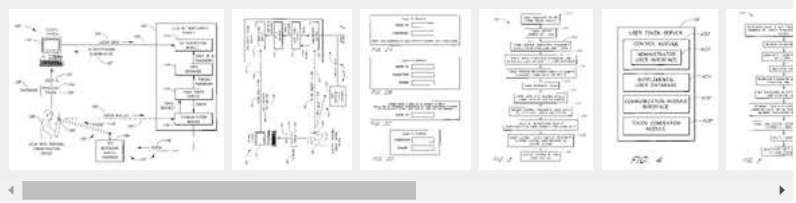
Patents

Use of personal communication devices for user authentication

Abstract

A password setting system for a secure system includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. The server creates a new password by concatenating a secret passcode that is known to the user with the token. The server sets the password associated with the user's user ID to be the new password. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user. The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. Accordingly, access to the system is based upon: nonsecret information known to the user, such as the user ID; secret information known to the user, such as the passcode; and information provided to the user through an object possessed by the user, such as the token.

Images (12)



Classifications

H04L63/083 Network architectures or network communication protocols for network security for supporting authentication of entities communicating through a packet data network using passwords

View 3 more classifications

US6993658B1
United States

Download PDF | Find Prior Art | Similar

Inventor: Sten-Olov Engberg, Ake Jonsson

Current Assignee : Dynapass Ip Holdings LLC

Worldwide applications

2000 ~~US~~ 2001 ~~AU~~ WO

Application US09/519,829 events

2000-03-06 • Application filed by April System Design AB

2000-03-06 • Priority to US09/519,829

2006-01-31 • Application granted

2006-01-31 • Publication of US6993658B1

2020-03-06 • Anticipated expiration

2022-06-17 • US case filed in Texas Eastern District Court

Status • Expired - Lifetime

Show all events

Info: Patent citations (17), Non-patent citations (8), Cited by (206), Legal events, Similar documents, Priority and Related Applications

External links: USPTO, USPTO PatentCenter, USPTO Assignment, Espacenet, Global Dossier, Discuss

Claims (7)

Hide Dependent

1. A method of authenticating a user on a first secure computer network, the user having a user account on said first secure computer network, the method comprising:

   associating the user with a personal communication device possessed by the user, said personal communication device in communication over a second network, wherein said second network is a cell phone network different from the first secure computer network;

   receiving a request from the user for a token via the personal communication device, over the second network;

   generating a new password for said first secure computer network based at least upon the token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user;

   setting a password associated with the user to be the new password;

   activating access the user account on the first secure computer network;

   transmitting the token to the personal communication device;

   receiving the password from the user via the first secure computer network; and

   deactivating access to the user account on the first secure computer network within a predetermined amount of time after said activating, such that said user account is not accessible through any password, via said first secure computer network.

2. The method of claim 1, wherein the new password is generated by concatenating the token and the passcode.

3. The method of claim 1, wherein the personal communication device is a mobile phone.

4. The method of claim 1, wherein the personal communication device is a pager.

5. A user authentication system comprising:

   a computer processor;

a user database configured to associate a user with a personal communication device possessed by the user, said personal communication device configured to communicate over a cell phone network with the user authentication system;

a control module executed on the computer processor configured to create a new password based at least upon a token and a passcode, wherein the token is not known to the user and wherein the passcode is known to the user, the control module further configured to set a password associated with the user to be the new password;

a communication module configured to transmit the token to the personal communication device through the cell phone network; and

an authentication module configured to receive the password from the user through a secure computer network, said secure computer network being different from the cell phone network, wherein the user has an account on the secure computer network, wherein the authentication module activates access to the account in response to the password and deactivates the account within a predetermined amount of time after activating the account, such that said account is not accessible through any password via the secure computer network.

6. The system of claim 5, wherein the communication module is further configured to receive a request from the user for the token, and wherein the control module is further configured to create the new password in response to the request.

7. The system of claim 6, wherein the request is transmitted by the user through the personal communication device.

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates generally to the authentication of users of secure systems and, more particularly, the invention relates to a system through which user tokens required for user authentication are supplied through personal communication devices such as mobile telephones and pagers.

2. Description of the Related Art

Secure systems have traditionally utilized a user ID and password pair to identify and authenticate system users. Operating systems that control local area networks of workstations within a business or institution such as Novell NetWare, Microsoft NT, Windows 2000, and UNIX/Linux typically require submission of a user ID and password combination before allowing access to a workstation.

The incorporation of remote connectivity to secure systems over the Internet has weakened traditional controls imposed by a user's required physical presence within a company's premises and has exposed systems to additional security threats. External users accessing by dial-in or over the Internet, complicated by frequent personnel turnover, require frequent changes in password lists.

Passwords created by users are often combinations of words and names, which are easy to remember but also easily guessed. Guessing passwords is a frequent technique used by “hackers” to break into systems. Therefore, many systems impose regulations on password formats that require mixtures of letters of different cases and symbols and that no part of a password be a word in the dictionary. A user's inability to remember complex combinations of letters, numbers, and symbols often results in the password being written down, sometimes on a note stuck to the side of a workstation.

Present systems face several problems: users dread frequent password changes, frequent password changes with hard-to-remember passwords inevitably result in users surreptitiously writing down passwords, and security is compromised when users write down their passwords.

The SecurID product, which is distributed by RSA Security Inc., solves many of the aforementioned problems by requiring a two-factor authentication process. The first factor is a user passcode or personal identification number. The second factor is a SecurID card that is possessed by the user. The SecurID card generates and displays unpredictable, one-time-only access codes that automatically change every 60 seconds. The user supplies the displayed code upon logging into a system. The system has a corresponding code generator that allows verification of possession of the card.

The SecurID product, however, requires users to carry an additional item on their person in order to access a secure system. It would be advantageous if the benefits of the SecurID system could be achieved using a device that many users already carry—a personal communication device such as a mobile phone or a pager.

SUMMARY OF THE INVENTION

A preferred embodiment of the present invention is a password setting system for setting user passwords for a secure system, such as a computer system or a secure area of a building. The password setting system preferably includes a user token server and a communication module. The user token server generates a random token in response to a request for a new password from a user. The server creates a new password by concatenating a secret passcode that is known to the user with the token. The server sets the password associated with the user's user ID to be the new password. The communication module transmits the token to a personal communication device, such as a mobile phone or a pager carried by the user. The user concatenates the secret passcode with the received token in order to form a valid password, which the user submits to gain access to the secure system. Accordingly, access to the system is based upon: nonsecret information known to the user, such as the user ID; secret information known to the user, such as the passcode; and information provided to the user through an object possessed by the user, such as the token.

One aspect of the invention is a method for setting passwords. The method includes associating a user ID with a phone number of a personal communication device. The method also includes generating a new password based at least upon a token. The method also includes setting a password associated with the user ID to be the new password. The method also includes transmitting the token to the personal communication device using the phone number associated with the user ID. In another aspect, the method also includes associating the user ID with a passcode. In another aspect, the new password is generated based additionally upon the passcode. In another aspect, the method also includes receiving a request for the user token. In another aspect, the personal communication device is a mobile phone. In another aspect, the personal communication device is a pager.

An additional aspect of the invention is a password setting system. The system includes a first user database configured to associate a user ID with a phone number of a personal communication device. The system also includes a control module configured to create a password based at least upon a token. The control module is further configured to cause a second user database to associate the password with the user ID. The system also includes a communication module interface configured to cause a communication module to transmit the token to the personal communication device using the phone number associated with the user ID. In another aspect, the first user database and the second user database are the same database. In another aspect, the first user database is further configured to associate the user ID with a passcode, and the control module is further configured to create the password based additionally upon the passcode.

An additional aspect of the invention is a method of regulating access to a secure system. The method includes transmitting a user token to a personal communication device. The method also includes receiving login data in response to a request for authentication information, wherein the login data is based at least upon the user token. The method also includes granting access to the secure system based upon the received login data. In another aspect, the login data is additionally based upon a user ID. In another aspect, the login data comprises a user ID. In another aspect, the login data is additionally based upon a passcode. In another aspect, the login data comprises a user ID and a password. In another aspect, the password comprises a passcode and the token. In another aspect, the password is a concatenation of the passcode and the token. In another aspect, the password is a hashed concatenation of the passcode and the token. In another aspect the method also includes generating the user token. In another aspect the method also includes receiving a request for the user token. In another aspect, the personal communication device is a mobile phone. In another aspect, the personal communication device is a pager.

An additional aspect of the invention is an access control system. The system includes a user token server configured to transmit a token to a personal communication device. The user token server is further configured to generate a valid password based at least upon the token. The system also includes an authentication module configured to receive at least a submitted password in response to a request for authentication of a user. The authentication module is further configured to grant access to the user if at least the submitted password is based at least upon the token and matches the valid password. In another aspect, the user token server is further configured to generate the valid password based additionally upon a valid passcode that is known to the user. In another aspect, the user token server is further configured to transmit the token in response to a request by the user. In another aspect, the user token server is further configured to associate the valid password with a valid user ID, the authentication module is further configured to receive a submitted user ID in response to the request for authentication, and the authentication module is further configured to grant access to the user if, in addition, the submitted user ID matches the valid user ID.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described below in connection with the attached drawings in which:

FIG. 1 illustrates an overview, including system components, of a user authentication system according to a preferred embodiment of the present invention;

FIGS. 2A–D illustrate login screens that can be used in conjunction with various embodiments of the invention;

FIG. 3 illustrates a preferred process performed by the system to authenticate users;

FIG. 4 illustrates a preferred embodiment of a user token server;

FIG. 5 illustrates a preferred process by which the user token server provides tokens and administrates user accounts;

FIGS. 6A–C illustrate three embodiments of a token delivery communication link;

FIGS. 7A–B illustrate two embodiments of a token request communication link; and

FIG. 8 illustrates an embodiment of a combined token request and delivery communication link.

DETAILED DESCRIPTION OF THE EMBODIMENTS

In the following description, reference is made to the accompanying drawings, which form a part hereof, and which show, by way of illustration, specific embodiments or processes in which the invention may be practiced. Where possible, the same reference numbers are used throughout the drawings to refer to the same or like components. In some instances, numerous specific details are set forth in order to provide a thorough understanding of the present invention. The present invention, however, may be practiced without the specific details or with certain alternative equivalent devices and methods to those described herein. In other instances, well-known methods and devices have not been described in detail so as not to unnecessarily obscure aspects of the present invention.

I. Overview and System Components

FIG. 1 illustrates an overview, including system components, of a user authentication system **100** according to a preferred embodiment of the present invention. FIG. 2A illustrates a login screen that can be used in accordance with the preferred embodiment. FIGS. 2B–D illustrate login screens that can be used in accordance with alternative embodiments.

The user authentication system **100** includes an authentication server **102**, a text messaging service provider **104**, a personal communication device **106** carried by a user **108**, and a secure system **110** to which the authentication system **100** regulates access. The personal communication device **106** is preferably a pager or a mobile phone having SMS (short message service) receive capability. SMS is a secure text messaging capability that is incorporated into most digital mobile phones. The secure system **110** is preferably a Windows NT computer workstation, but may be any system, device, account, or area to which it is desired to limit access to authenticated users. The secure system **110** may be, for example, a user account on a network of computer workstations, a user account on a web site, or a secure area of a building. The secure system **110** is preferably connected to the user authentication server **102** by a computer network **103**. In one embodiment, the user authentication server **102** is integrated into the secure system **110**.

The user authentication server **102** preferably includes a program or a suite of programs running on a computer system to perform user authentication services. The user authentication server **102** may also include the computer system and hardware upon which the programs run. The user authentication server **102** is preferably configured to require that the user **108** supply authentication information through the secure system **110** in order to gain access to the secure system **110**.

The authentication information preferably includes a user ID **152**, a passcode **154** and a user token **156**. The user **108** preferably commits to memory the user ID **152** and passcode **154**. The user ID **152** may be publicly known and used to identify the user **108**. The passcode **154** is preferably secret and only known to the user **108**. The token **156** is preferably provided only to the user **108** by the user authentication server **102** through the user's personal communication device **106** on an as needed basis. The token **156** preferably has a limited lifespan, such as 1 minute or 1 day. Accordingly, the user **108** needs to be in possession of his personal communication device **106** in order to gain access to the secure system **110**. Therefore, if the user's user ID **152** and passcode **154** are compromised, a malicious party still cannot access the secure system without possession of the personal communication device **106**.

In the preferred embodiment, the user **108** combines the token **156** with the passcode **154** to form a password **158**. For example, the user **108** can combine a valid, memorized passcode of "abcd" with a valid token of "1234" to form a valid password of "abcd1234." In this manner, a login screen such as is illustrated in FIG. 2A, which is similar or identical to standard login screens that require a user ID **152** and a password **158**, can be used. In an alternative embodiment, the passcode **154** and the token **156** are submitted separately, as is illustrated in FIG. 2B. In another embodiment, the passcode **154** is null in which case the token **156** alone is used as the password **158**. In still another embodiment, the token **156** can be requested through the secure system **110** as is illustrated in FIGS. 2C–D.

The user authentication server **102** is preferably a secure system itself and may be a part or component of the secure system **110**. The user authentication server **102** preferably includes an authentication module **112** and a user database **114**. The authentication module **112** is preferably identical to the code or software provided with operating systems such as Windows NT that authenticates users upon login. In alternative embodiments, the authentication module **112** may be any code, device, or

module capable of authenticating a user based upon a supplied user ID **152** supplemented by a supplied password **158** or a passcode **154** and a token **156** combination. The authentication module **112** preferably responds to an authentication request transmitted over the computer network **103** by supplying an authentication confirmation **162** over the network **103**. If the user **108** has been authenticated, the confirmation **162** instructs the secure system **110** to allow access to the user **108**. The user database **114** is preferably similar or identical to the database accessed by the authentication module **112** that stores user ID and password data (or passcode and token data) in operating systems such as Windows NT. In alternative embodiments, the user database **114** can be any database capable of storing user ID and password data.

The user authentication server **102** preferably also includes a user token server **116** that responds to requests for tokens **160** by generating a token **156** and transmitting the token **156** to the user's personal communication device **106**. The user authentication server **102** preferably also resets passwords in the user database **114** based upon generated tokens and passcode data. The user authentication server **102** preferably transmits the tokens **156** over a token delivery communication link **105** to the user's personal communication device **106**.

The user authentication server **102** preferably also includes a communication module **118**, which is also part of the token delivery communication link **105**. The communication module **118** forwards tokens **156** to a text messaging service provider **104**, which may be a pager or mobile phone service provider. The text messaging service provider **104** then forwards the token **156** preferably in the form of a secure text message to the personal communication device **106**.

In the preferred embodiment, the communication module **118** is a mobile phone with SMS text messaging send capability. One applicable mobile phone is the presently available Ericsson T-**28**. The mobile phone **118** is preferably connected to the user authentication server **102** via a presently available serial port cable that makes the phone accessible in a manner similar to a computer modem. Accordingly, the user authentication server **102** can send tokens **156** via the server's mobile phone **118** to the user's mobile phone **106** using SMS. In this case, the server's mobile phone **118** transmits a message including the token **156** to the user's personal communication device **106** using the phone number of the user's personal communication device **106**. During the transmission, the message is relayed by the mobile phone service provider **104** to its final destination.

Preferably, the communication module **118** is also configured to receive requests for tokens **160**. The user preferably transmits a request for tokens **160** over a request communication link **107**. The request communication link **107** may be the same communication link as the delivery communication link **105** or it may be a different link. Various embodiments of the token delivery communication link **105** and the token request communication link **107** will be discussed in Section III below.

In the preferred embodiment, the communication module **118** is a mobile phone that also has SMS text messaging receive capability. The communication module **118** receives an SMS message from the user's mobile SMS send enabled mobile phone **106**, and the token server **116** preferably processes the message as a token request **160**. The incoming SMS message is tagged with the sending phone's phone number, which the user token server **116** can use to identify the requesting user and respond with a new token **156**. The token request **160** may also be in the form of a phone call, in which case the user token server **116** may use a caller ID feature to identify the calling phone number as a valid user's personal communication device **106**. The user token server **116** can then respond with a new token **156**. Alternatively, the user token server **116** may allow a calling user **108** to enter the phone number of his personal communication device **106** using the mobile phone keypad once a connection has been established.

In an alternative embodiment, the communication module **118** is an ISDN card that is connected to the text messaging service provider **104** preferably via an X.25 connection. The ISDN card **118** preferably transmits new tokens directly to the text messaging service provider **104** for forwarding to the user's personal communication device **106**. The ISDN card **118** may also be configured to be accessible at a phone number to receive calls for requests for tokens **160**.

FIG. 3 illustrates a preferred process **300** performed by the system **100** to authenticate users. At a step **302**, the user **108** requests a token from the user token server **116** through the token request communication link **107**. In the preferred embodiment, the user's mobile phone **106** has SMS send capability and the user sends an SMS message to the communication module **118** requesting a new token **156**. The SMS message need not contain any data in its body since the phone number of the sending mobile phone is automatically sent along with the message. The user token server **116** preferably identifies the user's mobile phone **106** based upon the phone number with which the SMS message is tagged. In an alternative embodiment, the user **108** makes a phone call with his personal communication device **106** to the communication module **118**. The user token server **116** identifies the user's personal communication device **106** preferably based upon a caller ID feature. Alternatively, the user **108** may call from any phone and enter in the phone number of his personal communication device **106**. As another alternative, the user **108** may request the token **156** through the secure system **110** itself as illustrated in FIGS. 2C–D. As another alternative, the step **302** may be omitted altogether. In this case, the user token server **116** can automatically send tokens **156** to the user **108** at predetermined intervals, such as once per day where the tokens have a lifespan of one day.

At a step **304** the user token server **116** generates a token **156**. The token **156** may be generated by any of a number of methods that preferably produces a random or pseudo-random sequence of numbers and/or digits. The token **156** is preferably long enough such that it cannot be guessed, but short enough such that it is relatively easy to enter, such as six to eight characters.

At a step **306**, the token server **116** generates a new password **158**. The token server **116** preferably creates the new password **158** by combining the user's passcode **154**, which is stored by the user token server **116**, with the newly generated token **156**. At a step **308**, the token server updates the user database **114** with the new password **158**. In the case that the user's account in the user database **114** is inactive or deactivated, the token server **116** activates the user's account.

In the preferred embodiment, the token server creates a hash of the password **158** and stores the hash of the password **158** in the user database **114** rather than storing the password **158** itself. The hash is typically performed using a one-way hashing algorithm where the same password always produces the same hash, but where the password cannot be determined from the hash. In typical systems, passwords **158** are stored as hashes rather than as plain text in order to prevent system administrators and others from being able to determine users' passwords by examining the user database **114**. Also, when a user **108** submits a password **158** upon login to a secure system **110**, the submitted password **158** is immediately hashed using the same one-way hashing algorithm before transmission to the authentication module **112**. The authentication module **112** then compares hashes of passwords rather than the passwords themselves to authenticate the user **108**. In this manner, passwords **158** need not be transmitted over any communication links or computer networks as clear text. It will be apparent to one skilled in the art that the present invention can be implemented with or without the hashing of passwords and that incorporating hashing of passwords does not substantively affect the scope or spirit of the invention. So as not to unnecessarily obscure aspects of the present invention, a password as referred to herein may be an unhashed or a hashed password. For example, a receipt of a password may be a receipt of an unhashed or hashed password, and a comparison of passwords may be a comparison of unhashed or hashed passwords.

At a step **310**, the token server **116** transmits the token **156** to the user's personal communication device **106** via the token delivery communication link **105**. In the preferred embodiment, the communication module **118** is a mobile phone, and the user token server **116** uses the SMS send capability of the phone **118** to send an SMS message including the token **156** to the user's personal communication module **106**. At a step **312**, the user **108** receives the token through his personal communication device **106**.

At a step **314**, the user **108** logs into the secure system **110** using the user ID **152** and the password **158**. In the preferred embodiment, the user **108** combines the passcode **154** and the token **156** by concatenation to form the password **158**. In an alternative embodiment, the passcode **154** and the token **156** are submitted separately.

At a step **316**, the secure system **110** transmits login data **159** to the user authentication server **102** over the computer network **103** for authentication of the user **108**. The login data **159** preferably includes the user ID **152** and a hash of the password **158** that the secure system **110** creates in order to avoid sending the password **158** over the computer network **103** in clear text. Alternatively, the login data **159** may include a hash of the passcode **154** and the token **156**. As another alternative, the password **158**, or the passcode **154** and token **156** are not hashed.

At a step **318**, the user authentication server **102** authenticates the user **108** based upon the login data **159**. In order to authenticate the user **108**, the authentication server **102** preferably compares the login data to the password **158** (hashed or unhashed) or the passcode **154** and token **156** (hashed or unhashed) corresponding to the user ID **152** stored in the user database **114**.

At a step **320**, the user authentication server **102** transmits an authentication confirmation **162** to the secure system **110**. At a step **322**, the secure system **110** allows the user **108** access based upon the authentication confirmation **162**.

II. The User Token Server

FIG. 4 illustrates a preferred embodiment of the user token server **116**. The user token server **116** preferably includes a process or program running on or in conjunction with the user authentication server **102**. The user token server **116** may, however, include a computer upon which the process or program executes. The user token server **116** preferably includes a control module **402**, a supplemental user database **404**, a communication module interface **406**, and a token generation module **408**. The various modules and components of the user token server **116** are described herein from a functional perspective. The various functional components may, however, be seamlessly integrated into one or more executable programs, data structures, and/or physical components.

The control module **402** preferably serves as the top level component of the user token server **116**. The control module **402** preferably handles any tasks or functions not handled by the other modules of the token server **116**, in addition to controlling the other modules. The control module **402** preferably maintains a supplemental user database **404**, which preferably stores associations of user IDs with passcodes, phone numbers of users' personal communication devices, and any other supplemental user data. The other supplemental user data may include one or more of: whether an account is active, the expiration time of passwords, and the frequency with which tokens may be automatically distributed. The supplemental user database **404** is preferably accessed and modified through an administrator user interface **403** provided by the control module **402**. The administrator user interface **403** allows administration of user privileges by adding, modifying and removing user IDs, passcodes, and phone numbers from the supplemental user database **404**.

In the preferred embodiment, the supplemental user database **404** is maintained separately from the user database **114** of the user authentication server **102**. In this configuration, the user database **114** supplied with an OEM system need not be modified or reconfigured. The user token server **116** can be added to existing secure systems in order to provide additional security functionality. In an alternative embodiment, the supplemental user database **404** may be integrated into the user database **114**. In this case, user authentication module **102** is preferably configured and supplied as a single integrated component.

FIG. 5 illustrates a preferred process **500** by which the user token server **116** provides tokens **156** and administers user accounts. The process **500** is described below in conjunction with the description of the functionality of the various modules and components of the user token server **116**.

At a step **502**, the control module **402** associates a user ID with a passcode **154** and a phone number of a user's personal communication device **106**. Upon initially setting up an account, the association can be performed manually by a system administrator through the administrator user interface **403**. The administrator user interface **403** preferably solicits a desired user ID **152**, passcode **154**, and phone number from a system administrator. The control module **402** then preferably creates a deactivated user account with a user ID **152** for the secure system **110** on the user database **114** of the user authentication server **102**. The control module **402** preferably accesses the user database **114** using an application program interface (API) (not illustrated), which is typically provided with OEM systems. The control module **402** also preferably creates an entry in the supplemental user database **404** including the user ID **152**, the passcode **154**, and the phone number.

At a step **504**, the user token server **116** receives a token request **160** from the user **108**, possibly in order to activate his deactivated account. The token request **160** is preferably received through the communication module **118**, which the control module **402** preferably controls through a communication module interface **406**. The communication module interface **406** is preferably a device driver tailored for the specific implementation of the communication module **118**. In alternative embodiments, the user may request the token **156** through the secure system **110** itself, as illustrated in FIGS. 2C–D. In this case, the request **160** may be received through the computer network **103**.

At a step **506**, the control module **402** associates the token request **160** with a valid user ID **152**. The control module **402** may make this association based upon a supplied phone number by querying the supplemental user database **404**. In one embodiment, if the user ID **152** is supplied in conjunction with the request **160**, the step **506** is not performed.

At a step **508**, the token generation module **408** generates a token by a method that produces a random or pseudo-random sequence of numbers or digits or both numbers and digits. Many methods are presently known for producing such random sequences. The token generation module **408** preferably passes the newly generated token **156** to the control module **402**.

At a step **510**, the control module **402** generates a new password **158** based upon the generated token **156** and the passcode **154** associated with the user ID **152** as listed in the supplemental user database **404**. The new password **158** is preferably generated by concatenating the passcode **154** and the token **156**.

At a step **512**, the control module **402** sets or resets the password associated with the user ID **152** in the user database **114**. In the preferred embodiment, the control module **402** sets the password to be a one-way hash of the newly generated password **158**. In alternative embodiments, the password **158** need not be hashed. In the case the user's account has been deactivated, the control module **402** activates the user ID **152** in the user database **114**. The control module **402** preferably accesses the user database **114** through the database API (not illustrated).

At a step **514**, the control module **402** transmits the token **156** to the user's personal communication device **106** preferably based upon the phone number associated with the user ID **152** in the supplemental user database **404**. In the preferred embodiment, the control module **402** causes the communication module **118** to generate and send an SMS message containing the token **156** to the user's mobile phone. In an alternative embodiment, the communication module **118** may call the phone number of the user's pager and transmit the token **156** as the page data.

At a step **516**, the user **108** is able to access the secure system **110** by logging in using the supplied token **156**. The user **108** preferably concatenates his memorized secret passcode **154** with the valid token **156** to create the password **158**. The user then logs in using his user ID **152** and the password **158**.

At a step **518**, if the token has an expiry time, the token **156** expires. At a step **520**, upon expiration of the token **156**, the control module **402** deactivates the user account in the user database **114**.

Finally, the process **500** repetitively continues either from the step **502**, if a new user **108** is to be added, or from the step **504** if an existing user **108** requests a token **156**.

III. Token Delivery and Request Communication Links

FIGS. 6A–C illustrate three embodiments of the token delivery communication link **105**. FIGS. 7A–B illustrate two embodiments of the token request communication link **107**. In some embodiments, the same communication link may be used as the token delivery communication link **105** and the token request communication link **107**. FIG. 8 illustrates an embodiment of a combined token request and delivery communication link that can function in conjunction with a mobile phone without text messaging capability. Additionally, communication technologies other than those illustrated here by example may be used to implement the communication links **105** and **107**.

FIG. 6A illustrates a preferred embodiment of the token delivery communication link **105**. The communication module **118** is a mobile phone **602** with SMS send capability. The mobile phone **602** sends an SMS message **603** including the token **156** to the user's mobile phone **604**. While in transit, the message **603** is received and retransmitted by the SMS system **606** of a mobile phone service provider.

FIG. 6B illustrates a first alternative embodiment of the token delivery communication link **105**. In this case, the communication module **118** is an ISDN card or an X.25 connection card **612** that connects to an SMS gateway **616** of a mobile phone service provider via an ISDN or X.25 connection **613**. The card **612** transmits the token **156** to the SMS gateway **616**, which then creates an SMS message **615** and transmits the message **615** to the user's mobile phone **614**.

FIG. 6C illustrates a second alternative embodiment of the token delivery communication link **105**. In this case, the communication module **118** is a phone dialer **622**, the personal communication device **106** is a pager **624**, and the text messaging service provider is a paging service **626**. In order to transmit a token **156**, the phone dialer **622** places a phone call **623** to the phone number of the user's pager **624**. The paging service provider **626** answers and the phone dialer **622** enters a numeric token **156** to be transmitted to the pager **624**. The paging service provider **626**, in turn, sends a page **625** containing the token **156** to the user's pager **624**.

FIG. 7A illustrates a preferred embodiment of the token request communication link **107**. The personal communication device **106** is preferably the mobile phone **604**, the communication module **118** is preferably the mobile phone **602**, and the text messaging service provider **104** is preferably the SMS system **606** of the preferred embodiment of the token delivery communication link **105** (FIG. 6A). Alternatively, the communication module **118** may be the ISDN card or X.25 connection card **612** connected through the ISDN or X.25 connection **613** as in the first alternative embodiment of the token delivery communication link **105** (FIG. 6B). The mobile phone **604** preferably sends an SMS message **703** as a token request **160** to the mobile phone **602** or the ISDN card **612**. The SMS message **703** may have a blank message body but the message preferably includes the sending phone's phone number in a tag or header field. While in transit, the message **603** is received and retransmitted by the SMS system **606**. The user token server **116** preferably identifies the sending phone's phone number, and if the phone number matches a valid user ID **152**, the token server **116** processes the message **703** as a token request **160**.

FIG. 7B illustrates a first alternative embodiment of the token request communication link **107** in accordance with the token request and login screens of FIGS. 2C–D. The user **108** makes the token request **160** through a first login screen (FIG. 2C) on the secure system **110**. The token request **160** in this case preferably includes the user's user ID **152** and is preferably transmitted through the computer network **103** to the user token server **116** through a network interface card **702**. In this case, the token request **160** need not be communicated through the communication module **118**. Also, the personal communication device **106** need not be used in requesting the token **156** but is preferably used in delivering the token **156**.

FIG. 8 illustrates a combined token request and delivery link in which the personal communication device **106** is preferably a mobile phone. The communication module **118** is preferably an automated telephone response system **802** with a caller ID capability. The user **108** places a phone call **803** to the telephone response system **802**, which identifies the calling phone **804** using caller ID. The telephone response system **802** interprets the call as a token request **160** and responds by generating a voice synthesized recitation of the token **156** that the user hears through the mobile phone **804**. The mobile phone **804**, in this case, need not have any text messaging or SMS capability.

In still other embodiments, various other technologies and combinations of technologies, which will be apparent to one skilled in the art, can be used to implement the token delivery **105** and token request **107** communication links. For example, a token request may be made through a land line phone, and in response, a token may be delivered to a mobile phone.

IV. Conclusion

Although the invention has been described in terms of certain preferred embodiments, other embodiments that are apparent to those of ordinary skill in the art, including embodiments which do not provide all of the features and advantages set forth herein, are also within the scope of this invention. Accordingly, the scope of the invention is defined by the claims that follow. In the claims, a portion shall include greater than none and up to the whole of a thing; encryption of a thing shall include encryption of a portion of the thing; a password may be an unhashed or a hashed password. In the method claims, reference characters are used for convenience of description only, and do not indicate a particular order for performing the method.

Patent Citations (17)

Publication number	Priority date	Publication date	Assignee	Title
US5153919A *	1991-09-13	1992-10-06	At&T Bell Laboratories	Service provision authentication protocol
US5265155A *	1991-07-31	1993-11-23	Integrated Communications, Ltd.	Method and apparatus for prepayment of telecommunication connections in a telecommunication switching network
US5323146A *	1990-03-20	1994-06-21	Siemens Nixdorf Informationssysteme Ag	Method for authenticating the user of a data station connected to a computer system
US5497411A *	1994-03-14	1996-03-05	Pellerin; Joseph C. E.	Telecommunications card-access system
US5590198A	1995-12-19	1996-12-31	Pitney Bowes Inc.	Open metering system with super password vault access
US5749075A *	1995-06-06	1998-05-05	Interactive Media Works, L.L.C.	Method for providing prepaid internet access and/or long distance calling including the distribution of specialized calling cards
EP0875871A2	1997-04-29	1998-11-04	Kim Schmitz	Authorization method in data transfer systems
US5875394A *	1996-12-27	1999-02-23	At & T Wireless Services Inc.	Method of mutual authentication for secure wireless service provision
US5923763A	1996-03-21	1999-07-13	Walker Asset Management	Method and apparatus for secure document timestamping

			Limited Partnership	
US5949882A *	1996-12-13	1999-09-07	Compaq Computer Corporation	Method and apparatus for allowing access to secured computer resources by utilzing a password and an external encryption algorithm
US5956633A *	1995-06-19	1999-09-21	Nokia Mobile Phones Limited	Method and apparatus for controlling the right of use/activating of a mobile station which uses at least two predefined codes which are pre-stored in a SIM module
US6049877A	1997-07-16	2000-04-11	International Business Machines Corporation	Systems, methods and computer program products for authorizing common gateway interface application requests
US6075860A *	1997-02-19	2000-06-13	3Com Corporation	Apparatus and method for authentication and encryption of a remote terminal over a wireless link
US6161182A	1998-03-06	2000-12-12	Lucent Technologies Inc.	Method and apparatus for restricting outbound access to remote equipment
US6173400B1	1998-07-31	2001-01-09	Sun Microsystems, Inc.	Methods and systems for establishing a shared secret using an authentication token
US6226364B1 *	1997-12-08	2001-05-01	Bellsouth Intellectual Property Management Corporation	Method and system for providing prepaid and credit-limited telephone services
US6795852B1 *	1995-09-11	2004-09-21	Nomadix, Inc.	Automatic network connection
Family To Family Citations				

* Cited by examiner, † Cited by third party

Non-Patent Citations (8)

Title
24-hour cellphone cyberwatch-Internet-printed on May 19, 2000.
ACE/Server, http://www.computerps.com/internet/security/secdyn/aceserv.html, last modified Jul. 15, 1998.
International Search Report for PCT/US01/07058 (3-pages).
Menezes, "Handbook of Applied Cryptography," 1997, p. 390. *
Monkey (mobile network key)-Internet-6 pages, printed on May 19, 2000.
Monkey as authentication software-Internet-2 pages, printed on May 19, 2000.
RSA Security Inc.-RSA SecurID Two-Factor Authenication System, http://www.securid.com/products/securid/index.html., printed on Mar. 3, 2000.
Security Dynamics-SecurID Tokens Datasheet, http://www.computerterps.com/internet/security/secdyn/tokens.html., last modified Jul. 31, 1998.

* Cited by examiner, † Cited by third party

Cited By (206)

Publication number	Priority date	Publication date	Assignee	Title
US20030046546A1 *	2001-09-04	2003-03-06	Hitoshi Endo	Identifying method
US20030163694A1 *	2002-02-25	2003-08-28	Chaing Chen	Method and system to deliver authentication authority web services using non-reusable and non-reversible one-time identity codes
US20040073802A1 *	2001-03-02	2004-04-15	Dong-Seok Seol	User identification with an improved password input method
US20040073795A1 *	2002-10-10	2004-04-15	Jablon David P.	Systems and methods for password-based connection
US20040107143A1 *	2002-11-29	2004-06-03	Aki Niemi	Method for authorizing indirect content download
US20040143730A1 *	2001-06-15	2004-07-22	Wu Wen	Universal secure messaging for remote security tokens
US20050021982A1 *	2003-06-11	2005-01-27	Nicolas Popp	Hybrid authentication
US20050081044A1 *	2003-10-14	2005-04-14	Ibm Corporation	Method and apparatus for pervasive authentication domains
US20050208891A1 *	2004-03-16	2005-09-22	Rajendra Khare	Integration of secure identification logic into cell phone
US20060004656A1 *	1999-12-28	2006-01-05	Jong-Il Lee	Electronic money management method and system using mobile communication terminal
US20060020799A1 *	2004-07-06	2006-01-26	Kemshall Andrew C	Secure messaging

US20060053281A1 *	2000-08-15	2006-03-09	Stefan Andersson	Network authentication
US20060059359A1 *	2004-09-15	2006-03-16	Microsoft Corporation	Method and system for controlling access privileges for trusted network nodes
US20060095785A1 *	2004-10-29	2006-05-04	Electronic Data Systems Corporation	System, method, and computer program product for user password reset
US20060107068A1 *	2004-11-18	2006-05-18	Michael Fiske	Method of generating access keys
US20060107064A1 *	2004-11-18	2006-05-18	Michael Fiske	API for a system having a passcode authenticator
US20060143705A1 *	2004-12-29	2006-06-29	Lucent Technologies	User authentication in a conversion system
US20060230284A1 *	2004-12-20	2006-10-12	Michael Fiske	System for generating requests to a passcode protected entity
US20070006286A1 *	2005-07-02	2007-01-04	Singhal Tara C	System and method for security in global computer transactions that enable reverse-authentication of a server by a client
US20070015492A1 *	2001-05-24	2007-01-18	International Business Machines Corporation	Methods and apparatus for restricting access of a user using a cellular telephnoe
US20070016796A1 *	2002-08-12	2007-01-18	Singhal Tara C	Systems and methods for remote user authentication
US20070016804A1 *	2005-07-13	2007-01-18	Kemshall Andrew C	Password management system
US20070037552A1 *	2005-08-11	2007-02-15	Timothy Lee	Method and system for performing two factor mutual authentication
US20070157018A1 *	2005-12-30	2007-07-05	Honeywell International, Inc.	Method and apparatus for using SMS short code messaging to facilitate the transmission of a status update for a security system
US20070207773A1 *	2006-03-06	2007-09-06	Braunstein Andrew S	Remote personnel tracking
US20070249375A1 *	2006-03-31	2007-10-25	Ontela, Inc.	Method and system for phone-number discovery and phone-number authentication for mobile communications devices
US20070271464A1 *	2002-01-15	2007-11-22	Rico Novella Francisco J	Method of sending and validating documents
US20080027857A1 *	2006-07-26	2008-01-31	Benson Tracey M	Method of Preventing Fraud
US20080077526A1 *	2006-09-20	2008-03-27	First Data Corporation	Online payer authorization systems and methods
US20080089521A1 *	2003-04-29	2008-04-17	Eric Le Saint	Universal secure messaging for cryptographic modules
US20080098461A1 *	2006-10-24	2008-04-24	Avatier Corporation	Controlling access to a protected network
US20080098464A1 *	2006-10-24	2008-04-24	Authernative, Inc.	Two-channel challenge-response authentication method in random partial shared secret recognition system
US20080120395A1 *	2002-02-12	2008-05-22	Smith Steven G	Methods and Systems for Communicating with Service Technicians in a Telecommunications System
US20080118041A1 *	2006-11-22	2008-05-22	Alexander Finogenov	Secure access to restricted resource
US20080200156A1 *	2007-02-16	2008-08-21	Mary Anne Hicks	Methods and apparatus to provide medical information using a communication system
US20080295169A1 *	2007-05-25	2008-11-27	Crume Jeffery L	Detecting and defending against man-in-the-middle attacks
US20080305769A1 *	2007-06-08	2008-12-11	Nahum Rubinstein	Device Method & System For Facilitating Mobile Transactions
US20090045253A1 *	2006-03-10	2009-02-19	Min Gyu Han	System and method for providing virtual discernment information
WO2009040495A1 *	2007-09-26	2009-04-02	British Telecommunications Public Limited Company	Password management
US20090106138A1 *	2007-10-22	2009-04-23	Smith Steven E	Transaction authentication over independent network
US20090119759A1 *	2005-10-03	2009-05-07	Petter Taugbol	Method and Arrangement for Secure Authentication
US20100011222A1 *	2004-11-18	2010-01-14	Michael Fiske	Interfacing with a system that includes a passcode authenticator
US7650509B1 *	2004-01-28	2010-01-19	Gordon & Howard Associates, Inc.	Encoding data in a password
WO2010039487A2 *	2008-09-23	2010-04-08	Peer 1	Password management systems and methods
US20100100725A1 *	2008-10-20	2010-04-22	Microsoft Corporation	Providing remote user authentication
US20100100945A1 *	2008-10-20	2010-04-22	Microsoft Corporation	User authentication management
US20100269162A1 *	2009-04-15	2010-10-21	Jose Bravo	Website authentication

US20110138483A1 *	2009-12-04	2011-06-09	International Business Machines Corporation	Mobile phone and ip address correlation service
US8046012B2	2005-01-31	2011-10-25	Destine Systems Co. L.L.C.	Permission based text messaging
US8166311B1 *	2002-06-20	2012-04-24	At&T Intellectual Property I, Lp	Methods and systems for promoting authentication of technical service communications in a telecommunications system
US20120179915A1 *	2011-01-07	2012-07-12	Apple Inc.	System and method for full disk encryption authentication
US20130054414A1 *	2011-08-25	2013-02-28	Teliasonera Ab	Online payment method and a network element, a system and a computer program product therefor
US20130069778A1 *	2005-10-25	2013-03-21	Nxstage Medical, Inc.	Safety features for medical devices requiring assistance and supervision
KR101250230B1	2011-07-21	2013-04-03	주식회사 모비솔루션	Two channel authentication system and method based position value
US8442527B1	2009-01-23	2013-05-14	Sprint Communications Company L.P.	Cellular authentication for authentication to a service
US8484698B2	2000-09-05	2013-07-09	Strikeforce Technologies, Inc.	Multichannel device utilizing a centralized out-of-band authentication system (COBAS)
US8508349B2	2008-12-12	2013-08-13	Gordon*Howard Associates, Inc.	Automated geo-fence boundary configuration and activation
US8566914B2 *	2011-10-21	2013-10-22	Cellco Partnership	Triple authentication: mobile hardware, mobile user, and user account
US20130295882A1 *	2011-01-27	2013-11-07	Tencent Technology (Shenzhen) Company Limited	System, server and method for invalidating a password remembered by an application associated with a mobile terminal
US8581711B2	2011-03-22	2013-11-12	Gordon*Howard Associates, Inc.	Methods and systems of rule-based intoxicating substance testing associated with vehicles
US8581712B2	2008-12-12	2013-11-12	Gordon * Howard Associates, Inc .	Methods and systems related to establishing geo-fence boundaries
US20140052223A1 *	2012-08-17	2014-02-20	Zoom Tan, Inc.	System and method for controlling a tanning bed
US8659404B2	2008-12-12	2014-02-25	Gordon Howard Associates, Inc.	Methods and systems related to establishing geo-fence boundaries and collecting data
US8689297B2 *	2010-11-19	2014-04-01	Blackberry Limited	System, devices and method for secure authentication
US8686841B2	2008-12-12	2014-04-01	Gordon*Howard Associates, Inc.	Methods and systems related to activating geo-fence boundaries and collecting location data
US8781900B2	2011-09-09	2014-07-15	Gordon*Howard Associates, Inc.	Method and system of providing information to an occupant of a vehicle
GB2510002A *	2012-07-26	2014-07-23	Highgate Labs Ltd	Authenticating a user using a pair of user devices by transferring a token between them.
US8838988B2	2011-04-12	2014-09-16	International Business Machines Corporation	Verification of transactional integrity
US20140298432A1 *	2013-03-28	2014-10-02	Wendell Brown	Method and apparatus for automated password entry
US20140359703A1 *	2011-06-08	2014-12-04	Genmsecure	Method for securing an action that an actuating device must carry out at the request of a user
US8917826B2	2012-07-31	2014-12-23	International Business Machines Corporation	Detecting man-in-the-middle attacks in electronic transactions using prompts
US8928471B2	2013-03-14	2015-01-06	Gordon*Howard Associates, Inc.	Methods and systems related to remote tamper detection
US8935769B2	2012-09-28	2015-01-13	Liveensure, Inc.	Method for mobile security via multi-factor context authentication
US9009797B1 *	2008-06-13	2015-04-14	West Corporation	MRCP resource access control mechanism for mobile devices
US9013333B2	2013-06-24	2015-04-21	Gordon*Howard Associates, Inc.	Methods and systems related to time triggered geofencing
US20150109100A1 *	2002-02-01	2015-04-23	Comcast Cable Communications, Llc	Lifestyle multimedia security system
US9027099B1	2012-07-11	2015-05-05	Microstrategy Incorporated	User credentials
US9026267B2	2007-03-09	2015-05-05	Gordon*Howard Associates, Inc.	Methods and systems of selectively enabling a vehicle by way of a portable wireless device
US9035756B2	2013-03-14	2015-05-19	Gordon*Howard Associates, Inc.	Methods and systems related to remote tamper detection
US9060057B1	2013-03-07	2015-06-16	Serdar Artun Danis	Systems and methods for caller ID authentication, spoof detection and list based call handling

US9154303B1	2013-03-14	2015-10-06	Microstrategy Incorporated	Third-party authorization of user credentials
US9160724B2	2014-01-27	2015-10-13	Canon Kabushiki Kaisha	Devices, systems, and methods for device provisioning
US20150317625A1 *	2009-05-15	2015-11-05	Ayman Hammad	Verification of portable consumer devices
US20150333915A1 *	2013-03-15	2015-11-19	Arris Technology, Inc.	Method and apparatus for embedding secret information in digital certificates
US20150372834A1 *	2014-06-23	2015-12-24	Google Inc.	Methods and apparatus for using smart environment devices via application program interfaces
US20150381593A1 *	2014-06-27	2015-12-31	International Business Machines Corporation	Privileged access gateway for accessing systems and/or applications
US20160005042A1 *	2014-07-02	2016-01-07	Mistral Mobile	Host card emulation out-of-bound device binding verification
US9235697B2 *	2012-03-05	2016-01-12	Biogy, Inc.	One-time passcodes with asymmetric keys
US20160050199A1 *	2011-04-19	2016-02-18	Authentify, Inc.	Key management using quasi out of band authentication architecture
US9277049B1	2013-03-07	2016-03-01	Serdar Artun Danis	Systems and methods for caller ID and call destination authentication
US9378480B2	2013-03-14	2016-06-28	Gordon*Howard Associates, Inc.	Methods and systems related to asset identification triggered geofencing
US20160239657A1 *	2015-02-13	2016-08-18	Yoti Ltd	Digital identity system
US20160274759A1	2008-08-25	2016-09-22	Paul J. Dawes	Security system with networked touchscreen and gateway
US20170019395A1 *	2002-04-25	2017-01-19	Intertrust Technologies Corporation	Secure authentication systems and methods
US9582801B2	2009-05-15	2017-02-28	Visa International Service Association	Secure communication of payment information to merchants using a verification token
US9589268B2	2010-02-24	2017-03-07	Visa International Service Association	Integration of payment capability into secure elements of computers
WO2017040638A1 *	2015-09-02	2017-03-09	Jpmorgan Chase Bank, N.A.	System and method for mobile device limits
US9640001B1	2012-11-30	2017-05-02	Microstrategy Incorporated	Time-varying representations of user credentials
US9648496B2	2015-02-13	2017-05-09	Yoti Ltd	Authentication of web content
US9665997B2	2013-01-08	2017-05-30	Gordon*Howard Associates, Inc.	Method and system for providing feedback based on driving behavior
US9701279B1	2016-01-12	2017-07-11	Gordon*Howard Associates, Inc.	On board monitoring device
US9703938B2	2001-08-29	2017-07-11	Nader Asghari-Kamrani	Direct authentication system and method via trusted authenticators
US9715681B2	2009-04-28	2017-07-25	Visa International Service Association	Verification of portable consumer devices
US9727864B2	2001-08-29	2017-08-08	Nader Asghari-Kamrani	Centralized identification and authentication system and method
US9754097B2	2014-02-21	2017-09-05	Liveensure, Inc.	Method for peer to peer mobile context authentication
US20170272425A1 *	2016-03-18	2017-09-21	Beijing Xiaomi Mobile Software Co., Ltd.	Method and device for accessing smart camera
US9785764B2	2015-02-13	2017-10-10	Yoti Ltd	Digital identity
US9788039B2	2014-06-23	2017-10-10	Google Inc.	Camera system API for third-party integrations
US9792611B2	2009-05-15	2017-10-17	Visa International Service Association	Secure authentication system and method
US9840229B2	2013-03-14	2017-12-12	Gordon*Howard Associates, Inc.	Methods and systems related to a remote tamper detection
US9852285B2	2015-02-13	2017-12-26	Yoti Holding Limited	Digital identity
US9880186B2	2014-09-29	2018-01-30	Laird Technologies, Inc.	Telematics devices and methods for vehicle speeding detection
US9886569B1	2012-10-26	2018-02-06	Microstrategy Incorporated	Credential tracking
US9887992B1	2012-07-11	2018-02-06	Microstrategy Incorporated	Sight codes for website authentication
US20180176017A1 *	2015-02-13	2018-06-21	Yoti Ltd	Digital Identity System
US10009177B2	2009-05-15	2018-06-26	Visa International Service Association	Integration of verification tokens with mobile communication devices

US10027619B2	2004-11-22	2018-07-17	Seven Networks, Llc	Messaging centre for forwarding e-mail
US10051078B2	2007-06-12	2018-08-14	Icontrol Networks, Inc.	WiFi-to-serial encapsulation in systems
US10062245B2	2005-03-16	2018-08-28	Icontrol Networks, Inc.	Cross-client sensor user interface in an integrated security network
US10062273B2	2010-09-28	2018-08-28	Icontrol Networks, Inc.	Integrated security system with parallel processing architecture
US10078958B2	2010-12-17	2018-09-18	Icontrol Networks, Inc.	Method and system for logging security event data
US10079839B1	2007-06-12	2018-09-18	Icontrol Networks, Inc.	Activation of gateway device
US10091014B2	2005-03-16	2018-10-02	Icontrol Networks, Inc.	Integrated security network with security alarm signaling system
US10127801B2	2005-03-16	2018-11-13	Icontrol Networks, Inc.	Integrated security system with parallel processing architecture
US10142392B2	2007-01-24	2018-11-27	Icontrol Networks, Inc.	Methods and systems for improved system performance
US10142166B2	2004-03-16	2018-11-27	Icontrol Networks, Inc.	Takeover of security network
US10140840B2	2007-04-23	2018-11-27	Icontrol Networks, Inc.	Method and system for providing alternate network access
US10142394B2	2007-06-12	2018-11-27	Icontrol Networks, Inc.	Generating risk profile using data of home monitoring and security system
US20180343562A1 *	2017-05-26	2018-11-29	Honeywell International Inc.	Systems and methods for providing a secured password and authentication mechanism for programming and updating software or firmware
US10156959B2	2005-03-16	2018-12-18	Icontrol Networks, Inc.	Cross-client sensor user interface in an integrated security network
US10156831B2	2004-03-16	2018-12-18	Icontrol Networks, Inc.	Automation system with mobile interface
US10200504B2	2007-06-12	2019-02-05	Icontrol Networks, Inc.	Communication protocols over internet protocol (IP) networks
US10237237B2	2007-06-12	2019-03-19	Icontrol Networks, Inc.	Communication protocols in integrated systems
US10237806B2	2009-04-30	2019-03-19	Icontrol Networks, Inc.	Activation of a home automation controller
US10268843B2	2011-12-06	2019-04-23	AEMEA Inc.	Non-deterministic secure active element machine
US10282724B2	2012-03-06	2019-05-07	Visa International Service Association	Security system incorporating mobile device
US10313303B2	2007-06-12	2019-06-04	Icontrol Networks, Inc.	Forming a security network including integrated security system components and network devices
US10326759B2 *	2015-04-02	2019-06-18	Syracuse University	Website authentication using an internet-connected device
US10339791B2	2007-06-12	2019-07-02	Icontrol Networks, Inc.	Security network integrated with premise security system
US10348575B2	2013-06-27	2019-07-09	Icontrol Networks, Inc.	Control system user interface
US10365810B2	2007-06-12	2019-07-30	Icontrol Networks, Inc.	Control system user interface
US10380871B2	2005-03-16	2019-08-13	Icontrol Networks, Inc.	Control system user interface
US10382452B1	2007-06-12	2019-08-13	Icontrol Networks, Inc.	Communication protocols in integrated systems
US10389736B2	2007-06-12	2019-08-20	Icontrol Networks, Inc.	Communication protocols in integrated systems
US10423309B2	2007-06-12	2019-09-24	Icontrol Networks, Inc.	Device integration framework
US10440627B2	2014-04-17	2019-10-08	Twilio Inc.	System and method for enabling multi-modal communication
US10469670B2	2012-07-24	2019-11-05	Twilio Inc.	Method and system for preventing illicit use of a telephony platform
US10498830B2	2007-06-12	2019-12-03	Icontrol Networks, Inc.	Wi-Fi-to-serial encapsulation in systems
US10523689B2	2007-06-12	2019-12-31	Icontrol Networks, Inc.	Communication protocols over internet protocol (IP) networks
US10521623B2	2015-02-13	2019-12-31	Yoti Holding Limited	Digital identity system
US10522026B2	2008-08-11	2019-12-31	Icontrol Networks, Inc.	Automation system user interface with three-dimensional display
US10530839B2	2008-08-11	2020-01-07	Icontrol Networks, Inc.	Integrated cloud system with lightweight gateway for premises automation
US10560495B2	2008-04-02	2020-02-11	Twilio Inc.	System and method for processing telephony sessions
US10576927B2	2006-02-07	2020-03-03	Gordon*Howard Associates, Inc	Starter-interrupt device incorporating global positioning system

				functionality
US10616075B2	2007-06-12	2020-04-07	Icontrol Networks, Inc.	Communication protocols in integrated systems
US10666523B2	2007-06-12	2020-05-26	Icontrol Networks, Inc.	Communication protocols in integrated systems
US10692085B2	2015-02-13	2020-06-23	Yoti Holding Limited	Secure electronic payment
US10694042B2	2008-04-02	2020-06-23	Twilio Inc.	System and method for processing media requests during telephony sessions
US10721087B2	2005-03-16	2020-07-21	Icontrol Networks, Inc.	Method for networked touchscreen with integrated interfaces
US10747216B2	2007-02-28	2020-08-18	Icontrol Networks, Inc.	Method and system for communicating with and controlling an alarm system from a remote server
US10785319B2	2006-06-12	2020-09-22	Icontrol Networks, Inc.	IP device discovery systems and methods
US10841381B2	2005-03-16	2020-11-17	Icontrol Networks, Inc.	Security system with networked touchscreen
US10979389B2	2004-03-16	2021-04-13	Icontrol Networks, Inc.	Premises management configuration and control
US10999254B2	2005-03-16	2021-05-04	Icontrol Networks, Inc.	System for data routing in networks
US11062319B1	2015-11-06	2021-07-13	Wells Fargo Bank, N.A.	Systems and methods for funds transfers via a token management system
US11089122B2	2007-06-12	2021-08-10	Icontrol Networks, Inc.	Controlling data routing among networks
US11113950B2	2005-03-16	2021-09-07	Icontrol Networks, Inc.	Gateway integrated with premises security system
US20210306324A1 *	2020-03-31	2021-09-30	Konica Minolta Business Solutions U.S.A., Inc.	Authentication server and method that allow user to log into application or service provided via client devices
US11146637B2	2014-03-03	2021-10-12	Icontrol Networks, Inc.	Media content management
US11153266B2	2004-03-16	2021-10-19	Icontrol Networks, Inc.	Gateway registry methods and systems
US11182060B2	2004-03-16	2021-11-23	Icontrol Networks, Inc.	Networked touchscreen with integrated interfaces
US11201755B2	2004-03-16	2021-12-14	Icontrol Networks, Inc.	Premises system management using status signal
US11210387B2 *	2018-08-16	2021-12-28	Cyberark Software Ltd.	Detecting and preventing unauthorized credential change
US11212192B2	2007-06-12	2021-12-28	Icontrol Networks, Inc.	Communication protocols in integrated systems
US11218878B2	2007-06-12	2022-01-04	Icontrol Networks, Inc.	Communication protocols in integrated systems
US11240059B2	2010-12-20	2022-02-01	Icontrol Networks, Inc.	Defining and implementing sensor triggered response rules
US11237714B2	2007-06-12	2022-02-01	Control Networks, Inc.	Control system user interface
US11244545B2	2004-03-16	2022-02-08	Icontrol Networks, Inc.	Cross-client sensor user interface in an integrated security network
US11258625B2	2008-08-11	2022-02-22	Icontrol Networks, Inc.	Mobile premises automation platform
US11277465B2	2004-03-16	2022-03-15	Icontrol Networks, Inc.	Generating risk profile using data of home monitoring and security system
US11310199B2	2004-03-16	2022-04-19	Icontrol Networks, Inc.	Premises management configuration and control
US11316753B2	2007-06-12	2022-04-26	Icontrol Networks, Inc.	Communication protocols in integrated systems
US11316958B2	2008-08-11	2022-04-26	Icontrol Networks, Inc.	Virtual device systems and methods
US11328325B2	2012-03-23	2022-05-10	Secureads, Inc.	Method and/or system for user authentication with targeted electronic advertising content through personal communication devices
US11330098B1	2020-11-06	2022-05-10	Sevis Systems, Llc	System and method for enabling trusted caller identity and spoofed call prevention
US11343380B2	2004-03-16	2022-05-24	Icontrol Networks, Inc.	Premises system automation
US11368327B2	2008-08-11	2022-06-21	Icontrol Networks, Inc.	Integrated cloud system for premises automation
US11398147B2	2010-09-28	2022-07-26	Icontrol Networks, Inc.	Method, system and apparatus for automated reporting of account and sensor zone information to a central station
US11405463B2	2014-03-03	2022-08-02	Icontrol Networks, Inc.	Media content management
US11424980B2	2005-03-16	2022-08-23	Icontrol Networks, Inc.	Forming a security network including integrated security system components

US11423756B2	2007-06-12	2022-08-23	Icontrol Networks, Inc.	Communication protocols in integrated systems
US11451409B2	2005-03-16	2022-09-20	Icontrol Networks, Inc.	Security network integrating security system and network devices
US11489812B2	2004-03-16	2022-11-01	Icontrol Networks, Inc.	Forming a security network including integrated security system components and network devices
US11496568B2	2005-03-16	2022-11-08	Icontrol Networks, Inc.	Security system with networked touchscreen
US11582065B2	2007-06-12	2023-02-14	Icontrol Networks, Inc.	Systems and methods for device communication
US11601810B2	2007-06-12	2023-03-07	Icontrol Networks, Inc.	Communication protocols in integrated systems
US11615697B2	2005-03-16	2023-03-28	Icontrol Networks, Inc.	Premise management systems and methods
US11632308B2	2022-04-22	2023-04-18	Icontrol Networks, Inc.	Communication protocols in integrated systems
Family To Family Citations				
US20060059344A1	2004-09-10	2006-03-16	Nokia Corporation	Service authentication
US7949114B2 *	2005-03-15	2011-05-24	Avaya Inc.	Granting privileges to a telecommunications terminal based on the relationship of a first signal to a second signal
EP1739588A1 *	2005-06-30	2007-01-03	Exo System Italia SRL	Method and system for registration and user identification of web users
EP2536096A1 *	2011-06-17	2012-12-19	ABB Research Ltd.	Securing an industrial control system
JP5759305B2 *	2011-08-19	2015-08-05	キヤノン株式会社	Access management system, access management method, access management server, linkage server, and program
WO2013044307A1 *	2011-09-30	2013-04-04	Cocoon Data Holdings Limited	A system and method for distributing secured data
CN103581105B *	2012-07-18	2017-09-22	财付通支付科技有限公司	Login validation method and login authentication system
EP2991014A1 *	2014-08-25	2016-03-02	Oberthur Technologies	Distributing tokens for token-based transactions

* Cited by examiner, † Cited by third party, ‡ Family to family citation

Similar Documents

Publication	Publication Date	Title
US6993658B1	2006-01-31	Use of personal communication devices for user authentication
US6161185A	2000-12-12	Personal authentication system and method for multiple computer platform
US7555655B2	2009-06-30	Apparatus, system, and method for generating and authenticating a computer password
US8196193B2	2012-06-05	Method for retrofitting password enabled computer software with a redirection user authentication method
US7707626B2	2010-04-27	Authentication management platform for managed security service providers
US8955076B1	2015-02-10	Controlling access to a protected resource using multiple user devices
JP4384117B2	2009-12-16	Data processing system user authentication method and system
US7512967B2	2009-03-31	User authentication in a conversion system
ES2517865T3	2014-11-04	Methods, devices and software to use a token to calculate time-limited password on cell phone
US20070250914A1	2007-10-25	Method and system for resetting secure passwords
JPH10341224A	1998-12-22	Authentication method in data transmission system and system to execute the authentication method
US20020169988A1	2002-11-14	Method and apparatus for providing user authentication using a back channel
US20060288230A1	2006-12-21	One time password integration with Kerberos
US20030061520A1	2003-03-27	Method and system to securely change a password in a distributed computing system
US20050021975A1	2005-01-27	Proxy based adaptive two factor authentication having automated enrollment
NZ541711A	2006-10-27	Human factors authentication using abstract definitions of viewable or audible objects
EP1107089A1	2001-06-13	Strong authentication method using a telecommunications device
JPH1066158A	1998-03-06	Security with respect to access control system
JP2007516512A5	2011-06-16	

KR20010041363A	2001-05-15	Method, arrangement and apparatus for authentication through a communications network
EP1878161A1	2008-01-16	Method and system for electronic reauthentication of a communication party
GB2379040A	2003-02-26	Controlling user access to a remote service by sending a one-time password to a portable device after normal login
KR101537097B1	2015-07-15	Otp certification method using the sms and system thereof
US6711610B1	2004-03-23	System and method for establishing secure internet communication between a remote computer and a host computer via an intermediate internet computer
JPH11187016A	1999-07-09	Network authenticating system

Priority And Related Applications

Priority Applications (3)

Application	Priority date	Filing date	Title
US09/519,829	2000-03-06	2000-03-06	Use of personal communication devices for user authentication
AU2001245448A	2000-03-06	2001-03-06	Use of personal communication devices for user authentication
PCT/US2001/007058	2000-03-06	2001-03-06	Use of personal communication devices for user authentication

Applications Claiming Priority (1)

Application	Filing date	Title
US09/519,829	2000-03-06	Use of personal communication devices for user authentication

Legal Events

Date	Code	Title	Description
2000-06-19	AS	Assignment	**Owner name**: APRIL SYSTEM DESIGN AB, SWEDEN **Free format text**: ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNORS:ENGBERG, STEN-OLOV;JONSSON, AKE;REEL/FRAME:010912/0873 **Effective date**: 20000511
2006-01-11	STCF	Information on status: patent grant	**Free format text**: PATENTED CASE
2007-04-03	CC	Certificate of correction	
2009-04-06	FPAY	Fee payment	**Year of fee payment**: 4
2011-11-14	AS	Assignment	**Owner name**: DYNAPASS INC., CALIFORNIA **Free format text**: ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:APRIL SYSTEM DESIGN AB;REEL/FRAME:027223/0817 **Effective date**: 20111107
2013-09-13	REMI	Maintenance fee reminder mailed	
2013-09-25	FPAY	Fee payment	**Year of fee payment**: 8
2013-09-25	SULP	Surcharge for late payment	**Year of fee payment**: 7
2014-02-21	AS	Assignment	**Owner name**: DYNAPASS, INC., CALIFORNIA **Free format text**: CHANGE OF ADDRESS;ASSIGNOR:DYNAPASS, INC.;REEL/FRAME:032322/0510 **Effective date**: 20140221
2017-09-11	FEPP	Fee payment procedure	**Free format text**: MAINTENANCE FEE REMINDER MAILED (ORIGINAL EVENT CODE: REM.)

2018-02-05	PRDP	Patent reinstated due to the acceptance of a late maintenance fee	**Effective date**: 20180206
2018-02-06	FEPP	Fee payment procedure	**Free format text**: SURCHARGE, PETITION TO ACCEPT PYMT AFTER EXP, UNINTENTIONAL. (ORIGINAL EVENT CODE: M2558); ENTITY STATUS OF PATENT OWNER: SMALL ENTITY **Free format text**: PETITION RELATED TO MAINTENANCE FEES GRANTED (ORIGINAL EVENT CODE: PMFG) **Free format text**: PETITION RELATED TO MAINTENANCE FEES FILED (ORIGINAL EVENT CODE: PMFP)
2018-02-06	MAFP	Maintenance fee payment	**Free format text**: PAYMENT OF MAINTENANCE FEE, 12TH YR, SMALL ENTITY (ORIGINAL EVENT CODE: M2553) **Year of fee payment**: 12
2022-01-02	AS	Assignment	**Owner name**: DYNAPASS IP HOLDINGS LLC, DELAWARE **Free format text**: ASSIGNMENT OF ASSIGNORS INTEREST;ASSIGNOR:DYNAPASS, INC.;REEL/FRAME:058521/0700 **Effective date**: 20211112
2023-02-21	IPR	Aia trial proceeding filed before the patent and appeal board: inter partes review	**Free format text**: TRIAL NO: IPR2023-00425 **Opponent name**: UNIFIED PATENTS, LLC **Effective date**: 20230106 **Free format text**: TRIAL NO: IPR2023-00367 **Opponent name**: BANK OF AMERICA CORPORATION, BANK OF AMERICA, N.A., BOKF, N.A., OKTA, INC., TRUIST BANK, TRUIST FINANCIAL CORP., WELLS FARGO BANK, N.A., WELLS FARGO COMPANY, PNC BANK, N.A.,4 AND THE PNC FINANCIAL SERVICES GROUP, INC. **Effective date**: 20230103

Data provided by IFI CLAIMS Patent Services