



- (51) International Patent Classification:
G06F 21/45 (2013.01)
- (21) International Application Number:
PCT/CN2012/079397
- (22) International Filing Date:
31 July 2012 (31.07.2012)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US):
GOOGLE INC. [US/US]; 1600 Amphitheatre Parkway,
Mountain View, California 94043 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **Dong, Xiaohu**
[CN/CN]; Jilijiayuan 3#1010, Shaoyaoju, Chaoyang Dis-
trict, Beijing 100029 (CN). **Zhang, Chi** [CN/CN]; Xi
Wang Zhuang 13-4-202, Haidian District, Beijing 100083
(CN). **Fang, Kun** [CN/CN]; Room 608, Building 1, Shui
Qing Mu Hua Yuan, Haidian District, Beijing 100084
(CN).
- (74) Agent: **KING & WOOD MALLESONS**; 20th Floor, East
Tower, World Financial Centre, No. 1 Dongsanhuan Zhon-
glu, Chaoyang District, Beijing 100020 (CN).
- (81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.
- (84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ,
TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK,
EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: AUTOMATING PASSWORD MAINTENANCE

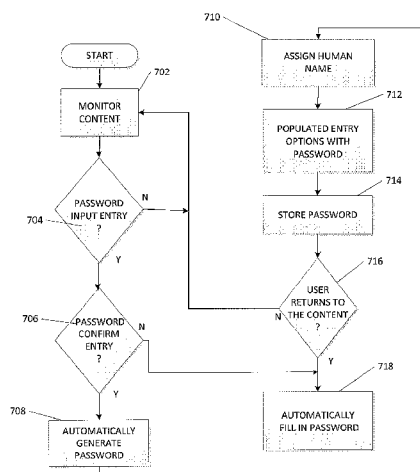


Figure 7

(57) Abstract: Techniques for proving improved convenience and security in managing passwords are described. Content such as for example secure websites that include password input entry and password confirm entry options are detected. In response to detecting the entry options, a strong and unique password is automatically generated. A human friendly identifier is assigned to the automatically generated password. The password input entry and password confirm entry are automatically populated with the automatically generated password. The automatically generated password and the human friendly identifier are stored in a central server that has proper access control. When the user returns to the content that includes a password entry option, the password input entry option is automatically populated with the automatically generated password. This Abstract is submitted with the understanding that it will not be used to interpret or limit the scope or meaning of the claims.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Published:**
ML, MR, NE, SN, TD, TG).

— *with international search report (Art. 21(3))*

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

AUTOMATING PASSWORD MAINTENANCE

BACKGROUND

[0001] Much electronic content is secure, and requires a sign in from authorized users to gain access. This sign in typically includes use of a password. A password is a secret word or string of characters used for authentication, to prove identity or to gain access to a resource; however, the easier a password is for the owner to remember, the easier it is for hackers to guess. Counterintuitively, complex passwords that are difficult to remember also can reduce the security of a system because users often write down or electronically store the password. In addition, users often share passwords among multiple websites, again reducing security. *See, for example*, J. Yan, A. Blackwell, R. Anderson and A. Grant, "Password Memorability and Security: Empirical Results", IEEE Security & Privacy, Vol. 2 No. 5 (2004).

SUMMARY

[0002] Described herein are techniques for providing improved convenience and security in managing passwords. Automated password maintenance is provided. Content such as for example secure websites or secure applications that include password input entry and password confirm entry options are detected. In response to detecting the password input entry and the password confirm entry, and without user input, a strong and unique password is automatically generated. A human friendly identifier is assigned to the automatically generated password. The password input entry and password confirm entry are automatically populated with the automatically generated password. The automatically generated password and the human friendly identifier are stored in a central server that has proper access control. When the user returns to the content that includes a password

entry option, without user input the password input entry option is automatically populated with the automatically generated password.

[0003] This Summary introduces concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is this Summary intended to be used as an aid in determining the scope of the claimed subject matter. The term 'techniques', for instance, refers to device(s), system(s), method(s) and/or computer-readable instructions as permitted by the context above and throughout the document.

BRIEF DESCRIPTION OF THE FIGURES

[0004] The detailed description refers to the following accompanying drawings:

[0005] Figure 1 displays a high-level block diagram of example computer architecture in which techniques for password maintenance in accordance with one or more implementations described herein can be employed.

[0006] Figure 2 displays a high-level block diagram of example client-server architecture in which techniques for password maintenance in accordance with one or more implementations described herein can be employed.

[0007] Figure 3 displays a high-level block diagram of example client application architecture in which techniques for password maintenance in accordance with one or more implementations described herein can be employed.

[0008] Figure 4 displays a screen shot of an example GUI in which techniques for password maintenance in accordance with one or more implementations described herein can be employed.

[0009] Figure 5 displays a screen shot of an example GUI in techniques for password maintenance in accordance with one or more implementations described herein can be employed.

[0010] Figure 6 displays a screen shot of an example GUI for in which techniques for password maintenance in accordance with one or more implementations described herein can be employed.

[0011] Figure 7 displays a flow chart of an example process which techniques for password maintenance in accordance with one or more implementations described herein can be employed.

DETAILED DESCRIPTION

Overview

[0012] Passwords are readily incorporated in most software, require no extensive computer/server modifications, and are very familiar to users. While passwords can be secure, however, a weakness arises in how users choose and manage passwords. For example, a frequent recommendation is that passwords contain not less than eight characters. A further recommended is that a password contain a mix of four different types of characters – upper case letters, lower case letters, numbers, and special characters such as !@#%&*.

[0013] In addition, a password should not be a name, a slang word or any word in the dictionary. A password should not include any part of the user's name, address or e-mail address. A different password should be used for each website – even for websites where privacy is not an issue.

[0014] These recommendations, however, are seldom followed. Because of complexity, maintaining passwords is a burden for users and can cause security problems.

Among various issues in password maintenance, users select weak passwords, record their passwords in unsecure locations, and share password among multiple websites. An added problem is that most users do more than one of these mistakes. This makes it easy for hackers, crackers, malware, and cyber thieves to break into individual accounts, small and medium businesses, multi-international corporations, government agencies, institutions, and the like. It is protecting against vulnerabilities such as these that makes improving password management important.

[0015] Software exists that helps a user organize passwords. The software typically has a local database or a file that holds the user selected password for logon onto computers, networks, websites, and application data files. Password managers can also work as a form filler. These fill the user selected password automatically into forms.

[0016] Described herein are techniques for improved convenience and security in managing passwords. Automated password maintenance is provided. Content such as for example secure websites or secure applications that include password input entry and password confirm entry options are detected. In response to detecting the password input entry and the password confirm entry, and without user input, a strong and unique password is automatically generated. A human friendly identifier is assigned to the automatically generated password.

[0017] The password input entry and password confirm entry are automatically populated with the automatically generated password. The automatically generated password and the human friendly identifier are stored in a central server that has proper access control. When the user returns to the content that includes a password entry option, without user input the password input entry option is automatically populated with the automatically generated password. By utilizing the techniques for improved convenience

and security in managing passwords described herein, passwords can be pre-fetched, for example, when the user is still typing or selecting website address, reducing user perceptible latency.

[0018] This brief overview, as well as section titles and corresponding summaries, are provided for the reader's convenience and are not intended to limit the scope of the claims or the proceeding sections.

The Internet

[0019] The Internet connects a global network of computers. Network servers support hypertext capabilities that permit the Internet to link together websites. Hypertext is text displayed on a computer or other electronic devices with references (for example, hyperlinks) to other text. Users navigate the Internet through graphical user interfaces (GUI). Uniform-resource locators (URLs) identify specific websites and web pages. URLs also identify the address of the website to be retrieved from a network server. The transfer control protocol / internet protocol (TCP/IP) transfers information.

[0020] The World-Wide Web (the WWW or the Web) allows material from any computer, from any format to be translated into a common language of words, images, and addresses. The Internet typically uses a hypertext language referred to as the hypertext mark-up language (HTML). HTML permits content providers to place hyperlinks within web pages. These hyperlinks link related content or data, which may be found on multiple Internet-host computers. HTML document links retrieve remote data by use of hypertext transfer protocol (HTTP). When a user clicks on a link in a web document, the link icon in the document contains the URL that the client application employs to initiate the session with the server storing the linked document. HTTP is a protocol used to support the information transfer.

[0021] A uniform resource identifier (URI) is a string of characters used to identify a name or a resource. Such identification enables interaction with representations of the resource over a network (WWW) using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI.

Password Management

[0022] As previously introduced, electronic content on the Internet often is secure, and requires a sign in from authorized users to gain access. Prior attempts have been made to manage passwords. For example, OpenID provides for users to be authenticated in a decentralized manner, allowing users to consolidate their digital identities. OpenID is an open standard administered by the OpenID Foundation, 2400 Camino Ramon, Suite 375, San Ramon, California 94583 USA. Users may create accounts with their preferred OpenID identity providers, and use those accounts as the basis for signing on to websites that accept OpenID authentication. The OpenID standard provides a framework for the communication that must take place between the identity provider and the OpenID acceptor (the 'relying party').

[0023] OpenID enables an end user – the entity that wants to assert a particular identity – to communicate with a relying party (RP), the website that wants to verify the identifier of the end user. This communication occurs through the exchange of an identifier or OpenID, which is the URL chosen by the end user to name the end user's identity. An identity provider or OpenID provider is a service that specializes in registering OpenID URLs. The OpenID provider provides the OpenID authentication. The exchange is enabled by a user agent, which is the program used by the end user to communicate with the relying party and OpenID provider.

[0024] However, many websites do not support OpenID. In addition, some have suggested that OpenID has security weaknesses and may prove vulnerable to phishing attacks. Other security issues identified with OpenID involve lack of privacy and failure to address the trust problem. Vulnerability is present in the redirect URL from the identity provider to the relying party. Hackers who obtain this URL (for example, by sniffing the wire) can replay the URL and log into the website as the victim user. In addition, the OpenID authentication procedure is strictly sequential, thus preventing prefetching or other optimization techniques, resulting in long latency.

[0025] Another example is Windows Live ID™ available from Microsoft Corporation, One Microsoft Way, Redmond, Washington 98025. Windows Live ID is a single sign-on web service that allows users to log in to many websites using one account. Users are allowed to sign in to websites that support Windows Live ID using a single set of credentials. Users' credentials are checked by a Microsoft account authentication server.

[0026] A new user signing into a Microsoft account-enabled website is first redirected to the nearest authentication server, which asks for username and password over a secure-sockets layer (SSL) connection. A user may select to have a computer remember the user's login. A newly signed-in user has an encrypted, time-limited cookie stored on the computer and receives a triple data encryption standard (DES) encrypted ID-tag previously agreed upon between the authentication server and the Microsoft account-enabled website. This ID-tag is sent to the website, upon which the website plants another encrypted HTTP cookie in the computer, also time-limited. As long as these cookies are valid, the user is not required to supply a username and password. If the user actively logs out of their Microsoft account, the cookies will be removed.

[0027] Again, many websites do not support Windows Live ID. In addition, some have suggested that Windows Live ID has security weaknesses. Other security issues identified with Windows Live ID involve lack of privacy and failure to address the trust problem. In addition, Windows Live ID authentication procedure is strictly sequential, thus preventing prefetching or other optimization techniques, resulting in long latency.

System Architecture

[0028] Figure 1 displays a high-level block diagram of example system architecture in which the password maintenance techniques described herein can be employed. The computer system 100 can include, in addition to hardware, computer-executable instructions stored in memory 104. A bus couples the memory 104 for storing information and instructions executable by processor 102. Special purpose logic circuitry can supplement or incorporate the processor 102 and the memory 104.

[0029] The instructions may be stored in the memory 104 and implemented in one or more computer program products. Computer program products can be one or more modules of computer program instructions encoded on a computer readable medium for execution by, or to control the operation of, the computer system 100. Memory 104 may store temporary variable or other intermediate information during execution of instructions executable by the processor 102.

[0030] The computer system 100 further includes data storage 106 coupled to bus 108. The data storage 106 stores information and instructions. An input/output module 110 may couple computer system 100 to various devices. The input/output module 110 can be any input/output module. Examples of input/output modules 110 include data ports such as universal serial bus (USB) ports. The input/output module 110 is configured to connect to a

communications module 112. Examples of communications modules 112 include networking interface cards, such as Ethernet cards and modems.

[0031] The input/output module 110 is configured to connect to a number of devices, such as an input 114 and/or an output 116. Examples of input devices 114 include a keyboard and a pointing device such as, for example, a mouse, by which a user can provide input to the computer system 100. Examples of output devices 116 include display devices such as, for example, a liquid crystal display (LCD) monitor for displaying information to the user.

[0032] According to one aspect, the techniques can be implemented using a computer system 100 in response to processor 102 executing one or more sequences of one or more instructions contained in memory 104. Another machine-readable medium, such as data storage 106, may read such instructions into memory 104. Execution of the sequences of instructions contained in memory 104 causes processor 102 to perform the process steps described herein.

[0033] Figure 2 illustrates a schematic of an example infrastructure of a client-server network 200, according to some implementations of the password maintenance techniques described herein. The network 200 includes a number of clients 202a, 202b, 202c and a server 220. The client 202 includes an application 204, a client assistant 206, and a client cache 208. The client-side application 204 is used to support the serving of content to the client device.

[0034] The client assistant 206 may establish communication channels with the client application 204, the client cache 208, and a remote cache server 224 residing in the server 220. The client assistant 206 and the remote cache server 224 facilitate the process of responding to a content request initiated by a user of the client 202. In some

implementations, cache assistant 206 may be located on a computer remote from client 202, for example, a client-side proxy server (not shown).

[0035] In some implementations, the client application 204 does not have an associated cache, but instead directs user requests to the client assistant 206. While the following discussion assumes, for ease of explanation, that the client application 204 is a web browser, the application can be any application that uses contents whose source is a network address such as, for example, a URL, whether the resource is located somewhere in the network or on the client 202.

[0036] An advantage of the implementation shown in Figure 2 is that the web browsers or other applications in the client 202 can share the same client cache 208 and thereby avoid data duplication. But in alternative implementations, the web browser 204 may use its own cache (not shown). In such implementation, the client assistant 206 keeps the application cache 204 in sync with the client cache 208.

[0037] The server 220 includes at least a server cache 222. In some implementations, the server 220 and/or the server cache 222 are deployed over multiple computers in order to provide fast access to a large number of cached contents. For convenience of explanation, the server 220 will be referenced herein as though it were a single computer.

[0038] The server 220, through its server cache 222, manages a large number of content that have been downloaded from various web hosts 234 (for example, web servers and other hosts) over the network 232. In some implementations, the server 220 also includes a cookie cache 225, a domain name system (DNS) cache 226, and a DNS master 230. In alternative implementations, server 220 does not include the DNS cache and DNS master. In some implementations, these various components co-exist in a single computer; in some other implementations, these various components are distributed over multiple computers.

[0039] The remote cache server 224 communicates with other components in the server 220 over an intranet (not shown), and communicates with web hosts 234a, 234b and domain name servers (DNS) 236a, 236b over a network 232 such as the Internet. The DNS servers 236 contain the hierarchical distributed naming system for computers, services or any resource connected to the Internet. The server 220 also includes a password manager 228 described in detail, below.

[0040] Figure 3 displays a high-level block diagram of example client application architecture 204 in which techniques for password maintenance described herein can be employed. The client 204 includes a browser 301, a browser plug-in 303, a browser toolbar plug-in 305, etc. The browser 301 retrieves, presents, and traverses information resources on the WWW. An information resource is identified by a URI and may be a web page, image, video or other piece of content. The browser plug-in 303 adds the ability of the browser to play video, scan for viruses, display new file types, and the like. The browser toolbar plug-in 305 is a graphical user interface widget on which on-screen buttons, icons, menus, or other input or output elements are placed. The browser 301 works with a password manager 228 in the server 220 in enabling the techniques for automating password maintenance.

Cloud-Based Password Maintenance

[0041] As previously introduced, techniques for improved convenience and security in managing passwords are described. Automated password maintenance is provided. Content such as for example secure websites or secure applications that include password input entry and password confirm entry options are detected.

[0042] A strong and unique password is automatically generated. In one implementation, the strong and unique password contains at least eight characters. In a further implementation, the strong and unique password contains at least one of upper case

letters, lower case letters, numbers, and special characters such as !@#%&*. In a further implementation, the strong and unique password is checked to ensure it does not contain a name, a slang word, any word in the dictionary, and any part of the user's name, address or e-mail address. A different password is generated for each website – even for websites where privacy is not an issue.

[0043] The password input entry and password confirm entry are automatically populated with the automatically generated password. Once the sign-up succeeds, the automatically generated password is stored under a human friendly identifier. In one implementation, the human friendly identifier is readable to a human, and conveys information about the user and the website. In a further implementation, the human friendly identifier contains the application name and user account name, for example, "Password for Alice@Secureapp".

[0044] The automatically generated password and the human friendly identifier are stored in a central server that has proper access control. In some implementations, access control can include authentication, authorization, and audit of the central server. Access control also can include measures such as physical devices, including biometric scans and metal locks, hidden paths, digital signatures, encryption, social barriers, and monitoring by humans and automated systems.

[0045] By storing the automatically generated password and the human friendly identifier in a central server, what is meant is that the automatically generated password and the human friendly identifier are not stored locally to the user in, for example, a user device. Rather, the automatically generated password and the human friendly identifier are stored in the cloud: end users access the automatically generated password and the human

friendly identifier through a web browser, with the automatically generated password and the human friendly identifier stored on servers at a remote location.

[0046] When the user returns to a website where the content includes a password entry option, the password input entry option is automatically populated with the automatically generated password. By utilizing techniques for improved convenience and security in managing passwords described herein, instead of maintaining multiple passwords for multiple websites, users only need to maintain a human friendly identifier.

[0047] In various implementations, the techniques for improved convenience and security in managing passwords can be implemented as a password manager, browser, browser plugin, application, and even an integrated part of operation system. Server 220 stores the passwords, which can only be accessed with proper credential. The server 220 can be any content provider that provides such service. In practice, a user should choose a trustworthy content provider and make sure the access control is secure.

[0048] In one implementation, the password manager 228 is enabled with techniques for automating password maintenance. The browser 301 properly authenticates itself with the server 220. The browser 301 opens a sign-up page for a website. Referring to Figure 4, a screen shot of an example sign-up page 401 for a secure website is seen. The sign-up page includes a 'User Name' entry box 403, a 'Chose a Password' entry box 405, and a 'Confirm Password' entry box 407. The password manager 228, via the browser 301, detects the password input entry box 405 and password confirm entry box 407. The password manager 228, via the browser 301, presents an option to automatically generate a password, for example via a button 409 in a pop-up window 411 stating 'Generate Password' along the two entries.

[0049] When the option to automatically generate a password is chosen, for example by clicking the 'Generate Password' button 409, the 'Chose a Password' entry box 405 and the 'Confirm Password' entry box 407 are filled with an automatically generated, secure password. Once the sign-up succeeds, the server 220 stores the account identifier and automatically generated password. The account name and automatically generated password are stored under the human friendly identifier, which contains the website name and user account name, for example, 'Password for Bob at securewebsite.com'.

[0050] Referring to Figure 5, a screen shot on an example login page 501 for a secure website is seen. When the browser opens the login page, the website, a 'User Name' entry box 503, and a 'Password' entry box 505 are detected.

[0051] The browser retrieves the account name and automatically generated password for the website from the server 220. The browser automatically fills the account name into the 'User Name' entry box 503. The browser also automatically fills automatically generated password into the 'Password' entry box 505.

[0052] If there is more than one candidate, the password manager 228 provides an easy way for user to choose. The password manager 228 provides to the user the candidate password in the form of the human friendly identifier. Since the human friendly identifier is readable to a human, and conveys information about the user and the website (for example, containing the application name and user account name), the user should be able to choose easily the right candidate.

[0053] In another implementation, a mobile operation system is enabled with techniques for automating password maintenance. The mobile operation system authenticates itself with the server 220. The mobile operating system opens a sign-up page for an application. Referring to Figure 6, an example mobile client 601 showing a screen shot

of an example sign-up page is seen. The mobile client 601 includes a display screen 602 and a keypad 604. The sign-up page is displayed on the display screen 602. The sign-in page includes a 'User Name' entry box 603, a 'Chose a Password' entry box 605, and a 'Confirm Password' entry box 607.

[0054] The mobile client 601 detects the password input entry 605 and password confirm entry 607. An option to generate automatically a secured password, for example by adding a menu item in the context menu 609 of these entries, which says 'Generate Password' 611, is generated. When the option to automatically generate a password is selected, for example by using the keypad 604 to choose the menu item in the context menu 609 which says 'Generate Password' 611, the 'Chose a Password' entry box 605 and the 'Confirm Password' entry box 607 are filled with the secure, automatically generated password. Once the sign-up succeeds, the mobile operating system asks the server to store the automatically generated password under the human friendly identifier, which contains the application name, and user account name.

[0055] When the application prompts a user to sign in, the mobile operating system retrieves the account name and password and fills them in automatically. Given inputting special characters are difficult on mobile devices, this actually removes the cumbersome requirement of inputting password on mobile devices.

[0056] The account name and password can be encrypted by a publicly trusted third party. This way, the sensitive account information of the user, including the usernames/passwords, is kept secure and private – only known to the user itself, not to any other parties.

[0057] Referring to Figure 7, a flow chart of an example process which techniques for password maintenance described herein can be employed is seen. Other

implementations perform the steps of Figure 7 in different orders. In addition, other implementations include different and/or additional steps than the steps described herein. Content is monitored (702). If content that includes password input entry is detected (704), then it is determined if the content includes a password confirm entry option (706); if content that includes password input entry is not detected, then content continues to be monitored.

[0058] If the content includes a password confirm entry option, then a secure password is automatically generated (708). A human friendly identifier is assigned to the generated password (710). The password input entry and password confirm entry options are automatically populated with the password (712). The password is stored in a central server that has access control (714). If the user returns to the content (716), then the password input entry option is automatically populated with the automatically generated password (718).

[0059] Thus, the described techniques for improved convenience and security in managing passwords address the issues of users selecting weak passwords and users share password among multiple websites. In addition, the described techniques for managing passwords address the inconvenience of inputting password in mobile device. Still further, by utilizing the techniques for improved convenience and security in managing passwords described herein, passwords can be pre-fetched, for example, when the user is still typing or selecting website address, reducing user perceptible latency.

Concluding Notes

[0060] The implementation described herein is not inherently related to any particular hardware or other apparatus. The operations of the techniques for password

maintenance can be controlled through either hardware or through computer programs installed in computer storage and executed by the processors of servers.

[0061] When embodied as hardware, the hardware may be specially constructed for the required purposes or the hardware may include a general-purpose computer selectively activated or reconfigured by a computer program stored on a computer-readable medium. In addition, the implementation described herein is not limited to any particular programming language.

[0062] The password maintenance techniques may be implemented using a single computer or a network of computers, including cloud-based computing. The computers can be server-class computers including one or more high-performance central processing units (CPUs), memory such as, for example, one gigabyte (1GB) or more of main memory, as well as 500GB to two terabyte (2TB) of computer-readable persistent storage, network interface, peripheral interfaces, and other well-known components.

[0063] The computers can run an operating system. Examples include the LINUX® computer-operating system or variants thereof and the like. LINUX® computer-operating system is an open-source operating system that is available under a general-public license administered by The Linux Foundation, 1796 18th Street, Suite C, San Francisco, California 94107. Of course, other types of operating system and computers can be used, and it is expected that more powerful computers developed in the future can be configured in accordance with the teachings herein.

[0064] In addition to the Internet, the network may be any network. Examples of networks include local area networks (LAN), metropolitan area networks (MAN), campus area networks (CAN), wide area networks (WAN), mobile wired or wireless networks, private networks, virtual private networks, and the like. In addition, all or some of links can

be encrypted using conventional encryption technologies. Examples include the SSL, secure http, virtual private networks (VPNS), and the like. Other implementations utilize custom and/or dedicated data communications technologies instead of, or in addition to, the communications technologies described above.

[0065] The terms client and content provider as used herein may refer to software providing client and content-providing functionality, to hardware devices on which the software executes or to the entities operating the software and/or hardware. The term 'website' represents any computer system adapted to serve content using any internetworking protocols, and is not limited to content uploaded or downloaded via the Internet or HTTP.

[0066] The term computer-readable media includes computer-storage media. Example include magnetic-storage devices such as hard disks, floppy disks, and magnetic tape; optical disks such as compact disks (CD) and digital-versatile disks (DVD); magnetic-storage devices such as digital tapes, floppy disks, and magneto-resistive-random-access memory (MRAM); non-volatile memory such as read-only memory (ROM), erasable-programmable-read-only memory (EPROMs), and electrically-erasable-programmable-read-only memory (EEPROMs); volatile memory such as random-access memory (RAM), dynamic random access memory (DRAM), ferroelectric-random-access memory (FeRAM), and static-random-access memory (SRAM); or any type of media suitable for storing electronic instructions.

[0067] Furthermore, at times arrangements of operations have been referred to by functional names, without loss of generality. The division of functionality between components, the naming of components, attributes, data structures or any other programming or structural aspect is merely exemplary, and not mandatory or significant. In

addition, other implementations may distribute the described functionality in a different manner. Functions performed by a component may instead be performed by multiple components, and functions performed by multiple components may instead performed by a single component. In general, functions described in one implementation as performing on the server side can be performed on the client side in other implementations and vice versa, if appropriate.

[0068] Although the subject matter has been described with a specific implementation, other alternatives, modifications, and variations will be apparent to those skilled in the art. Accordingly, the disclosure is intended to be illustrative, but not limiting, and all such alternatives, modifications, and variations are within the spirit and scope of the following claims.

What is claimed is:

1. One or more computing devices configured to manage passwords, the one or more computing devices comprising:

a password manager configured to:

receive, from a browser, detected content that includes a password input entry;

receive, from the browser, detected content that includes a password confirm entry;

without user input, automatically generate a password;

assign a human friendly identifier to the automatically generated password; and

send, to the browser, the automatically generated password, enabling the browser to automatically populate the password input entry and password confirm entry with the automatically generated password;

memory contained in a central server, the central server having access control, the memory configured to receive from the password manager and store the automatically generated password and the human friendly identifier; and

the password manager further configured such that, when the user returns to the content that includes the password entry option, the password manager automatically populates the password input entry option without user input with the automatically generated password.

2. The one or more computing devices of claim 1 wherein the password manager is further configured such that, after receiving detected content that

includes password input entry and password confirm entry options but prior to automatically generating a password, the password manager sends, to a browser, a request to obtain user permission to automatically generate a password.

3. The one or more computing devices of claim 1 wherein the password manager is further configured such that the human friendly identifier comprises an application name and user account name.

4. The one or more computing devices of claim 1 wherein the password manager is further configured to automatically generate a password containing at least eight characters.

5. The one or more computing devices of claim 1 wherein the password manager is further configured to automatically generate a password containing at least one selected from the group consisting of upper case letters, lower case letters, numbers, special characters, and combinations thereof.

6. The one or more computing devices of claim 1 wherein the password manager is further configured to, for a given user visiting subsequent websites, automatically generate a different password for each websites.

7. The one or more computing devices of claim 1 wherein the password manager is further configured to detect a website that includes a password input entry.

8. The one or more computing devices of claim 1 wherein, if more than one candidate password is identified, the password manager is further configured to

provides to the user the candidate passwords in the form of the human friendly identifier.

9. The one or more computing devices of claim 1 wherein the one or more computing devices is selected from the group consisting of digital assistants, personal digital assistants, cellular phones, mobile phones, smart phones, laptop computers, and combinations thereof.

10. A method implemented by one or more computing devices configured to manage passwords, the method comprising:

detecting content that includes a password input entry;

detecting content that includes a password confirm entry;

in response to detecting the password input entry and the password confirm entry, without user input automatically generating a password;

assigning a human friendly identifier to the automatically generated password;

automatically populating the password input entry and password confirm entry with the automatically generated password;

storing in a central server, the central server having access control, the automatically generated password and the human friendly identifier; and

when a user returns to the content that includes the password entry option, without user input automatically populating the password input entry with the automatically generated password.

11. The method of claim 10 further comprising, when more than one candidate password is present, providing a user with the human friendly identifier.

12. The method of claim 10 further comprising assigning a human friendly identifier comprising an application name and user account name.

13. The method of claim 10 further comprising, after detecting content that includes password input entry and password confirm entry and before automatically generating the password, providing a user an option to automatically generate a password.

14. The method of claim 10 further comprising automatically generating a password containing at least eight characters.

15. The method of claim 10 further comprising automatically generating a password containing at least one character selected from the group consisting of upper case letters, lower case letters, numbers, special characters, and combinations thereof.

16. The method of claim 10 further comprising automatically generating a password not containing a name, a slang word or any word in the dictionary.

17. The method of claim 10 further comprising automatically generating a password not containing any part of the name, address or e-mail address of a user.

18. The method of claim 10 further comprising, for a given user visiting subsequent content, automatically generating a different password for each content.

19. The method of claim 10 further comprising detecting content on a website that includes a password input entry.

20. The method of claim 10 further comprising, if more than one candidate password is identified, providing to the user the candidate passwords in the form of the human friendly identifier.

21. One or more computer-readable media storing processor-executable instructions that, when executed, cause one or more processors to perform operations that recommend related content, the operations comprising:

detecting content that includes password input entry;

detecting content that includes password confirm entry;

in response to detecting the password input entry and the password confirm entry, without user input automatically generating a password;

assigning a human friendly identifier to the automatically generated password;

automatically populating the password input entry and password confirm entry with the automatically generated password;

storing in a central server, the central server having access control, the automatically generated password and the human friendly identifier; and

when the user returns to the content that includes a password entry option, without user input automatically populating the password input entry with the automatically generated password.

22. The one or more computer-readable media storing processor-executable instructions of claim 21 further comprising, after detecting content that includes password input entry and password confirm entry and before automatically generating the password, providing a user with an option to automatically generate a password.

23. The one or more computer-readable media storing processor-executable instructions of claim 21 further comprising automatically generating a password not containing a name, a slang word or any word in the dictionary.

24. The one or more computer-readable media storing processor-executable instructions of claim 21 further comprising automatically generating a password not containing any part of the name, address or e-mail address of a user.

25. The one or more computer-readable media storing processor-executable instructions of claim 21 further comprising, if more than one candidate password is identified, providing to the user the candidate passwords in the form of the human friendly identifier.

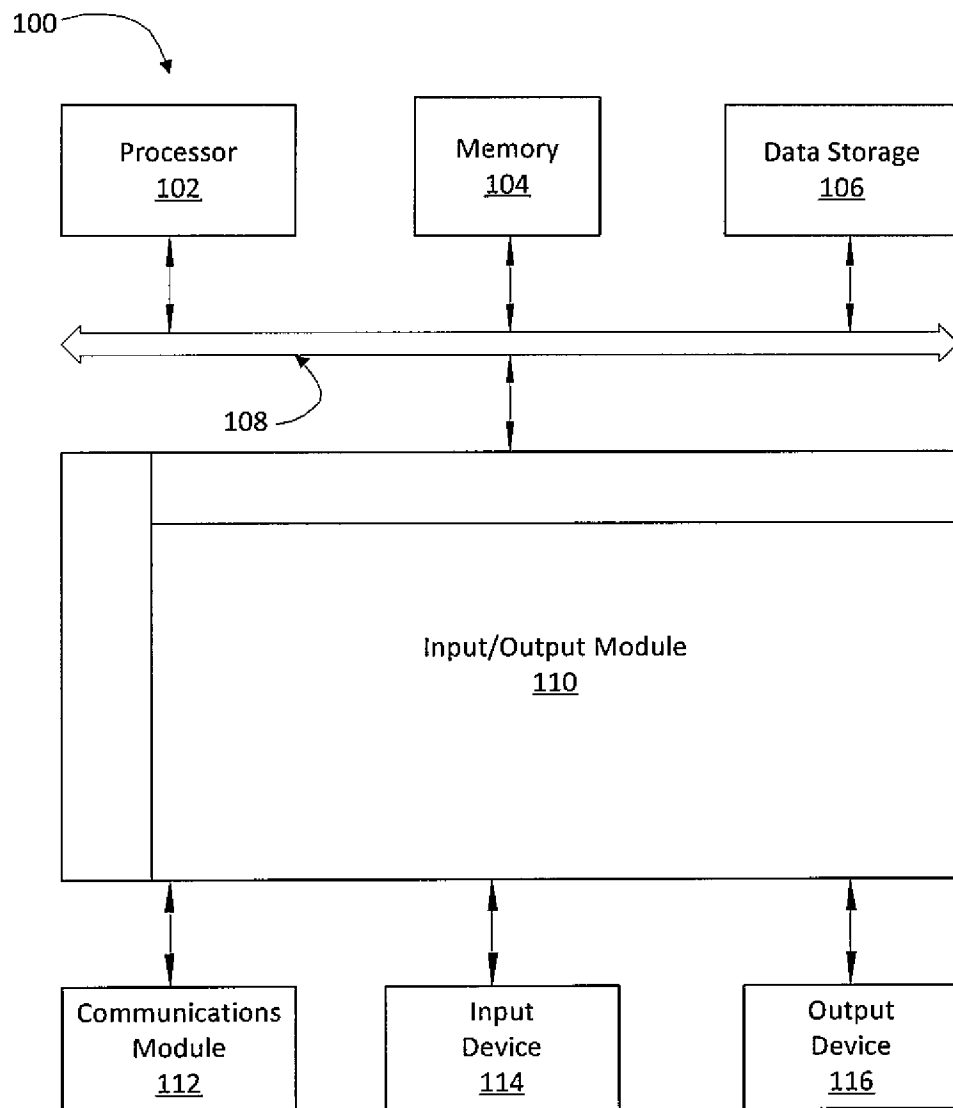


Figure 1

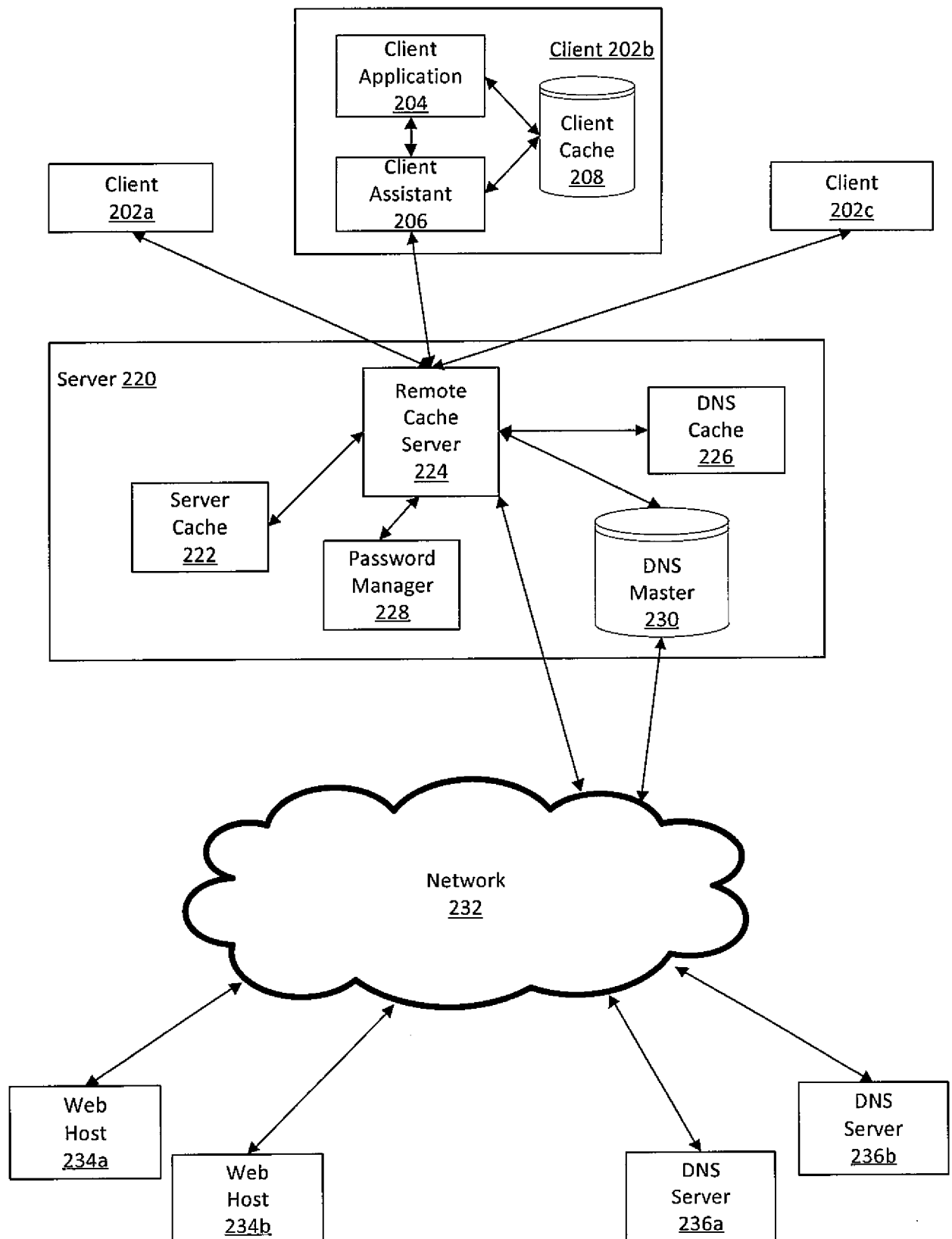


Figure 2

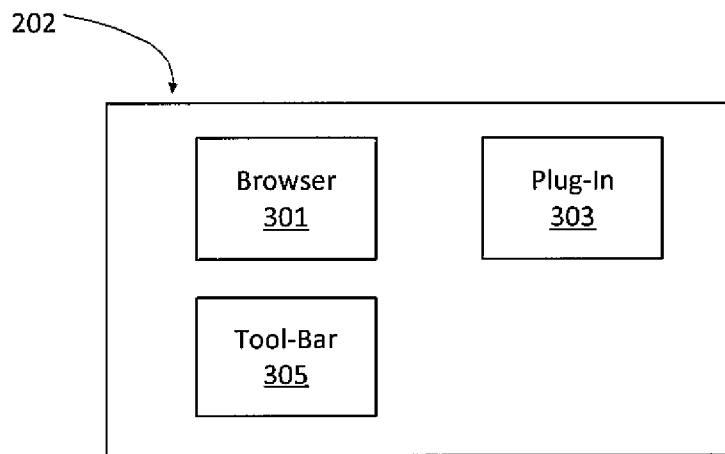


Figure 3

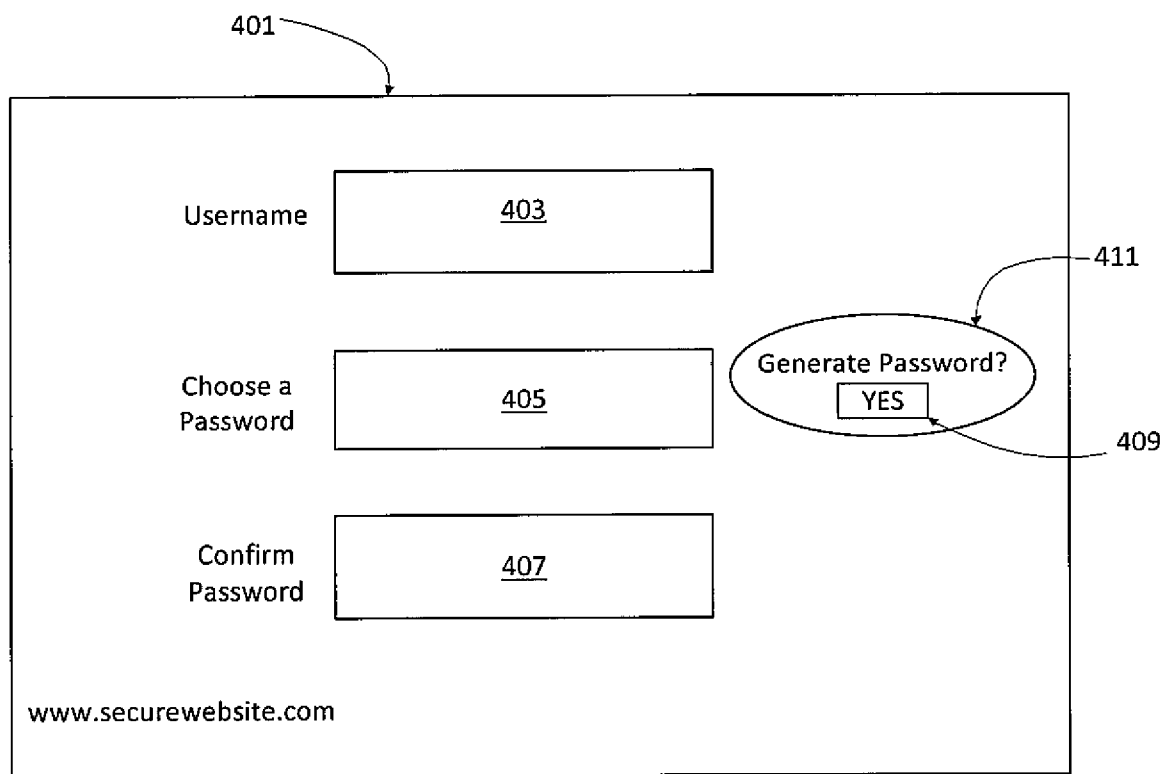


Figure 4

501

The diagram shows a login form within a rectangular frame. An arrow points from the label '501' to the top-left corner of the frame. Inside the frame, there are two input fields. The first field is preceded by the text 'Username' and contains the underlined text '503'. The second field is preceded by the text 'Password' and contains the underlined text '505'. At the bottom-left corner of the frame, the URL 'www.securewebsite.com' is displayed.

Username 503

Password 505

www.securewebsite.com

Figure 5

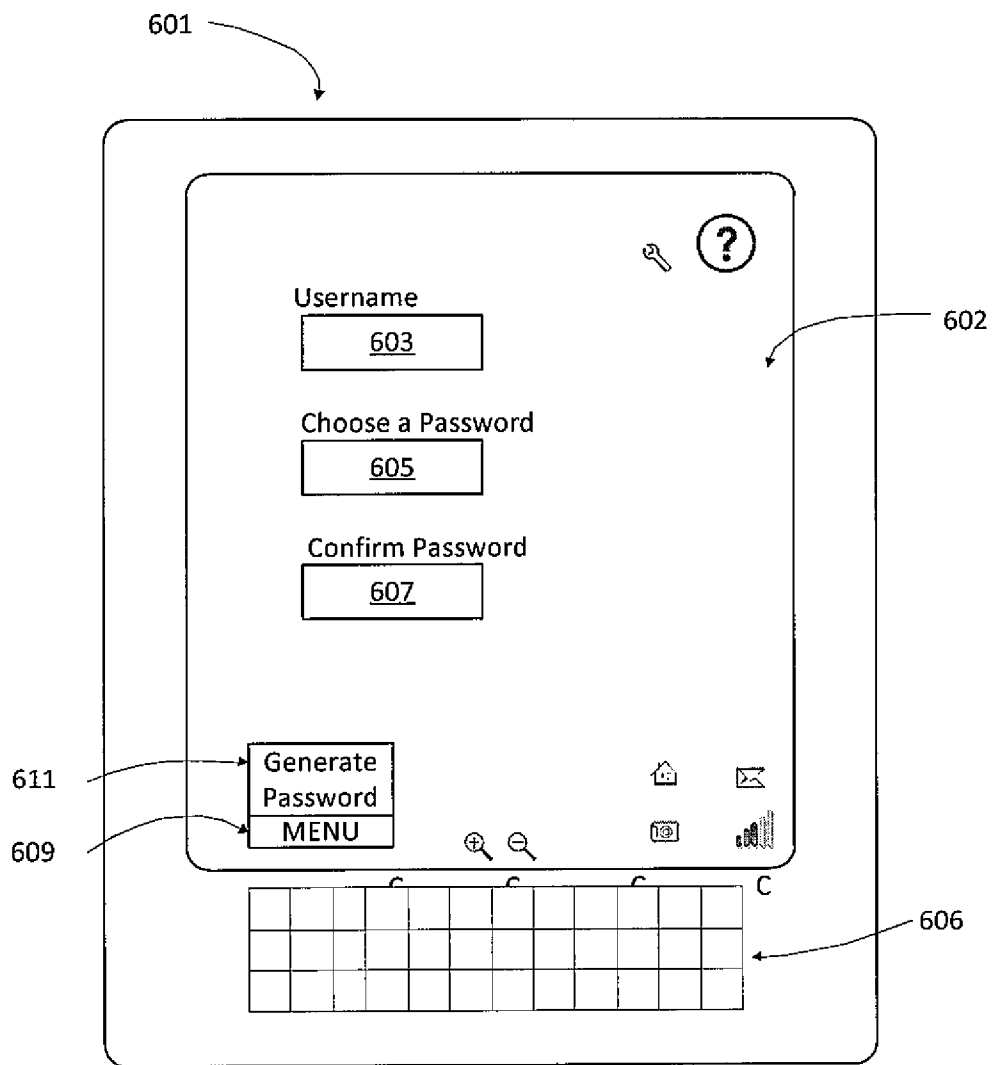


Figure 6

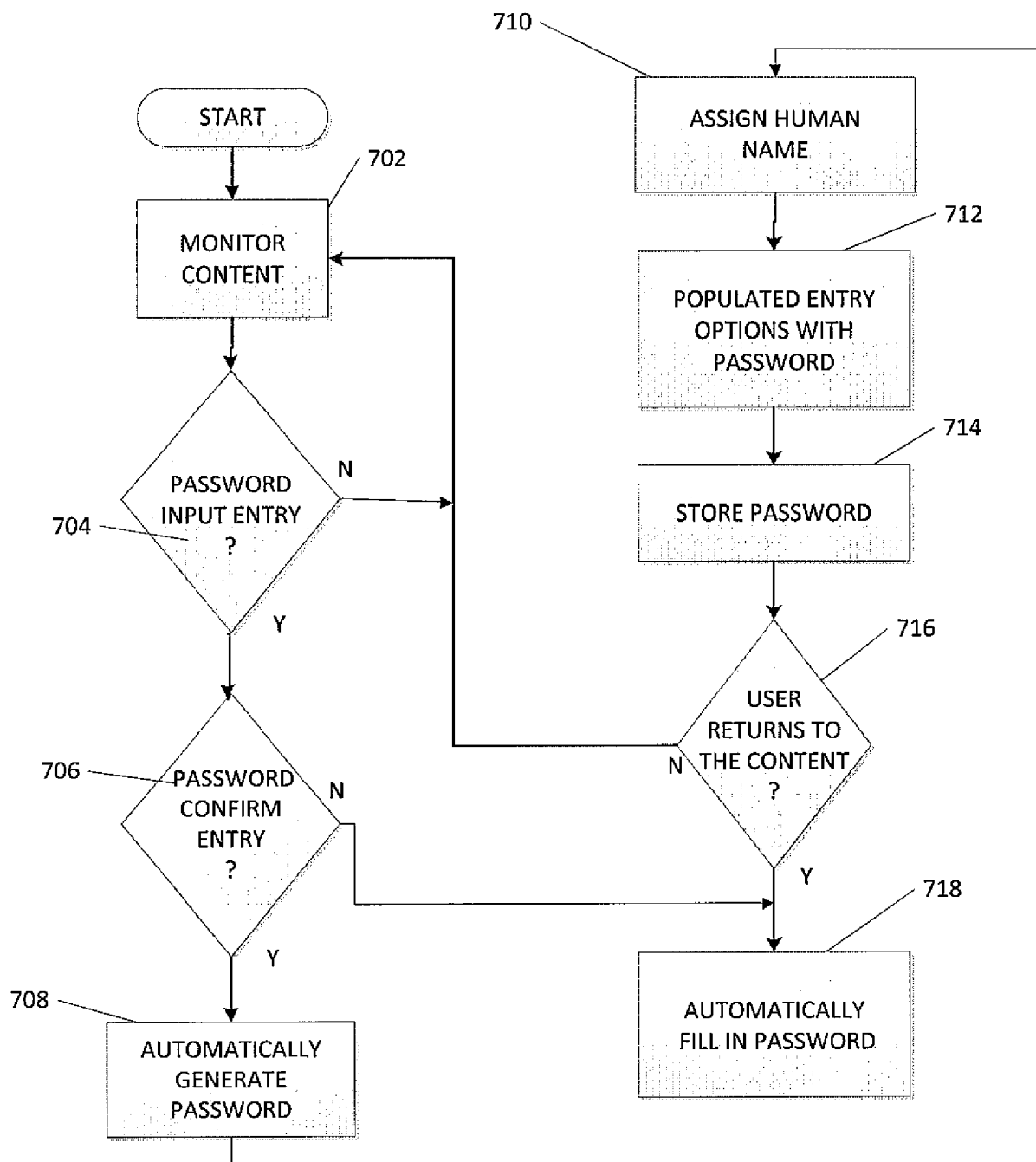


Figure 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2012/079397

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/45 (2013.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F21/-; H04L9/-; G06F3/048;

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

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

CNPAT,CNKI,WPI,EPODOC,GOOGLE: password, generate, create, populate, fill in, input entry, confirm entry, web, register, new user

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN101272237A (BEIJING FEITIAN CHENGXIN SCIENCE AND TECHNOLOGY CO., LTD.) 24 Sep.2008 (24.09.2008) see description pages 6-12	1-25
Y	GAO, Yixin. ASP Web Application Programming. Mar. 2005 (03.2005), pages 267-269, ISBN 7-115-13239-9/TP.4560	1-25
A	CN102132304A (MICROSOFT CORP.) 20 Jul.2011 (20.07.2011) see all document	1-25
A	CN1446331A (PHOENIX TECHNOLOGIES LTD.) 01 Oct.2003 (01.10.2003) see all document	1-25
A	CN1389807A (VIA ELECTRONICS INC.) 08 Jan.2003 (08.01.2003) see all document	1-25
A	US2010/0333195A1 (HONG FU JIN PRECISION INDUSTRY (SHENZHEN) CO., LTD. et al.) 30 Dec.2010 (30.12.2010) see all document	1-25

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 18 Apr.2013 (18.04.2013)	Date of mailing of the international search report 09 May 2013 (09.05.2013)
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer DONG Libo Telephone No. (86-10)62413705

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2012/079397

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN101272237A	24.09.2008	US2009/0265769A1	22.10.2009
CN102132304A	20.07.2011	EP2332114A2	15.06.2011
		JP2011-530740A	22.12.2011
		US2010/0037303A1	11.02.2010
		WO2010/017066A2	11.02.2010
CN1446331A	01.10.2003	KR2003-0010667A	05.02.2003
		TW1233739B	01.06.2005
		AU6816101A	17.12.2001
		WO01/95545A2	13.12.2001
		US2002/0067832A1	06.06.2002
		JP2003-536320A	02.12.2003
CN1389807A	08.01.2003	None	
US2010/0333195A1	30.12.2010	CN101930509A	29.12.2010