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

(19) **World Intellectual Property Organization**
International Bureau

(43) **International Publication Date**
12 January 2006 (12.01.2006)

PCT

(10) **International Publication Number**
WO 2006/004786 A1

(51) **International Patent Classification**^{7}: **H04L 29/06**

(21) **International Application Number:** PCT/US2005/022984

(22) **International Filing Date:** 27 June 2005 (27.06.2005)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**

60/583,765	28 June 2004 (28.06.2004)	US
60/598,364	3 August 2004 (03.08.2004)	US
60/652,121	11 February 2005 (11.02.2005)	US
60/653,411	16 February 2005 (16.02.2005)	US

(71) **Applicant** *(for all designated States except US)*: **JAPAN COMMUNICATIONS, INC.** [JP/JP]; 6-25-3 Minami-ohi, Shinagawa-ku, Tokyo, Tokyo 140-0013 (JP).

(72) **Inventors; and**

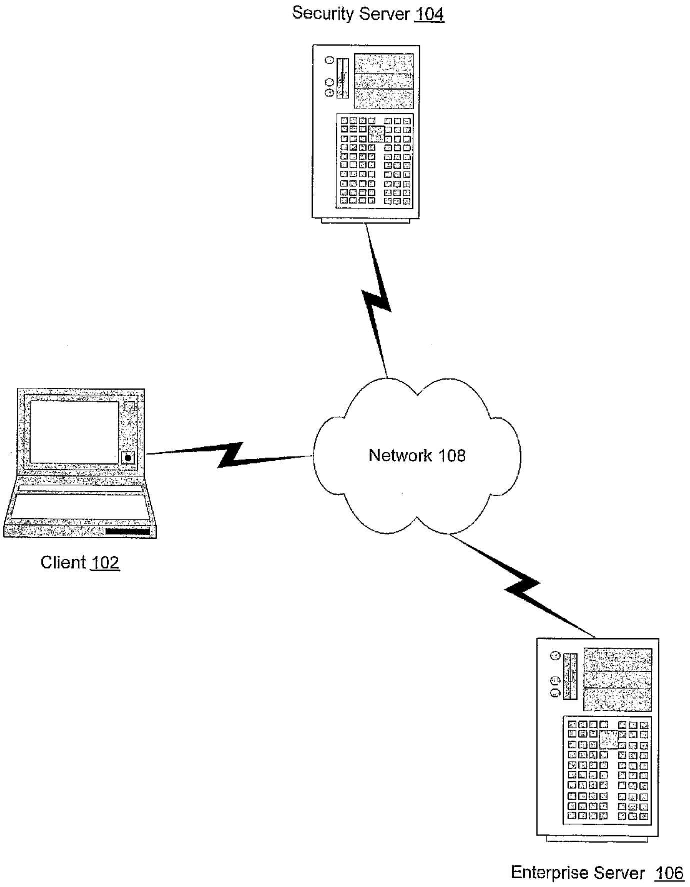
(75) **Inventors/Applicants** *(for US only)*: **SANDA, Frank, S.** [JP/US]; 29 Plandome Court, Manhasset, New York 11030 (US). **FUKUDA, Naohisa** [JP/JP]; #405, 6-1-8 Kita-Shinagawa, Shinagawa-ku, Tokyo, Tokyo 141-0001 (JP). **LAVES, Edward, W.** [US/US]; 1012 Sleepy Hollow Road, Golden, Colorado 80401 (US). **GURGONE, Raymond, T.** [US/US]; 807 N. Concord Drive, Woodstock, Illinois 60098 (US). **JOHNSTON, Robert, L.** [US/US]; 30 Midland Road, Colorado Springs, Colorado 80906 (US). **ROBINS, David, S.** [US/US]; 6 Wakefield Court, Buffalo Grove, Illinois 60089 (US). **TIDWELL, Justin, Owen** [US/US]; 19058 East Hampden Drive, Aurora, Colorado 80013 (US). **ZEITZ, Karlton, Mark** [US/US]; 6014 S. Zeno Court, Centennial, Colorado 80016 (US). **WORTHINGTON, Laura, J.** [US/US]; 6295 E. Jamison Circle North, Centennial, Colorado 80112 (US).

(74) **Agent: ALEMANNI, John, C.**; Kilpatrick Stockton LLP, 1001 West Fourth Street, Winston-Salem, North Carolina 27101, (US).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE,

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD FOR ENHANCED NETWORK CLIENT SECURITY



(57) **Abstract:** Systems are methods for enhanced network client security are described. One aspect of one embodiment of the present invention includes receiving a security-related policy associated with a user, determining a security model associated with the security-related policy, and applying the security model to a network connection on a client device. One aspect of another embodiment of the present invention includes receiving a first measure associated with a usage characteristic, the usage characteristic associated with a user, receiving a second measure associated with the usage characteristic, comparing the first measure and second measure, and determining the likelihood that an unauthorized access has occurred based at least in part on the comparison.

KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

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

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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

SYSTEM AND METHOD FOR ENHANCED NETWORK CLIENT SECURITY

RELATED APPLICATIONS

This application claims priority to Application Serial No. 60/583,765, filed on June 28, 2004, titled "Controlling Use of a Mobile Work Station Based on Network Environment," Application Serial No. 60/598,364, filed on August 3, 2004, titled "Systems and Methods for Enhancing and Optimizing a User's Experience on an Electronic Device," Application Serial No. 60/652,121, filed on February 11, 2005, titled "Remote Access Services," and Application Serial No. 60/653,411, filed on February 16, 2005, titled "Creating an Environment for Secure Mobile Access Anywhere," the entirety of all of which are incorporated herein by reference.

FIELD OF THE INVENTION

The present invention relates generally to computer networking and, more particularly to systems and methods for enhanced network client security.

BACKGROUND

As the workforce becomes more mobile, enterprises often must provide a means for their users to connect to the enterprise network remotely. Enterprises and their users have much greater flexibility in selecting methods of connecting to the enterprise network as well as other resources, such as the Internet. With this added flexibility comes a concomitant increase in complexity and risk. Thus, although remote access may be necessary, enterprises may resist providing their users with remote access.

Each remote method for connecting to an enterprise network opens a potential security hole that might be exploited. For instance, listeners on a network, such as rogue access points, may be able to determine a user's username/password combination for accessing the network. Also, remote users may expose username/password combinations by, for example, writing them on a card affixed to a laptop. Once exposed, unscrupulous persons may gain access to the username/password combinations and then log into an enterprise's systems, posing as the authorized user. The enterprise typically has limited means to determine that a user utilizing a valid username and password is actually unauthorized.

SUMMARY

Embodiments of the present invention provide systems and methods for enhanced network client security. One aspect of one embodiment of the present invention comprises receiving a security-related policy associated with a user, determining a security model associated with the security-related policy, and applying the security model to a network connection on a client device. One aspect of another embodiment of the present invention comprises receiving a first measure associated with a usage characteristic, the usage characteristic associated with a user, receiving a second measure associated with the usage characteristic, comparing the first measure and second measure, and determining the likelihood that an unauthorized access has occurred based at least in part on the comparison. In another embodiment, a computer-readable medium (such as, for example random access memory or a computer disk) comprises code for carrying out such methods.

These illustrative embodiments are mentioned not to limit or define the invention, but to provide examples to aid understanding thereof. Illustrative embodiments are discussed in the Detailed Description, and further description of the invention is provided there. Advantages offered by the various embodiments of the present invention may be further understood by examining this specification.

FIGURES

These and other features, aspects, and advantages of the present invention are better understood when the following Detailed Description is read with reference to the accompanying drawings, wherein:

Figure 1 is a block diagram showing an illustrative environment for implementation of one embodiment of the present invention;

Figure 2 is a block diagram illustrating the modules present on a client device 102 in one embodiment of the present invention;

Figure 3 is a block diagram illustrating the modules present on a security server 104 in one embodiment of the present invention;

Figure 4 is a block diagram illustrating the modules present on an enterprise server 106 in one embodiment of the present invention;

Figure 5 is a flowchart illustrating a process for applying a security model to a network connection in one embodiment of the present invention; and

Figure 6 is a flowchart illustrating a process for statistical attack determination in one embodiment of the present invention.

DETAILED DESCRIPTION

Embodiments of the present invention provide systems and methods for enhanced network client security. There are multiple embodiments of the present invention. By way of introduction and example, one illustrative embodiment of the present invention provides a method for centralized security management. In such an embodiment, an administrator establishes one or more security-related policies.

For instance, the administrator may determine that only client devices having a personal firewall and the latest virus definition files are to be allowed to connect to the enterprises confidential data via a Wi-Fi connection. However, only a VPN is required for a dial-up line. The administrator establishes the policies in a central policy server. When a user logs into the enterprise server, the policies are downloaded to the user's client device.

When the user next attempts to log in to the enterprise server via a Wi-Fi connection, a connection manager on the client device generates a security model based on the security-related policy. The connection manager then applies the connection model to the Wi-Fi connection. If the user does not have an active personal firewall and the latest virus definitions, the connection to the enterprise server is broken down. The user may still access the enterprise server via other network types, depending on the security model for each of the network types.

The administrator can modify and add policies based on changes to available network types, security threats, and other reasons. The changes are dynamically applied to the client in a manner that is transparent to the user.

This introduction is given to introduce the reader to the general subject matter of the application. By no means is the invention limited to such subject matter. Illustrative embodiments are described below.

System Architecture

Various systems in accordance with the present invention may be constructed. Referring now to the drawings in which like numerals indicate like elements throughout the several figures, Figure 1 is a block diagram showing an illustrative environment for implementation of one embodiment of the present invention. The system shown in Figure 1 includes a client 102. The client is in communication with a security server 104.

Communication with the security server 104 occurs via a network 108. The network 108 may comprise a public or private network and may include the Internet. The network may also comprise a plurality of networks, including, for example, dedicated phone lines between the various components. In one embodiment, the client 102 communicates with the security server 104 via a virtual private network ("VPN") established over the Internet.

The security server 104 is also in communication with an enterprise server 106 via a network. The network 108 may comprise various elements, both wired and wireless. In one embodiment, the communication between the security server 104 and enterprise server 106 occurs over a static VPN established over dedicated communication lines.

In one embodiment, a user connects a client device 102 to the network 108 using a network access user interface. The network access user interface is always on and only allows the user to connect to the network 108 via the interface. The network access user interface automatically causes the client 102 to connect to the security server 104 through the network 108. The security server 104 provides value added services to the client 102 and to one or more enterprises. Access to other services, such as the Internet, may be provided via the security server 104.

Although Figure 1 includes only a single client 102, security server 104, and enterprise server 106, an embodiment of the present invention will typically include a plurality of clients 102 and may include a plurality of security servers 104 and enterprise servers 106.

Figures 2 through 4 are block diagrams illustrating components on the client 102, security server 104, and enterprise server 106. Each of the components shown may be a third-party application, a custom application, or a combination of both. Each of the components may also be implemented in hardware, software, or a combination of hardware and software.

Client Devices

Figure 2 is a block diagram illustrating the modules present on a client device 102 in one embodiment of the present invention. Examples of client device 102 are personal computers, digital assistants, personal digital assistants, cellular phones, mobile phones, smart phones, pagers, digital tablets, laptop computers, Internet appliances, and other processor-based devices. In general, a client device 102 may be any suitable type of processor-based platform that is connected to the network 108, and that interacts with one or more application programs. The client device 102 can contain a processor coupled to a computer-readable medium, such as RAM. Client device 102 may operate on any operating system, such as Microsoft® Windows® or Linux. The client device 102 is, for example, a laptop computer executing a network access user interface.

The modules shown in Figure 2 represent functionality of the client 102. The modules may be implemented as one or more computer programs that include one or more modules. For instance, in one embodiment, all the modules shown in Figure 2 are contained within a single network access application. Also, the functionality shown on the client 102 may be implemented on a server in other embodiments of the present invention. Likewise, functionality shown in Figures 3 and 4 as being on a server may be implemented on the client 102 in some embodiments of the present invention.

The client 102 shown in Figure 2 comprises a VPN client 202. The VPN client 202 allows the client 102 to connect to the enterprise server 106. In one embodiment of the present invention, the VPN client 202 is used to determine whether or not the VPN client 202 is active and whether or not the VPN client 202 is connected to a VPN server. For instance, an embodiment of the present invention may determine whether or not to connect to a particular service based on whether or not the VPN client 202 is enabled.

In another embodiment of the present invention, the VPN client 202 is used for four purposes: (1) to manage policy files, which include information, such as a gateway Internet Protocol (IP) address, secrecy and authentication level, and hash; (2) automatically connecting a VPN; (3) automatically disconnecting the VPN; and (4) monitoring the status of the VPN. Each of these four purposes may be affected by other modules, including, for example, the connection manager 210.

The client 102 also comprises a secure vault 204. The secure vault 204 protects content on the client 102. In one embodiment, the secure vault 204 is responsible for storing encrypted content on the client 102 and allowing access to the encrypted content based on a set of permissions or policies. In such an embodiment, a content creator can provide access via a viewer to secured content and allow a recipient of the content read-only access or allow the recipient to perform other tasks, such as modifying the content and forwarding it to other users. In another embodiment, the secure vault 204 allows the user to create and distribute secure content to other clients 102, the content creator can decide to send a document to several users and allow two of the users full access and one of the users read-only access.

The client 102 shown in Figure 2 also comprises a firewall 206. The firewall 206 allows port blocking via predefined policies. For instance, in one embodiment, an information technology ("IT") manager specifies port blocking based on two zones, a safe zone and a dangerous zone. The IT manager specifies one of these two zones for each of the network interface devices installed on the client 102. The IT manager is then able to set port-blocking rules by zone on the firewall 206.

For example, the IT manager may classify a Wireless Fidelity ("Wi-Fi") network interface as dangerous since it has traditionally been considered fairly unsafe. And the IT manager may apply more restrictive port-blocking rules to the dangerous zone than to the safe zone and network interface devices, such as those used to connect to a wired Local Area Network ("LAN") or a Personal Handyphone System ("PHS") cellular connection. The PHS standard is a TDD-TDMA based microcellular wireless communications technology and has been traditionally considered relatively safer than Wi-Fi connections. The PHS cellular connection may also be referred to as a wireless wide area network ("WWAN") as opposed to a dial-up connection providing access to a wide area network ("WAN").

In various other embodiments, the port-blocking rules of the firewall 206 may be based on time of day, client IP address, terminating IP address, terminating and originating port, protocol, and other variables. In one embodiment, the port-blocking rules are based on policy data associated with individual users logged into the client 102.

In one embodiment, the port-blocking rules of the firewall 206 include a blacklist. The blacklist allows an IT manager to prevent an application from executing on the client 102. For instance, an IT manager may blacklist a DVD player so that a user is unable to view DVD's on the client 102. The firewall 206 may provide a message to the user informing the user that an application is unavailable.

In another embodiment, the firewall 206 implements a white list. The white list is somewhat more restrictive than the blacklist described above. The white list allows only specified applications to execute. For example, an IT manager may allow only MS Word, Excel, PowerPoint, and Outlook to execute. No other applications will be permitted to execute. The firewall 206 may be a custom firewall or a third-party firewall integrated into an embodiment of the present invention.

The embodiment shown in Figure 2 also includes an antivirus module 208. The antivirus module 208 shown determines whether policy files, virus dictionary, or other virus-related resources are out of date and provides the client 102 with a mechanism for updating the files or data. The antivirus module 208 may restrict access to various connections, applications, and other functionality when the policy files are out of date. For instance, the antivirus module 208 may restrict the client 102 to connecting to a single gateway through which the policy files are available. In one embodiment, the antivirus module 208 comprises a third-party antivirus product that is integrated with the other modules on the client 102.

The client 102 also comprises a connection manager 210, which includes a rules processor. In one embodiment, the connection manager 210 assigns a priority number to every connection, e.g., one to one hundred, and selects the connection with the highest number to connect to.

The connection manager 210 may provide a connection to a variety of networks, including, for example, dial-up, LAN, digital subscriber line ("DSL"), cable modem, Wi-Fi, wireless local area network ("WLAN"), PHS, and satellite.

In one embodiment, the connection manager 210 differentiates between public and private connections. A public connection is a connection provided by a service provider who has a relationship with the administrator of the security server 104, which allows the security server 104 to authenticate the connection. For instance, the security server 104 administrator may have a business arrangement with a hotspot provider. In order to connect, the client 102 connects to a local access point and the authentication of the user occurs automatically at the security server 104. In contrast, a private connection requires that all aspects of the authentication mechanism for a connection are managed in the absence of the security server 104, although the connection manager may provide certain facilities to allow for automated authentication where possible.

In one embodiment, the connection manager 210 makes connections available or unavailable to the client 102 based on policies present on the client 102. The connection manager 210 may also download changes to policy data and transmit quality of service ("QoS") and other data to the security server 104 or the enterprise server 106.

In one embodiment, the connection manager 210 determines the type of connections that are available based on signals provided by hardware associated with the client 102. For example, when the client 102 passes near a hotspot, a Wi-Fi card in the client 102 senses the hotspot and sends a signal to the connection manager 210. For instance, the Wi-Fi card may sense a broadcast service set identifier ("SSID"). Once the signal exceeds a threshold, the connection manager 210 provides a signal to a user of the client 102 that the network is available or may automatically connect to the hotspot. Alternatively, the Wi-Fi card may poll for a non-broadcast SSID. The connection manager 210 may provide a single connection to the client 102 at one time or may provide multiple connections to the client 102.

The client 102 shown in Figure 2 also comprises a QoS collector 212. The QoS collector 212 collects data values, including, for example, the number of bytes sent and received, the average transfer rate, the average signal strength at connection, termination cause, failed connections, and a network identifier. In another embodiment, the QoS collector 212 collects data during the session to determine when a connection provides inconsistent performance.

In one embodiment, the QoS collector 212 collects data regarding a connection during a session but does not send the data for a session until the next session. Thus, if a session is terminated abnormally, the QoS data will still be collected and transferred successfully. In another embodiment, the QoS collector 212 transfers data only when a particular type of connection is detected, such as a high-speed or low cost connection.

The client 102 also comprises a session statistics module 214. The session statistics module stores data representing user characteristics. For instance, the session statistic module 214 may store a list of the applications a user generally accesses, how often the user is connected, the typical CPU and memory utilization measure, keyboard sequences, and other characteristics of a user. If a particular user deviates from the expected characteristics by greater than a threshold, such as N standard deviations, and the significance of the statistic is more than a specified amount, the session statistics module 214 can identify the current user as a potential unauthorized user.

The session statistics module 214 may perform other tasks as well. For instance, in one embodiment, the session statistics module 214 pre-loads applications based on a user's general usage patterns.

The client 102 shown in Figure 2 also comprises a policy reader 216. In one embodiment, a company's policies are housed on the enterprise server 106. For instance, individual groups and users within an enterprise are identified and associated with policies, such as what types of connections they are able to access and what a user's VPN profile is. The user may also be able to specify a VPN policy on the client 102. In such an embodiment, the policy reader 216 downloads the policy rules from the enterprise server 106 and accesses local user policies and reconciles any conflicts between the two.

For example, an IT manager may establish a VPN profile to be used by a user when connecting to a Wi-Fi network. However, the user may wish to create a secondary VPN profile to be used if the first VPN becomes unavailable. The policy reader 216 loads both local and enterprise VPN profiles, resolving any conflict between the two VPN profiles.

In one embodiment, the policy reader 216 accesses data at an enterprise, department, and user level. In such an embodiment, some of the policy rules may be stored in a lightweight directory access protocol ("LDAP") server on the client 102, security server 104, or enterprise server 106. In another embodiment, the policy reader 216 receives only changes to policy data and does not typically download all of the policy data at once. Policies downloaded by the policy reader 216 may be provided to the rules processor of the connection manager 210.

The client 102 may also comprises a client security module 216. In one embodiment, the client security module 216 implements a client asset protection process. When the client security module 216 receives a signal indicating that the client asset protection process is to be executed, the client security module 216 may, for example, disable devices and interfaces on the client device 102 and may, in some embodiments, encrypt the hard drive of the client device 102 so that the files stored on the drive are not easily accessible.

The client 102 may also comprise a user interface 220. The user interface 220 may control the underlying operating environment or the user's view of the underlying environment. For example, in one embodiment, the user interface 220 supplants the Microsoft® Windows operating system interface from the user's perspective. In other words, the user is unable to access many of the standard Windows features. Such a user interface may be implemented to limit the applications and configuration setting a user is able to access. In some embodiments, such as a personal digital assistant ("PDA"), no user interface is provided by an embodiment of the present invention; the standard PDA user interface is utilized.

The user interface 220 provides the user with an easy-to-use mechanism for accessing network connections. In one embodiment, when the user interface 220 is visible, it provides a very easy-to-use format that displays network connection types and provides other functionality to the user. For example, during complex operations, such as connecting to a new network type, the user can simply select a single button within the user interface 220 and the client 102 will properly disconnect from the previous network, acquire the new network, perform all authentication and policy-based requirements, and then allow the user to continue using an application on the new network. This simple, easy-to-use user interface 220, the complexity of which may be hidden and completely automatic, allows a less-technical user to successfully operate the client 102. All network connection, authentication, secure sign on, VPN parameters, and other aspects of the connection are managed by the user interface 220.

The client 102 shown in Figure 2 also comprises a security agent 222. In some embodiments, the security agent 222 is also referred to as a "bomb." In one embodiment, an IT manager indicates that the security agent 222 should be activated when the client 102 next connects to the enterprise server 106. The IT manager may do so because the client 102 has been reported stolen. Subsequently, the client 102 connects to the enterprise server 106, either directly or indirectly and receives the message to initiate the security agent 222.

In one embodiment, when the security agent 222 activates, it stops all applications from being able to run and encrypts the data on the hard drive of the client 102. For instance, the security agent 222 may implement a white list as described above and then implement a secure vault for all data on the client 102. The connection manager 210 may also be configured so that no connections are possible.

In one such embodiment, since the data is merely encrypted by security agent 222, rather than erased, the data may be recovered if the client 102 is subsequently recovered. For instance, the enterprise may retain the key needed for decrypting the local drive. The client

102 is returned to the enterprise, which then decrypts the drive. In another embodiment, the data on the local drive of the client is rendered inaccessible by, for example, writing over the data multiple times.

The client 102 shown in Figure 2 also comprises an out-of-band communication receiver 224. The out-of-band communication receiver 224 allows the client to receive communications other than through a network-based connection. The connection manager 210 may manage the out-of-band communication. For instance, the command to activate the security agent 222 may be transferred via a short messaging service ("SMS") communication received by the out-of-band communication receiver 224.

Security Server

Figure 3 is a block diagram illustrating the modules present on a security server 104 in one embodiment of the present invention. The security server 104 shown in Figure 3 comprises a remote authentication dial-in user service ("RADIUS") server 302, which may also be referred to as an AAA (authentication, authorization, and accounting) server. RADIUS is the standard by which applications and devices communicate with an AAA server.

The RADIUS server 302 provides authentication services on the security server 104. In some embodiments of the present invention, the RADIUS server 302 proxies to a RADIUS server on the enterprise server 106. In one embodiment, the RADIUS server 302 provides mutual authentication for the client 102 using Extensible Authentication Protocol Transport Layer Security ("EAP-TLS"). Although EAP-TLS itself is strictly an 802.1x authentication protocol, designed primarily for Wi-Fi connections, the underlying TLS authentication protocol may be deployed in both wired and wireless networks. EAP-TLS performs mutual secured sockets layer ("SSL") authentication. This requires both the client device 102 and the RADIUS server 302 to have a certificate. In mutual authentication, each side may prove its identity to the other using its certificate and its private key.

The security server shown in Figure 3 also comprises an LDAP server 304. The LDAP server 304 uses the LDAP protocol, which provides a mechanism for locating users, organizations, and other resources on the network. In one embodiment of the present invention, the LDAP server 304 provides access control at the network layer to various components that an enterprise customer may or may not purchase. For example, a customer may choose to implement a secure vault as described in relation to Figure 1. In such a case, the customer or users or groups associated with the customer are also associated with the firewall module. The LDAP entry is then used to determine that the firewall is to be enabled on a client.

In some embodiments, the LDAP server 304 is implemented as a list of user identifiers not using the LDAP protocol. In another embodiment, data in the LDAP server 304 is propagated from data present in the enterprise server 106.

The security server 104 shown in Figure 3 also comprises a session manager 306. The session manager 306 controls sessions, including sessions between the client 102 and enterprise server 106. In some embodiments, the session manager 306 also determines how to route data requests. For instance, the session manager 306 may determine that a particular data request should be routed to the Internet rather than to the enterprise server 106. This may be referred to as "splitting the pipe" and provides a mechanism to replace "split tunneling" (a traditional configuration option with most standard VPN clients) at the client device by the more secure split of traffic not intended for the enterprise at the security server, allowing monitoring of all traffic without the enterprise incurring the expense of the extra bandwidth required.

In some embodiments, the client 102 and enterprise server 106 establish a VPN for communication. In such an embodiment, the session manager 306 may be unable to route requests to any location other than the enterprise – the packets are encrypted and thus, cannot be separately evaluated.

In one embodiment, the session manager 306 performs automated authentication of a client device 102 or user. For example, if the session manager 306 determines that a client 102 is approaching a Wi-Fi hotspot, the session manager 306 is able to pre-populate the hotspot with the certificate that the hotspot requires to authenticate the user. In this manner, the authentication appears very fast to the user. The session manager 306 may also control the manner in which data is queued for download to the client device 102.

In one such embodiment, the session manager 306 provides two modes for data queuing. In a first mode, the session manager 306 determines that the network down time will be brief, e.g., the user is moving through a tunnel, which interferes with network access. In such a case, the session manager queues a minimal amount of data. In a second mode, the session manager 306 determines that the network down time will be of a longer duration, e.g., the user is boarding a plane from New York to Tokyo. In such a case, the session manager 306 may queue a larger amount of data. In one such embodiment, the session manager 306 determines the mode by querying the user for the downtime interval. When the user reconnects to the security server 104, the session manager 306 determines the best manner of downloading the queued data and begins the download.

In one embodiment, the session manager 306 comprises a packet shaper (not shown). The packet shaper provides various functional capabilities to the session manager 306. For example, in one embodiment, the packet shaper provides a mechanism for prioritizing packets sent between the enterprise server 106 and the client 102. In one embodiment, the packet shaper utilizes Multiprotocol Label Switching ("MPLS"). MPLS allows a specific path to be specified for a given sequence of packets. MPLS allows most packets to be forwarded at the switching (layer 2) level rather than at the (routing) layer 3 level. MPLS provides a means for providing QoS for data transmissions, particularly as networks begin to carry more varied traffic.

The session manager 306 may also provide session persistence capabilities. For instance, in one embodiment, when a user drops a connection or moves from one provider network coverage area to another, the connection manager 306 persists a virtual connection as the first connection is terminated and the second is initiated.

The session manager 306 may include a server-side rules engine. The server-side rules engine may use historical information, such as the session statistics described above, for statistical attack determination. For instance, session manager 306 may access a stored statistic regarding a client device 102 and based on monitoring of the current statistics for the client device 102 determine that an unauthorized user is using the client device 102.

The security server 104 shown in Figure 3 also comprises a real-time monitor 308. The real-time monitor 308 monitors the status of communications, such as which clients and users are logged on, the amount of data being transferred, ongoing QoS measures, ports in use, and other information.

When the real-time monitor 308 detects a problem, it may issue an alert to network support. In one embodiment, data from the real-time monitor 308 is provided to users via a portal available on the security server 308. In another embodiment, the real-time portal 308 transfers information to the enterprise server 106, from which users access the data.

The embodiment shown in Figure 3 also comprises a historical monitor 310. The historical monitor 310 provides information similar to the real-time monitor 310. However, the underlying data is historical in nature. For instance, in one embodiment, the historical monitor 310 provides audit information for making intelligent business decisions and for dealing with regulatory compliance issues.

The information available via the historical monitor 310 may include, for example, historical QoS data, registration compliance data, and metrics consistency data. The historical data monitor 310 may be used to determine that certain clients are not performing optimally by comparing metrics of various clients over time. For instance, by evaluating information available via the historical data monitor 310, a support person may be able to determine that a radio tuner on a specific client device 102 is failing. If the user of one client device 102 is complaining about the availability of service, but other users are able to successfully access service, then the client device's radio may be the problem.

The historical data monitor 310 may also be used to reconcile information captured on the security server 104 regarding connections and data provided by telecommunication carriers. The data may be used to determine when certain resources need to be increased and when a certain carrier is not performing adequately.

The security server also comprises a database 312. In embodiments of the present invention, the database 312 may be any type of database, including, for example, MySQL, Oracle, or Microsoft SQL Server relational databases. Also, although the database 312 is shown as a single database in Figure 2, the database 312 may actually comprise multiple databases, multiple schemas within one or more databases, and multiples tables within one or more schemas. The database 312 may also be present on one or more other machines, e.g., database servers.

In one embodiment of the present invention, the database 312 stores customer information regarding enterprises served by the security server 104, such as a list of valid users, a list of valid cellular cards, the relationships between the individual users and groups within the enterprise, and other customer information.

For example, in one embodiment, the database 312 stores an association between users and cellular data cards. The enterprise may allocate a single user to a specific data card. Alternatively, the enterprise may associate a group of users with a group of cellular data cards. Other types of data may also be stored in the database 312, such as billing data.

The security server 104 shown in Figure 3 also comprises a QoS server 314. The QoS server 314 uploads information from the QoS collector 212 on the client device 102 and stores the QoS data. The QoS server 314 can collect data from multiple clients and store it in the database 312.

The security server also comprises a QoS tools engine 316. The QoS tools engine 316 displays data made available by the QoS server 314 and other processes, such as the real-time monitor 308.

In one embodiment, the QoS tools engine 316 provides an aggregation of QoS data in a spreadsheet. In another embodiment, the QoS tools engine 316 provides data using map views, pie charts, and graphs. The QoS tools engine 316 may also provide the capability for setting QoS-based alarms and may provide data to users via a portal.

In the embodiment shown in Figure 3, the security server 104 also comprises a portal server 318. The portal server 318 may be, for example, a web server. Any standard web server application may be utilized, including Microsoft® Internet Information Server ("IIS") or Apache.

Although the security server 104 shown in Figures 1 and 3 is illustrated as a single server, it may comprise multiple servers. For example, in one embodiment of the present invention, the security server 104 comprises multiple regional servers.

Also, the description above suggests that data is provided to and queried from the security server 104 by the client 102, i.e., the client pulls the data. However, in some embodiments, the client 102 also comprises a listener (not shown) so that the security server 104 can push data to the client 102.

Enterprise Server

Figure 4 is a block diagram illustrating the modules present on an enterprise server 106 in one embodiment of the present invention. The enterprise server 106 may also be referred to herein as a customer server and may comprise one or more servers for one or more enterprises linked to one or more security servers 104.

The enterprise server 106 shown in Figure 4 comprises a policy server 402. The policy server 402 provides a means for managing the policy rules, including, for example, available VPN profiles, available transports (e.g. Wi-Fi, LAN, PHS, Dialup), firewall rules, such as blacklists and white lists, connection rules, and antivirus rules. The policy server 402 may include other rules as well, such as the level of data throttling to perform for each client or group of clients. Data throttling limits the data transfer rate to a particular client 102 so that connection resources can be optimized.

The policies may be managed at one or more levels. For example, an IT manager may wish to create a VPN profile for the enterprise as a whole, but a different VPN profile for an engineering group since the engineering group needs access to various unique applications.

The policy server 402 may also provide a mechanism for configuring the location of various servers that the client 102 will utilize. For instance, the policy server 402 may allow an IT manager to specify the IP address of an acceleration server 404 or a vault server 406

In one embodiment, the policy server also allows the IT manager to specify which users receive updates for various components on the client 102. The policy server 402 may also allow the IT manager to perform connection configuration. For instance, the IT manager may use the policy server to specify phone numbers for PHS connections, Wi-Fi SSID's for private connections, and other connection configuration information.

The enterprise server 106 shown in Figure 4 also comprises an acceleration server 404. The acceleration server 404 performs processes to improve the performance of data transfer. For instance, the acceleration server 404 may automatically compress images that are to be transferred to a client 102.

In one embodiment, the acceleration server 404 communicates with the policy server 402. An IT manager sets acceleration rules using the policy server 402, and the acceleration server 404 uses these rules to determine what level of acceleration to use for a particular communication. In one embodiment, the IT manager sets a default level of acceleration for all communication and a specific level of acceleration for one group of users. The specific level of acceleration may be referred to as an override.

The enterprise server 106 also comprises a vault server 406. The vault server comprises two components, an automatic component and an administration component. In one embodiment, the automatic component integrates with an enterprise's mail server (not shown) and performs operations on emails to and from the mail server. For instance, the vault server 406 may quarantine an email, automatically encrypt the email before it is sent, add a legal disclaimer to an email, or perform other functions on the email.

In one embodiment, the automatic component of the vault server 406 searches an email based on words or based on the domain or specific address to which the email is addressed or from which the email originated. Using this information, the user can perform functions on the email, such as those described above.

The administration component of the vault server 406 allows a user to terminate access to secure content, either by a specific user or by all users. It also logs activity. Using one embodiment of the vault server 406, a user can indicate that a set of users whose employment has been terminated will no longer have access to any secure content. In an alternative embodiment of the vault server 406, a user can indicate that a given element of secure content, say a price list, is now out of date, and so that piece of secure content will no longer be viewable by any user. When each user accesses the secure content, the vault server 406 logs the event. So for each secure content element, the vault server 406 creates a log of all activity on the secure content.

In one embodiment, the vault server 406 also compresses data. For instance, one embodiment utilizes standard PKZIP compression to compress all content. In another embodiment, an IT manager may identify three types of images and specify a different level of compression for each type of image based on the level of resolution necessary for each type of image.

The enterprise server 108 also comprises a RADIUS server 408 and LDAP server 410, which are similar to those described above in relation to the security server 104. The RADIUS server 302 on the security server 104 may proxy to the RADIUS server 408 on the enterprise server 106. Similarly, data in the LDAP server 410 may be propagated to the LDAP server 204 on the security server 104.

The enterprise server 106 also comprises a one-time password ("OTP") server 412. The OTP server 412 provides a mechanism for authentication. For instance, in one embodiment of the present invention, the enterprise server 106 uses the OTP server 412 to perform a mutual authentication process.

The enterprise server 106 also comprises a concentrator 414. The concentrator 414 provides remote access capability to the client 102. For instance, the concentrator 414 may serve as a means for terminating a VPN between the client 102 and enterprise server 106.

The enterprise server 104 shown in Figure 4 also comprises a portal server 416. The portal server 416 may comprise a standard web server, such as IIS or Apache. The portal server 416 may provide one or more portals. For example, in one embodiment, the portal server 416 provides two portals, portal one and portal two.

Portal one provides a configuration interface for managing the various elements shown in Figures 2 and 3, including, for example, the policy server 402 and LDAP server 410. Portal two provides an interface for accessing data, such as QoS data and session data.

For instance, a user may use historical QoS data on portal two to determine how a particular provider is performing in terms of throughput, user connections, and other QoS metrics. Portal two may also provide real-time information, such as how many users are currently connected.

For instance, in one embodiment, an IT manager determines that twenty users have been rejected by a carrier in the last three minutes due to authentication failure and five users with the same user identifier are currently logged on to five different devices. The IT manager uses this information to detect a potential security problem. Portal two may also be used to set alerts as described above.

It should be noted that the present invention may comprise systems having a different architecture than that which is shown in Figures 1 through 4. For example, in some systems according to the present invention, the security server 104 and enterprise server 106 may comprise a plurality of security and enterprise servers. The system 100 shown in Figures 1 through 4 is merely illustrative, and is used to help explain the illustrative systems and processes discussed below.

Illustrative Methods of Enhanced network client security

The following illustrative embodiments utilize a central policy server 402 on an enterprise server 106. In one embodiment, the client device 102 downloads security-related policies from the policy server 402 and the connection manager 210 utilizes the policies to generate one of more security models and applies the security models to connections. Figure 5 is a flowchart illustrating a process for applying a security model to a network connection in one embodiment of the present invention. In the embodiment shown, the connection manager 210 receives an indication that a network connection is established 502. For example, a user may click a button on the user interface 220 to cause the connection manager 210 to disconnect from a first network connection and connect to a second network connection. The connection manager 210 is able to determine when the second connection has been successfully completed.

The connection manager 210 then determines the network type 504. If the connection manager 210 established the second network connection, the connection manager 210 may store the network type as part of the process of establishing the connection. In another embodiment, the connection manager 210 analyzes an existing connection to determine the network type. The connection manager 210 may obtain other attributes of the network, such as the speed, provider, reliability, and other attributes. The connection manager 210 may obtain the attributes by examining the network or may obtain attributes of the network that have been previously stored, such as performance metrics.

In the embodiment shown in Figure 5, the connection manager 210 next receives a security-related policy associated with the user 506. The security-related policy may be downloaded from a centralized policy management data store. For example, in one embodiment, an administrator establishes security-related policies in the policy server 402. The policy reader 216 on the client 102 downloads policies from the policy server 402. The connection manager 210 then receives the security-related policies from the policy reader 216. The policies may be in the form of an XML file, database, or other data store.

The connection manager 210 next determines a security model associated with the security-related policy 508. For instance, the connection manager 210 may determine that a particular level of firewall and anti-virus protection is required for the network type currently accessed by the client 102. In one embodiment, the security model may require that a VPN be established in order to use a particular network type. In another embodiment, a particular white list or blacklist may be required for the current network type. In other embodiments, each security model may comprise a different combination of firewall, VPN, anti-virus and other attributes, which can be used in combination to implement a security-related policy.

Once the connection manager 210 determines the security model associated with the security-related policy, the connection manager 210 applies the security model to the network connection 510. For instance, if a particular level of firewall protection is necessary for the network type utilized by the network connection, the connection manager 210 causes the firewall to provide the requisite level of protection. In one embodiment, if the anti-virus or firewall protection is insufficient to support the type of connection the client 102 is attempting to access, the connection manager 210 will not permit the connection to occur. In one embodiment, the connection manager 510 utilizes one or more security models to determine the most appropriate connection to utilize based on a security-related policy and connects automatically to that network. In another embodiment, the connection manager 210 disables or hides connections if the client does not have sufficient security components, e.g., the appropriate firewall, for establishing the connection.

In one embodiment, a component on the client device compares a user's behavior with the user's past behavior based on usage characteristics. If the present behavior and the past behavior differ significantly, the current user may be identified as an unauthorized user, e.g., someone who discovered the user's username and password. The process of identifying a user as invalid based on usage characteristics may be referred to as statistical attack detection. Figure 6 is a flowchart illustrating a process for statistical attack determination in one embodiment of the present invention. In the embodiment shown, a session statistics module 214 receives a first measure associated with a usage characteristic 502. The first measure may be, for example, a mean, median, maximum, minimum, or other summary measure of a usage characteristic. Each measure may comprise a plurality of measurements. In one embodiment, the measure is a code representing the history of a usage characteristic. For instance, in one embodiment, the measure is related to a keystroke sequence usage characteristic. The measure is a code indicating how often a particular keystroke sequence is used during the first five minutes a client 102 is connected to a network 108.

In embodiments of the present invention, the usage characteristic may be a characteristic that provides information about how a particular user utilizes a client 102. For example, in one embodiment, the usage characteristic comprises at least one usage characteristic selected from the group consisting of a uniform resource locator visited, an application launched, a number of systems calls per specified duration, a keystroke sequence, a system call, a processor utilization measure, and a memory utilization measure. In another embodiment, the usage characteristic comprises at least one usage characteristic selected from the group consisting of a traffic level associated with a connection, a protocol used, and a port hit.

The session statistics module next receives a second measure associated with the usage characteristic 504. The second measure may be an actual measure of activity at a point in time. For instance, in one embodiment, the first measure is average processor utilization by a particular user on a particular client 102. The second measure is actual processor utilization at a point in time by the user on the client 102.

The session statistics module 214 compares the first measure and the second measure 608. The session statistics module 214 then determines whether the first and second measures differ significantly 610. For instance, the session statistics module 214 may perform a statistical linear regression on the measures collected for the user and client 102 previously and the current measure.

If the measures differ significantly, the session statistics module signals an unauthorized access 612. For example, the session statistics module 214 may send a signal to the enterprise server 106, indicating an unauthorized access. In another embodiment, the client device 102 disconnects from the enterprise server 106 and does not allow the user to make any further network connections. Once the signal has been sent or a determination made that the measures do not differ significantly, the process ends 614.

In response to the indication, the enterprise server 106 may disable a user's access to confidential information. The enterprise server 106 may also disable a user's access to any network connections. In one embodiment, the enterprise server 106 or security server 104 monitors the usage characteristics for particular users and causes their access to be suspended if a potential attack is identified. Such a server-based embodiment may rely on a subset of the data available to a client-based embodiment.

In one embodiment of the present invention, the session statistics module 214 uses measures of the usage characteristics to pre-load applications. For instance, if a user generally opens an email client application as soon as the boot process on the client device

102 is complete, the session statistics module 214 may cause the application to be pre-loaded, saving the user from having to manually start the application or explicitly add the application to a startup group.

General

The foregoing description of the embodiments of the invention has been presented only for the purpose of illustration and description and is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Numerous modifications and adaptations thereof will be apparent to those skilled in the art without departing from the spirit and scope of the present invention.

That which is claimed:

1. A method comprising:

receiving a security-related policy associated with a user;

determining a security model associated with the security-related policy; and

applying the security model to a network connection on a client device.

2. The method of claim 1, wherein the security model comprises at least one rule.

3. The method of claim 2, wherein the rule comprises a rule selected from the group consisting of a firewall rule, an antivirus rule, and a virtual private network rule.

4. The method of claim 1, wherein the security policy is associated with a connection type.

5. The method of claim 4, wherein the connection type comprises a connection type selected from the group consisting of Wifi, local area network, wide area network, wireless wide area network, personal handy network, dial-up, and satellite.

6. The method of claim 1, wherein the security policy comprises a secure zone and a non-secure zone.

7. The method of claim 1, wherein the user is associated with a user group.

8. The method of claim 1, wherein receiving the security policy comprises receiving the security policy from a policy server.

9. The method of claim 8, further comprising:

creating a security policy; and

associating the security policy with the user.

10. A method comprising:

receiving a first measure associated with a usage characteristic, the usage characteristic associated with a user;

receiving a second measure associated with the usage characteristic;

comparing the first measure and second measure; and

determining the likelihood that an unauthorized access has occurred based at least in part on the comparison.

11. The method of claim 10, wherein the usage characteristic comprises at least one usage characteristic selected from the group consisting of a uniform resource locator visited, an application launched, an number of systems calls per specified duration, a keystroke sequence, a system call, a processor utilization measure, and a memory utilization measure.

12. The method of claim 10, wherein the usage characteristic comprises at least one usage characteristic selected from the group consisting of a traffic level associated with a connection, a protocol used, and a port hit.

13. The method of claim 10, wherein comparing the first measure and second measure comprises performing a statistical linear regression.

14. A computer-readable medium on which is encoded program code, the program code comprising:

program code for receiving a security-related policy associated with a user;

program code for determining a security model associated with the security-related policy; and

program code for applying the security model to a network connection on a client device.

15. A computer-readable medium on which is encoded program code, the program code comprising:

program code for receiving a first measure associated with a usage characteristic, the usage characteristic associated with a user;

program code for receiving a second measure associated with the usage characteristic;

program code for comparing the first measure and second measure; and

program code for determining the likelihood that an unauthorized access has occurred based at least in part on the comparison.

16. A system comprising:

a policy reader operable to determine a policy associated with a user; and

a client security module operable to:

receive a security-related policy associated with a user;

determine a security model associated with the security-related policy; and

apply the security model to a network connection on a client device.

17. A system comprising:

a policy reader operable to determine a policy associated with a user; and

a unauthorized access detector operable to:

receive a first measure associated with a usage characteristic, the usage characteristic associated with a user;

receive a second measure associated with the usage characteristic;

compare the first measure and second measure; and

determine the likelihood that an unauthorized access has occurred based at least in part on the comparison.

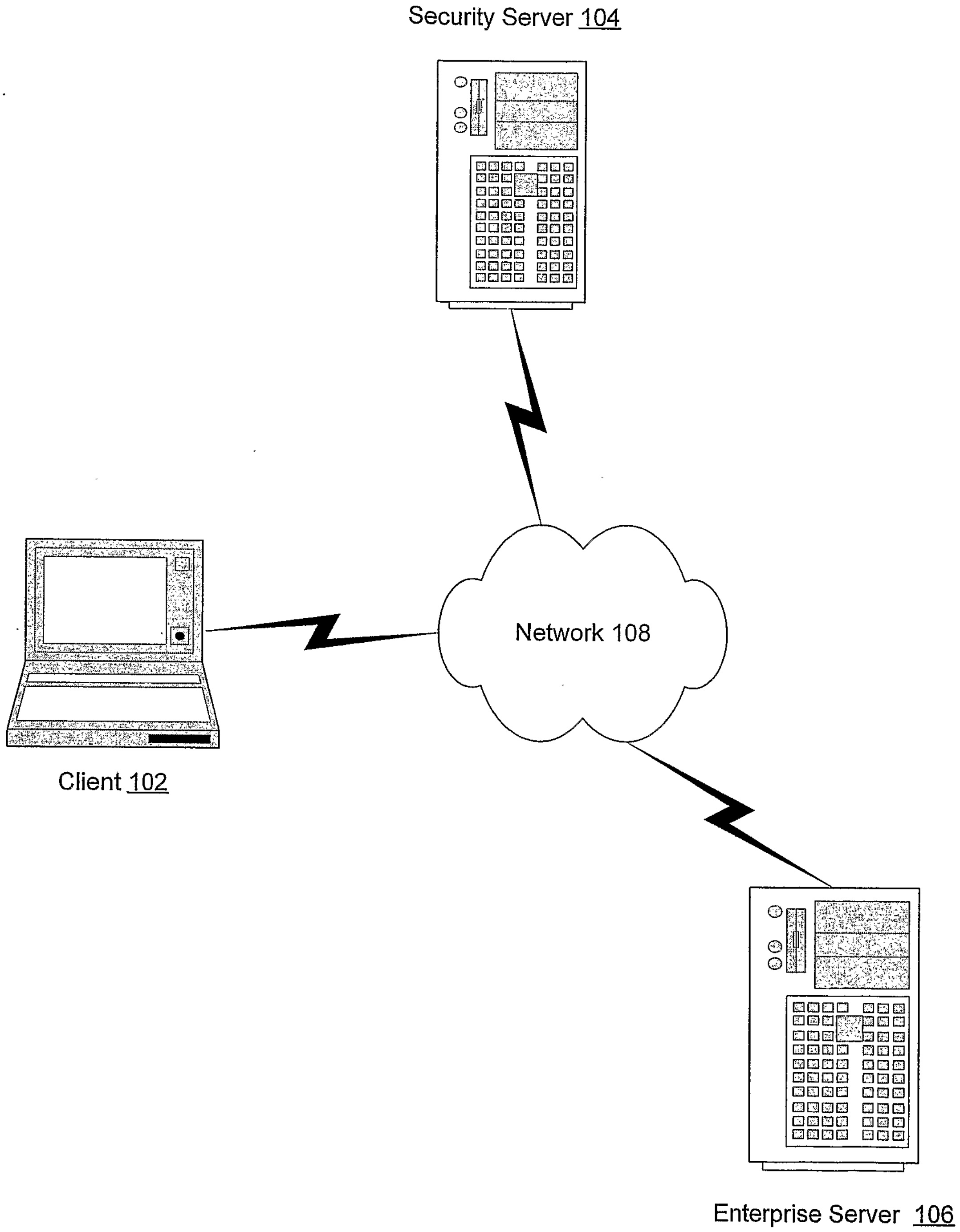

Security Server 104
Client 102
Network 108
Enterprise Server 106

Figure 1

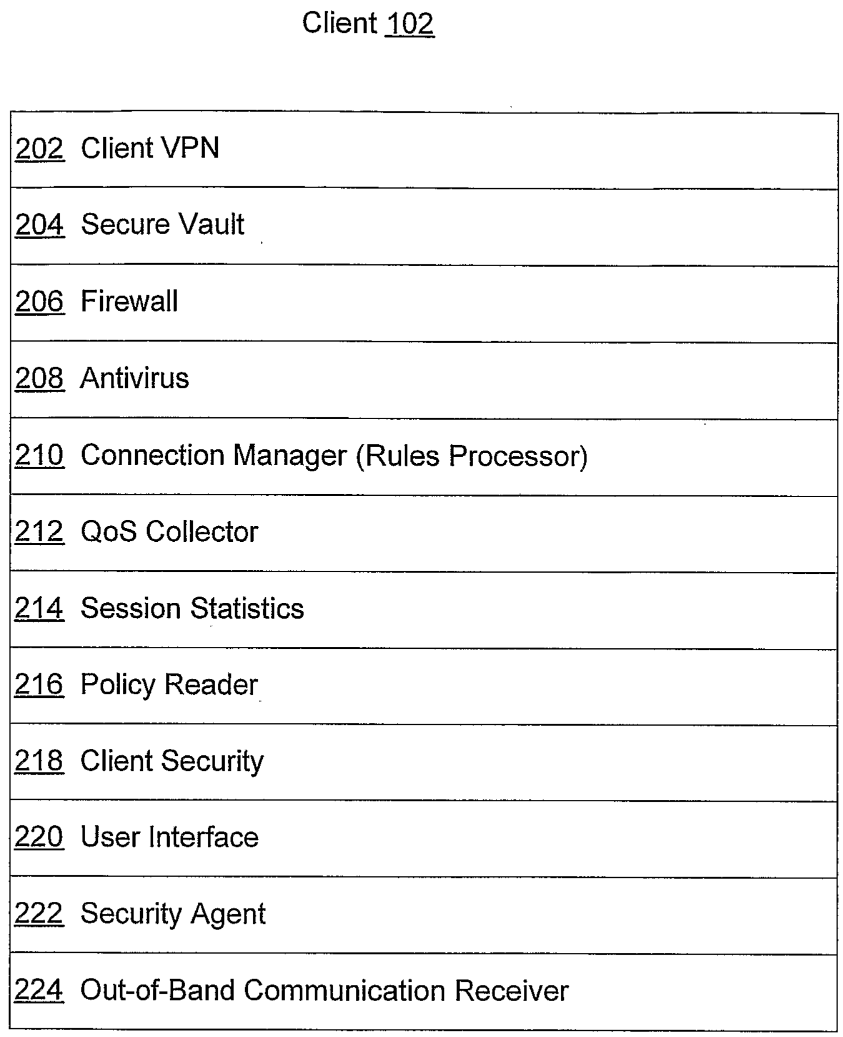

Client 102
202 Client VPN
204 Secure Vault
206 Firewall
208 Antivirus
210 Connection Manager (Rules Processor)
212 QoS Collector
214 Session Statistics
216 Policy Reader
218 Client Security
220 User Interface
222 Security Agent
224 Out-of-Band Communication Receiver

Figure 2

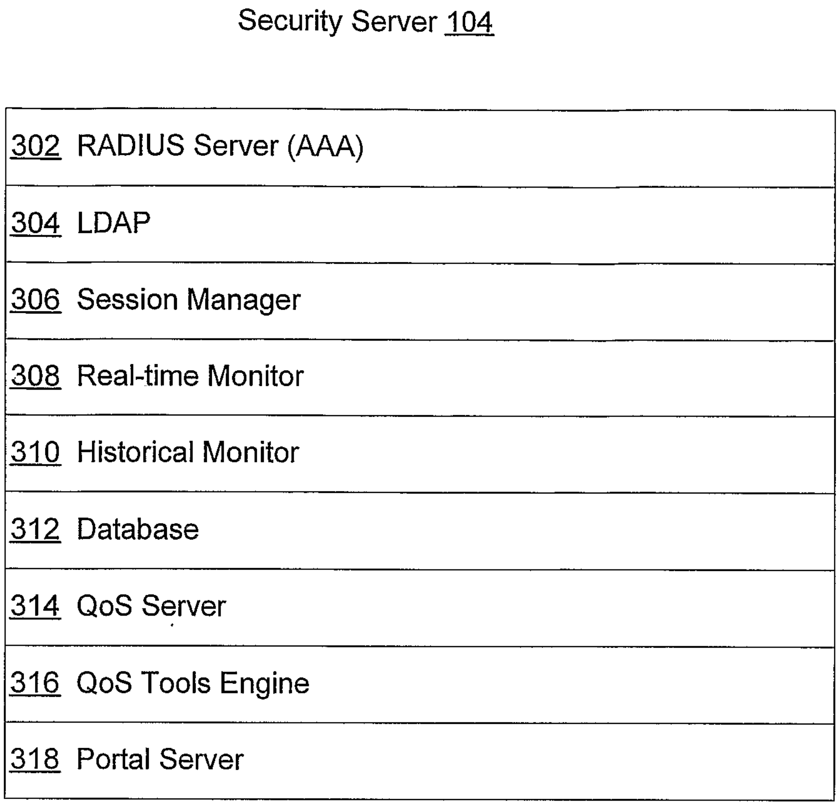

Security Server 104
302 RADIUS Server (AAA)
304 LDAP
306 Session Manager
308 Real-time Monitor
310 Historical Monitor
312 Database
314 QoS Server
316 QoS Tools Engine
318 Portal Server

Figure 3

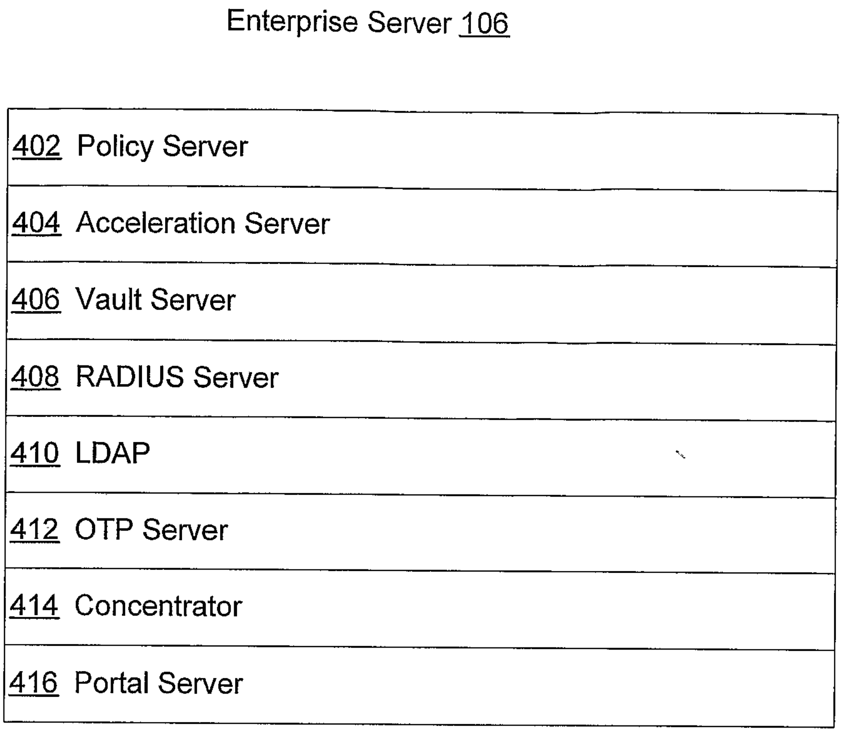

Enterprise Server 106
402 Policy Server
404 Acceleration Server
406 Vault Server
408 RADIUS Server
410 LDAP
412 OTP Server
414 Concentrator
416 Portal Server

Figure 4

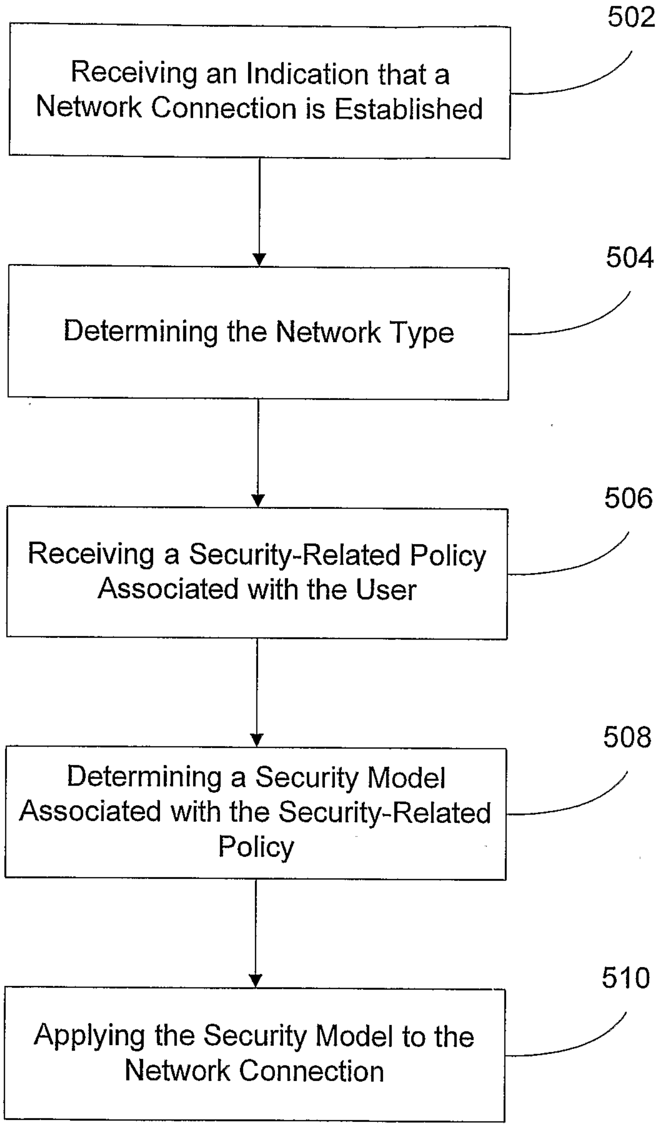

Receiving an Indication that a Network Connection is Established
502
Determining the Network Type
504
Receiving a Security-Related Policy Associated with the User
506
Determining a Security Model Associated with the Security-Related Policy
508
Applying the Security Model to the Network Connection
510

Figure 5

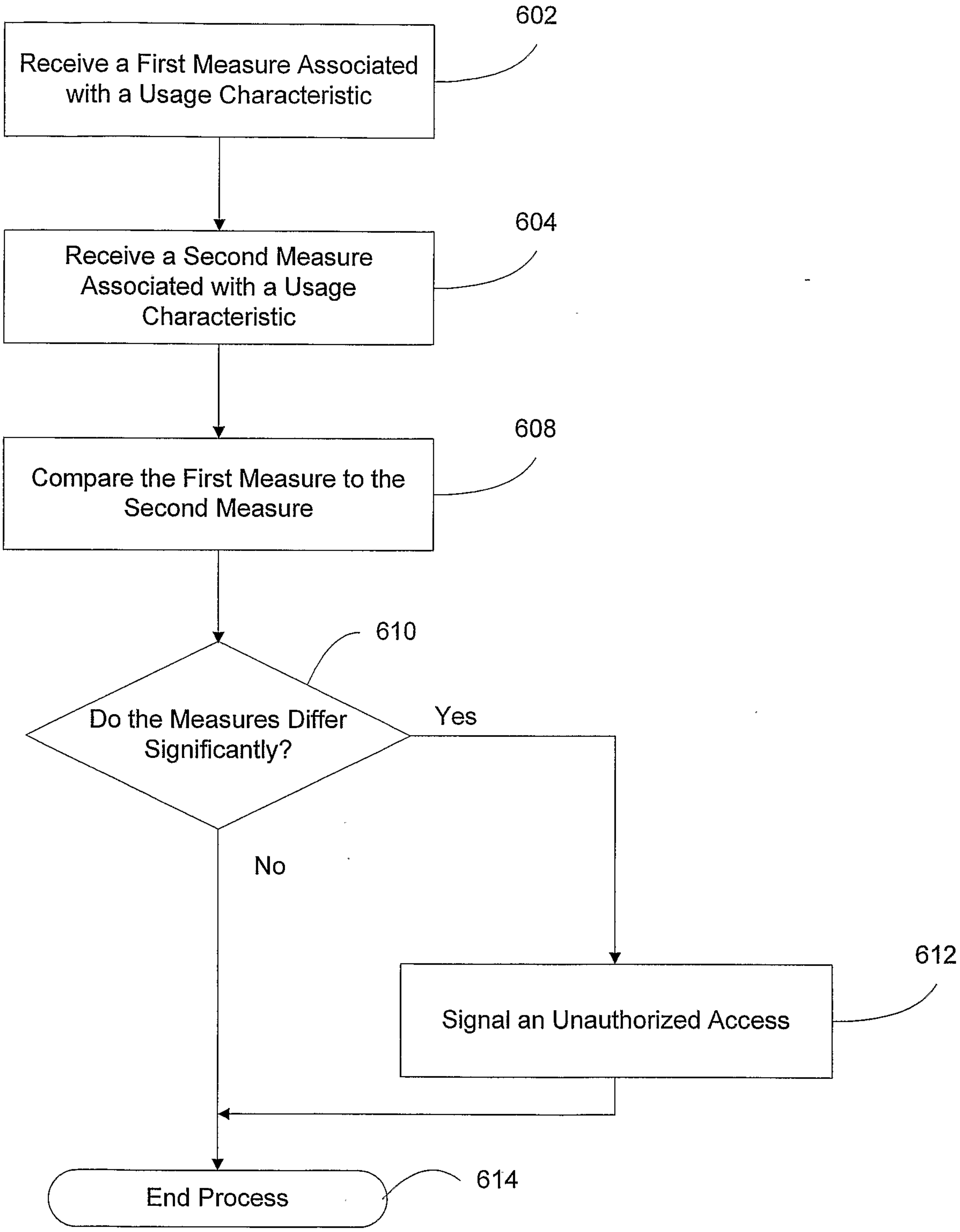

602
Receive a First Measure Associated with a Usage Characteristic
604
Receive a Second Measure Associated with a Usage Characteristic
608
Compare the First Measure to the Second Measure
610
Do the Measures Differ Significantly?
Yes
No
612
Signal an Unauthorized Access
614
End Process

Figure 6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022984

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

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

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

EPO-Internal, WPI Data, PAJ, COMPENDEX, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DOD: "DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA" THE RAINBOW BOOKS, 26 December 1985 (1985-12-26), XP002927150 abstract * Chapter 5.3.1.1 * * Chapter 5.3.1.2 * * Chapter 6.1 * ----- -/--	1-17

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

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

"E" earlier document but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

27 October 2005

Date of mailing of the international search report

04/11/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31–70) 340–2040, Tx. 31 651 epo nl,
Fax: (+31–70) 340–3016

Authorized officer

Kopp, K

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022984

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/005331 A1 (WILLIAMS TIMOTHY C) 2 January 2003 (2003-01-02) abstract figures 1,4 paragraph ‘0001! - paragraph ‘0005! paragraph ‘0007! - paragraph ‘0008! paragraph ‘0015! - paragraph ‘0016! paragraph ‘0021! paragraph ‘0026! - paragraph ‘0027! paragraph ‘0030! -----	1-17
X	US 2003/056116 A1 (BUNKER NELSON WALDO ET AL) 20 March 2003 (2003-03-20) abstract paragraph ‘0012! paragraph ‘0019! paragraph ‘0021! paragraph ‘0073! paragraph ‘0076! paragraph ‘0090! - paragraph ‘0091! paragraph ‘0100! paragraph ‘0172! paragraph ‘0195! paragraph ‘0341! paragraph ‘0346! paragraph ‘0355! - paragraph ‘0356! paragraph ‘0362! paragraph ‘0374! paragraph ‘0376! -----	1-17
X	WO 2004/021114 A (TD SECURITY, INC., DBA TRUST DIGITAL, LLC; SHAHBAZI, MAJID) 11 March 2004 (2004-03-11) page 2, line 17 - page 3, line 24 page 5, line 10 - line 25 -----	1-17
A	US 5 748 084 A (ISIKOFF ET AL) 5 May 1998 (1998-05-05) abstract figures 3,4 column 1, line 4 - line 7 column 1, line 48 - column 3, line 4 column 3, line 46 - line 53 column 4, line 3 - line 33 column 4, line 62 - column 5, line 33 column 5, line 59 - column 6, line 15 column 6, line 31 - line 54 column 9, line 53 - column 10, line 31 -----	1-17

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022984

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003005331 A1	02-01-2003	AU 750858 B2	01-08-2002
		AU 1595400 A	06-03-2000
		CA 2339637 A1	24-02-2000
		EP 1101161 A2	23-05-2001
		NZ 509570 A	28-03-2003
		WO 0010278 A2	24-02-2000
		US 6304973 B1	16-10-2001
US 2003056116 A1	20-03-2003	US 2003009696 A1	09-01-2003
		US 2003028803 A1	06-02-2003
WO 2004021114 A	11-03-2004	AU 2003260071 A1	19-03-2004
		EP 1540446 A2	15-06-2005
US 5748084 A	05-05-1998	NONE	