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

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
25 September 2008 (25.09.2008)

(10) International Publication Number
WO 2008/114256 A2

(51) **International Patent Classification:**
***H04L** 9/32* (2006.01)

(21) **International Application Number:**
PCT/IL2008/000382

(22) **International Filing Date:** 19 March 2008 (19.03.2008)

(25) **Filing Language:** English

(26) **Publication Language:** English

(30) **Priority Data:**
60/919,820 22 March 2007 (22.03.2007) US

(71) **Applicant** *(for all designated States except US):* **NEOCLEUS LTD.** [IL/IL]; 26 Habarzel Street, 69710 Ramat Hahayel (IL).

(72) **Inventor; and**
(75) **Inventor/Applicant** *(for US only):* **BOGNER, Etay** [IL/IL]; 39 Even Sapir Street, 69546 Tel-aviv (IL).

(74) **Agents: SANFORD T. COLB & CO.** et al.; P.O. Box 2273, 76122 Rehovot (IL).

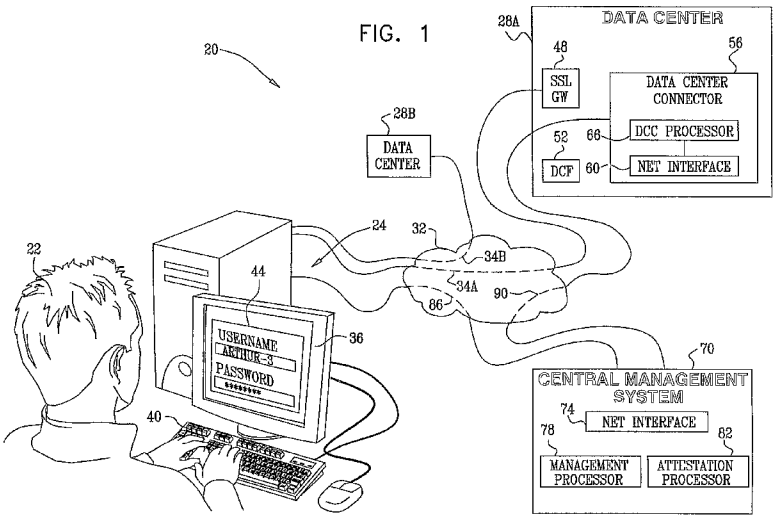
(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available):* AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

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

(54) **Title:** TRUSTED LOCAL SINGLE SIGN-ON

FIG. 1



(57) **Abstract:** A method includes running on a computer (24) a first operating environment (104) for performing general-purpose operations and a second operating environment (108), which is configured exclusively for interacting with multiple servers (28) in respective secure communication sessions and is isolated from the first operating environment. Multiple server-specific credentials for authenticating a user of the computer to the respective servers, as well as a single set of master credentials for authenticating the user to the second operating environment, are stored in the second operating environment. A secure communication session is established between the computer and a given server under control of a program running in the second operating environment, by authenticating the user using the master credentials and, responsively to authenticating the user, selecting one of the server-specific credentials and authenticating the user to the given server using the selected server-specific credentials.

WO 2008/114256 A2

TRUSTED LOCAL SINGLE STGN-ON

FIELD OF THE INVENTION

The present invention relates generally to computer networks, and particularly to methods and systems for secure communication over data communication networks.

BACKGROUND OF THE INVENTION

Various applications allow users to interact with a computer system of an organization over the Internet or other public network. Such applications are often referred to as extranet applications. For example, extranet applications enable users to carry out financial transactions with organizations such as banks or insurance companies and make purchases using electronic commerce (e-commerce) web-sites. Employees can access organization data remotely over the Internet, and physicians can access medical records maintained by health institution database systems.

Communication security is often a prime consideration in the design and deployment of extranet applications, especially since extranet communication traffic traverses a public network and since user computers are often not under the control of the organization. Several methods and systems for increasing the security of extranet communication are known in the art. For example, U.S. Patent Application Publication 2002/0029276, whose disclosure is incorporated herein by reference, describes methods and systems for enabling a network connection between first and second processors using at least one additional processor separate from the first and second processors. As another example, U.S. Patent 7,210,169, whose disclosure is incorporated herein by reference, describes an originator device, which allows for a unique pass-phrase to be communicated to a service system. The originator device has a fixed token, in which a unique platform identifier is recorded, and a processor that generates a representation of the platform configuration. The representation is communicated to a registry service as a unique, platform-specific pass-phrase associated with the originator.

Some security methods and systems attempt to verify the integrity of the operating environment of a server or user computer, i.e., verify that the operating environment has not been corrupted or tampered with. For example, U.S. Patent Application Publication 2005/0221766, whose disclosure is incorporated herein by reference, describes a method and apparatus for performing dynamic attestation for a communication system. Several methods for measuring and reporting the integrity of a system, such as a wireless device, are described. U.S. Patent Application Publication 2005/0132031, whose disclosure is incorporated herein by reference, describes a system and method for providing attestation and/or integrity of a server

execution environment. One or more parts of the server environment are selected for measurement. The selected parts are measured, and the measurements result in a unique fingerprint for each selected part. The unique fingerprints are aggregated by an aggregation function to create an aggregated value, which is determinative of running programs in the server environment. A measurement parameter may include the unique fingerprints, the aggregated value or a base system value and may be sent over a network interface to indicate the server environment status or state.

STJMMARY OF THE INVENTION

Embodiments of the present invention provide a computing method, including:

running on a user computer a first operating environment for performing general-purpose operations and a second operating environment, which is configured exclusively for interacting with multiple servers in respective secure communication sessions and is isolated from the first operating environment;

storing in the second operating environment multiple server-specific credentials for authenticating a user of the user computer to the respective servers, and a single set of master credentials for authenticating the user to the second operating environment; and

establishing a secure communication session between the user computer and a given server under control of a program running in the second operating environment, by authenticating the user in the second operating environment using the master credentials and, responsively to successfully authenticating the user, automatically selecting one of the server-specific credentials in the second operating environment and authenticating the user to the given server using the selected server-specific credentials.

In some embodiments, the method includes conducting the secure communication session with the given server responsively to successfully authenticating the user computer to the given server.

Li an embodiment, the second operating environment is isolated from the first operating environment such that the general-purpose operations performed in the first operating environment do not affect operation of the second operating environment, and running the second operating environment includes verifying a trustworthiness of the second operating environment by communication between the second operating environment and a Central Management System (CMS) that is external to the user computer.

Establishing the secure communication session may include authenticating the user to the given server using the selected server-specific credentials only upon successfully verifying the trustworthiness of the second operating environment by the CMS.

In an embodiment, storing the server-specific credentials includes providing at least one of the server-specific credentials to the CMS, and sending the at least one of the server-specific credentials from the CMS to the user computer for storage in the second operating environment. Providing the at least one of the server-specific credentials may further include providing a security policy of at least one of the servers to the CMS, and enforcing the security policy with respect to the second operating environment by the CMS. Additionally or alternatively, storing the server-specific credentials may include providing at least one of the server-specific credentials to the user computer independently of the CMS.

In another embodiment, the master credentials are uniquely associated with the user computer, and authenticating the user using the master credentials includes verifying that the user computer matches the master credentials. In still another embodiment, storing the server-specific credentials includes encrypting the server-specific credentials, and authenticating the user to the given server using the selected server-specific credentials includes decrypting the selected credentials. In an embodiment, storing the master credentials includes encrypting the master credentials, and authenticating the user using the master credentials includes decrypting the master credentials.

In some embodiments, storing the server-specific credentials includes storing a self-contained data element including one of the server-specific credentials and a software application that is to run in the second operating environment for communicating with a respective one of the servers. The self-contained data element may further include attributes of the software application. In an embodiment, the self-contained data element includes the master credentials, the multiple server-specific credentials and respective multiple software applications for communicating with the servers.

In some embodiment, establishing the secure communication session includes, in response to successfully authenticating the user to the given server, causing a packet filter of the given server to allow packets arriving from the user computer to reach the given server.

There is additionally provided, in accordance with an embodiment of the present invention, a user computer, including:

an interface, which is operative to communicate with multiple servers over a communication network; and

a processor, which is coupled to run a first operating environment, which is configured to perform general-purpose operations, and a second operating environment, which is configured exclusively for interacting with the multiple servers in respective protected communication sessions and is isolated from the first operating environment, to store in the second operating environment multiple server-specific credentials for authenticating a user of the user computer to the respective servers and a single set of master credentials for authenticating the user to the second operating environment, and to establish a secure communication session between the user computer and a given server under control of a program running in the second operating environment, by authenticating the user in the second operating environment using the master credentials and, responsively to successfully authenticating the user, automatically selecting one of the server-specific credentials in the second operating environment and authenticating the user to the given server using the selected server-specific credentials.

There is further provided, in accordance with an embodiment of the present invention a computer software product for use in a user computer, the product including a computer-readable medium, in which instructions are stored, which instructions, when executed by the user computer, cause the user computer to communicate with multiple servers over a communication network, to run a first operating environment for performing general-purpose operations, to run a second operating environment, which is configured exclusively for interacting with the multiple servers in respective communication sessions and is isolated from the first operating environment, to store in the second operating environment multiple server-specific credentials for authenticating a user of the user computer to the respective servers and a single set of master credentials for authenticating the user to the second operating environment, and to establish a secure communication session between the user computer and a given server under control of a program running in the second operating environment, by authenticating the user in the second operating environment using the master credentials and, responsively to successfully authenticating the user, automatically selecting one of the server-specific credentials in the second operating environment and authenticating the user to the given server using the selected server-specific credentials.

The present invention will be more fully understood from the following detailed description of the embodiments thereof, taken together with the drawings in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram that schematically illustrates a system for secure communication, in accordance with an embodiment of the present invention;

Fig. 2 is a block diagram that schematically illustrates a user computer, in accordance with an embodiment of the present invention; and

Fig. 3 is a flow chart that schematically illustrates a method for performing secure local single sign-on, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS

OVERVIEW

Establishing communication between a user computer and a server typically involves authenticating the user using a certain set of credentials, such as a username-password pair. In many cases, a certain user has multiple different credentials, which are used for authentication with different servers. For example, a user may have one set of credentials for logging in to his e-mail account, another set of credentials for logging in to his bank web portal, and yet another set of credentials for purchasing from a given e-commerce web site. Some users may have dozens of different credentials for authentication with different servers.

Users often find it difficult to define, remember and use a large number of different credentials. Some users simplify this task by using simple, easy-to-remember credentials. Some users write the credentials on paper, and other users use the same credentials with different servers. AU of these examples demonstrate that the complexity of managing a large set of credentials ultimately results in reduced-quality credentials and/or increased security risks.

Embodiments of the present invention provide improved methods and systems for enabling a user to maintain multiple credentials for use with multiple different servers, while still having to remember and enter only a single set of credentials. The feature of accessing multiple different servers or applications with a single set of credentials is commonly known as "single sign-on."

In some embodiments that are described hereinbelow, the user computer runs two operating environments, which are referred to herein as a General-Purpose Operating Environment (GPOE) and a Trusted Operating Environment (TOE). The GPOE performs general-purpose operations of the user computer. The TOE, on the other hand, is configured exclusively for conducting protected communication sessions with protected servers.

Typically, the TOE is isolated from the GPOE and its trustworthiness is verified by an external Central Management System (CMS).

The TOE stores multiple sets of server-specific credentials, for authenticating the user to respective predefined protected servers. The TOE also stores a single set of master credentials, which are used for authenticating the user to the TOE.

In order to establish a secure communication session with one of the predefined protected servers, the TOE carries out a two-stage authentication process. First, the user authenticates with the TOE by providing the master credentials. Upon successful authentication of the user's identity, the TOE automatically selects the appropriate server-specific credentials and authenticates the user to the server using the selected credentials.

Thus, by using the methods and systems described herein, the user is able to use any desired number of different credentials with different servers, while having to remember and provide only a single set of credentials. Since the trustworthiness of the TOE is continually assessed by the CMS, the credentials stored in the TOE and provided to the servers can be regarded as trustworthy, as well.

Moreover, in some embodiments the master credentials are local, i.e., uniquely associated with a particular user computer. hi these embodiments, the master credentials are valid only when used from the particular user computer with which they are associated. Thus, even if the master credentials are disclosed to an illegitimate party, they cannot be used for authentication from other computers.

Some known authentication methods store and manipulate security credentials in the general-purpose operating environment. Unlike these methods, the methods and systems described herein store and use credentials from within the isolated TOE, whose trustworthiness is continually assessed by a trusted external entity (the CMS). Thus, the immunity of the user computer against password theft and other security threats is considerably enhanced. The enhanced security provided by the disclosed methods and systems enables organizations to deploy extranet applications with improved cost-effectiveness, ease-of-use and user satisfaction and with reduced risk of attack or information leakage.

SYSTEM DESCRIPTION

Fig. 1 is a block diagram that schematically illustrates a system 20 for secure communication, in accordance with an embodiment of the present invention. In system 20, a user 22 operating a user computer 24 interacts with one or more servers, also referred to as data centers. In the present example, the user interacts with two data centers 28A and 28B. For

example, the user may access his bank account using one server, log in to his e-mail account using another server, carry out an e-commerce transaction with yet another server, and/or interact with different servers in order to conduct any other type of communication session.

The interaction of user computer 24 with data centers 28A and 28B is controlled and protected using methods that are described in detail below. Data centers 28A and 28B are sometimes referred to herein as protected data centers. The protected data centers may comprise, for example, e-commerce web-sites, computer systems of financial institutions or other organizations, database servers, web sites in which the user has personal accounts and/or any other suitable computing platforms that interact with users and whose interaction with the users involves authentication. Each data center may comprise one or more computing platforms. Users may comprise, for example, customers, suppliers, employees or partners of the organization operating a given data center. Although Fig. 1 shows a single user and two data centers for the sake of clarity, a typical system comprises multiple users and multiple servers that are active at any given time.

User computer 24 and data centers 28A and 28B communicate over a communication network 32, via respective secure connections 34A and 34B. Network 32 may comprise a Wide Area Network (WAN), such as the Internet, a Metropolitan Area Network (MAN), a Local Area Network (LAN), a wired or wireless data network, or any other suitable network or combination of network types. Typically, at least part of network 32 is public.

User computer 24 may comprise a personal computer, a mobile computing/communication device or any other suitable user terminal. In the context of the present patent application and in the claims, the term "user computer" is used broadly and refers to any type of computing platform that is capable of communicating over a network. Computer 24 comprises a display 36 for displaying information to user 22, and an input device, such as a keyboard 40 or a mouse, for receiving user input. The internal structure of computer 24 is described in greater detail in Fig. 2 below. In particular, the user computer runs two separate operating environments, referred to as a General-Purpose Operating Environment (GPOE) and a Trusted Operating Environment (TOE).

User 22 interacts with each data center in a protected communication session. In order to initiate the secure session, the user computer authenticates with the data center by providing a certain set of credentials, such as a certificate or a username-password pair. Typically, the same user has different sets of credentials for authenticating with different data centers. The credentials that are used for authenticating the user vis-a-vis a particular data center are referred to herein as server-specific credentials. Nevertheless, using methods that are described

in detail hereinbelow, user 22 need not remember and enter the server-specific credentials. Instead, the user enters only a single set of credentials, regardless of the server with which the session is initiated. This single set of credentials is referred to herein as master credentials 44.

Secure connections 34A and 34B, which connect user computer 24 with data centers 28A and 28B, may comprise connections that use the well-known Secure Sockets Layer (SSL) protocol. Each data center typically comprises an SSL Gateway (SSL GW) 48, which terminates the SSL connection at the data center end, and is able to allow or deny connection to the data center. Typically but not necessarily, users connect to the data center by connecting to a web server of the data center and accessing a web portal using a web browser. The SSL GW and web server may comprise separate computing platforms or be integrated in a single platform. In some embodiments, the data center comprises a Data Center packet Filter (DCF) 52, which filters packets arriving at the data center.

In some embodiments, system 20 comprises a Central Management System (CMS) 70, which monitors, configures and controls the TOE of computer 24. CMS 70 comprises a network interface 74, which is connected to network 32. The CMS typically comprises a management processor 78, which carries out the monitoring, control and configuration functions of the CMS and an attestation processor 82, which carries out attestation tests on the user computers.

The CMS communicates with the TOE of the user computer over network 32 using a secure connection 86, such as an SSL connection. The CMS monitors the TOE and attempts to detect situations in which the TOE has been corrupted or modified. The CMS reports the monitoring results to the data center. Since the exclusive task of the TOE is communicating with the data center, and since it typically has a fixed configuration, reliable detection of deviations from normal behavior, configuration and/or performance is feasible.

Some data centers may be connected to the CMS, and others may not. System operation with these two types of data centers is addressed below. Li the example of Fig. 1, data center 28A is connected to the CMS, whereas data center 28B is not. Data center 28A comprises a Data Center Connector (DCC) 56, which serves as an interface between the CMS and the data center. The DCC communicates with the CMS over network 32 using a secure connection 90, such as an SSL connection. In addition to serving as an interface, the DCC sometimes maintains policies that define how different TOEs are treated by the data center as a function of their trustworthiness, as monitored and reported by the CMS.

DCC 56 comprises a network interface 60 for communicating over network 32, and a DCC processor *66* that carries out the different DCC functions. In some embodiments, DCC

56 comprises a hardware/software unit that is separate from the data center. Alternatively, the functions of the DCC can be embodied in one or more processors of the data center. The DCC may participate in provisioning of certificates and may enable minor changes in the web portal accessed by the users.

Although Fig. 1 shows two data centers and a single user computer, this configuration was chosen purely for the sake of conceptual clarity. In some embodiments, the methods and systems described herein can be carried out exclusively by the user computer and data center. Thus, CMS 70 may be omitted in some system configurations. In alternative embodiments, a particular CMS may control multiple user computers. Additionally or alternatively, a particular CMS can operate with multiple data centers or other servers. In some case, each data center belongs to a different organization. In other cases, a certain organization may operate multiple data centers.

Fig. 2 is a block diagram that schematically illustrates user computer 24, in accordance with an embodiment of the present invention. Computer 24 comprises hardware 100, typically comprising a processor that carries out the methods described herein, memory devices and any other suitable components or subsystems normally found in computing platforms. The computer comprises a network interface 116, which connects the computer with network 32, such as for communicating with data center 28 and/or CMS 70.

Computer 24 (or, more accurately, the processor in hardware 100) runs two operating environments in parallel. A Trusted Operating Environment (TOE) 108 is configured exclusively for communicating with the protected data centers. A General-Purpose Operating Environment (GPOE) 104 runs the different applications of the computer other than the protected data center applications. For example, in some embodiments the GPOE comprises a Microsoft® Windows® operating system, and the TOE comprises a Linux® operating system that runs a Firefox® browser. Alternatively, any other suitable operating system, such as Apple® Mac OS®, can also be used.

GPOE 104 and TOE 108 are decoupled, or isolated, from one another. In other words, the behavior, configuration and performance of one operating environment have little or no effect on the behavior, configuration and performance of the other. In particular, the performance and behavior of the TOE is insensitive to the operation of the GPOE. In some embodiments, the configuration of the TOE may not be entirely fixed, and the TOE may perform certain tasks other than communication with the data center. Thus, the terms "fixed configuration" and "configured exclusively for-interacting with the data center" are meant to describe a situation in which the effect of any additional tasks carried out by the TOE is

sufficiently minor, such that the TOE configuration is sufficiently fixed to allow reliable detection of anomalous behavior or performance.

Computer 24 comprises a virtualization layer 112, which controls the hardware resources and other resources of computer 24, and allocates the resources to the GPOE and TOE. Any suitable virtualization means, which may be implemented in hardware and/or software, can be used for this purpose. Although the computer configuration of Fig. 2 shows a single TOE for communicating with the different protected data centers, computer 24 may alternatively run two or more TOEs, which are decoupled from one another and from the GPOE, for securely connecting to multiple separate data centers.

Typically, hardware 100 of user computer 24, processors 78 and 82 of CMS 70 and DCC processor *66* of DCC 56 comprise general-purpose processors, which are programmed in software to carry out the functions described herein. The software may be downloaded to the processors in electronic form, over a network, for example, or it may alternatively be supplied to the processors on tangible, computer-readable media, such as CD-ROM. In particular, the TOE configuration may be distributed to the user computer as software code on suitable tangible media. For example, the user may be provided with tangible storage media storing a self-extracting file, which comprises a pre-configured Linux operating system and a Firefox browser that is pre-configured for exclusive communication with a given data center.

Additional aspects of implementing security features using computers that run trusted operating environments are described in PCT Publication WO 2008/018055, entitled "Extranet Security," filed July 31, 2007, whose disclosure is incorporated herein by reference.

PERFORMING SECURE LOCAL SINGLE SIGN-ON

In many cases, user 22 has multiple different credentials, which are used for authentication with different servers or data centers. For example, one set of credentials may be used for logging in to the user's e-mail account, another set of credentials may be used for performing financial transactions via an Internet portal of the user's bank, and other sets of credentials may authenticate the user vis-a-vis different e-commerce sites. As explained above, however, the complexity of managing multiple different credentials typically results in reduced-quality credentials and/or increased security risks.

Embodiments of the present invention provide improved methods and systems for enabling a user to maintain multiple credentials for use with multiple different servers, while still having to remember and enter only a single set of credentials.

In some embodiments, server-specific credentials are stored in the TOE of the user computer. Each set of server-specific credentials is used for authenticating the user to a given predefined protected server. In addition, the TOE stores a single set of credentials, referred to as master credentials, which are used for authenticating the user to the TOE. In order to establish a secure communication session with one of the predefined protected servers, the TOE carries out a two-stage authentication process, which first authenticates the user using the master credentials, and then automatically authenticates the user with the desired protected server using the appropriate server-specific credentials. Since the trustworthiness of the TOE is continually assessed by the CMS, the credentials stored in the TOE and provided to the servers can be regarded as trustworthy, as well.

Fig. 3 is a flow chart that schematically illustrates a method for performing secure local single sign-on, in accordance with an embodiment of the present invention. The method begins by provisioning users to access multiple protected servers, at a provisioning step 120. For each protected server, provisioning a user comprises predefining server-specific credentials that, when provided by the user, verify the user's identity to the server. Any suitable type of security credentials known in the art can be used as server-specific credentials, such as, for example, various kinds of personal certificates, username-password schemes, secure tokens, biometric schemes and/or smartcards.

The TOE of the user computer stores the multiple server-specific credentials, at a credentials storage step 124. The TOE also stores a single set of master credentials, using which the user authenticates with the TOE. The master credentials may comprise any suitable type of credentials known in the art.

Typically, the TOE secures the stored server-specific and master credentials, such as by encrypting them prior to storage. Although the TOE provides real time protection of the stored credentials, the credentials may be retrieved from the user computer using other means. For example, the computer or its hard disk may be stolen and read not via the TOE. Encryption is used to protect the stored credentials against such scenarios.

During operation of the user computer, the computer monitors the operation of the GPOE, at a monitoring step 128. The computer checks whether the user attempts to initiate a secure communication session with one of the predefined protected servers, at a checking step 132. The user may initiate the secure session, for example, by typing a Uniform Resource Locator (URL) of a predefined protected server in the GPOE browser, by using a shortcut of the GPOE operating system, by selecting an entry from a "favorites" menu or by clicking a hyperlink in a certain web page.

If no secure session initiation is detected, the method loops back to step 128 above, to continue monitoring the GPOE. If, on the other hand, an initiation of a secure session is detected, the user computer automatically switches operation from the GPOE to the TOE_5 at a switching step 136. Certain additional aspects of detecting session initiation attempts and of switching between the GPOE and TOE are addressed in PCT Publication WO 2008/018055, cited above.

Having switched to the TOE, the TOE authenticates the user by requesting the user to enter the master credentials, at a master authentication step 140. If the user fails to provide the correct master credentials, authentication fails and the method terminates. If the user does provide the correct master credentials, the TOE automatically authenticates with the protected server, at a server-specific authentication step 144. The TOE selects the server-specific credentials corresponding to the protected server with which the user initiated the secure session, from among the stored sets of server-specific credentials. The TOE then automatically authenticates with the server on behalf of the user using the selected server-specific credentials.

When the TOE contacts the protected server, the server requests the server-specific credentials (e.g., a password or a personal certificate with which the user was provisioned). Typically, the server-specific credentials are delivered to the server only when the TOE is proven to be trustworthy. As noted above, the CMS continuously assesses the trustworthiness of the TOE. The TOE provides the requested credentials only if the TOE is currently regarded as trustworthy by the CMS.

After server-specific authentication is completed, the user computer goes on to establish and conduct the secure session with the desired protected server, at a server interaction step 148. Although the description above refers to sessions that are conducted via the TOE, sessions may also be conducted via the GPOE.

In some embodiments, the data center notifies the data center packet filter of the successful authentication. In response to the notification, the packet filter allows data packets arriving from the authenticated user computer to pass and reach the data center. Notifications to the data center packet filter can also be sent by the CMS.

Thus, the method of Fig. 3 enables the user to remember and provide only the master credentials, whereas authentication with the different servers using the server-specific credentials is carried out automatically by the TOE. Since the trustworthiness of the TOE is continuously assessed by the external CMS, the TOE is regarded as a safe location for storing security credentials, and the credentials stored in the TOE can thus be trusted.

Moreover, in some embodiments, the master credentials axe predefined as local, i.e., uniquely associated with the particular user computer. In these embodiments, the master credentials are valid only if provided on the same machine (user computer) for which they are defined. When using this technique, even if the master credentials are disclosed (intentionally or unintentionally) to an illegitimate party, they are useless when entered at another computer. IQ order to authenticate successfully, the illegitimate party needs to obtain the master credentials, as well as gain physical access to the computer for which they were defined. Thus, the locality of the master credentials provides protection against "phishing" attacks and other password theft schemes.

In some embodiments, the user provisioning process is carried out in coordination between the server and the CMS. In these embodiments, the server issues a set of credentials for the user and provides these credentials to the CMS. The CMS provides the credentials to the user computer. In addition to credentials, the server may define various security policies, which are enforced and/or propagated to the user computers by the CMS. Such schemes may be used, for example, when the organization operating the server has a suitable business relationship with the organization operating the CMS. Ia alternative embodiments, user provisioning can be carried out directly between the user computer and the server, without involving the CMS. Such schemes may be used, for example, with legacy servers that do not support CMS interfaces, and in situations in which there is no cooperation between the organization operating the server and the organization operating the CMS.

In some embodiments, a given user may be provisioned with one or more servers in coordination with the CMS, and with one or more other servers directly. Fig. 1 above, for example, shows a configuration in which one data center is connected to the CMS and another data center is not.

hi some embodiments, the CMS carries out various management functions with regard to the server-specific credentials. For example, the type of user provisioning performed and the desired authentication process may vary from one protected server to another. The applicable policy of each server may be stored in the CMS and applied to the TOEs of user computers that are provisioned to access the server.

As another example, different servers may have different updating policies with regard to security credentials. A given server may request that passwords be changed every three months. Another server may not impose such a requirement, or specify a different updating period. In some embodiments, the CMS stores and manages the different credentials management policies of the different servers. The user maybe notified of the changes or asked

for permission to perform them. Such notifications and requests are initiated by the CMS and propagated to the TOEs of the applicable user computers.

The CMS may store and enforce policies that apply to the master credentials, as well. For example, the locality of the master credentials may be switched on and off, or defined in different ways. Such locality policies may be managed by the CMS.

In some embodiments, the user computer is provisioned to use a certain application and/or certain attributes for establishing and conducting a secure session with a certain protected server. Different protected servers may use different applications and/or attributes on the user computer side.

For example, consider a user computer that is provisioned to access two protected servers. One server comprises a web site providing Internet services, and the other server comprises a corporate site that provides financial services to customers. In order to connect to the first server, the TOE is provisioned to use a particular Internet browser having a predefined configuration with fixed communication settings. The browser configuration may also define one or more server-specific "cookies." Secure connection with the second server, on the other hand, is performed using a dedicated Java™ application that uses a specific version of a Java Virtual Machine (JVM) and one or more associated libraries.

In some embodiments, the TOE stores a self-contained data element, which serves as a digital identity of the user for each protected server. The self-contained data element comprises the server-specific credentials for accessing the server and the software application (e.g., browser) to be used for connecting to the server, and may comprise additional attributes (e.g., policies and/or data) for use in connecting to the servers. The TOE typically secures each "digital identity," such as using encryption. Using this technique, a composite digital identity can be transferred from one computer to another, backed-up or otherwise manipulated as a single data element.

In some embodiments, a set of composite digital identities of a given user, along with the master credentials of this user, are managed as a single composite data element. When the user initiates connection to a protected server, the TOE verifies the user's identity using the master credentials, retrieves and decrypts the appropriate digital identity, and then connects to the server using the application, attributes and server-specific credentials specified in the retrieved identity. If the user requests to connect to another protected server, the TOE retrieves and applies the digital identity defined for the other server. Ia some embodiments, the TOE

may request the user to re-authenticate using the master credentials, such as after a predetermined idle period.

Although the embodiments described herein mainly address extranet applications in which communication is transported over public networks, the principles of the present invention can also be used for enhancing the security of intranet applications in which communication is confined to a private network.

It will thus be appreciated that the embodiments described above are cited by way of example, and that the present invention is not limited to what has been particularly shown and described hereinabove. Rather, the scope of the present invention includes both combinations and sub-combinations of the various features described hereinabove, as well as variations and modifications thereof which would occur to persons skilled in the art upon reading the foregoing description and which are not disclosed in the prior art.

CLAIMS

1. A computing method, comprising:

running on a user computer a first operating environment for performing general-purpose operations and a second operating environment, which is configured exclusively for interacting with multiple servers in respective secure communication sessions and is isolated from the first operating environment;

storing in the second operating environment multiple server-specific credentials for authenticating a user of the user computer to the respective servers, and a single set of master credentials for authenticating the user to the second operating environment; and

establishing a secure communication session between the user computer and a given server under control of a program running in the second operating environment, by authenticating the user in the second operating environment using the master credentials and, responsively to successfully authenticating the user, automatically selecting one of the server-specific credentials in the second operating environment and authenticating the user to the given server using the selected server-specific credentials.

2. The method according to claim 1, and comprising conducting the secure communication session with the given server responsively to successfully authenticating the user computer to the given server.

3. The method according to claim 1, wherein the second operating environment is isolated from the first operating environment such that the general-purpose operations performed in the first operating environment do not affect operation of the second operating environment, and wherein running the second operating environment comprises verifying a trustworthiness of the second operating environment by communication between the second operating environment and a Central Management System (CMS) that is external to the user computer.

4. The method according to any of claims 1-3, wherein establishing the secure communication session comprises authenticating the user to the given server using the selected server-specific credentials only upon successfully verifying the trustworthiness of the second operating environment by the CMS.

5. The method according to any of claims 1-3, wherein storing the server-specific credentials comprises providing at least one of the server-specific credentials to the CMS, and sending the at least one of the server-specific credentials from the CMS to the user computer for storage in the second operating environment.

6. The method according to claim 5, wherein providing the at least one of the server-specific credentials further comprises providing a security policy of at least one of the servers to the CMS, and enforcing the security policy with respect to the second operating environment by the CMS.

7. The method according to any of claims 1-3, wherein storing the server-specific credentials comprises providing at least one of the server-specific credentials to the user computer independently of the CMS.

8. The method according to any of claims 1-3, wherein the master credentials are uniquely associated with the user computer, and wherein authenticating the user using the master credentials comprises verifying that the user computer matches the master credentials.

9. The method according to any of claims 1-3, wherein storing the server-specific credentials comprises encrypting the server-specific credentials, and wherein authenticating the user to the given server using the selected server-specific credentials comprises decrypting the selected credentials.

10. The method according to any of claims 1-3, wherein storing the master credentials comprises encrypting the master credentials, and wherein authenticating the user using the master credentials comprises decrypting the master credentials.

11. The method according to any of claims 1-3, wherein storing the server-specific credentials comprises storing a self-contained data element comprising one of the server-specific credentials and a software application that is to run in the second operating environment for communicating with a respective one of the servers.

12. The method according to claim 11, wherein the self-contained data element further comprises attributes of the software application.

13. The method according to claim 11, wherein the self-contained data element comprises the master credentials, the multiple server-specific credentials and respective multiple software applications for communicating with the servers.

14. The method according to any of claims 1-3, wherein establishing the secure communication session comprises, in response to successfully authenticating the user to the given server, causing a packet filter of the given server to allow packets arriving from the user computer to reach the given server.

15. A user computer, comprising:

an interface, which is operative to communicate with multiple servers over a communication network; and

a processor, which is coupled to run a first operating environment, which is configured to perform general-purpose operations, and a second operating environment, which is configured exclusively for interacting with the multiple servers in respective protected communication sessions and is isolated from the first operating environment, to store in the second operating environment multiple server-specific credentials for authenticating a user of the user computer to the respective servers and a single set of master credentials for authenticating the user to the second operating environment, and to establish a secure communication session between the user computer and a given server under control of a program running in the second operating environment, by authenticating the user in the second operating environment using the master credentials and, responsively to successfully authenticating the user, automatically selecting one of the server-specific credentials in the second operating environment and authenticating the user to the given server using the selected server-specific credentials.

16. The user computer according to claim 15, wherein the processor is coupled to conduct the secure communication session with the given server responsively to successfully authenticating the user computer to the given server.

17. The user computer according to claim 15, wherein the second operating environment is isolated from the first operating environment such that the general-purpose operations performed in the first operating environment do not affect operation of the second operating environment, and wherein the processor is coupled to communicate with a Central Management System (CMS) that is external to the user computer using the second operating environment, so as to enable the CMS to verify a trustworthiness of the second operating environment.

18. The user computer according to any of claims 15-17, wherein the processor is coupled to authenticate the user to the given server using the selected server-specific credentials only when the trustworthiness of the second operating environment is successfully verified by the CMS.

19. The user computer according to any of claims 15-17, wherein the processor is coupled to receive at least one of the server-specific credentials from the CMS, and to store the received at least one of the server-specific credentials in the second operating environment.

20. The user computer according to any of claims 15-17, wherein the processor is coupled to store at least one of the server-specific credentials independently of the CMS.

21. The user computer according to any of claims 15-17, wherein the master credentials are uniquely associated with the user computer, and wherein the processor is coupled to authenticate the user using the master credentials by verifying that the user computer matches the master credentials.

22. The user computer according to any of claims 15-17, wherein the processor is coupled to encrypt the stored server-specific credentials, and to decrypt the selected credentials so as to authenticate the user to the given server.

23. The user computer according to any of claims 15-17, wherein the processor is coupled to encrypt the stored master credentials, and to decrypt the master credentials so as to authenticate the user.

24. The user computer according to any of claims 15-17, wherein the processor is coupled to store a self-contained data element comprising one of the server-specific credentials and a software application that is to run in the second operating environment for communicating with a respective one of the servers.

25. The user computer according to claim 24, wherein the self-contained data element further comprises attributes of the software application.

26. The user computer according to claim 24, wherein the self-contained data element comprises the master credentials, the multiple server-specific credentials and respective multiple software applications for communicating with the servers.

27. A computer software product for use in a user computer, the product comprising a computer-readable medium, in which instructions are stored, which instructions, when executed by the user computer, cause the user computer to communicate with multiple servers over a communication network, to run a first operating environment for performing general-purpose operations, to run a second operating environment, which is configured exclusively for interacting with the multiple servers in respective communication sessions and is isolated from the first operating environment, to store in the second operating environment multiple server-specific credentials for authenticating a user of the user computer to the respective servers and a single set of master credentials for authenticating the user to the second operating environment, and to establish a secure communication session between the user computer and a given server under control of a program running in the second operating environment, by

authenticating the user in the second operating environment using the master credentials and, responsively to successfully authenticating the user, automatically selecting one of the server-specific credentials in the second operating environment and authenticating the user to the given server using the selected server-specific credentials.

5

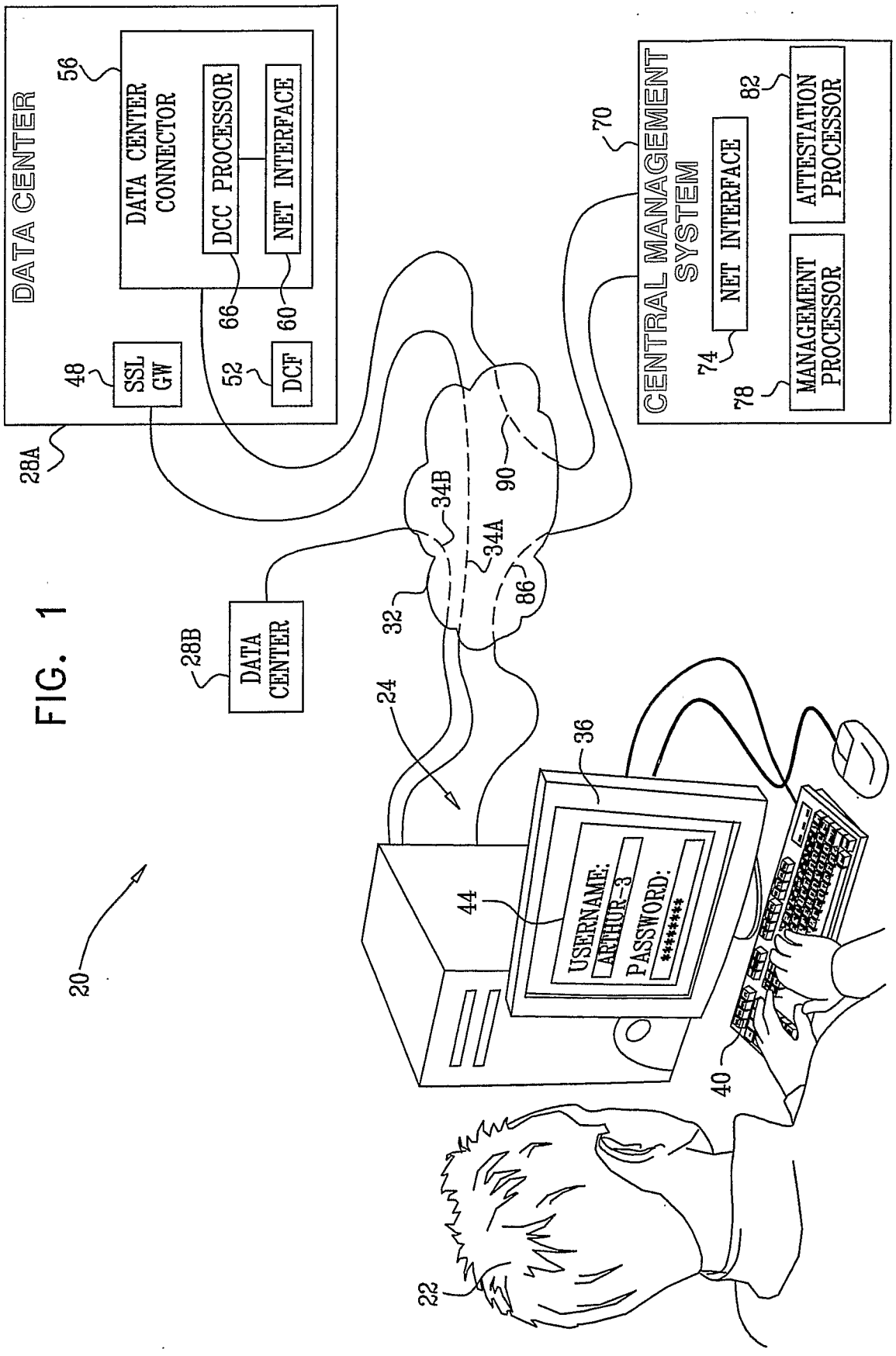

DATA CENTER
56
DATA CENTER CONNECTOR
DCC PROCESSOR
NET INTERFACE
66
60
48
SSL GW
52
DCF
28A
70
CENTRAL MANAGEMENT SYSTEM
NET INTERFACE
74
82
ATTESTATION PROCESSOR
MANAGEMENT PROCESSOR
78
34B
90
34A
86
32
28B
DATA CENTER
24
36
USERNAME:
ARTHUR-3
PASSWORD:
****
44
40
22
20

FIG. 1

FIG. 2

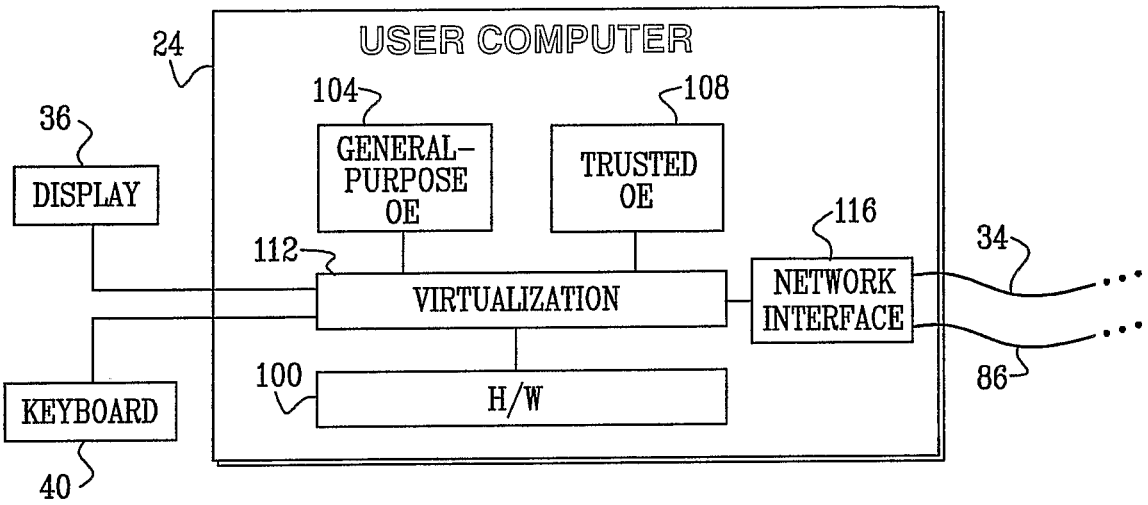
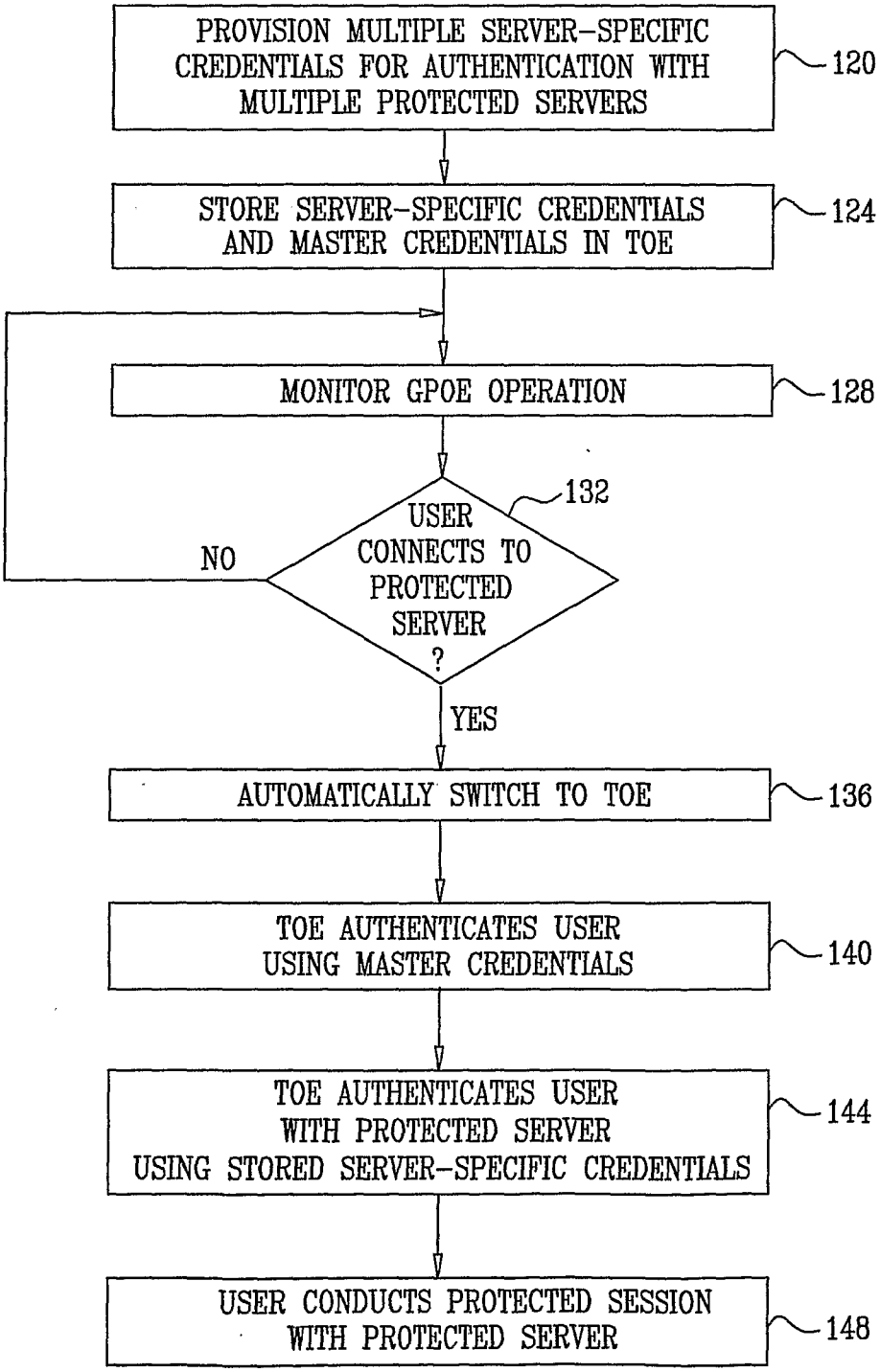

USER COMPUTER
24
104
108
36
DISPLAY
GENERAL-PURPOSE OE
TRUSTED OE
116
112
34
VIRTUALIZATION
NETWORK INTERFACE
100
H/W
KEYBOARD
86
40

FIG. 3


PROVISION MULTIPLE SERVER-SPECIFIC CREDENTIALS FOR AUTHENTICATION WITH MULTIPLE PROTECTED SERVERS
120
STORE SERVER-SPECIFIC CREDENTIALS AND MASTER CREDENTIALS IN TOE
124
MONITOR GPOE OPERATION
128
132
USER CONNECTS TO PROTECTED SERVER ?
NO
YES
AUTOMATICALLY SWITCH TO TOE
136
TOE AUTHENTICATES USER USING MASTER CREDENTIALS
140
TOE AUTHENTICATES USER WITH PROTECTED SERVER USING STORED SERVER-SPECIFIC CREDENTIALS
144
USER CONDUCTS PROTECTED SESSION WITH PROTECTED SERVER
148