

SYSTEM AND METHOD FOR MANAGING A MULTIPLE AUTHENTICATION SYSTEM

FIELD OF THE INVENTION

The present invention relates to a system and method for managing a multiple authentication system on a pre-existing data structure. In particular, the present invention relates to a system and method for validating both the physical identity of an user and that user's pre-determined authority to gain access into one or more applications or services, the invention has particular use in a data structure where each application or service has different authentication mechanism.

BACKGROUND ART

A computer system may provide various applications or services for users. In general, access to the system as to particular applications and/or services may be limited to authorized users. Authorized users are identified via user authentication and one example of user authentication is a login process where a user is required to enter a user name and a password.

In spite of new developments in technology, the combination of the user name and password remains one of the most common access control devices. However, passwords may be disadvantageous because those that are easily remembered are the easiest to determine and those that are complicated and hard to determine are easily forgotten.

The integrity of these types of systems is generally based on keeping the password secret. However, there are many known ways of determining a password, including guessing, applying a dictionary of common passwords or even all known words, brute force attempts including applying all combinations of characters, monitoring network traffic for passwords during exchanges with the server, "shoulder surfing" (looking over a user's shoulder during login), key logging (storing or conveying a user's keystrokes during login), etc.

Known defensive measures against these types of attacks include making passwords longer to make them more difficult to guess, and making dictionary application and brute force techniques more difficult. Other defensive measures include prohibiting the use of "meaningful" passwords such as user-related names, phone numbers, dates of birth, etc., displaying a non-meaningful character such as an asterisk when a user enters a password, the shoulder surfer can see only asterisks, encrypting

passwords before sending them over a network to prevent detection by network monitoring.

One method of access control and authentication is the use of one time passwords (OTP), where a user uses a different password each time they log in, thus rendering many of the above-mentioned attack techniques useless. To intercept, keylog, or otherwise determine a password offers no advantage because the password obtained can't be reused.

Most generally available OTP systems share more or less the same protocol. As part of the login process, the server sends the user a so called 'challenge', which may simply be a large random number. The user enters this number into an OTP generator, for example, a special physical device or software that generates an OTP. The user enters the OTP. The server also enters the challenge into its own OTP generator. If the server OTP and the user OTP match, the user is authenticated.

Where the OTP generator is a physical device (e.g., smart card, token, biometric device, etc.), the cost and inconvenience of a lost, broken, or stolen OTP generator may be of concern.

In instances where the password-producing algorithm is the same for all users, each user is assigned a secret key in order to make the outcome unique. This key is generally embedded in the user's OTP generator and is also stored in the server's database. There are several variations of this OTP generation scheme, for example, the time of day may be used to synchronize a user and server instead of a challenge. In most cases, security relies upon the integrity of the user's secret key. If the key is compromised, the system becomes ineffective. As a result, like a password, the key becomes the subject of various types of attack, with brute force being one of the most popular. An additional layer of security is provided by protecting the algorithms that calculate the OTP, however, with some persistence, the algorithms may be determined and are not a reliable security element.

In a networked environment 100, as shown in Figure 1, a server generally provides various services and applications to a user. The server operates to verify a user in order to properly authorize the use of a particular service or application. This is typically accomplished by the standard login process described above, where the server matches a presently entered user name and password with a stored user name and password.

In other words, in a networked environment, the user would have to perform a login to each of the services and applications as each of the services and applications have different authentication

mechanism. Such multiple logins is time consuming to the user who may have to remember different user names and passwords for each of the services and applications.

It is an object of the present invention to overcome, or at least substantially ameliorate, the disadvantages and shortcoming in the existing networked environment.

Other objects and advantages of the present invention will become apparent from the following description, taken in connection with the accompanying drawings, wherein, by way of illustration and example, an embodiment of the present invention is disclosed.

SUMMARY OF THE INVENTION

In accordance with a first aspect of the invention, there is provided an authentication system comprising: a credential interface in communication with a supervisor layer, the supervisory layer in communication with one or more subsystem authentication system, the subsystem authentication system corresponding to a subsystem, wherein the supervisory layer retrieves information from the subsystem authentication system upon verification of a credential value from a user, and subsequently generates a unified credential permit which allows the user to access the subsystem.

Preferably, the system further includes creating an authentication key in the form of a user formula.

Preferably, an extra security measure may be performed to secure the retrieved information from the subsystem authentication system.

Preferably, the security measures include encryption.

Preferably, the security measures include encoding.

In accordance with a second aspect of the invention, there is provided a method of managing multiple authentication system, comprising: inputting a credential value, verifying the credential value, retrieving relevant information from a subsystem authentication system, generating an

unified credential permit by a supervisory layer , permitting access to a subsystem which correspond to the subsystem authentication system.

Preferably, an extra security measure may be performed to secure the retrieved information from the subsystem authentication system.

Preferably, the security measures include encryption.

Preferably, the security measures include encoding.

BRIEF DESCRIPTION OF THE FIGURES

Further objects of this invention, together with additional features contributing thereto and advantages accruing therefrom, will be apparent from the following description of an embodiment of the present invention which is shown in the accompanying drawings with like reference numerals indicating corresponding parts throughout and which is to be read in conjunction with the following drawings, wherein:

Figure 1 shows a prior art of the authentication system;

Figure 2 shows the schematic drawings of the present authentication system;

Figure 3 shows the method of the present authentication system;

Figure 4 shows an example embodiment of the present authentication system;

These and additional embodiments of the invention may now be better understood by turning to the following detailed description wherein an illustrated embodiment is described.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Throughout this description, the embodiments and examples shown should be considered as exemplars, rather than limitations on the apparatus and methods of the present invention.

Referring to Figure 2, a user authentication system 200 incorporating features of the present invention is illustrated. Although the present invention will be described with reference to the embodiment shown in the drawings, it should be understood that the present invention can be embodied in many alternate forms of embodiments. In addition, any suitable size, shape or type of elements or materials could be used.

As shown in Figure 2, the user authentication system 200 generally includes a credential interface, shown in this example as user credential interface 201, which is in communication with a supervisory layer, shown in the example as a unified authentication management system 202.

The present invention includes creating an authentication key in the form of a user formula. Upon initiation of an authentication session at the user credential interface 201, a user is presented with an arrangement of variables, each assigned a value. The user applies the values associated with the presented variables to matching variables in the user formula and enters the result.

The supervisory layer or the unified authentication management system 202 may be in communication with at least one subsystem authentication server 203 which correspond to a subsystem 205. Once the unified authentication management system 202 receives the user's credential, the unified authentication management system 202 would then verify the user's credential against the records. Once the verification succeeds, the authentication management system 202 will performs a series of operations. In particular, the unified authentication management system 202 retrieves all relevant information, related to the user, from the subsystem authentication server 203. Subsequently, an additional operation may be performed to secure this retrieved information. For instance, extra security measures such as encoding and encryption to ensure information integrity and confidentiality are sometimes performed. A "unified" credential permit 204 which may also be known as an actor credential permit, is generated by the unified authentication management system 202 to allow the user to gain access to the subsystem 205.

The invention is explained in more detail with reference to the flow chart of Figure 3. A user formula is generated and may be constructed by a user from a set of variables and operations. The

authentication system may provide an application to assist the user by providing lists of variables and operations from which to choose. The authentication system may also provide an application that may generate a user formula automatically for a user. The resulting formula is usually memorized by the user. It should be noted that the user is also sometimes known as an actor. An actor may be a form of representation of a person, application, system or anything that interacts with the system from the outside the system boundary.

At step 301, the user logs into the supervisory layer or the unified user authentication system via the user credential interface. The user would log in with the resulting formula, which may be known as the credential information. Verification of the credential information is performed at step 302. If the result is negative, the operation proceeds to step 308, which prompts the user to re-enter the credential information. If the result is positive, the operation proceeds to step 304 where the unified authentication management system retrieves all relevant information from each subsystem authentication. Subsequently, at step 305, an additional operation is performed to secure this retrieved information. For instance, extra security measures such as encoding and encryption to ensure information integrity and confidentiality are sometimes performed. A credential permit, which can also be known as actor credential permit is generated at step 306 which subsequently allows the user access to the individual subsystems is at step 307.

An example embodiment of the present invention is illustrated in Figure 4. In this example embodiment, a sample scenario for a “Corporate Reporting System” is illustrated.

The example embodiment provided three subsystem authentication servers, that is, a Market Survey authentication server 404, a Sales Referral authentication server 405 and a Sales Report authentication server 406. Each of these subsystem authentication servers correspond to a Market Survey subsystem 410, a Sales Referral subsystem 411 and a Sales Report subsystem 412.

It is assumed that the records of user credential mapping to each subsystem authentication servers have been created in ‘Unify Authentication Management’ as an example as follows:

User ID	Password	Subsystem	Subsystem's user Credential
John	***	Market Survey Subsystem	User ID = John-1 Password = @@@
		Sales Referral Subsystem	User ID = Sales\John-2 Password = ###
		Sales Report Subsystem	User ID = Sales\John-3 Password = \$\$\$

For instance, a user called 'John' launches the reporting application 401 and performs a 'read report' operation to the 'Corporate Reporting System'.

The system acknowledges John's new request and prompts him for a user credential 402 via a user credential interface, such as a graphical user interface (GUI) dialog box. John inputs in all the necessary information such as username and password, and submits to the system.

The supervisory layer or the unified authentication management system 403 receives John's credential. The unified authentication management system 403 would then verify John's credential against the records. Once the verification succeeds, the authentication management system 403 will perform a series of operations. In particular, the unified authentication management system 403 retrieves all relevant information, related to John, from each subsystem authentication server, that is, a Market Survey authentication server 404, a Sales Referral authentication server 405 and a Sales Report authentication server 406. Subsequently, an additional operation may be performed to secure this retrieved information. For instance, extra security measures such as encoding and encryption to assure information integrity and confidentiality are sometimes performed. "Unified" credential permits 407, 408, 409, which may also be known as actor credential permits, are generated which allows the user access to the individual subsystems, that is, a Market Survey subsystem 410, a Sales Referral subsystem 411 and a Sales Report subsystem 412.

Hence, the subsystems, that is the Market Survey subsystem 410, the Sales Referral subsystem 411 and the Sales Report subsystem 412 need not validate against its authentication server again. As a result, the 'Read Report' operation traversing different subsystems can be completed using a single authentication credential.

The advantage of this invention is the ability to reduce the frequency of authentication prompts to an actor. An actor needs to log in only once to the system, and subsequently, the subsystems need not prompt the actor for another level of authentication. It also eases actor in maintaining his credential to access various subsystems. An actor is required to maintain only a single credential, hence avoiding the need to keep track of multiple login credentials to different subsystems. Further, it also eases maintaining credential & identity integrity information of various subsystems by having a centralized site to manage adding new, amending and removing existing credential & identity. In addition, it eases the efforts of a system developer by pre-empting a need to extend the existing system. Developers need not be discomforted with adding or revising new subsystems with different authentication mechanisms, as a unified permit is used to validate against.

Although exemplary embodiments of the present invention have been shown and described, it will be apparent to those skilled in the art that a number of changes, modifications, or alternations to the invention as described herein may be made, none of which depart from the spirit of the present invention. All such changes, modifications and alterations should therefore be seen as within the scope of the present invention.

CLAIMS

1. An authentication system comprising:
 - a credential interface in communication with a supervisor layer,
 - the supervisory layer in communication with one or more subsystem authentication system, the subsystem authentication system corresponding to a subsystem,
 - wherein the supervisory layer retrieves information from the subsystem authentication system upon verification of a credential value from a user, and subsequently generates a unified credential permit which allows the user to access the subsystem,
 - wherein the system further includes creating an authentication key in the form of a user formula.
2. The authentication system according to claim 1, wherein an extra security measure may be performed to secure the retrieved information from the subsystem authentication system.
3. The authentication system according to claim 2, wherein the security measures includes encryption.
4. The authentication system according to claim 2, wherein the security measures includes encoding.
5. A method of managing multiple authentication system, comprising:
 - inputting a credential value,
 - verifying the credential value,
 - retrieving relevant information from a subsystem authentication system,
 - generating an unified credential permit by a supervisory layer ,
 - permitting access to a subsystem which correspond to the subsystem authentication system.
 - wherein an extra security measure may be performed to secure the retrieved information from the subsystem authentication system.

6. The method according to claim 5, wherein the security measures includes encryption.
7. The method according to claim 5, wherein the security measures includes encoding.