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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 May 2017 (11.05.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/078682 A1

(51) **International Patent Classification**:
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)

(21) **International Application Number**:
PCT/US2015/058789

(22) **International Filing Date**:
3 November 2015 (03.11.2015)

(25) **Filing Language**: English

(26) **Publication Language**: English

(71) **Applicant**: **HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP** [US/US]; 11445 Compaq Center Drive West, Houston, Texas 77070 (US).

(72) **Inventors**: **MORDECHAI, Eli**; Shabazi 26, 56100 Yehud (IL). **COHEN, Karen**; Shabazi 19, 56100 Yehud (IL).

(74) **Agents**: **WOODS, Ariana G.** et al.; Hewlett Packard Enterprise, 3404 E. Harmony Road, Mail Stop 79, Fort Collins, Colorado 80528 (US).

(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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, ST, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to the identity of the inventor (Rule 4.17(i))*

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

Published:

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

(54) **Title**: PASSWORD MODIFICATIONS

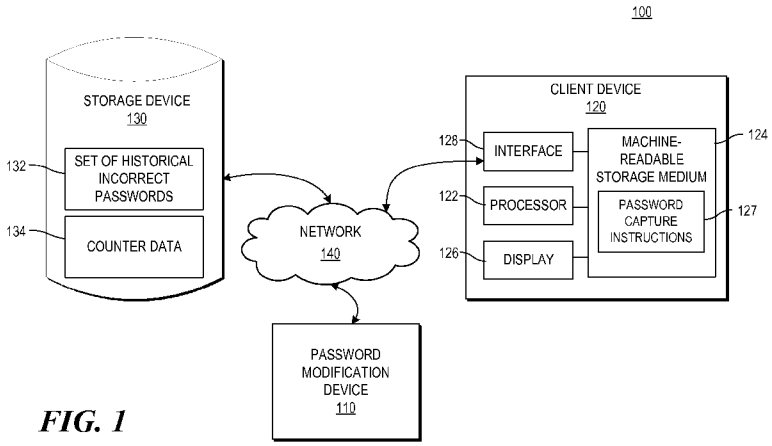


FIG. 1

(57) **Abstract**: Example implementations relate to determining password modifications. Some implementations may include a password confirmation engine to identify an incorrect password entered during a current user authentication session. Additionally, some implementations may include a password comparison engine to determine whether the incorrect password is the same as a number of historical incorrect passwords. For example, each of the number of historical incorrect passwords may occur during a particular historical user authentication session of a plurality of historical user authentication sessions, and may be followed by an original correct password entered during the particular historical user authentication session. Additionally, some implementations may include a password modification engine to modify the original correct password to the incorrect password if the incorrect passwords as the same as each of the number of historical incorrect passwords.

WO 2017/078682 A1

PASSWORD MODIFICATIONS

BACKGROUND

[0001] Secured systems may implement login procedures that involve authentication. This authentication may take the form of a password which must be properly entered before access to the secure system is granted.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The following detailed description references the drawings, wherein:

[0003] FIG. 1 is a block diagram of an example system for password modifications consistent with disclosed implementations;

[0004] FIG. 2 is a block diagram of an example password modification device consistent with disclosed implementations;

[0005] FIG. 3 is a block diagram of an example password modification device consistent with disclosed implementations;

[0006] FIG. 4 is a flow chart of an example process for password modifications consistent with disclosed implementations; and

[0007] FIG. 5 is a flow chart of an example process for password modifications consistent with disclosed implementations.

DETAILED DESCRIPTION

[0008] The following detailed description refers to the accompanying drawings. Wherever possible, the same reference numbers are used in the drawings and the following description to refer to the same or similar parts. While several examples are described in this document, modifications, adaptations, and other implementations are possible. Accordingly, the following detailed description does not limit the disclosed examples. Instead, the proper scope of the disclosed examples may be defined by the appended claims.

[0009] As discussed above, passwords may be used as authentication mechanisms for logging in to secured systems. In modern computing environments,

users may need to remember multiple passwords to access various secured systems. For example, users may have a separate password for work, a separate password for personal email, a separate password for social media, and the like. With all of these different passwords, users may struggle with remembering which password is the correct one for the particular system they are attempting to access, and may enter the incorrect password multiple times over various login sessions.

[0010] Some examples disclosed herein may help diminish that struggle by modifying a password to be consistent with or the same as an incorrectly entered password. For example, implementations consistent with the disclosure may identify an incorrect password entered during a current user authentication session, determine whether the incorrect password is the same as a number of historical incorrect passwords (where each of the number of historical incorrect passwords occurs during a particular historical user authentication session of a plurality of historical user authentication sessions and is followed by an original correct password entered during the particular historical user authentication session), and modify the incorrect password to a new correct password if the incorrect password is the same as each of the number of historical incorrect passwords.

[0011] Referring now to the drawings, FIG. 1 is a block diagram of an example system 100 for password modification. System 100 may be implemented in a number of different configurations without departing from the scope of the disclosed examples. In the example shown in FIG. 1, system 100 may include a password modification device 110, a client device 120, a storage device 130, and a network 140 for connecting password modification device 110 with client device 120 and/or storage device 130.

[0012] Password modification device 110 may be a computing system that performs various functions consistent with disclosed examples. For example, password modification device 110 may be a server, a desktop computer, a laptop computer, and/or any other suitable type of computing device. In some examples, password modification device 110 may process information received from client

device 120 and/or storage device 130. For example, password modification device 110 may receive an incorrect password entered during a current user authentication session, determine whether the incorrect password is the same as a number of historical incorrect passwords, and modify the original correct password to the incorrect password to generate a new correct password if the incorrect password is the same as each of the number of historical incorrect passwords. Examples of password modification device 110 and certain functions that may be performed by device 110 are described in greater detail below with respect to, for example, FIGs. 2-5.

[0013] Client device 120 may be a computing system operated by a user. For example, client device 120 may be a desktop computer, a laptop computer, a tablet computing device, a mobile phone, and/or any other suitable type of computing device. In some examples, client device 120 may be a computing device to perform operations consistent with certain disclosed implementations. For example, client device 120 may transmit authentication information, such as login names, passwords, user authentication session identification numbers ("session IDs"), and the other information related to the authentication to password modification device 110.

[0014] Client device 120 may include a processor to execute instructions stored in a machine-readable storage medium. In the example shown in FIG. 1, client device 120 may include a processor 122, a machine-readable storage medium 124, a display device 126, and an interface 128. Processor 122 of client device 120 may be at least one processing unit (CPU), microprocessor, and/or another hardware device to execute instructions to perform operations. For example, processor 122 may fetch, decode, and execute instructions stored in machine-readable storage medium 124 (such as password capture instructions 127) to capture passwords during user authentication sessions. Machine-readable storage medium 124 may be any electronic, magnetic, optical, or other non-transitory storage device that stores instructions executed by processor 122. Display 126 may be any type of display device that presents information, such as a user interface to capture passwords and

the like, from client device 120. Interface 128 may be any combination of hardware and/or programming that facilitates the exchange of data between the internal components of client device 120 and external components, such as password modification device 110. In some examples, interface 128 may include a network interface device that allows client device 120 to receive and send data to and from various components, such as to and from password modification device 110 via network 140.

[0015] Storage device 130 may be any type of storage system configuration that facilitates the storage of data. For example, storage device 130 may facilitate the locating, accessing, and retrieving of data related to passwords entered during user authentication sessions (e.g., SaaS, SQL, Access, etc. databases). Storage device 130 can be populated by a number of methods. For example, password modification device 110 may populate storage device 130 by receiving, generating, and/or otherwise accessing data related to incorrect passwords entered during user authentication sessions (e.g., historical user authentication sessions that occurred prior to a current user authentication session) and storing the data in storage device 130 as a set of historical incorrect passwords 132. This data may include the user, the user's login name, session ID numbers, timestamps, and/or any other suitable information. In some implementations, additional information related to how many times a particular historical incorrect password was entered during different (e.g,. separate) user authentication sessions may be stored with the set of historical incorrect passwords 132, or may be stored separately as counter data 134. While in the example shown in FIG. 1 storage device 130 is a single component external to components 110 and 120, storage device 130 may comprise separate components and/or may be part of devices 110, 120, and/or another device. In some implementations, storage device 130 may be managed by components of device 110 and/or other devices that are capable of accessing, creating, controlling and/or otherwise managing data remotely through network 140.

[0016] Network 140 may be any type of network that facilitates communication between remote components, such as password modification device 110 and client device 120. For example, network 140 may be a local area network (LAN), a wide area network (WAN), a virtual private network, a dedicated intranet, the Internet, and/or a wireless network.

[0017] The arrangement illustrated in FIG. 1 is simply an example, and system 100 may be implemented in a number of different configurations. For example, while FIG. 1 shows one password modification device 110, client device 120, storage device 130, and network 140, system 100 may include any number of components 110, 120, 130, and 140, as well as other components not depicted in FIG. 1. For example, system 100 may omit any of components 110, 120, 130, and 140, and/or the functionality of at least one of components 110, 120, 130, and 140 may be incorporated into another component (e.g., components 110, 120, 130, 140, and/or a component not shown in FIG. 1).

[0018] FIG. 2 is a block diagram of an example password modification device 210 consistent with disclosed implementations. In certain aspects, password modification device 210 may correspond to password modification device 110 of FIG. 1. Password modification device 210 may be implemented in various ways. For example, device 210 may be a special purpose computer, a server, a mainframe computer, and/or any other suitable type of computing device. In the example shown in FIG. 2, password modification device 210 may include a processor 220 and a machine-readable storage medium 230.

[0019] Processor 220 may be at least one processing unit (CPU), microprocessor, and/or another hardware device to execute instructions to perform operations. For example, processor 220 may fetch, decode, and execute identification instructions 240 (e.g., instructions 242, 244, and/or 246) stored in machine-readable storage medium 230 to perform operations consistent with disclosed examples.

[0020] Machine-readable storage medium 230 may be any electronic, magnetic, optical, and/or other physical storage device that stores executable instructions.

Thus, machine-readable storage medium 230 may be, for example, memory, a storage drive, an optical disc, and the like. In some implementations, machine-readable storage medium 230 may be a non-transitory machine-readable storage medium, where the term "non-transitory" does not encompass transitory propagating signals. Machine-readable storage medium 230 may be encoded with instructions that, when executed by processor 230, perform operations consistent with disclosed implementations. For example, machine-readable storage medium 240 may include instructions that perform operations to identify an incorrect password entered during a current user authentication session, determine whether the incorrect password is the same as a number of historical incorrect passwords, and modify the original correct password to the incorrect password to generate a new correct password if the incorrect password is the same as each of the number of historical incorrect passwords. In the example shown in FIG. 2, machine-readable storage medium 230 may include password confirmation instructions 242, password comparison instructions 244, and password modification instructions 246.

[0021] Password confirmation instructions 242 may function to identify an incorrect password entered during a current user authentication session. In some implementations, when password confirmation instructions 242 are executed by processor 220, password confirmation instructions 242 may cause processor 220 and/or another processor to compare a password entered (e.g., by a user) during the current user authentication session to an original correct password. For example, if the password entered during the current user authentication session does not match the original correct password, the password may be identified by password modification device 210 as an incorrect password. If the password does match the original correct password, the password may be identified by password modification device 210 as a correct password.

[0022] In some implementations, if a user enters the original correct password (e.g., enters the original correct password into client device 120) prior to entering the incorrect password, a set of historical incorrect passwords may be automatically

cleared to help ensure that patterns related to using the same incorrect passwords repeatedly are maintained. For example, if an initial session password (e.g., the first password entered during a user authentication session (e.g., the current user authentication session)) has been identified as a correct password, password confirmation instructions 242, when executed, may automatically cause the clearing of a set of historical incorrect passwords and/or counter data related to the set of historical incorrect passwords, such as the set of historical incorrect passwords 132 and counter data 134 stored in storage device 130. For example, the set of historical incorrect passwords corresponding to the particular user involved in the user authentication session may be removed from a storage device, such as storage device 130. In some implementations, if an incorrect password is not followed (e.g., immediately followed) by the original correct password, password confirmation instructions 242, when executed, may automatically cause the clearing of the set of historical incorrect passwords and/or counter data related to the set of historical incorrect passwords. Examples of identifying an incorrect password entered during a current user authentication session are described in further detail below with respect to, for example, FIGs. 3-5.

[0023] Password comparison instructions 244 may function to determine whether an incorrect password is the same as a number of historical incorrect passwords, where each of the number of historical incorrect passwords may occur during a particular historical user authentication session of a plurality of historical user authentications sessions and/or may be followed by an original correct password during the particular historical user authentication session. For example, in some implementations, when password comparison instructions 244 are executed by processor 220 and/or another processor, password comparison instructions 244 may query a storage device, such as storage device 130, for data related to historical incorrect passwords and may parse the data received in response to the query to identify whether and how many times an entered incorrect password is present in a set of historical incorrect passwords (e.g., set of historical incorrect passwords 132)

stored on the storage device. In some implementations, if the incorrect password is present a predetermined number of times, then password comparison instructions 244 may determine that the incorrect password is the same as a number of historical incorrect passwords. In some implementations, the number of historical incorrect passwords may be a threshold number that identifies a minimum number of historical incorrect passwords, such as a minimum number that may need to be exceeded before password modification device 210 may cause the generation of a request to modify the original incorrect password to the incorrect password. In some implementations, each of the number of historical incorrect passwords may correspond with a different one of the plurality of historical user authentication sessions. For example, each of the historical incorrect passwords may have been entered during different and/or separate user authentication sessions. For example, if the minimum number of historical incorrect passwords was greater than one, there each of the number of historical incorrect passwords may have been entered during a different user authentication session and stored in a storage device (e.g., storage device 130) in a manner that associated it with the particular user authentication session during which it was entered (e.g., by storing it with the session ID).

[0024] In some implementations, when password comparison instructions 244 are executed by processor 220, password comparison instructions 244 may cause processor 220 to determine whether a user entered the incorrect password during a last historical user authentication session of a plurality of historical user authentication sessions, where the last historical user authentication session immediately precedes the current user authentication session. For example, password comparison instructions 244, when executed, may determine whether the user tried the same incorrect password in the user's last authentication session prior to the current authentication session. If the incorrect password is not entered during the last historical user authentication session, password comparison instructions 244, when executed, may cause the clearing of the number of historical incorrect passwords. For example, if the incorrect password is not entered during the last historical user

authentication session, password comparison instructions 244, when executed, may cause the clearing of a set of historical incorrect passwords, where the set includes the number of historical incorrect passwords. For example, an entire set of historical incorrect passwords (e.g., set of historical incorrect passwords 132, and or data related to how many times particular historical incorrect passwords may have been entered (e.g., counter data 134) may be removed from a storage device (e.g., storage device 130). In some implementations, password comparison instructions 244, when executed, may determine whether the incorrect password was tried more than a particular number of times (e.g., 3 times, 5 times, etc.). If not, the counter data 134 (e.g., increased by 1) and the user can continue to the login process. If so, then password comparison instructions 244, when executed, may cause a display of a request to modify the correct password (e.g. an original correct password) to the incorrect password (e.g., generating a new correct password) based on the comparison. Examples of determining whether the incorrect password is the same as a number of historical incorrect passwords are described in further detail below with respect to, for example, FIGs. 3-5.

[0025] Password modification instructions 246 may function to modify the original correct password to generate a new correct password. For example, when password modification instructions 246 are executed by processor 220, password modification instructions 246 may cause processor 220 to modify the original correct password to the incorrect password to generate a new correct password if the incorrect password is the same as each of the number of historical incorrect passwords. For example, in response to a request to change the original correct password to the new correct password, password modification instructions 246, when executed, may clear the original correct password, store the incorrect password as the new correct password (e.g., stored in a manner that associates it with the particular user), and/or use the new correct password during future user authentication sessions. For example, passwords entered in future user authentication sessions may be compared to the new correct password rather than the original correct password. Examples of

modifying the incorrect password to a new correct password are described in further detail below with respect to, for example, FIGs. 3-5.

[0026] FIG. 3 is a block diagram of an example password modification device 310 consistent with disclosed implementations. In certain aspects, password modification device 310 may correspond to password modification device 110 of FIG. 1 and/or password modification device 210 of FIG. 2. Device 310 may be implemented in various ways. For example, device 310 may be a special purpose computer, a server, a mainframe computer, and/or any other suitable type of computing system. In the example shown in FIG. 3, device 310 may include a password confirmation engine 320, a password comparison engine 330, and a password modification engine 340.

[0027] Engines 320, 330, and 340 may be electronic circuitry for implementing functionality consistent with disclosed examples. For example, engines 320, 330, and 340 may represent combinations of hardware devices and programming to implement the functionality consistent with disclosed implementations. In some examples, the functionality of engines 320, 330, and/or 340 may correspond to operations performed by password modification device 210 of FIG. 2, such as operations performed when identification instructions 240 are executed by processor 220 (described above with respect to FIG. 2). In FIG. 3, password confirmation engine 320 may represent a combination of hardware and programming that performs operations similar to those performed when processor 220 executes password confirmation instructions 242. Similarly, password comparison engine 330 may represent a combination of hardware and programming that performs operations similar to those performed when processor 220 executes password comparison instructions 244, and password modification engine 340 may represent a combination of hardware and programming that performs operations similar to those performed when processor 220 executes password modification instructions 246.

[0028] FIG. 4 is a flow chart of an example process 400 for password modification consistent with disclosed implementations. Although execution of process 400 is

described below with reference to system 100 of FIG. 1 and/or specific components of system 100, other suitable systems for execution of at least one step of process 400 may be used. For example, processes described below as being performed by password modification device 110 may be performed by password modification device 210, password modification device 310, and/or any other suitable system. Process 400 may be implemented in the form of executable instructions stored on a machine-readable storage medium and/or in the form of electronic circuitry.

[0029] Process 400 may start (step S405) after a current user authentication session has been initiated. For example, processor 122 of client device 120 may execute password capture instructions 127 to capture passwords entered during the current user authentication session. Client device 120 may transmit the captured passwords and information relating to the current user authentication session to password modification device 110 and/or storage device 130 using, for example, interface 128 and network 140. In some implementations, the transmitted passwords may be stored in a manner that links them with the information related to the current user authentication session (such as user, date, time, session number, and the like).

[0030] Process 400 may include determining whether an incorrect password entered during a current user authentication session is followed by an original correct password entered during the user authentication session (step S410). In some implementations, password modification device 110 may analyze the sequence of passwords entered during the current user authentication session to determine whether an incorrect password was followed by an original correct password. For example, in response to receipt of an entered password, password modification device 110 may compare the entered password to a password that is associated with the user account of the secured system the user is attempting to access. If the entered password and user account password match, then password modification device 110 may identify the entered password as an original correct password. If the entered password and user account password do not match, password modification device 110 may identify the entered password as an incorrect password and, in some

examples, may monitor any additional passwords entered during the same current user authentication session (e.g. entered immediately after the entry of the incorrect password and/or sometime after the entry of the incorrect password) to determine whether one of the additional passwords is an original correct password. If not, password modification device may determine that an incorrect password was not entered during the current user authentication session and/or that an incorrect password was entered but not followed by an original correct password. In some examples, if the incorrect password is not followed by the original correct password, password modification device 110 may cause a display of a notification that the incorrect password is incorrect (e.g., cause a display of text, graphics, and/or any other suitable information) (step S430). If so, password modification device may determine that an incorrect password entered during the current user authentication session was followed by an original correct password entered during the current user authentication session. In some implementations, password modification device 110 may automatically cause the clearing of the set of historical incorrect passwords if a user enters the original correct password prior to entering the incorrect password using, for example, the methods described above. In some implementations, password modification device 110 may automatically cause the clearing of the set of historical incorrect passwords if the incorrect password is not followed by the original correct password using, for example, the methods described above.

[0031] Process 400 may also include, if the incorrect password is followed by the original correct password, determining whether the incorrect password was entered a particular number of times in different historical user authentication sessions (step S420). In some implementations, password modification device 110 may determine whether the incorrect password was entered a particular number of times by determining a number of matches between the incorrect password and historical incorrect passwords stored in a set of historical incorrect passwords, and/or comparing the number of matches to a threshold number using, for example, the methods described above. For example, a storage device (such as storage device

130) may store a set of historical incorrect passwords (such as set of historical incorrect passwords 132), and password modification device 110 may query the storage device to obtain information related to whether and/or how many times that particular user has previously entered the password during a different historical user authentication session (e.g., an authentication session that occurred prior to the current user authentication session). Password modification device 110 may parse the data received in response to the query to determine the number of matches, and may determine whether the number of matches is above or below a threshold number (e.g., a predetermined number, such as three).

[0032] Process 400 may also include, if the incorrect password is followed by the original correct password, causing a display of a request to modify the original correct password to the incorrect password to generate a new correct password if the incorrect password was entered the particular number of times (step S450). For example, if the incorrect password was entered the particular number of times, password modification device 110 may cause a display of a graphical interface on display 126 of client device 120. The graphical interface may include an area where the user can identify whether they would like to modify the original correct password. For example, the graphical interface may include an area for text input, a radio button, a checkbox, or any other suitable means of capturing information related to a request to modify the original correct password.

[0033] In some implementations, password modification device 110 may automatically generate the new correct password based on a response to the request, the response indicating to generate the new correct password based on the incorrect password. For example, if the request includes information (e.g., information captured during a user interaction with the graphical user interface described above) indicating that the user wishes to change the password from the original correct password to the incorrect password, password modification device 110 may modify the original correct password to become the incorrect password (e.g., delete the original correct password, overwrite the original correct password,

and/or otherwise replace the original correct password with the incorrect password). In some implementations, password modification device 110 may automatically cause the clearing of the set of historical incorrect passwords based on a response to the request, the response indicating not to generate the new correct password based on the incorrect password. For example, if the request includes information (e.g., information captured during a user interaction with the graphical user interface described above) indicating that the user does not wish to change the password from the original correct password to the incorrect password, password modification device 110 may maintain the original correct password and may delete the set of historical incorrect passwords using, for example, the methods described above (e.g., deleting the set of historical incorrect passwords from a storage device, such as storage device 130).

[0034] Process 400 may also include, if the incorrect password is followed by the correct password, causing a storing of the incorrect password as a historical incorrect password in a set of historical incorrect passwords if the incorrect password was not entered the particular number of times (step S460). For example, password modification device 110 may cause the storing of the incorrect password in a storage device, such as storage device 130. In some implementations, password modification device 110 may store the incorrect password along with information related to the historical user authentication session in a storage device, such as storage device 130. For example, password modification device 110 may transmit the incorrect password and/or the information related to the historical user authentication session to storage device 130 via network 140. For example, in some implementations each historical user authentication session may have a separate user ID that password modification device may use to distinguish between user authentication sessions. Sessions with the same user authentication session ID may be considered to be the same session. Sessions with different user authentication session IDs may be considered to be different user authentication sessions. Thus, in some examples, the separate session identification numbers may be used by

password modification device 110 to distinguish current user authentication sessions from historical user authentication sessions, to distinguish between each of the historical user authentication sessions, to otherwise ensure that passwords entered during a particular session are linked to that particular session, and the like. Once steps 410, 420, 430, 440, and/or 450 are complete, process 400 may end (step S465).

[0035] FIG. 5 is a flow chart of an example process 500 for password modification consistent with disclosed implementations. Although execution of process 500 is described below with reference to system 100 of FIG. 1 and/or specific components of system 100, other suitable systems for execution of at least one step of process 500 may be used. For example, processes described below as being performed by password modification device 110 may be performed by password modification device 210, password modification device 310, and/or any other suitable system. Process 500 may be implemented in the form of executable instructions stored on a machine-readable storage medium and/or in the form of electronic circuitry.

[0036] Process 500 may start (step S505) after a current user authentication session has been initiated. For example, process 400 may begin when a user enters a password (either a correct password or an incorrect password) during the current user authentication session. Process 500 may include identifying when a correct password was entered after an incorrect password during a current user authentication session (step S510). For example, password modification device may identify when a correct password was entered after an incorrect password during a current user authentication session by, for example, using the methods described above (e.g., monitoring a sequence of passwords entered during a user authentication session and identifying when the passwords matched or did not match an original correct password). Process 500 may also include in response to the identification, determining a particular number of times where the correct password was entered after the incorrect password during different historical user authentication sessions (e.g., separate historical user authentication sessions having different

session IDs) (step S520). For example, password modification device 110 may compare the incorrect password to a historical incorrect password of a set of historical incorrect passwords; determine a counter value associated with the historical incorrect password, and assign the counter value as the particular number of times. For example, password modification device may employ a counter to keep track of the number of times the particular password was used in different (e.g., separate and distinct) historical user authentication sessions, and password modification device 110 may determine the counter value associated with a historical incorrect password that matches the incorrect password entered during the current user authentication session. In some implementations, the stored set of historical incorrect passwords may be cleared if more than one incorrect password is entered during the current user authentication session. For example, the incorrect password described above may be considered to be a first incorrect password (e.g., the incorrect password is a first incorrect password) and the stored set of historical incorrect passwords may be cleared from a storage device if a second incorrect password is entered during the current user authentication session.

[0037] Process 500 may also include comparing the particular number of times to a threshold number (step S530) using, for example, the methods described above. Additionally, process 500 may also include causing a display of a request to modify the correct password to the incorrect password based on the comparison (step S540). For example, if the particular number of times exceeds (or in some instances is smaller than) the threshold number, password modification device 110 may cause the display of the request. Once steps 510, 520, 530, and/or 540 are complete, process 500 may end (step S555).

[0038] The disclosed examples may include systems, devices, machine-readable storage media, and methods for password modifications. For purposes of explanation, certain examples are described with reference to the components illustrated and/or described in FIGS. 1-5. The functionality of the illustrated components may overlap, however, and may be present in a fewer or greater number

of elements and components. Further, all or part of the functionality of illustrated elements may co-exist or be distributed among several geographically dispersed locations. Moreover, the disclosed examples may be implemented in various environments and are not limited to the illustrated examples.

[0039] Moreover, as used in the specification and the appended claims, the singular forms “a,” “an,” and “the” are intended to include the plural forms as well, unless the context indicates otherwise. Additionally, although the terms first, second, etc. may be used herein to describe various elements, these elements should not be limited by this terms. Instead, these terms are used to distinguish one element from another.

[0040] Further, the sequence of operations described in connection with FIGs. 1-5 are examples and are not intended to be limiting. Additional or fewer operations or combinations of operations may be used or may vary without departing from the scope of the disclosed examples. Furthermore, implementations consistent with the disclosed examples need not perform the sequence of operations in any particular order, including those described with respect to FIGS. 1-5. Thus, the present disclosure merely sets forth possible examples of implementations, and many variations and modifications may be made to the described examples. All such modifications and variations are intended to be included within the scope of this disclosure and protected by the following claims.

CLAIMS

We claim:

1. A system for password modification comprising:

a password confirmation engine to identify an incorrect password entered during a current user authentication session;

a password comparison engine to determine whether the incorrect password is the same as a number of historical incorrect passwords, each of the number of historical incorrect passwords:

occurring during a particular historical user authentication session of a plurality of historical user authentication sessions; and

being followed by an original correct password entered during the particular historical user authentication session; and

a password modification engine to modify the original correct password to the incorrect password to generate a new correct password if the incorrect password is the same as each of the number of historical incorrect passwords.

2. The system of claim 1, wherein each of the number of historical incorrect passwords corresponds with a different one of the plurality of historical user authentication sessions.

3. The system of claim 1, wherein the number is a threshold number that identifies a minimum number of historical incorrect passwords.

4. The system of claim 1, wherein the password comparison engine is to determine whether the incorrect password is the same as a number of historical incorrect passwords by determining whether the user entered the incorrect password during a last historical user authentication session of the plurality of historical user authentication sessions, the last historical user authentication session immediately preceding the current user authentication session.

5. The system of claim 4, wherein if the incorrect password is not entered during the last historical user authentication session, the password comparison engine is to cause the clearing of the number of historical incorrect passwords from a storage device.

6. The system of claim 5, wherein if the incorrect password is not entered during the last historical user authentication session, the password comparison engine is to cause the clearing of a set of historical incorrect passwords, the set including the number of historical incorrect passwords.

7. A method comprising:

determining, using a processor, whether an incorrect password entered during a user authentication session is followed by an original correct password entered during the user authentication session;

if the incorrect password is followed by the original correct password:

determining, using the processor, whether the incorrect password was entered a particular number of times in different historical user authentication sessions;

causing, using the processor, a display of a request to modify the original correct password to the incorrect password to generate a new correct password if the incorrect password was entered the particular number of times; and

causing, using the processor, a storing of the incorrect password as a historical incorrect password if the incorrect password was not entered the particular number of times; and

if the incorrect password is not followed by the original correct password:

causing, using the processor, a display of a notification that the incorrect password is incorrect.

8. The method of claim 7, wherein determining whether the incorrect password was entered the particular number of times comprises:

determining a number of matches between the incorrect password and historical incorrect passwords in a stored set of historical incorrect passwords; and

comparing the number of matches to a threshold number.

9. The method of claim 8, comprising:

automatically causing the clearing of the set of historical incorrect passwords if a user enters the original correct password prior to entering the incorrect password.

10. The method of claim 8, comprising:

automatically causing the clearing the set of historical incorrect passwords if the incorrect password is not followed by the original correct password.

11. The method of claim 7, comprising:

automatically generating the new correct password based on a response to the request, the response indicating to generate the new correct password based on the incorrect password.

12. The method of claim 7, comprising:

automatically causing the clearing of the set of historical incorrect passwords based on a response to the request, the response indicating not to create the new correct password based on the incorrect password.

13. A non-transitory machine-readable storage medium including instructions which, when executed by a processor, cause the processor to:

identify when a correct password was entered after an incorrect password during a current user authentication session;

in response to the identification, determining a particular number of times where the correct password was entered after the incorrect password during different historical user authentication sessions;

comparing the particular number of times to a threshold number; and

causing a display of a request to modify the correct password to the incorrect password based on the comparison.

14. The non-transitory machine-readable storage medium of claim 14, wherein determining the particular number of times where the correct password was entered after the incorrect password during differing historical user authentication sessions comprises:

comparing the incorrect password to a historical incorrect password in a stored set of historical incorrect passwords;

determining a counter value associated with the historical incorrect password; and

assigning the counter value as the particular number of times.

15. The non-transitory machine-readable storage medium of claim 14, wherein:

the incorrect password is a first incorrect password; and

the stored set of historical incorrect passwords is cleared from a storage device if a second incorrect password is entered during the current user authentication session.

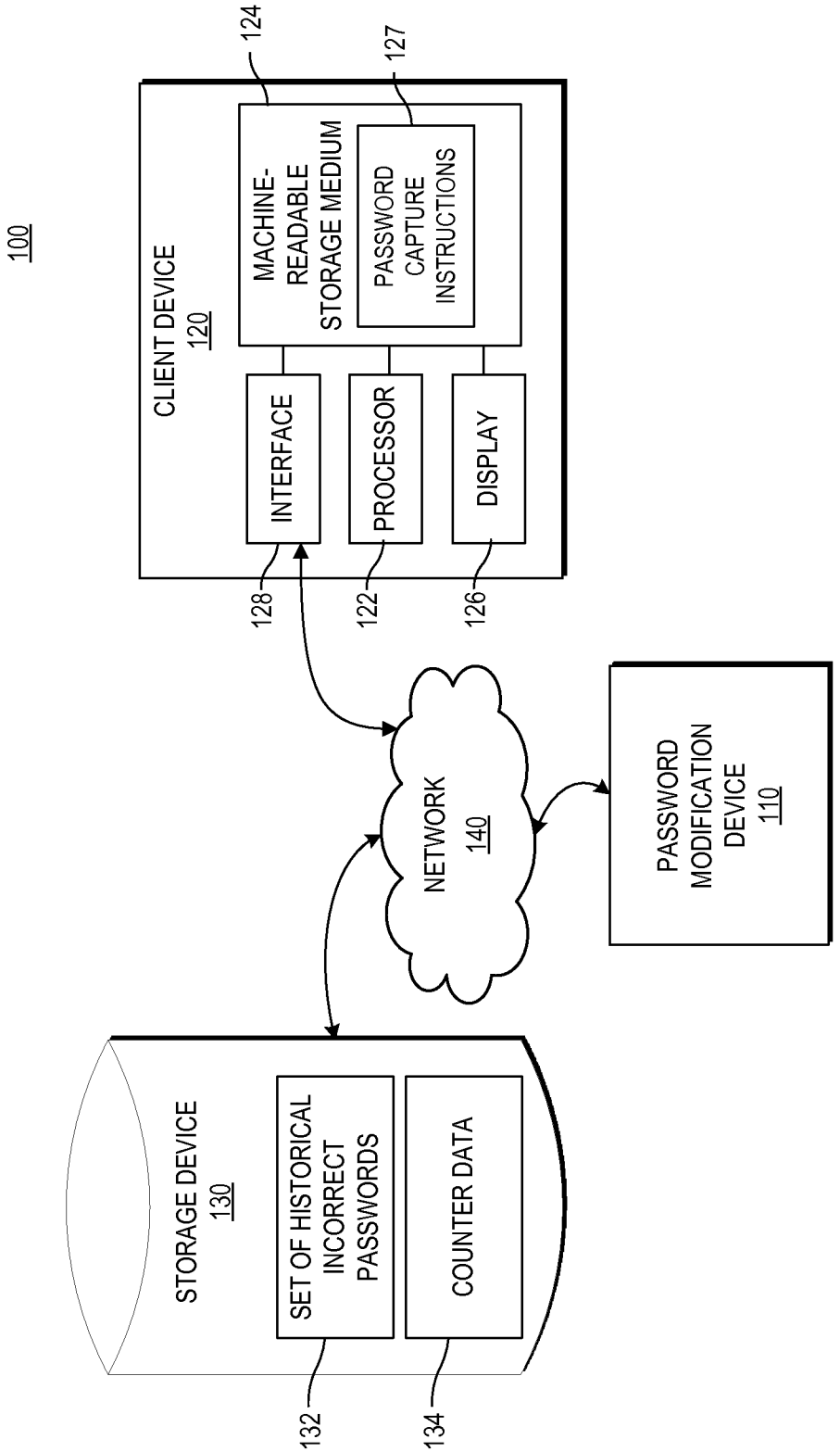

100
CLIENT DEVICE
120
MACHINE-READABLE STORAGE MEDIUM
124
PASSWORD CAPTURE INSTRUCTIONS
127
INTERFACE
PROCESSOR
DISPLAY
128
122
126
NETWORK
140
PASSWORD MODIFICATION DEVICE
110
STORAGE DEVICE
130
SET OF HISTORICAL INCORRECT PASSWORDS
COUNTER DATA
132
134

FIG. 1

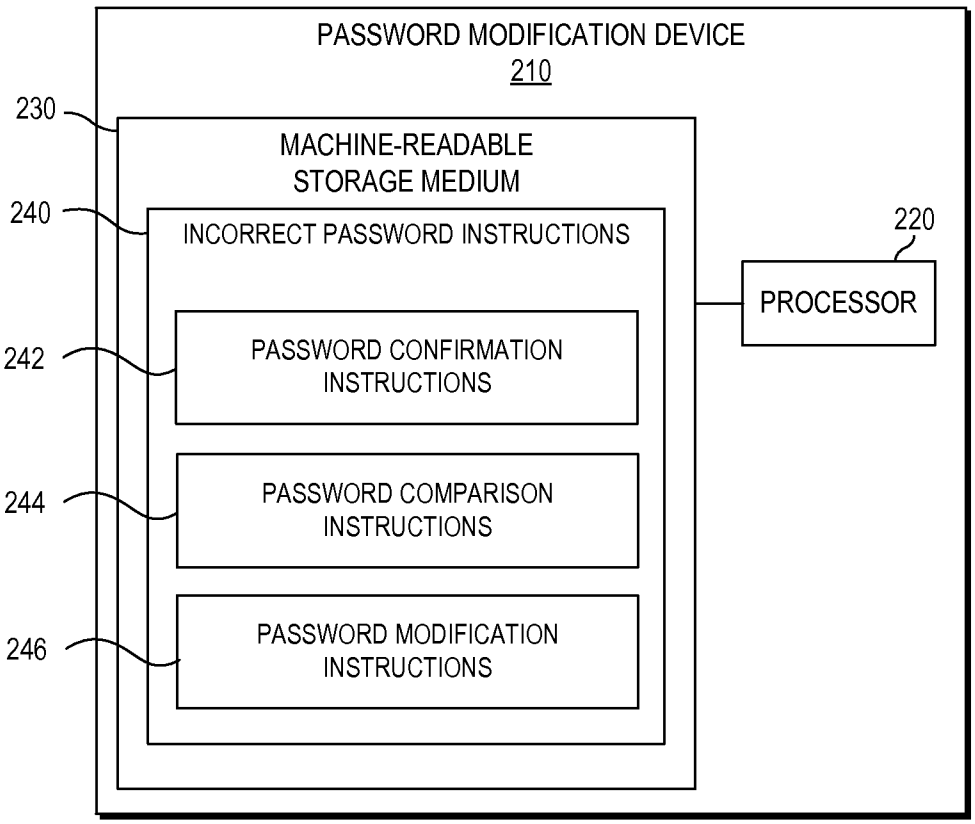

PASSWORD MODIFICATION DEVICE
210
230
MACHINE-READABLE
STORAGE MEDIUM
240
INCORRECT PASSWORD INSTRUCTIONS
220
PROCESSOR
242
PASSWORD CONFIRMATION
INSTRUCTIONS
244
PASSWORD COMPARISON
INSTRUCTIONS
246
PASSWORD MODIFICATION
INSTRUCTIONS

FIG. 2

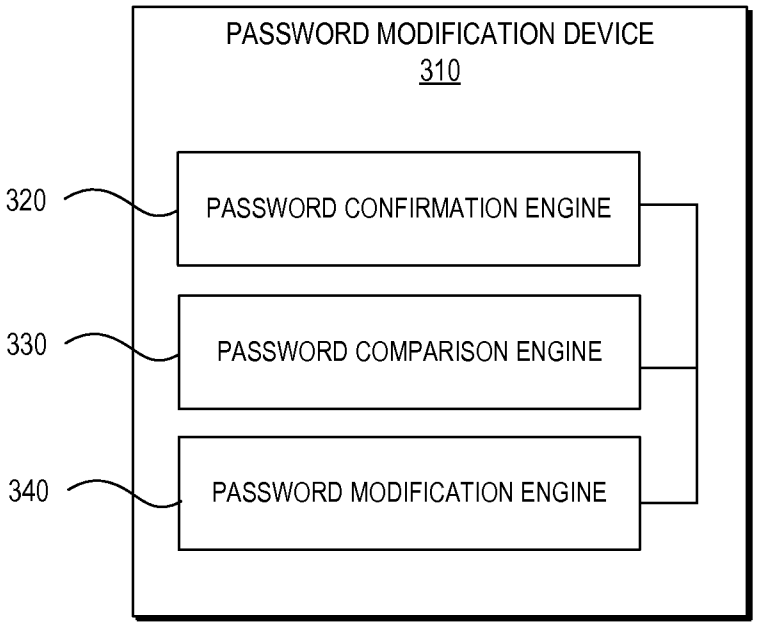

PASSWORD MODIFICATION DEVICE
310
320
PASSWORD CONFIRMATION ENGINE
330
PASSWORD COMPARISON ENGINE
340
PASSWORD MODIFICATION ENGINE

FIG. 3

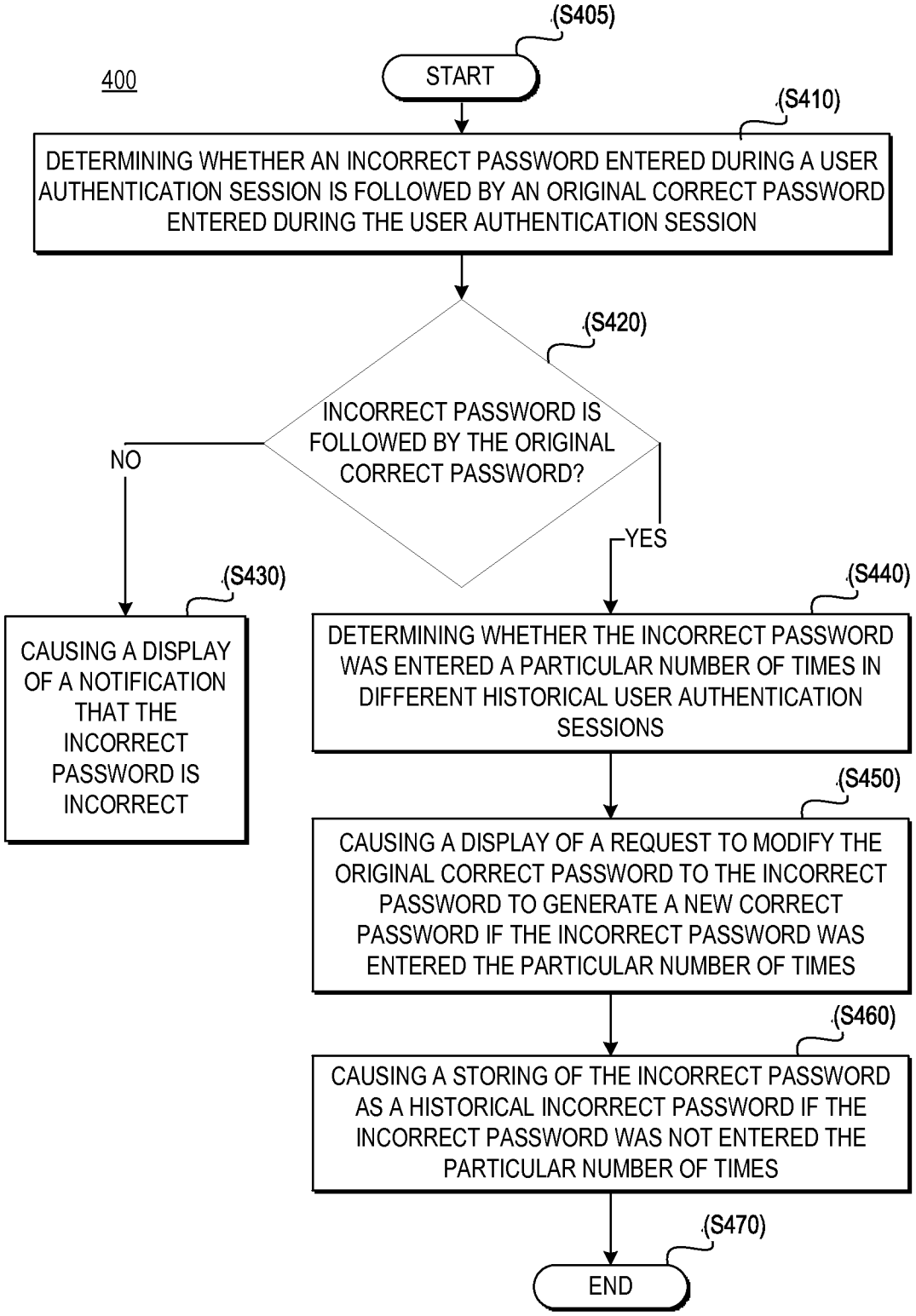
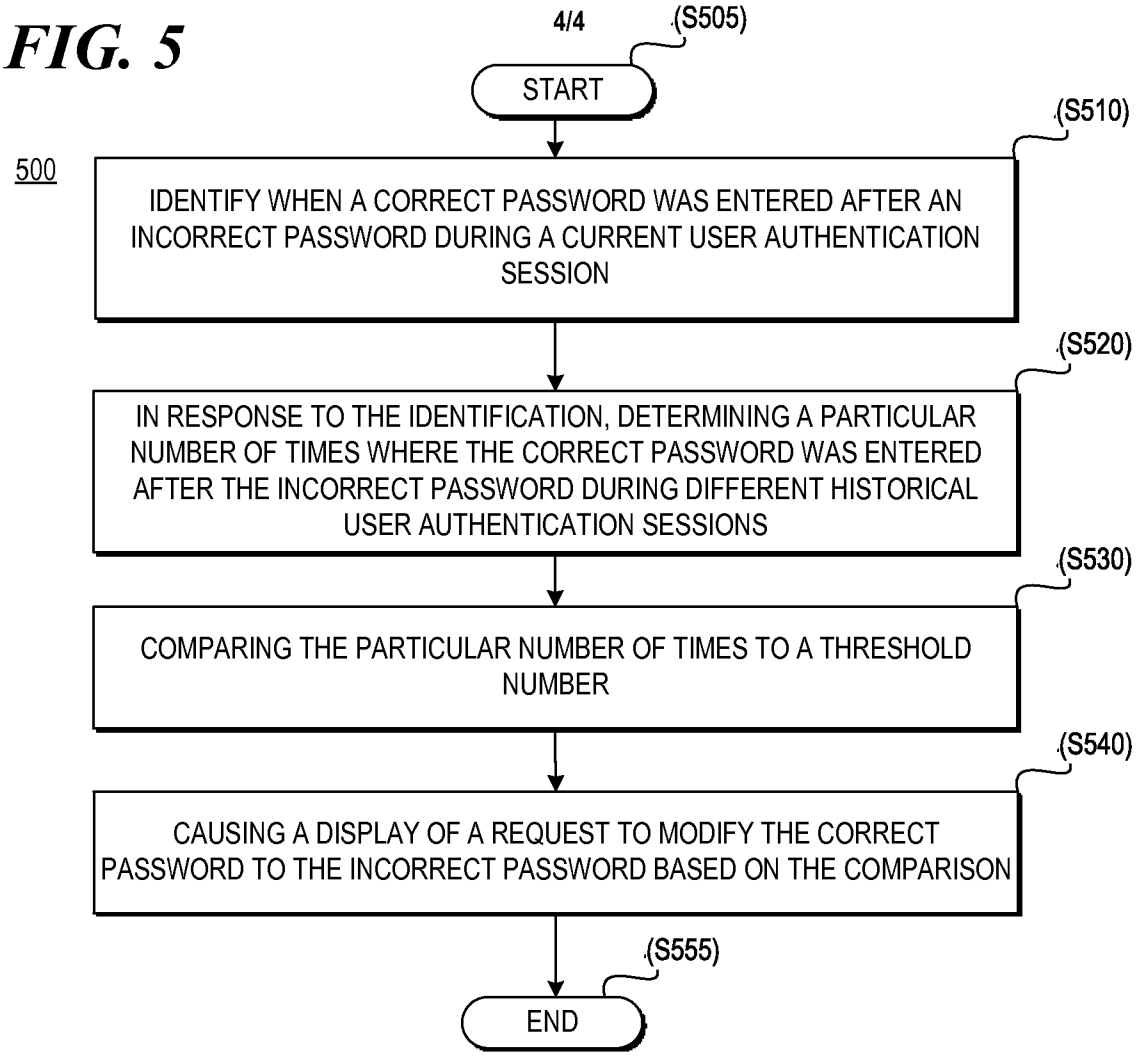

400
(S405)
START
(S410)
DETERMINING WHETHER AN INCORRECT PASSWORD ENTERED DURING A USER AUTHENTICATION SESSION IS FOLLOWED BY AN ORIGINAL CORRECT PASSWORD ENTERED DURING THE USER AUTHENTICATION SESSION
(S420)
INCORRECT PASSWORD IS FOLLOWED BY THE ORIGINAL CORRECT PASSWORD?
NO
YES
(S430)
CAUSING A DISPLAY OF A NOTIFICATION THAT THE INCORRECT PASSWORD IS INCORRECT
(S440)
DETERMINING WHETHER THE INCORRECT PASSWORD WAS ENTERED A PARTICULAR NUMBER OF TIMES IN DIFFERENT HISTORICAL USER AUTHENTICATION SESSIONS
(S450)
CAUSING A DISPLAY OF A REQUEST TO MODIFY THE ORIGINAL CORRECT PASSWORD TO THE INCORRECT PASSWORD TO GENERATE A NEW CORRECT PASSWORD IF THE INCORRECT PASSWORD WAS ENTERED THE PARTICULAR NUMBER OF TIMES
(S460)
CAUSING A STORING OF THE INCORRECT PASSWORD AS A HISTORICAL INCORRECT PASSWORD IF THE INCORRECT PASSWORD WAS NOT ENTERED THE PARTICULAR NUMBER OF TIMES
(S470)
END

FIG. 4

FIG. 5


4/4
(S505)
START
(S510)
500
IDENTIFY WHEN A CORRECT PASSWORD WAS ENTERED AFTER AN INCORRECT PASSWORD DURING A CURRENT USER AUTHENTICATION SESSION
(S520)
IN RESPONSE TO THE IDENTIFICATION, DETERMINING A PARTICULAR NUMBER OF TIMES WHERE THE CORRECT PASSWORD WAS ENTERED AFTER THE INCORRECT PASSWORD DURING DIFFERENT HISTORICAL USER AUTHENTICATION SESSIONS
(S530)
COMPARING THE PARTICULAR NUMBER OF TIMES TO A THRESHOLD NUMBER
(S540)
CAUSING A DISPLAY OF A REQUEST TO MODIFY THE CORRECT PASSWORD TO THE INCORRECT PASSWORD BASED ON THE COMPARISON
(S555)
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/058789

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04L 9/08(2006.01)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)
H04L 9/32; G06F 3/02; G06F 11/30; G06F 15/00; E05B 49/00; G06F 21/20; H04L 29/06; G06F 12/14; H04L 9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords:password modification, historical incorrect password

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-030147 A (NEC YONEZAWA LTD.) 31 January 2003 See paragraphs [0018], [0029]-[0031], [0039]-[0041]; claim 6; and figures 1, 3.	1-15
Y	US 2014-0325591 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 30 October 2014 See paragraphs [0039], [0041]; and figure 2.	1-15
A	US 8312540 B1 (CLIFFORD E. KAHN et al.) 13 November 2012 See column 10, lines 8-50; column 18, lines 25-32; and figures 3, 5.	1-15
A	JP 2006-099356 A (FUJI XEROX CO., LTD.) 13 April 2006 See paragraphs [0026]-[0031]; and figure 1.	1-15
A	KR 10-0881099 B1 (SANG OK LEE) 02 February 2009 See claim 1 and figure 3.	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

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

Date of the actual completion of the international search	Date of mailing of the international search report
08 August 2016 (08.08.2016)	**08 August 2016 (08.08.2016)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
KIM, Do Weon
Telephone No. +82-42-481-5560

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/058789

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
JP 2003-030147 A	31/01/2003	None	
US 2014-0325591 A1	30/10/2014	US 2010-100948 A1 US 8875261 B2 US 9231981 B2	22/04/2010 28/10/2014 05/01/2016
US 8312540 B1	13/11/2012	None	
JP 2006-099356 A	13/04/2006	None	
KR 10-0881099 B1	02/02/2009	None	