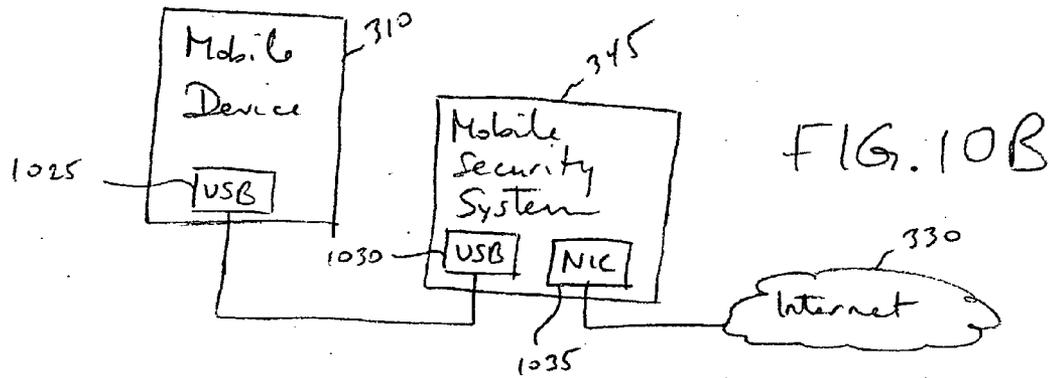
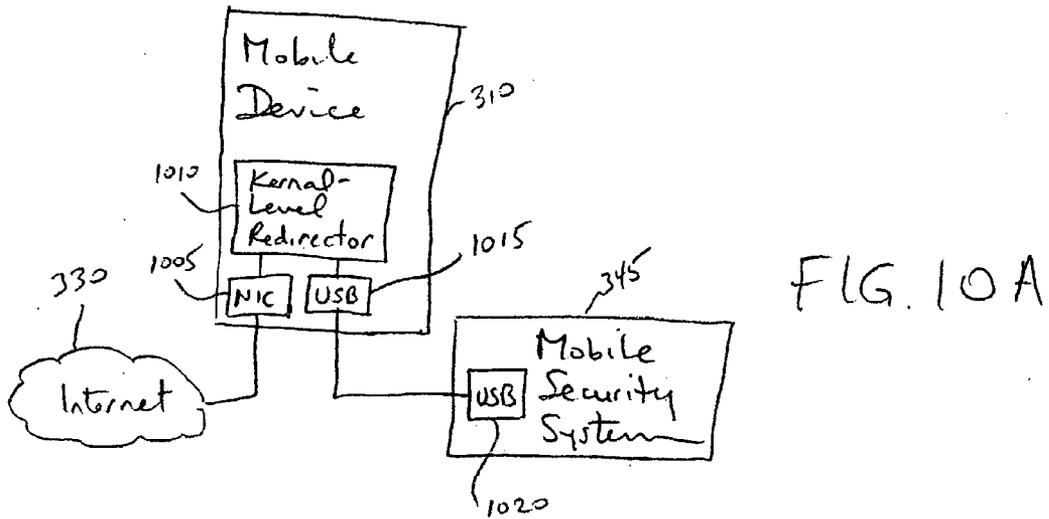


FIG. 9



Data Exchange System  
1100

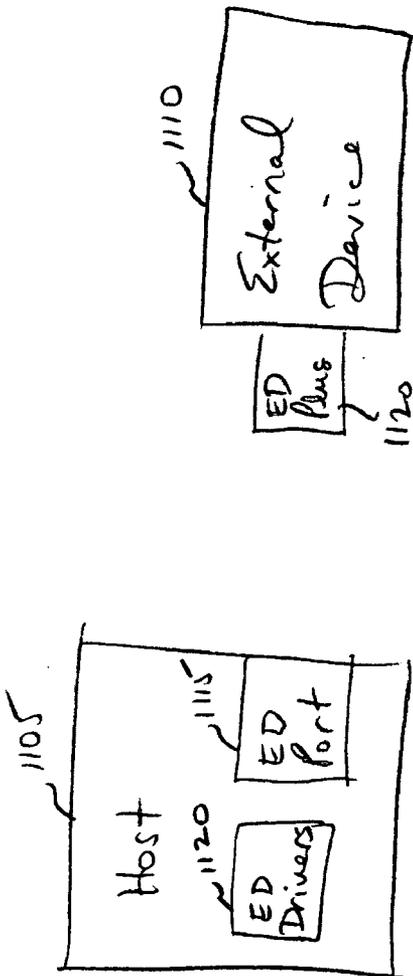


Figure 11  
(Prior Art)

Data Exchange System 1200

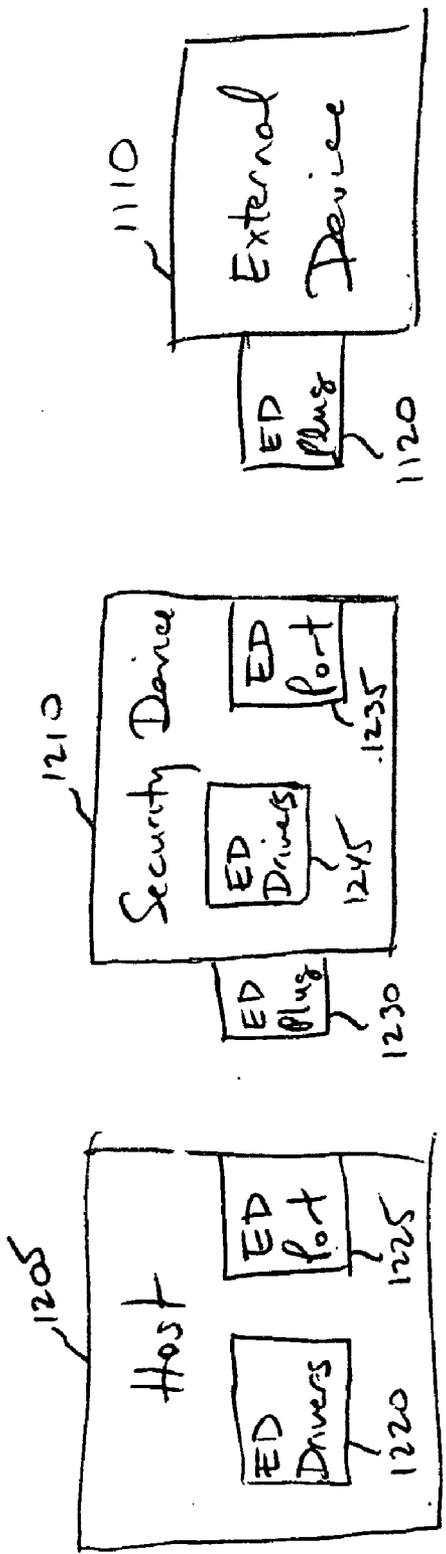


Figure 12

Security Device  
1210

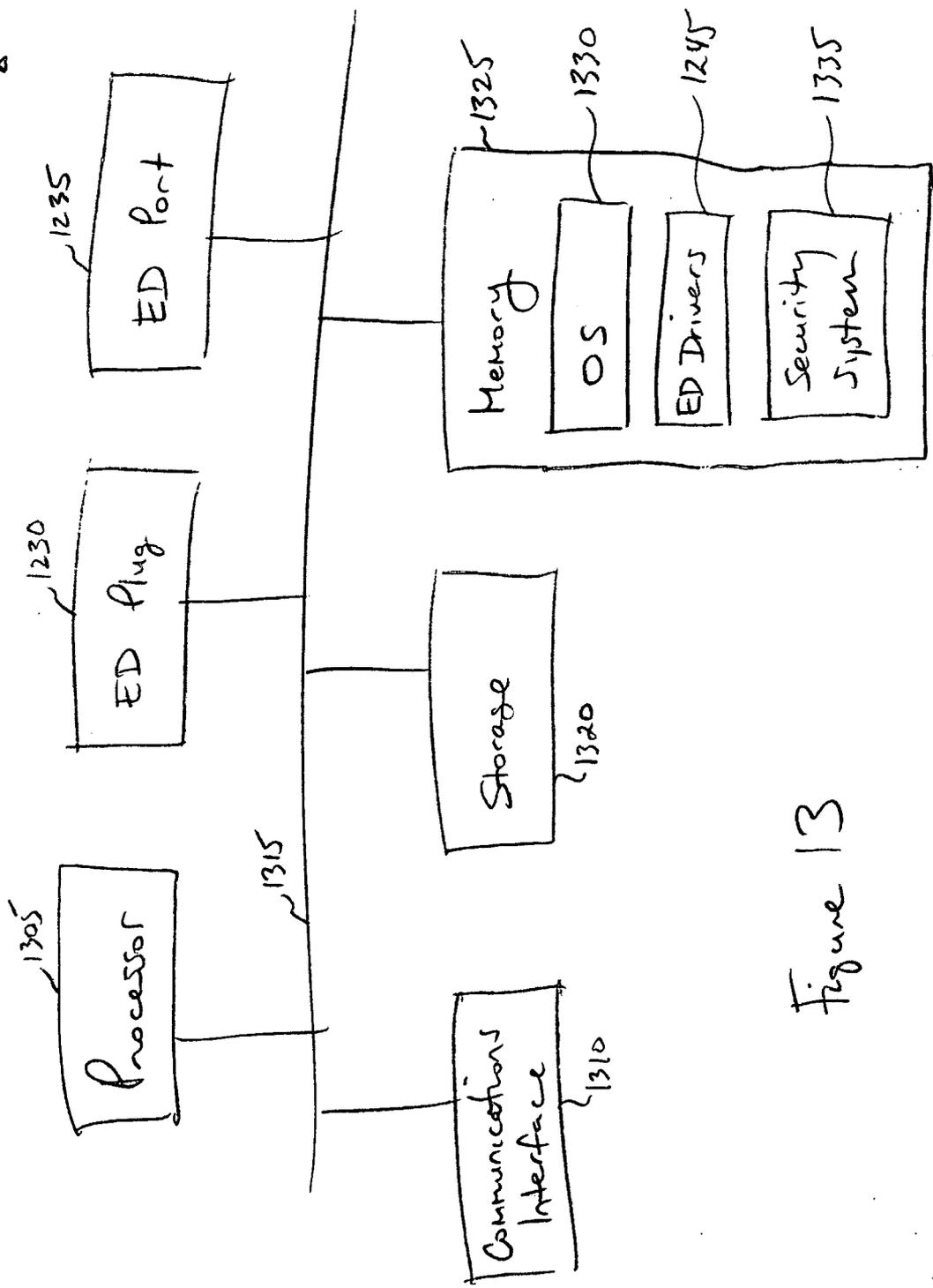


Figure 13

Security System 1335

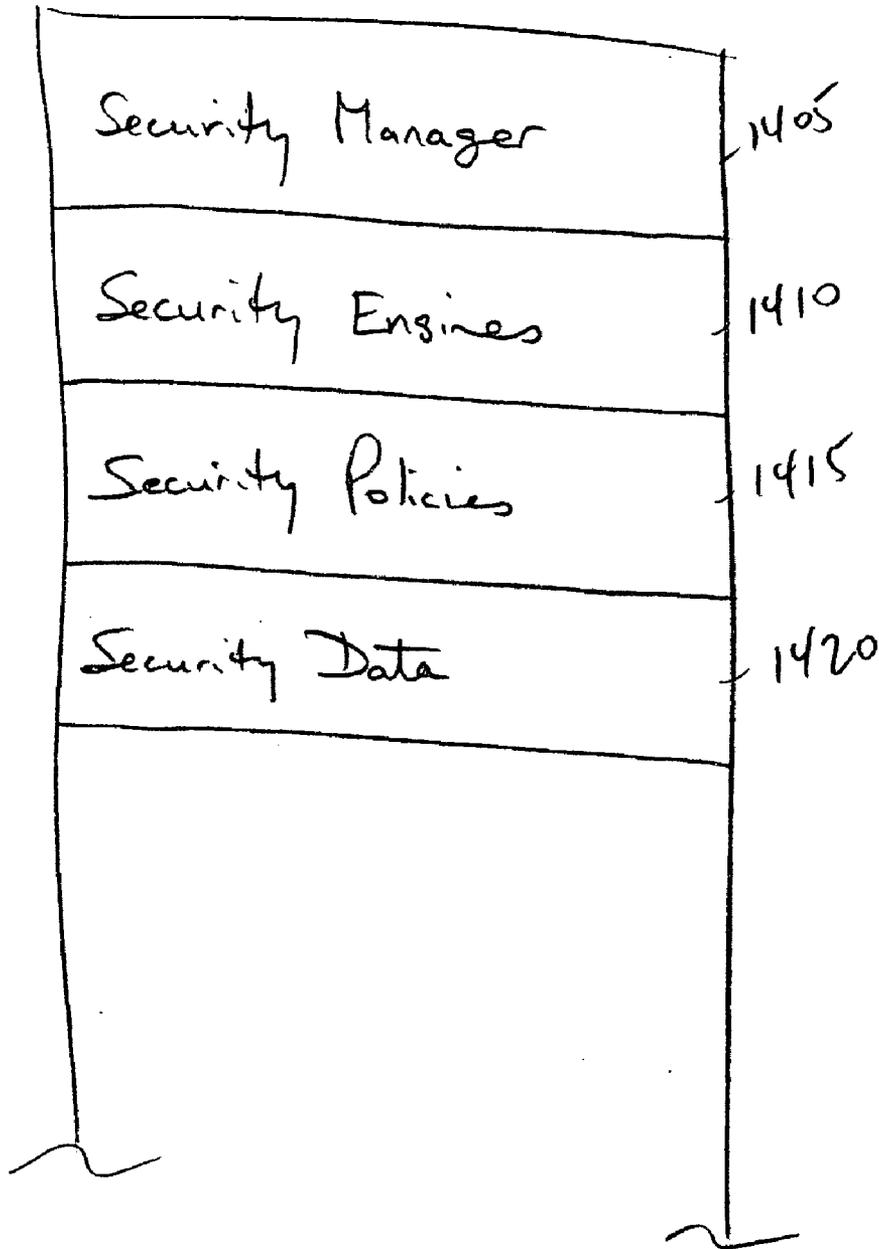


Figure 14

Data Exchange System 1500

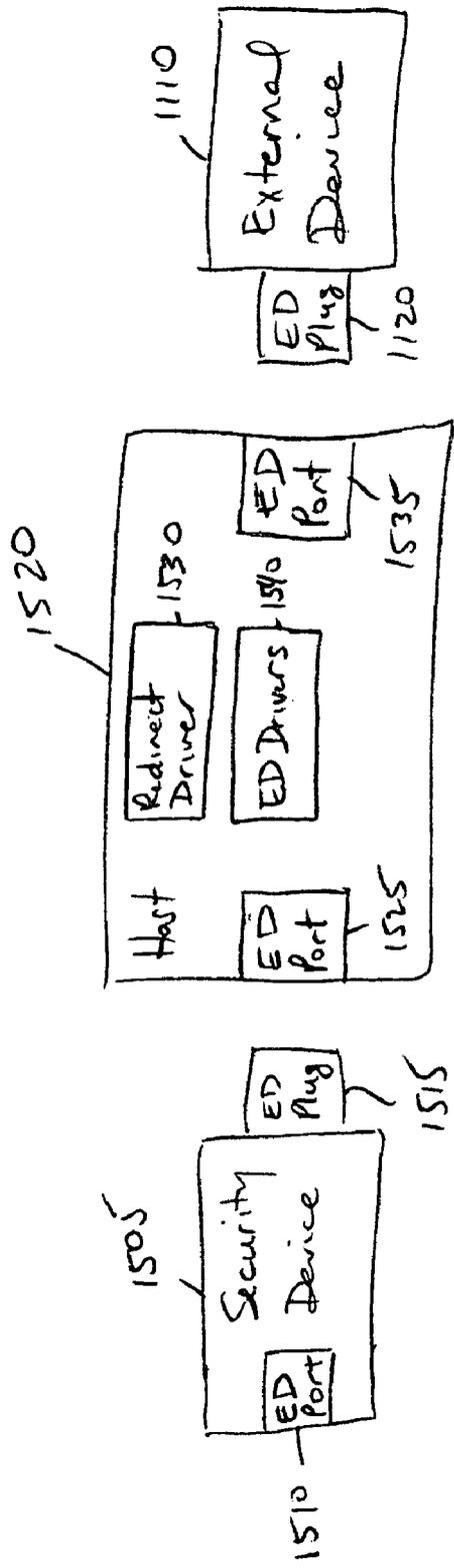
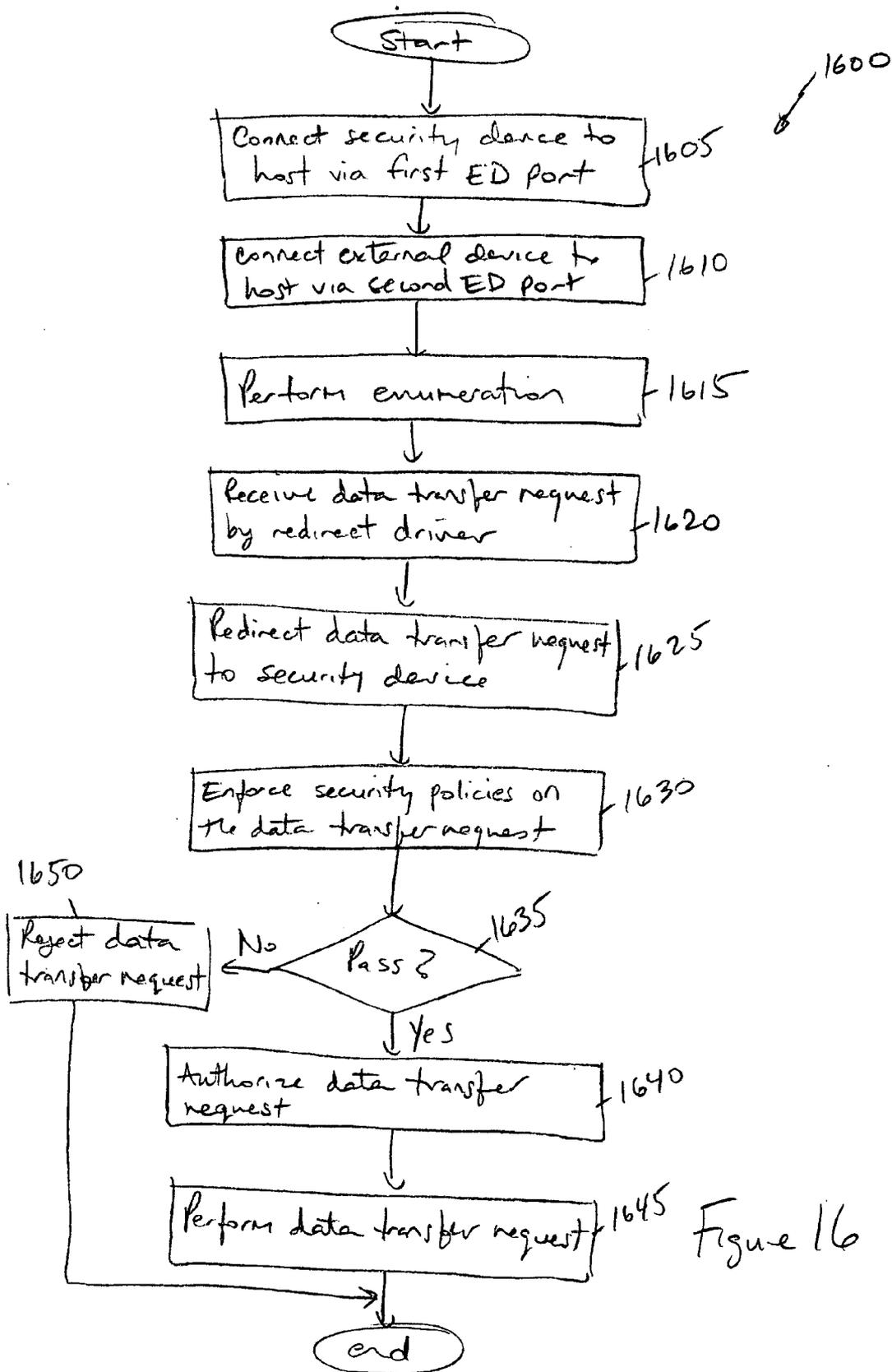


Figure 15



**SYSTEM AND METHOD FOR PROVIDING DATA AND DEVICE SECURITY BETWEEN EXTERNAL AND HOST DEVICES**

**PRIORITY CLAIM**

[0001] This application claims benefit of U.S. provisional patent application Ser. No. 60/893,109 and is a continuation-in-part of U.S. patent application Ser. No. 11/376,919, which claims benefit of U.S. provisional patent application Ser. No. 60/750,326, all of which are hereby incorporated by reference.

**TECHNICAL FIELD**

[0002] This invention relates generally to computer security, and more particularly provides a system and method for providing data and device security between external and host devices.

**BACKGROUND**

[0003] The internet is an interconnection of millions of individual computer networks owned by governments, universities, nonprofit groups, companies and individuals. While the internet is a great source of valuable information and entertainment, the internet has also become a major source of system damaging and system fatal application code, such as “viruses,” “spyware,” “adware,” “worms,” “Trojan horses,” and other malicious code.

[0004] To protect users, programmers design computer and computer-network security systems for blocking malicious code from attacking both individual and network computers. On the most part, network security systems have been relatively successful. A computer that connects to the internet from within an enterprise’s network typically has two lines of defense. The first line of defense includes a network security system, which may be part of the network gateway, that includes firewalls, antivirus, antispyware and content filtering. The second line of defense includes individual security software on individual machines, which is not typically as secure as the network security system and is thus more vulnerable to attacks. In combination, the first and second lines of defense together provide pretty good security protection. However, when a device connects to the internet without the intervening network security system, the device loses its first line of defense. Thus, mobile devices (e.g., laptops, desktops, PDAs such as RIM’s Blackberry, cell phones, any wireless device that connects to the internet, etc.) when traveling outside the enterprise network are more vulnerable to attacks.

[0005] FIG. 1 illustrates an example network system 100 of the prior art. Network system 100 includes a desktop 105 and a mobile device 110, each coupled to an enterprise’s intranet 115. The intranet 115 is coupled via a network security system 120 (which may be a part of the enterprise’s gateway) to the untrusted internet 130. Accordingly, the desktop 105 and mobile device 110 access the internet 130 via the network security system 120. A security administrator 125 typically manages the network security system 120 to assure that it includes the most current security protection and thus that the desktop 105 and mobile device 110 are protected from malicious code. Demarcation 135 divides the trusted enterprise 140 and the untrusted public internet 130. Because the desktop 105 and the mobile device 110 are connected to the internet 130 via the network security system 120, both have two lines of defense (namely, the network security system

120 and the security software resident on the device itself) against malicious code from the internet 130. Of course, although trusted, the intranet 115 can also be a source of malicious code.

[0006] FIG. 2 illustrates an example network system 200 of the prior art, when the mobile device 110 has traveled outside the trusted enterprise 140 and reconnected to the untrusted internet 130. This could occur perhaps when the user takes mobile device 110 on travel and connects to the internet 130 at a cybercafé, at a hotel, or via any untrusted wired or wireless connection. Accordingly, as shown, the mobile device 110 is no longer protected by the first line of defense (by the network security system 120) and thus has increased its risk of receiving malicious code. Further, by physically bringing the mobile device 110 back into the trusted enterprise 140 and reconnecting from within, the mobile device 110 risks transferring any malicious code received to the intranet 115.

[0007] As the number of mobile devices and the number of attacks grow, mobile security is becoming increasingly important. The problem was emphasized in the recent Info-Security Conference in New York on Dec. 7-8, 2005. However, no complete solutions were presented.

[0008] Similarly, when a host device is connected to an external device such as a USB flash drive, iPod, external hard drive, etc., both devices are vulnerable to receipt of malicious code or transfer of private data. FIG. 11 illustrates an example prior art data exchange system 1100 that includes a host computer (host) 1105 and an external device 1110. The host 1105 includes a external device (ED) port 1115, such as a USB port, for receiving the external device 1110. The host 1105 also includes ED drivers 1120 for performing enumeration and enabling communications between the external device 1110 and the host 1105. The external device 1110 includes an ED plug, such as a USB plug, for communicating with the ED port 1115. Both of the host 1105 and external device 1110 are vulnerable to receipt of malicious code or transfer of private data.

[0009] Accordingly, there is a need for a system and method of providing security to host and external devices.

**SUMMARY**

[0010] Per one embodiment, the present invention provides a security device comprising an external device plug operative to communicatively couple with a host; an external device port operative to communicatively couple with an external device; a processor; and memory storing an operating system, an external device driver operative to control communication with the external device, and a security engine operative to enforce a security policy on a data transfer request between the external device and the host. The security device may be operative with a driver on the host. At least one of the external device plug and the external device port may follow a USB standard. At least one of the external device plug and the external device port may include a wireless connection. The security engine may protect against the transfer of at least one of viruses, spyware and adware. The security engine may protect against the unauthorized transfer of private data.

[0011] Per one embodiment, the present invention provides a secure data exchange system, comprising a security device including a first external device plug, and a security engine operative to enforce a security policy on data transfer requests received from the host; an external device including a second external device plug; and a host including a first external

device port operative to communicatively couple with the first external device plug, a second external device port operative to communicatively couple with the second external device plug, and a redirect driver operative to transfer a data transfer request from the host to the security device before executing the data transfer request. The external device may include a USB drive. The external device may include one of a PDA or a cell phone. The host may include one of a laptop, desktop, PDA or cell phone. The host may launch the redirect driver upon detecting connection of the secure device to the host.

[0012] Per one embodiment, the present invention may provide a method comprising communicatively coupling a security device to a host; communicatively coupling an external device to the security device; receiving by the security device a data transfer request from the host; and enforcing by the security device a security policy on the data transfer request before allowing the data transfer request to be performed. The communicatively coupling a security device to a host may include using a wired or wireless connection. The communicatively coupling an external device to the host may include using a wired or wireless connection. The data transfer request may include a request to transfer data from the host to the external device. The data transfer request may include a request to transfer data from the external device to the host. The enforcing may include reviewing the data being transferred for at least one of viruses, spyware and adware. The enforcing may include determining whether the data transfer request includes a request for private data. The enforcing may include requiring an additional security check before allowing the transfer of private data.

[0013] Per one embodiment, the present invention provides a method, comprising communicatively coupling a security device to a host; communicatively coupling an external device to the host; receiving by the host a data transfer request; using a redirect driver on the host to redirect the data transfer request to the security device; and enforcing by the security device a security policy on the data transfer request before allowing the data transfer request to be performed. The communicatively coupling a security device to a host may include using a wired or wireless connection. The communicatively coupling an external device to the host may include using a wired or wireless connection. The data transfer request may include a request to transfer data from the host to the external device. The data transfer request may include a request to transfer data from the external device to the host. The enforcing may include reviewing the data being transferred for at least one of viruses, spyware and adware. The enforcing may include determining whether the data transfer request includes a request for private data. The enforcing may include requiring an additional security check before allowing the transfer of private data.

#### BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 is a block diagram of a prior art network system in a first state.

[0015] FIG. 2 is a block diagram of a prior art network system in a second state.

[0016] FIG. 3 is a block diagram of a network system in accordance with an embodiment of the present invention.

[0017] FIG. 4 is a block diagram illustrating details of a computer system in accordance with an embodiment of the present invention.

[0018] FIG. 5 is a block diagram illustrating details of the mobile security system in accordance with an embodiment of the present invention.

[0019] FIG. 6 is a block diagram illustrating details of the mobile security system in accordance with a Microsoft Window's embodiment.

[0020] FIG. 7 is a block diagram illustrating details of a smart policy updating system in accordance with an embodiment of the present invention.

[0021] FIG. 8 is a block diagram illustrating details of network security measures relative to the OSI layers.

[0022] FIG. 9 is a block diagram illustrating details of the communication technique for spreading security code to the mobile security systems.

[0023] FIGS. 10A-10C are block diagrams illustrating various architectures for connecting a mobile device to a mobile security system, in accordance with various embodiments of the present invention.

[0024] FIG. 11 is a block diagram illustrating a prior art data exchange system.

[0025] FIG. 12 is a block diagram illustrating a secure data exchange system, in accordance with an embodiment of the present invention.

[0026] FIG. 13 is a block diagram illustrating details of a security device, in accordance with an embodiment of the present invention.

[0027] FIG. 14 is a block diagram illustrating details of a security system, in accordance with an embodiment of the present invention.

[0028] FIG. 15 is a block diagram illustrating a secure data exchange system, in accordance with another embodiment of the present invention.

[0029] FIG. 16 is a flowchart illustrating a method of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention.

#### DETAILED DESCRIPTION

[0030] The following description is provided to enable any person skilled in the art to make and use the invention, and is provided in the context of a particular application and its requirements. Various modifications to the embodiments may be possible to those skilled in the art, and the generic principles defined herein may be applied to these and other embodiments and applications without departing from the spirit and scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown, but is to be accorded the widest scope consistent with the principles, features and teachings disclosed herein.

[0031] An embodiment of the present invention uses a small piece of hardware that connects to a mobile device and filters out attacks and malicious code. The piece of hardware may be referred to as a "mobile security system" or "personal security appliance." Using the mobile security system, a mobile device can be protected by greater security and possibly by the same level of security offered by its associated corporation/enterprise.

[0032] FIG. 3 illustrates a network system 300 in accordance with an embodiment of the present invention. Network system 300 includes a desktop 305, a first mobile device 310a, and a second mobile device 310b. The first mobile device 310a is illustrated as within the enterprise network 340 at this time and is coupled via a mobile security system 345a to the enterprise's intranet 315. The desktop 305 and second mobile device 310b are also within the enterprise network

**340** but in this embodiment are coupled to the intranet **315** without an intervening mobile security system **345** such as mobile security system **345b**. The intranet **315** is coupled via a network security system **320** (which may be part of the enterprise's gateway) to the untrusted internet **330**. Accordingly, the first mobile device **310a**, the second mobile device **310b** and the desktop **305** access the untrusted internet **330** via the network security system **320**. Each may also be protected by a personal security system resident thereon (not shown). A third mobile device **310c** is currently outside the enterprise network **340** and is coupled via a mobile security system **345b** to the untrusted internet **330**. The third mobile device **310** may be in use by an employee of the trusted enterprise **340** who is currently on travel. A security administrator **325** manages the mobile security system **345a**, the mobile security system **345b**, and the network security system **320** to assure that they include the most current security protection. One skilled in the art will recognize that the same security administrator need not manage the various devices. Further, the security administrator could be the user and need not be within the trusted enterprise **340**.

[0033] Demarcation **335** divides the trusted enterprise **340** and the untrusted publicly accessible internet **330**. Each of mobile device **310a**, **310b** and **310c** may be referred to generically as mobile device **310**, although they need not be identical. Each mobile security system **345a** and **345b** may be referred to generically as mobile security system **345**, although they need not be identical.

[0034] As shown, although the mobile device **310c** has traveled outside the trusted enterprise **340**, the mobile device **310c** connects to the untrusted internet **330** via the mobile security system **345b** and thus retains two lines of defense (namely, the mobile security system **345b** and the security software resident on the device itself). In this embodiment, the mobile security system **345** effectively acts as a mobile internet gateway on behalf of the mobile device **310c**. In an embodiment, the mobile security system **345** may be a device dedicated to network security. In an embodiment, each mobile security system **345** may support multiple mobile devices **310**, and possibly only registered mobile devices **310**, e.g., those belonging to enterprise **340**.

[0035] Each mobile security system **345** (e.g., **345a**, **345b**) may be a miniature server, based on commercial hardware (with Intel's Xscale as the core), Linux OS and network services, and open-source firewall, IDS/IPS and antivirus protection. The mobile security system **345** may be based on a hardened embedded Linux 2.6.

[0036] In this embodiment, because the security administrator **325** is capable of remotely communicating with the mobile security system **345b**, IT can monitor and/or update the security policies/data/engines implemented on the mobile security system **345b**. The security administrator **325** can centrally manage all enterprise devices, remotely or directly. Further, the security administrator **325** and mobile security systems **345** can interact to automatically translate enterprise security policies into mobile security policies and configure mobile security systems **345** accordingly. Because the mobile security system **345** may be generated from the relevant security policies of the enterprise **340**, the mobile device **310c** currently traveling may have the same level of protection as the devices **305/310** within the trusted enterprise **340**.

[0037] The mobile security system **345** may be designed as an add-on to existing software security or to replace all security hardware and software on a traveling mobile device.

These security applications will preferably operate on different OSI layers to provide maximum security and malicious code detection, as shown in the example system illustrated in FIG. 8. Operating on the lower OSI layers and doing TCP/IP packets analysis only (by screening firewall or router packets) would miss virus and/or worm behavior. Also, many modern viruses use mobile code implemented on a "higher" level than the 7<sup>th</sup> OSI layer (Application—HTTP, FTP, etc.) and therefore cannot be interpreted at the packet layer nor at the application layer. For example, applying antivirus analysis only at the session or transport layer on a malicious Java Script (that is included in an HTML page), trying to match the signature with packets and without understanding the content type (Java Script), will not detect the malicious nature of the Java Script. To offer greater protection, the mobile security system **345** may act as corporate class security appliance and engage different security applications based on the content type and the appropriate OSI layers, (or even a "higher" level if content is encapsulated in the application layer). The mobile security system **345** may be configured to perform content analysis at different OSI layers, e.g., from the packet level to the application level. It will be appreciated that performing deep inspection at the application level is critical to detect malicious content behavior and improve detection of viruses, worms, spyware, Trojan horses, etc. The following software packages may be implemented on the mobile security system **345**:

[0038] Firewall and VPN—including stateful and stateless firewalls, NAT, packet filtering and manipulation, DOS/DDOS, netfilter, isolate user mobile devices from the internet and run VPN program on the device, etc.

[0039] Optional web accelerator and bandwidth/cache management based on Squid.

[0040] IDS/IPS—Intrusion detection and prevention system based on Snort. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol- and anomaly-based inspections.

[0041] Antivirus and antispyware based on ClamAV; additional AV and AS engines, e.g., McAfee, Kaspersky, Pandamay, may be offered for additional subscription fees.

[0042] Malicious Content Detection—on the fly heuristics that perform content analysis to detect malicious content before having signatures. This will be based on a rule base and updated rules and will be content dependent scanning.

[0043] URL Categorization Filtering—based on a commercial engine, such as Surfcontrol, Smart Filters or Websense. May provide around 70 categories of URLs such as gambling, adult content, news, webmail, etc. The mobile device **345** may apply different security policies based on the URL category, e.g., higher restriction and heuristics for Gambling or Adult content web sites, etc.

[0044] FIG. 4 is a block diagram illustrating details of an example computer system **400**, of which each desktop **305**, mobile device **310**, network security system **320**, mobile security system **345**, and security administrator **325** may be an instance. Computer system **400** includes a processor **405**, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel **410**. The computer system **400** further includes an input device **415** such as a keyboard or mouse, an output

device 420 such as a cathode ray tube display, a communications device 425, a data storage device 430 such as a magnetic disk, and memory 435 such as Random-Access Memory (RAM), each coupled to the communications channel 410. The communications interface 425 may be coupled directly or via a mobile security system 345 to a network such as the internet. One skilled in the art will recognize that, although the data storage device 430 and memory 435 are illustrated as different units, the data storage device 430 and memory 435 can be parts of the same unit, distributed units, virtual memory, etc.

[0045] The data storage device 430 and/or memory 435 may store an operating system 440 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, UNIX OS, LINUX OS and/or other programs 445. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology.

[0046] One skilled in the art will recognize that the computer system 400 may also include additional information, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc. One skilled in the art will also recognize that the programs and data may be received by and stored in the system in alternative ways. For example, a computer-readable storage medium (CRSM) reader 450 such as a magnetic disk drive, hard disk drive, magneto-optical reader, CPU, etc. may be coupled to the communications bus 410 for reading a computer-readable storage medium (CRSM) 455 such as a magnetic disk, a hard disk, a magneto-optical disk, RAM, etc. Accordingly, the computer system 400 may receive programs and/or data via the CRSM reader 450. Further, it will be appreciated that the term “memory” herein is intended to cover all data storage media whether permanent or temporary.

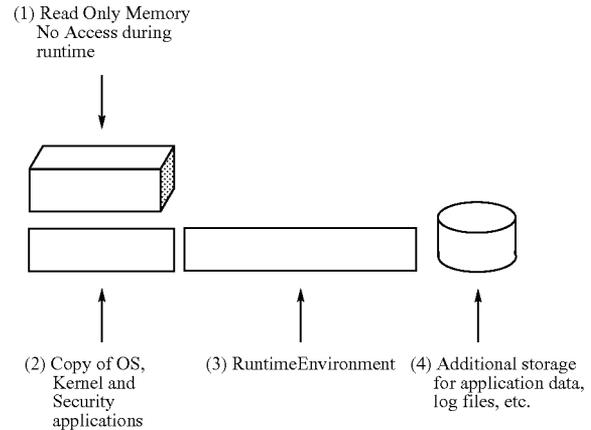
[0047] FIG. 5 is a block diagram illustrating details of the mobile security system 345 in accordance with an embodiment of the present invention. Mobile security system 345 includes adapters/ports/drivers 505, memory 510, a processor 515, a preboot flash/ROM memory module 520 storing a secure version of the mobile security system’s operating system and other applications, network connection module 525, security engines 530, security policies 535, security data 540, remote management module 550, distribution module 555, and backup module 560. Although these modules are illustrated as within the mobile security system 345, one skilled in the art will recognize that many of them could be located elsewhere, e.g., on the security administrator 325 or on third-party systems in communication with the mobile security system 345. The mobile security system 345 may be in a pocket-size, handheld-size or key-chain size housing, or possibly smaller. Further, the mobile security system 345 may be incorporated within the mobile device 310.

[0048] The adapters/ports/drivers 505 include connection mechanisms (including software, e.g., drivers) for USB, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection data ports on the mobile security system 345. In one embodiment, the adapters/ports/drivers 505 may be capable of connection to multiple devices 310 to provide network security to the multiple devices 310.

[0049] Memory 510 and processor 515 execute the operating system and applications on the mobile security system

345. In this example, the preboot flash 520 stores the operating system and applications. At boot time, the operating system and applications are loaded from the preboot flash 520 into memory 510 for execution. Since the operating system and applications are stored in the preboot flash 520, which cannot be accessed during runtime by the user, the operating system and applications in the preboot flash 520 are not corruptible. Should the copy of the operating system and applications in memory 510 be corrupted, e.g., by malicious code, the operating system and applications may be reloaded into the memory 510 from the preboot flash 520, upon restart. Although described as stored within the preboot flash 520, the OS and applications can be securely stored within other read-only memory devices, such as ROM, PROM, EEPROM, etc.

[0050] Memory (including memory 510 and preboot flash 520) on the mobile security system 345 may be divided into zones as follows:



Upon each “hard” restart, the boot loader (resident at area 1) of the mobile security system 345 copies the kernel and security applications (a fresh unchanged copy) from area 1 to 2. This causes a clean version of the OS and applications to be loaded into area 2 each time. That way, if a special mobile security system 345 attack is developed, the attack will be unable to infect the system, since the OS and applications are precluded from accessing memory area 1 during runtime. Further, any attack that does reach memory 510 will be able to run only once and will disappear upon a hard restart. A triggering mechanism may be available to restart the mobile security system 345 automatically upon infection detection.

[0051] The network connection module 525 enables network connection, e.g., to the internet 330 or the intranet 315 via network communication hardware/software including WiFi, WiMAX, CDMA, GSM, GPRS, Ethernet, modem, etc. For example, if the mobile device 310 wishes to connect to the internet 330 via a WiFi connection, the adapters/ports/drivers 505 may be connected to the PCI port, USB port or PCMCIA port of the mobile device 310, and the network connection module 525 of the mobile security system 345 may include a WiFi network interface card for connecting to wireless access points. Using the network connection module 425, the mobile security system 345 may communicate with the network as a secure gateway for the mobile device 310. Other connection architectures are described in FIGS. 10A-10C.

[0052] The security engines 530 execute security programs based on the security policies 535 and on security data 540, both of which may be developed by IT managers. Security engines 530 may include firewalls, VPN, IPS/IDS, antivirus, antispymware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. Each security engine 530 may have dedicated security policies 535 and security data 540 to indicate which procedures, content, URLs, system calls, etc. the engines 530 may or may not allow. The security engines 530, security policies 535 and security data 540 may be the same as, a subset of, and/or developed from the engines, policies and data on the network security system 320.

[0053] To provide a higher security level provided by anti-virus and antispymware software, the security engines 530 on each mobile security system 345 may implement content analysis and risk assessment algorithms. Operating for example at OSI Layer 7 and above (mobile code encapsulated within Layer 7), these algorithms may be executed by dedicated High Risk Content Filtering (HRCF) that can be controlled by a rules engine and rule updates. The HRCF will be based on a powerful detection library that can perform deep content analysis to verify real content types. This is because many attacks are hidden within wrong mime types and/or may use sophisticated tricks to present a text file type to a dangerous active script or ActiveX content type. The HRCF may integrate with a URL categorization security engine 530 for automatic rule adjustment based on the URL category. In one embodiment, when the risk level increases (using the described mechanism) the mobile security system 345 may automatically adjust and increase filtering to remove more active content from the traffic. For example, if greater risk is determined, every piece of mobile code, e.g., Java script, VB script, etc. may be stripped out.

[0054] Three aspects for integration with corporate policy server legacy systems include rules, LDAP and active directory, and logging and reporting as discussed below. In one embodiment, a policy import agent running on the security administrator 325 will access the rule base of Checkpoint Firewall-1 and Cisco PIX Firewalls and import them into a local copy. A rule analysis module will process the important rules and will offer out-of-the-box rules and policies for mobile security systems 345. This proposed policy will offer all mobile security systems 345 a best fit of rules that conform the firewall policy of the enterprise 340. The agent will run periodically to reflect any changes and generate updates for mobile security system 345 policies 535. The LDAP and Active Directory may be integrated with the directory service to maintain mobile security system 345 security policies 535 that respond to the enterprise's directory definitions. For example, a corporate policy for LDAP user Group "G" may automatically propagate to all mobile security systems 345 in "G" group. Mobile security system 345 local logs and audit trails may be sent in accordance to a logging and reporting policy to a central log stored at the security administrator 325. Using a web interface, IT may be able to generate reports and audit views related to all mobile device 310 users, their internet experiences, and attempts to bring infected devices back to the enterprise 340. IT will be able to forward events and log records into legacy management systems via SYSLOG and SNMP Traps.

[0055] The security engines 530 may perform weighted risk analysis. For example, the security engine 530 may analyze HTTP, FTP, SMTP, POP3, IM, P2P, etc. including any

traffic arriving from the internet 330. The security engine 530 may assign a weight and rank for every object based on its type, complexity, richness in abilities, source of the object, etc. The security engine 530 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 530 may assign weight to objects based on the category of the source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 530 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 530 may "learn" user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

[0056] In some embodiments, the security engines 530, security policies 535 and security data 540 may enable bypassing the mobile security system 345. The security policy 535, set by the security administrator 325, may include a special attribute to force network connection through the mobile security system 325 when outside the trusted enterprise 340. Thus, if this attribute is set "on," when a mobile device 310 attempts to connect to the internet 330 without the mobile security system 345 and not from within the trusted enterprise 340, all data transfer connections including LAN connection, USB-net, modem, Bluetooth, WiFi, etc. may be closed. The mobile device 310 may be totally isolated and unable to connect to any network, including the internet 330.

[0057] In one embodiment, to enable this, when first connecting the mobile security system 345 to the mobile device 310 using for example the USB cable (for both power and USB connection creation), the USB plug & play device driver will be sent into the mobile device 310. The installed driver may be "Linux.inf" which allows a USB-net connection for the mobile security system 345. This connection allows the mobile security system 345 to access the internet 330 via the USB port and using the mobile device 310 network connection plus additional code ("the connection client"). In a Windows example, the connection client may be installed at the NDIS level of the mobile device 310 above all the network interface cards of every network connection as shown in FIG. 6. The implementation will be as an NDIS Intermediate (IM) Driver or NDIS-Hooking Filter Driver. Both implementations may be at the kernel level, so that an end user cannot stop or remove it. When starting the mobile device 310, the connection client may attempt to connect to the security administrator 325 or the network security system 320 locally within the trusted enterprise 340. If the node is not found (finding via VPN is considered as not found in local LAN), the connection client will assume it is working from outside the trusted enterprise 340 and expects to find the mobile security system 345 connected, e.g., via USB-net or other connection mechanism. If the mobile security system 345 is not found, the connection client may avoid any communication to any network connection. By a policy definition, this behavior can be modified to allow communication to the enterprise 340 via VPN installed in the mobile device 310. Similarly, in case of a mobile device system 345 failure, all traffic may be disabled, except for the VPN connection into the enterprise 340.

[0058] It will be appreciated that NDIS is one possible implementation of intercepting traffic at the kernel level. For example, in another embodiment, the system may hook Winsock or apply other ways that may be in future Windows versions.

[0059] In an embodiment where the mobile security system 345 supports multiple mobile devices 310, the security engines 530, security policies 535 and security data 540 may be different for each mobile device 310 (e.g., based on for example user preferences or IT decision). Alternatively, it can apply the same engines 530, policies 535 and data 540 for all connected devices 310.

[0060] The remote management module 550 enables communication with security administrator 325 (and/or other security administrators), and enables local updating of security engines 530, security policies 535, security data 540 including signatures and other applications. In one embodiment, modification to the security policies 535 and data 540 can be done by the security administrator 325 only. The remote management module 550 of the mobile security system 345 may receive updates from an update authorities device (UAD), e.g., on the security administrator 325 via a secured connection. A UAD may operate on an update server at a customer IT center located on the internet 330 to forward updates to mobile security systems 345 that possibly do not belong to an enterprise 540 in charge of managing updates. A UAD may operate on a mobile security system 345. Security engine 530 updates may modify the antivirus engine DLL, etc. OS and security application updates may be implemented only from within the enterprise 540 while connecting to the security administrator 325 and via an encrypted and authenticated connection.

[0061] The security administrator 325 can modify URL black and white lists for remote support to traveling users. In case of false positives, the security administrator 325 may allow access to certain URLs, by bypassing the proactive heuristics security but still monitoring by firewall, antivirus, IPS/IDS, etc. Additional remote device-management features may enable the security administrator 325 to perform remote diagnostics, access local logs, change configuration parameters, etc. on the mobile security system 345. The security administrator 325 may delegate tasks to a helpdesk for support.

[0062] The remote management module 550 may communicate with a wizard (e.g., wizard 745), which may be on the security administrator 325, as illustrated in FIG. 7, or on another system. Details of the wizard 745 and details of the communication schemes between the remote management module 550 and the wizard 745 are described below with reference to FIG. 7.

[0063] The distribution module 555 enables distribution of updates, e.g., security policy 535 updates including rule updates, security data 540 updates including signature updates, security engine 530 updates, application/OS updates, etc. by the mobile security system 345 to N other mobile security systems 345. A routing table identifying the N other mobile security systems 345 to whom to forward the updates may be provided to the distribution module 555 to enable system 345 to system 345 communication. Updates may be implemented according to policies set by the security administrator 325. When forwarding updates, the distribution module 555 acts as a UAD.

[0064] Each mobile security system 345 may obtain its routing table with security information updates, periodically,

at predetermined times, upon login, etc. The routing tables may be maintained on a server, e.g., the security administrator 325 or another mobile security system 345. In one embodiment, the mobile security systems 345 may contact the server to retrieve the routing tables. Alternatively, the server may push the routing tables to the mobile security systems 345.

[0065] The distribution module 555 may enable rapid updates as shown in FIG. 9. Currently, all commercial anti-virus products available do not update devices faster than viruses spread. To assure that a new virus attack does not spread faster than for example signature updates, each mobile security system 345 may be an active UAD. In one embodiment, as shown in FIG. 9, each mobile security system 345 is responsible for forwarding the signature updates to four other devices 345. As one skilled in the art will recognize, all devices 345 need to forward to the same number of other devices 345. Multiple devices 345 may be responsible for forwarding to the same device 345. When necessary, offline devices 345 being activated may poll the server, e.g., the security administrator 325, for routing table updates. Many other updating techniques are also possible.

[0066] The backup module 560 may constantly backup image and changes of the boot sector and system files of the mobile device 310 into the flash memory 520 or into another persistent memory device. That way, in case of major failure, including a loss of the system or boot sector of the mobile device 310, the mobile security system 345 may be identified as a CD-ROM during reboot and may launch the backup module (or separate program) to restore the boot sector and system files on the mobile device 310, thereby recovering the mobile device 310 without the need for IT support. In an embodiment where the network security system 345 supports multiple mobile devices 310, the backup module 560 may contain separate boot sector and system files for each of the mobile devices 310, if different.

[0067] FIG. 7 is a block diagram illustrating details of a smart policy updating system 700 in accordance with an embodiment of the present invention. System 700 includes the security administrator 325 coupled to the network security system 320 and to the mobile security system 345. The network security system 320 includes security engines 705, including an antivirus engine 715, an IPS/IDS engine 720, a firewall engine 725, and other security engines. The network security system 320 also includes security policies and data 710, including antivirus policies and data 730, IPS/IDS policies and data 735, firewall policies and data 740, and other policies and data. Similarly, the mobile security system 345 includes an antivirus engine 755, an IPS/IDS engine 760, a firewall engine 765, and other engines. The mobile security system 345 also includes security policies and data 535/540, including antivirus security policies and data 770, IPS/IDS security policies and data 775, firewall security policies and data 780, and other security policies and data.

[0068] The security administrator 325 includes a wizard 745 for enabling substantially automatic initial and possibly dynamic setup of the security engines 530, security policies 535 and security data 540 on the mobile security system 345. In one embodiment, the wizard 745 may automatically load all security engines 705 and policies and data 710 of the network security system 320 as the security engines 530 and policies and data 535/540 on the mobile security system 345. In another embodiment, the wizard 745 may include all security engines 705 and policies and data 710 except those known to be irrelevant, e.g., those related to billing software

used by accounting, those relating to web software running only on the web servers, etc. In another embodiment, the engines 530 would need to be loaded by an IT manager, and would not be loaded automatically by the wizard 745.

[0069] In one embodiment, the wizard 745 may determine whether the mobile security system 345 requires a particular security engine 530, e.g., an antivirus engine 755, IPS/IDS engine 760, firewall engine 765, etc. If so determined, then the wizard 745 would load the engine 530 onto the mobile security system 345. The wizard 745 would then determine which policies and data sets, e.g., some for antivirus engine 755, some for the IPS/IDS engine 760, some for the firewall engine 765, etc. are important to the mobile security system 345. The wizard 745 will then determine which of the anti-virus policies and data 730 on the network security system 320 are relevant to the antivirus policies and data 770 on the mobile security system 345, which of the IPS/IDS policies and data 735 on the network security system 320 are relevant to the IPS/IDS policies and data 775 on the mobile security system 345, which of the firewall policies and data 740 on the network security system 320 are relevant to the firewall policies and data 780 on the mobile security system 345, and which of the other policies and data on the network security system 320 are relevant to the policies and data on the mobile security system 345. As stated above, the wizard 745 may determine that all security engines 705 or just a subset are needed on the mobile security system 345. The wizard 745 may determine that all policies and data 710 for a given engine type or just a subset should be forwarded. The wizard 745 may determine which relevant policies and data 710 should be forwarded to the mobile security system 345 based on rules developed by an IT manager, based on item-by-item selection during the setup procedure, etc. Alternative to the wizard 745, an IT manager can setup the engines 530 and policies and data 535/540 on the mobile security system 345 without the wizard 745.

[0070] The security administrator 325 may also include an update authorities device 750. The update authorities device 750 may obtain security system updates (e.g., signature updates) and may send the updates to the network security system 320 and to the mobile security system 345. One skilled in the art will recognize that the updates to the network security system 320 and the updates to the mobile security system 345 need not be the same. Further, the update authorities device 750 may obtain the updates from security managers, security engine developers, antivirus specialists, etc. The update authorities device 750 may forward the updates to all network security systems 320 and all mobile security systems 345, or may forward routing tables to all mobile security systems 345 and the updates only to an initial set of mobile security systems 345. The initial set of mobile security systems 345 may forward the updates to the mobile security systems 345 identified in the routing tables in a P2P manner, similar to the process illustrated in FIG. 9. As stated above, each mobile security system 345 operating to forward updates is itself acting as an update authorities device 750.

[0071] Other applications may be included on the mobile security system 345. For example, add-on applications for recurring revenue from existing customers may include general email, anti-spam, direct and secured email delivery, information vaults, safe skype and other instant messaging services, etc.

[0072] Email Security and Anti-spam—implementation of mail relay on mobile security systems 345 (including

the web security engine above) and a local spam quarantine (based on SendMail or similar process) may implement a complete mail security suite (SMTP and POP3) including anti-spam with real time indexing (via online web spam quarries). Users may have access to the quarantine to review spam messages, release messages, modify and custom spam rules, etc., via a web interface.

[0073] Direct and Secured Email Delivery based on mail relay will allow the mobile security system 345 to send user email directly from one mobile security system 345 to another mobile security system 345 without using in route mail servers. This allows corporate users to send emails that need not travel in the internet, thus leaving trace and duplicates on different unknown mail servers in route. This combined with the ability to use a secured pipe between two mobile security systems is valuable to corporations. Without such methodology, people could trace emails exchange without accessing to the enterprise's mail server, by tracking down copies in intermediate mail servers that were used to deliver the messages.

[0074] Information Vault—Application to encrypt and store end user information on the mobile security system 345 may be available only to authorized users via a web interface and a web server implemented on every mobile security system 345 (e.g., BOA, Apache, etc.)

[0075] Safe Skype and Other IM—implementing an instant messaging client on the mobile security system 345 can guarantee that the instant messaging system or P2P application has no access to data on the mobile device 310. Adding a chipset of AC/97 to provide a sound interface on the mobile security system 325 could allow users to talk and receive calls directly from/to the mobile security system 325.

[0076] Although not shown, a small battery may be included with the mobile security system 345. This battery may be charged by the USB connection during runtime or using the power adapter at any time. The battery may guarantee proper shutdown, e.g., when user disconnects the USB cable from the mobile security system 345. It will be signaled by the system which will launch applications and system shutdown. This will ensure a proper state of the file system and flashing open files buffers.

[0077] A multi-layered defense and detection abilities is required. This may be done by a special code that is constantly monitoring the scanning result by different systems (antivirus, IDS/IPS, firewall, antispysware, URL category, etc.) and at different levels to build a puzzle and identify an attack even if its not recognized by each of the individual subsystems. By doing this, the mobile security system 345 will maintain and in some cases even improve the security level provided within the enterprise 540.

[0078] One available benefit of the mobile security system 345 is its ability to enforce the policy of the enterprise 540 on the end user while they are traveling or working from home. Since the mobile security system 345 uses similar security engines and policy as when connected from within the enterprise 540 and since the end user cannot access the internet 330 without it (except via VPN connection into the enterprise 540), IT may be capable of enforcing its security policy beyond the boundaries of the enterprise 540. The OS may be under the entire supervision of IT, while the mobile security system 345OS acts as an end user OS under his control. This resolves the problems of who controls what and how security and productivity face minimal compromise.

[0079] A standalone version of the mobile security system 345 may offer the same functionality, and may provide a local management interface via web browser. Attractive to home users and small offices that lack an IT department, the mobile security system 345 enables the end user to launch a browser, connect to the mobile security system 345, set the different policies (update policy, security rules, etc.) including modifying the white and black URL lists, etc. There is also an opportunity to provide end users with a service of remote management of the mobile security systems 345 by subscription.

[0080] FIGS. 10A, 10B and 10C illustrate three example architectures of connecting a mobile security system 345 to a mobile device 310, in accordance with various embodiments of the present invention. In FIG. 10A, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1015 and 1020 and is coupled to the internet 330 via a NIC card 1005. The mobile device 310 receives internet traffic from the internet 330 via its NIC card 1005. A kernel-level redirector 1010 (e.g., via NDIS, Winsock, etc.) on the mobile device 310 automatically redirects the internet traffic via the USB connections 1015 and 1020 to the mobile security system 345, which scans, cleans and returns the cleaned internet traffic to the mobile device 310 via the USB connections 1015 and 1020. In FIG. 10B, the mobile device 310 is coupled to the mobile security system 345 via USB connections 1025 and 1030. The mobile security system 345 includes a NIC card 1035 for receiving internet traffic from the internet 330. The mobile security system 345 scans, cleans and forwards the internet traffic via the USB connections 1025 and 1030 to the mobile device 310. In FIG. 10C, the mobile device 310 is coupled to the mobile security system 345 via NIC cards 1040 and 1045. The mobile security system 345 receives internet traffic from the internet 330 via its NIC card 1045. The mobile security system 345 scans, cleans and forwards the internet traffic wirelessly via the NIC cards 1040 and 1045 to the mobile device 310. Other connection architectures are also possible.

[0081] FIG. 12 is a block diagram illustrating a secure data exchange system 1200, in accordance with an embodiment of the present invention. The secure data exchange system 1200 includes a host computer (host) 1205 coupled via a security device 1210 to an external device 1110. The host 1205 may include a laptop, desktop, PDA, mobile phone, or other processor-based device. The external device 1110 may be any external device with memory such as a USB drive, external hard drive, PDA, music player, cell phone, etc. The security device 1210 is communicatively coupled to the host 1205 via an ED port 1225 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and an ED plug 1230 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The external device 1110 is communicatively coupled to the security device 1210 via an ED port 1235 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection) and ED plug 1120 (USB, serial, parallel, Firewire, Ethernet, WiFi, WiMAX, GSM, CDMA, BlueTooth, PCMCIA and/or other connection). The connector type of the ED port 1225 and ED plug 1230 combination may be different than the collector type of the ED port 1235 and ED plug 1120 combination. In one embodiment, all ports 1225/1235 and plugs 1230/1120 are USB. Although the plugs 1120/1230 are illustrated as male

and ports 1225/1235 are shown as female, one skilled in the art will recognize that the opposite is possible (plugs 1120/1230 may be female and ports 1225/1235 may be male).

[0082] The host 1205 includes ED drivers 1220 for performing enumeration and enabling communication with the security device 1210. Similarly, the security device 1210 includes ED drivers 1245 for performing enumeration and enabling communication with the external device 1110.

[0083] In one embodiment, the security device 1210 includes a programmable hardware appliance capable of enforcing security policies to protect against malicious code such as viruses, spyware, adware, Trojan Horses, etc. and to protect against transfer of private data. In one embodiment, the security device 1210 is configured to protect both the host 1205 and the external device 1215. In one embodiment, the security device 1210 is configured to protect only one of the external device 1110 or the host 1205. Additional details of the security device 1210 are provided with reference to FIGS. 13 and 14.

[0084] FIG. 13 is a block diagram illustrating details of the security device 1210, in accordance with an embodiment of the present invention. The security device 1210 include a processor 1305, such as an Intel Pentium® microprocessor or a Motorola Power PC® microprocessor, coupled to a communications channel 1315. The security device 1210 further includes an ED plug 1230, an ED port 1235, a communications interface 1310, storage 1320 such as an EEPROM, and memory 1325 such as Random-Access Memory (RAM) or Read Only Memory (ROM), each coupled to the communications channel 1315. The communications interface 1310 may be coupled to a network such as the internet. One skilled in the art will recognize that, although the storage 1320 and memory 1325 are illustrated as different units, the data storage device 1320 and memory 1325 can be parts of the same unit, distributed units, virtual memory, etc. The term “memory” herein is intended to cover all data storage media whether permanent or temporary. One skilled in the art will recognize that the security device 1210 may include additional components, such as network connections, additional memory, additional processors, LANs, input/output lines for transferring information across a hardware channel, the internet or an intranet, etc.

[0085] As shown, memory 1325 stores an operating system 1330 such as the Microsoft Windows XP, the IBM OS/2 operating system, the MAC OS, Unix OS, Linux OS, etc. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. An embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, possibly using object oriented programming methodology. The memory 1325 also stores ED drivers 1245 and a security system 1335. The ED drivers 1245 may include standard drivers for standard external devices 1110 and proprietary drivers for proprietary external devices 1110. The ED drivers 1245 may be transferred onto the memory 1325 via ED plug 1230. The security system 1335 includes code for enforcing security policies on data transfer actions between the host 1205 and external device 1110.

[0086] FIG. 14 is a block diagram illustrating details of a security system 1335, in accordance with an embodiment of the present invention. The security system 1335 includes a security manager 1405, security engines 1410, security policies 1415, and security data 1420.

[0087] In one embodiment, the security manager 1405 includes code for performing enumeration, namely, to identify the external device 1110 or external device 1110 type and to identify the corresponding ED driver 1245 capable of establishing communication between the security device 1210 and the external device 1110. The security manager 1405 also includes code to control execution of the various security engines 1410 based on the security policies 1415 and security data 1420 to evaluate data transfer requests or other device requests. Further, the security manager 1405 includes code to communicate with the host 1205, which will be the source of the data transfer and/or other requests.

[0088] In one embodiment, the security engines 1410 includes code for securing the transfer of data between the host 1205 and the external device 1110 based on the security policies 1415 and security data 1420. The security engines 1410 may include firewalls, antivirus, antispyware, malicious content filtering, multilayered security monitors, Java and bytecode monitors, etc. The security engines 1410 may also include data privacy modules to enforce data privacy policies 1415. Each security engine 1410 may have dedicated security policies 1415 and security data 1420 to indicate which procedures, URLs, system calls, content, ID, etc. the data requested for transfer may contain or whether the data requested for transfer is considered nontransferable (or non-transferable without additional security measure such as a password and ID).

[0089] To provide a higher security level, the security engines 1410 may implement content analysis and risk assessment algorithms. In one embodiment, a security engine 1410 assigns a weight and rank for every transfer object based on its type, complexity, richness in abilities, source, etc. The security engine 1410 may assign weight based on the source using a list of known dangerous or known safe sources. The security engine 1410 may assign weight to objects based on the category of the source, e.g., a gambling source, an adult content source, a news source, a reputable company source, a banking source, etc. The security engine 1410 may calculate the weight, and based on the result determine whether to allow or disallow access to the content, the script to run, the system modification to occur, etc. The security engine 1410 may “learn” user content (by analyzing for a predetermined period of time the general content that the user accesses) and accordingly may create personal content profiles. The personal content profile may be used to calibrate the weight assigned to content during runtime analysis to improve accuracy and tailor weighted risk analysis for specific user characteristics.

[0090] Thus, upon receiving a data transfer and/or other request from the host 1205, the security manager 1405 will launch the appropriate security engines 1410 based on the security policies 1415. For example, the security policies 1415 may be configured not to allow specific ActiveX controls to be loaded from the host 1205 onto the external device 1110. The security policies 1415 may be configured not to allow data transfer from private folders on the host 1205 to the external device 1110. The security manager 1405 will launch the appropriate security engines 1410 to assure that these example security policies 1415 are met. Further, the security engines 1410 may use security data 1420, which may include definition files of malicious ActiveX controls, locations of private folders, etc.

[0091] Although not shown, the security system 1335 may include additional components such as the preboot flash 520

with OS and applications, the remote management module 550, the distribution module 555, and the backup module 560 discussed above with reference to FIG. 5. Other components are also possible.

[0092] FIG. 15 is a block diagram illustrating a secure data exchange system 1500, in accordance with another embodiment of the present invention. The secure data exchange system 1500 includes a security device 1505 communicatively coupled to the host 1520 via an ED plug 1515 on the security device 1505 and a first ED port 1525 on the host 1520. The secure data exchange system 1500 also includes an external device 1110 communicatively coupled to the host 1520 via the ED plug 1120 on the external device 1110 and a second ED port 1535 on the host 1520.

[0093] Because the external device 1110 is not directly coupled to the security device 1505, the security device 1505 is not physically intercepting the data transfer requests between the external device 1110 and the host 1520. Accordingly, in this embodiment, the host 1520 includes a redirect driver 1530, which is configured to redirect data transfer requests between the external device 1110 and the host 1520 regardless of data transfer direction. In one embodiment, the security device 1505 may be configured to protect only one of the external device 1110 or the host 1520. Further, in one embodiment, the security device 1505 does not contain any ED drivers, e.g., ED drivers 1245.

[0094] In one embodiment, if the security device 1505 is not coupled to the host 1520, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110. In one embodiment, the host 1520 is configured not to communicate with the external device 1110 until the security device 1505 is coupled to the host 1520. In one embodiment, the host 1520 uses the ED drivers 1540 to communicate with the external device 1110 only if additional security measures are taken, such as receipt of a password and ID, or until the security device 1505 is coupled to the host 1520.

[0095] In one embodiment, the host 1520 may conduct enumeration of the security device 1505 upon connection of the security device 1505 to the ED port 1525. Upon identifying the security device 1505 or security device 1505 type, the host 1520 may initiate the redirect driver 1530 to redirect all data transfer requests or other external device 1110 requests from all other ED ports 1535 to the security device 1505. In one embodiment, the redirect driver 1530 only accepts data transfer requests from the security device 1505, which presents the requests of the external device 1110 as a proxy. In one embodiment, the redirect driver 1530 performs data transfer requests received from the external device 1110 only after the security device 1505 has conducted its check and given its authorization. Other protocols are also possible.

[0096] FIG. 16 is a flowchart illustrating a method 1600 of secure data exchange between a host and an external device, in accordance with an embodiment of the present invention. The method 1600 begins in step 1605 with the security device 1505 being connected to the first ED port 1525 of the host 1520. The external device 1110 in step 1610 is connected to the second ED port 1535 of the host 1520. The host 1505 in step 1615 performs enumeration techniques to identify the security device 1505 and the external device 1110 and to install the appropriate drivers 1530/1540 to enable communication with the security device 1505 and the external device 1110. The redirect driver 1530 in step 1620 receives a data transfer request from either the host 1505 to the external device 1110 or from the external device 1110 to the host 1505.

The redirect driver **1530** in step **1625** redirects the data transfer request to the security device **1505**, which in step **1630** enforces its security policies (antivirus, antispysware, anti-adware, data privacy, etc.) on the data transfer request. The security device **1505** in step **1635** determines whether the data transfer request passes the security policies. If so, then the security device **1505** in step **1640** authorizes the data transfer request and the host **1520** in step **1645** performs the data transfer request. If not, then the security device **1505** in step **1650** rejects the data transfer request. Method **1600** then ends.

[0097] It will be appreciated that, in one embodiment, the security device **1210/1505** may be implemented as part of the host **1205/1520**, e.g., within the housing of the host **1205/1520** and/or as a security procedure executed by the host **1205/1520**.

[0098] The foregoing description of the preferred embodiments of the present invention is by way of example only, and other variations and modifications of the above-described embodiments and methods are possible in light of the foregoing teaching. Although the network sites are being described as separate and distinct sites, one skilled in the art will recognize that these sites may be a part of an integral site, may each include portions of multiple sites, or may include combinations of single and multiple sites. The various embodiments set forth herein may be implemented utilizing hardware, software, or any desired combination thereof. For that matter, any type of logic may be utilized which is capable of implementing the various functionality set forth herein. Components may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of interconnected conventional components and circuits. Connections may be wired, wireless, modem, etc. The embodiments described herein are not intended to be exhaustive or limiting. The present invention is limited only by the following claims.

1. A security device, comprising:
  - an external device plug operative to communicatively couple with a host;
  - an external device port operative to communicatively couple with an external device;
  - a processor; and
  - memory storing
    - an operating system,
    - an external device driver operative to control communication with the external device, and
    - a security engine operative to enforce a security policy on a data transfer request between the external device and the host.
2. The security device of claim 1, wherein the security device is operative with a driver on the host.
3. The security device of claim 1, wherein at least one of the external device plug and the external device port follows a USB standard.
4. The security device of claim 1, wherein at least one of the external device plug and the external device port includes a wireless connection.
5. The security device of claim 1, wherein the security engine protects against the transfer of at least one of viruses, spyware and adware.
6. The security device of claim 1, wherein the security engine protects against the unauthorized transfer of private data.

7. A secure data exchange system, comprising:
  - a security device including
    - a first external device plug; and
    - a security engine operative to enforce a security policy on data transfer requests received from the host;
  - an external device including
    - a second external device plug; and
  - a host including
    - a first external device port operative to communicatively couple with the first external device plug;
    - a second external device port operative to communicatively couple with the second external device plug; and
    - a redirect driver operative to transfer a data transfer request from the host to the security device before executing the data transfer request.
8. The secure data exchange system of claim 7, wherein the external device includes a USB drive.
9. The secure data exchange system of claim 7, wherein the external device includes one of a PDA or a cell phone.
10. The secure data exchange system of claim 7, wherein the host includes one of a laptop, desktop, PDA or cell phone.
11. The secure data exchange system of claim 7, wherein the host launches the redirect driver upon detecting connection of the secure device to the host.
12. A method comprising:
  - communicatively coupling a security device to a host;
  - communicatively coupling an external device to the security device;
  - receiving by the security device a data transfer request from the host; and
  - enforcing by the security device a security policy on the data transfer request before allowing the data transfer request to be performed.
13. The method of claim 12, wherein the communicatively coupling a security device to a host includes using a wired or wireless connection.
14. The method of claim 12, wherein the communicatively coupling an external device to the host includes using a wired or wireless connection.
15. The method of claim 12, wherein the data transfer request includes a request to transfer data from the host to the external device.
16. The method of claim 12, wherein the data transfer request includes a request to transfer data from the external device to the host.
17. The method of claim 12, wherein the enforcing includes reviewing the data being transferred for at least one of viruses, spyware and adware.
18. The method of claim 12, wherein the enforcing includes determining whether the data transfer request includes a request for private data.
19. The method of claim 18, wherein the enforcing includes requiring an additional security check before allowing the transfer of private data.
20. A method, comprising:
  - communicatively coupling a security device to a host;
  - communicatively coupling an external device to the host;
  - receiving by the host a data transfer request;
  - using a redirect driver on the host to redirect the data transfer request to the security device; and
  - enforcing by the security device a security policy on the data transfer request before allowing the data transfer request to be performed.

21. The method of claim 20, wherein the communicatively coupling a security device to a host includes using a wired or wireless connection.

22. The method of claim 20, wherein the communicatively coupling an external device to the host includes using a wired or wireless connection.

23. The method of claim 20, wherein the data transfer request includes a request to transfer data from the host to the external device.

24. The method of claim 20, wherein the data transfer request includes a request to transfer data from the external device to the host.

25. The method of claim 20, wherein the enforcing includes reviewing the data being transferred for at least one of viruses, spyware and adware.

26. The method of claim 20, wherein the enforcing includes determining whether the data transfer request includes a request for private data.

27. The method of claim 26, wherein the enforcing includes requiring an additional security check before allowing the transfer of private data.

\* \* \* \* \*