



- (51) **International Patent Classification:**
G06F 21/46 (2013.01) *G06F 21/31* (2013.01)
- (21) **International Application Number:**
PCT/US2012/065079
- (22) **International Filing Date:**
14 November 2012 (14.11.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** THOMSON LICENSING [FR/FR]; 1-5 rue Jeanne d'Arc, F-92130 Issy Les Moulineaux (FR).
- (72) **Inventors; and**
- (71) **Applicants :** FOOTE, Evan, Michael [US/US]; 14385 Avian Way, Carmel, Indiana 46033 (US). MAYHEW, Mark, Anthony [US/US]; 253 N. Arsenal Ave, Indianapolis, Indiana 46201 (US). VONDERSAAR, Benjamin, Thomas [US/US]; 10850 N. College Ave, Indianapolis, Indiana 46280 (US).
- (74) **Agents:** SHEDD, Robert, D. et al.; Thomson Licensing LLC, 2 Independence Way, Suite #200, Princeton, New Jersey 08540 (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, 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, PA, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title:** ENHANCED SERVER/CLIENT LOGIN METHOD

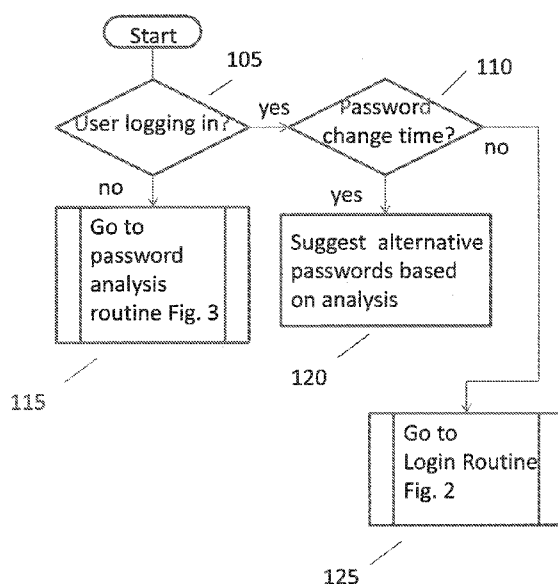


Fig. 1

(57) **Abstract:** A method for enhanced login is described including determining if a user is attempting to login to a particular account, performing analysis on the user's passwords if the user is not attempting to login to the particular account, determining if it is time to change a password on the particular account, if the user is attempting to login to the particular account, suggesting alternative passwords to the user based on the password analysis and performing a login procedure.

ENHANCED SERVER/CLIENT LOGIN METHOD

FIELD OF THE INVENTION

5 The present invention relates to password use to protect various user accounts, and in particular to a service in a server to obtain and discern passwords to better protect user accounts.

BACKGROUND OF THE INVENTION

10 Conventionally, most systems remember the user's previous N passwords, in order to have the user create a different password. This only keeps a history of that account, not from the person.

SUMMARY OF THE INVENTION

15 The present invention provides for a service to obtain and discern a user's likely passwords. One password likely has no information on its own. Several passwords put together may contain small bits of information about a user, such as hobbies or interests (especially if passwords are key words or phrases, or are somehow related to each other).

20 A method for enhanced login is described including determining if a user is attempting to login to a particular account, performing analysis on the user's passwords if the user is not attempting to login to the particular account, determining if it is time to change a password on the particular account, if the user is attempting to login to the particular account, suggesting alternative passwords to the user based on the password analysis and performing a login procedure.

BRIEF DESCRIPTION OF THE DRAWINGS

25 The present invention is best understood from the following detailed description when read in conjunction with the accompanying drawings. The drawings include the following figures briefly described below:

Fig. 1 is an overview flowchart of operation of a server in accordance with the principles of the present invention.

Fig. 2 is a flowchart of an exemplary login routine at the server in accordance with the principles of the present invention.

Fig. 3 is a flowchart of an exemplary password analysis routine at the server in accordance with the principles of the present invention.

5

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention provides for a service to obtain and discern a user's likely passwords. A single password likely has no information on its own. Several passwords put together may contain small bits of information about a user, such as hobbies or interests especially if passwords are keywords or phrases, or are somehow related to each other.

10 Passwords may also give information about a user's technical competence, such as their security practices (length of passwords, similarities, use of common "dictionary" words). A set of passwords may also give a mask of common characteristics, such as always capitalizing the third letter or always putting a punctuation at the beginning, or different words of varying lengths users may commonly modify (e.g., password must be 6 characters long, user always has "ball" and two special characters. Password must be 8 characters long, user always has "tennis" and two special characters. Password must be 12 characters long, user always has "tennis" and "ball", with two special characters.)

20 Once a service knows its user's likely passwords, it can do several things. First, it can determine if the user is using hobbies and interests to formulate their password, and market products towards the user. If the user is technically incompetent (i.e. passwords are matched against other very common passwords), it can guide the user as to how to pick a better password. If the user has a set of common characteristics between their passwords, the service can make recommendations to help the user diversify their passwords.

25 Also, as a consequence of the present invention, an account becomes more secure from a brute force attack. The owner of the account is likely to re-enter their password, where a brute force attempt will continue, and ignore the "wrong" password.

The present invention provides a method to obtain likely passwords a person has with other profiles or accounts (for instance, email accounts or logins unrelated to the current service.)

5 The present invention also can help to protect from brute force attacks on inactive accounts, by doubling the amount of time required to log in to an account.

When a user forgets their password for a particular service/account, before resetting their password they are likely to volunteer their “best guess” as to what their password might be, based on similar patterns they use for other accounts. Understanding this behavior, a service can trigger that behavior if the service detects the user is guessing
10 their password. The service will then automatically tell the user they are using the wrong password on their first try. The user may then volunteer their other “best guesses” in order to gain access to their account. If the first password was actually correct, and the user later enters that password, they will have access to their account. The user will then likely blame the lock out on a typo, and will have provided their other passwords.

15 These password guesses can be stored for later, and can be used to generate a profile of a user’s interests, a user’s technical or security competence, a user’s password pattern, or even help suggest a new password (which passwords not to use) in the event a password expires. Password information can also be used to help train a user to be more secure.

20 In order for the server to determine if the user can login, several steps must be taken. The first step, the most obvious, is if the password the user enters is correct or not. If the user enters the incorrect password, the user cannot log in. The server then records the details of the login attempt (e.g. account, time, password used). The server then checks the number of incorrect attempts, and if the number is greater than a threshold,
25 locks the account for a time period. If the threshold has not been reached, the server then allows the user to try logging in again.

If the user enters the correct password, several decisions have to be made. If the user has logged into their account recently, or if the user auto filled the field (time password was entered was near zero, as if the password was stored in the browser, as well

as a perfect match on the first attempt), the server is more likely to allow the user to log in directly.

If the user had not logged in recently, and the field was not auto filled, the server is more likely to tell the user that they are not allowed to log in. If the server tells the user it cannot log in even though the account details are correct, the threshold for number of log in attempts is increased. If the user enters the correct password again (twice in a row), the user is automatically allowed access.

During server idle time, the server can then examine passwords a user supplied incorrectly in an attempt to determine a common theme, as described above.

Fig. 1 is an overview flowchart of operation of a server in accordance with the principles of the present invention. At 105 the server determines if the user is attempting to login. If the user is attempting to login, then at 110 the server determines if it is time to change the password on the account. If it is not time to change the password on the account, then at 125 processing proceeds to the login routine shown in Fig. 2 and described below. If the user is not attempting to login, then at 125 during idle time the server, proceeds to the password analysis routine shown in Fig. 3 and described below. If it is time to change the password on the account, then at 120 the server suggests alternative passwords based on the analysis.

Fig. 2 is a flowchart of an exemplary login routine at the server in accordance with the principles of the present invention. At 205 the threshold and login attempt counter are initialized. At 210 the user is prompted to enter a password for the particular account that the user is attempting to access. At 215, the user's password entry is accepted. At 220, the login attempt counter is incremented. At 225, the details of the login attempt are recorded (stored). At 230, a test is performed to determine if the password entered is correct. If the password entered is correct then at 235 a test is performed to determine if there was a recent login attempt or if the password was entered by auto-filling a password pre-stored in the server. If there was a recent login attempt or if the password was entered by auto-filling a password pre-stored in the server then at 240 the user is permitted to login to the particular account that the user was attempting to access. If there was not a recent login attempt or if the password was not entered by auto-

filling a password pre-stored in the server then at 245 the user is denied access to the particular account that the user was attempting to access. At 250 the threshold is incremented. Processing then proceeds to 210. If the password was not correct, then at 255 a test is performed to determine if the login attempt counter was greater than the threshold. If the login attempt counter is greater than the threshold then at 260 the user is locked out of the particular account that the user was attempting to access for a pre-determined period of time and a timer is initialized. At 265 a test is performed to determine if the timer is greater than the pre-determined lock out period of time. If the timer is greater than the pre-determined lock out period of time, then processing proceeds to 210. If the timer is less than the pre-determined lock out period of time, then at 270 the timer is incremented and processing proceeds to 265. If the login attempt counter is greater than the threshold, then processing proceeds to 210.

Fig. 3 is a flowchart of an exemplary password analysis routine at the server in accordance with the principles of the present invention. At 305, the server, sorts the passwords for the various accounts to which the server has access. This includes sorting the passwords by length, by special characters, by capital letters, by lower case letter, and by embedded keywords (words, recurring character strings). At 310 the server inspects and analyzes the lists to determine if there are any patterns. At 315 based on the analysis, the server prepares recommendations for alternative passwords for the user.

It is to be understood that the present invention may be implemented in various forms of hardware, software, firmware, special purpose processors, or a combination thereof. Special purpose processors may include application specific integrated circuits (ASICs), reduced instruction set computers (RISCs) and/or field programmable gate arrays (FPGAs). Preferably, the present invention is implemented as a combination of hardware and software. Moreover, the software is preferably implemented as an application program tangibly embodied on a program storage device. The application program may be uploaded to, and executed by, a machine comprising any suitable architecture. Preferably, the machine is implemented on a computer platform having hardware such as one or more central processing units (CPU), a random access memory (RAM), and input/output (I/O) interface(s). The computer platform also includes an operating system and microinstruction code. The various processes and functions

described herein may either be part of the microinstruction code or part of the application program (or a combination thereof), which is executed via the operating system. In addition, various other peripheral devices may be connected to the computer platform such as an additional data storage device and a printing device.

5 It is to be further understood that, because some of the constituent system components and method steps depicted in the accompanying figures are preferably implemented in software, the actual connections between the system components (or the process steps) may differ depending upon the manner in which the present invention is programmed. Given the teachings herein, one of ordinary skill in the related art will be
10 able to contemplate these and similar implementations or configurations of the present invention.

CLAIMS:

1. A method for enhanced login, said method comprising:

determining if a user is attempting to login to a particular account;

performing analysis on said user's passwords if the user is not attempting

to login to said particular account;

determining is it is time to change a password on said particular account, if said user is attempting to login to said particular account;

suggesting alternative passwords to said user based on said password analysis; and

performing a login procedure.

2. The method according to claim 1, wherein said password analysis further comprises:

sorting said user's passwords into lists by multiple criteria;

analyzing said lists for patterns; and

preparing recommendations for alternative passwords for changing said password.

3. The method according to claim 2, wherein said multiple criteria include at least, length, special characters, capital letters, lower case letters, keywords and recurring character strings.

4. The method according to claim 1, wherein said login procedure further comprises:

initializing a threshold;

initializing a login attempt counter;

prompting said user for said password for said particular account;

accepting said user's password for said particular account;

incrementing said login attempt counter;

recording details of said login attempt;

determining if said password for said particular account is correct;

determining if said password for said particular account was auto-filled or there was a recent login attempt, if said password for said particular account is correct;

allowing said user to login and access said particular account if both said third and said fourth determining acts are positive;

denying said user access to said particular account if said fourth determining act is negative;

5 incrementing said threshold;

determining if said login attempt counter is greater than said threshold, if said password for said particular account is not correct;

initializing a timer;

10 denying said user access to said particular account for a pre-determined period of time if said login attempt counter is greater than said threshold;

determining if said timer is greater than said pre-determined period of time; and

incrementing said timer if said timer is less than said pre-determined period of time.

15

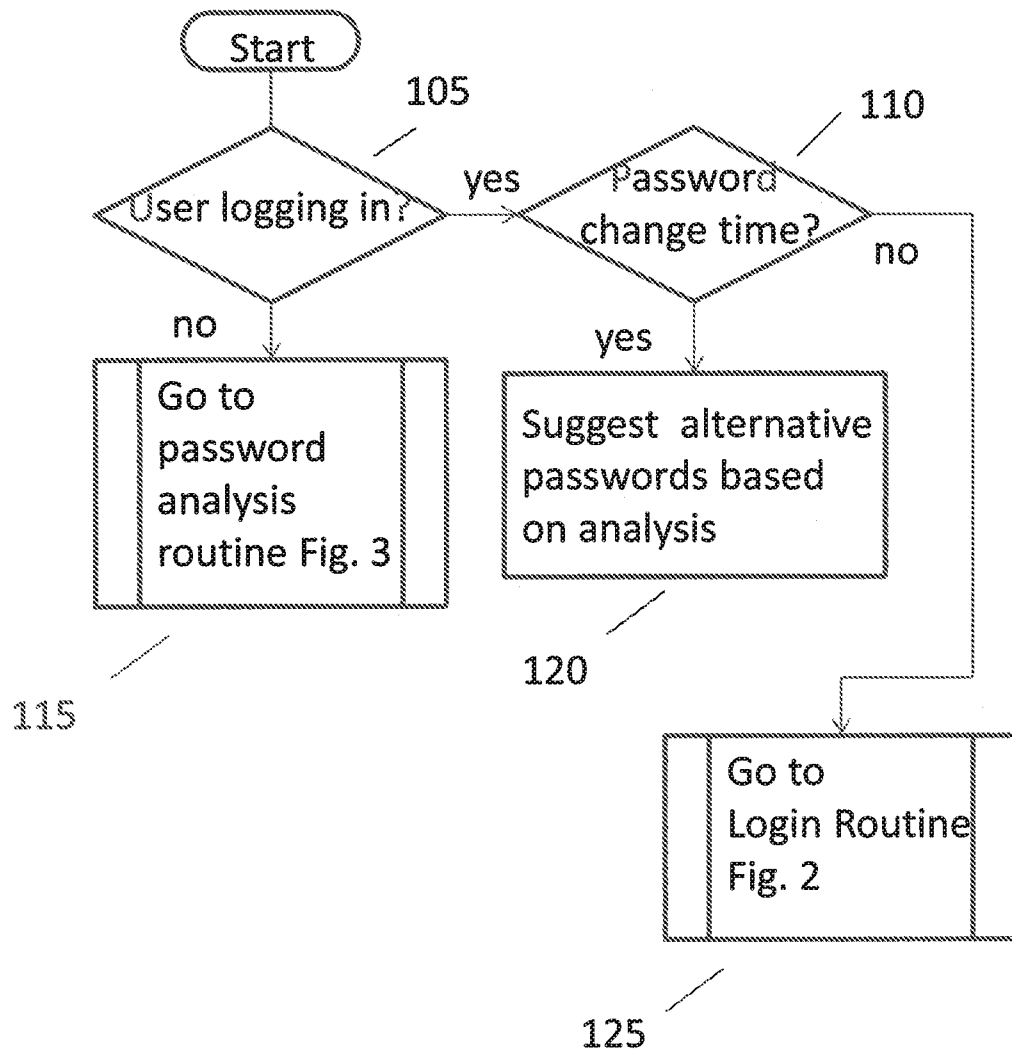


Fig. 1

2/3

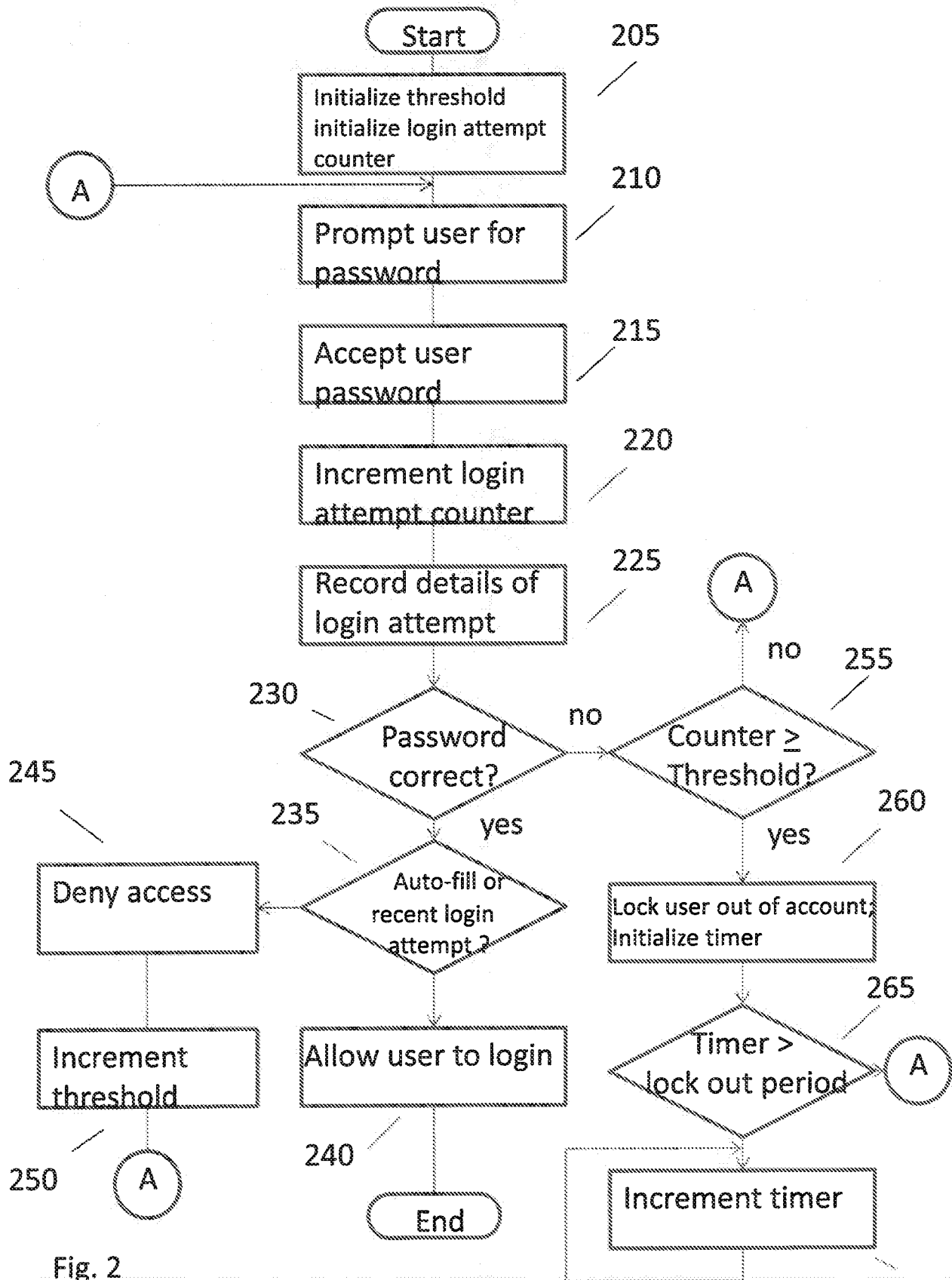


Fig. 2

270

3/3

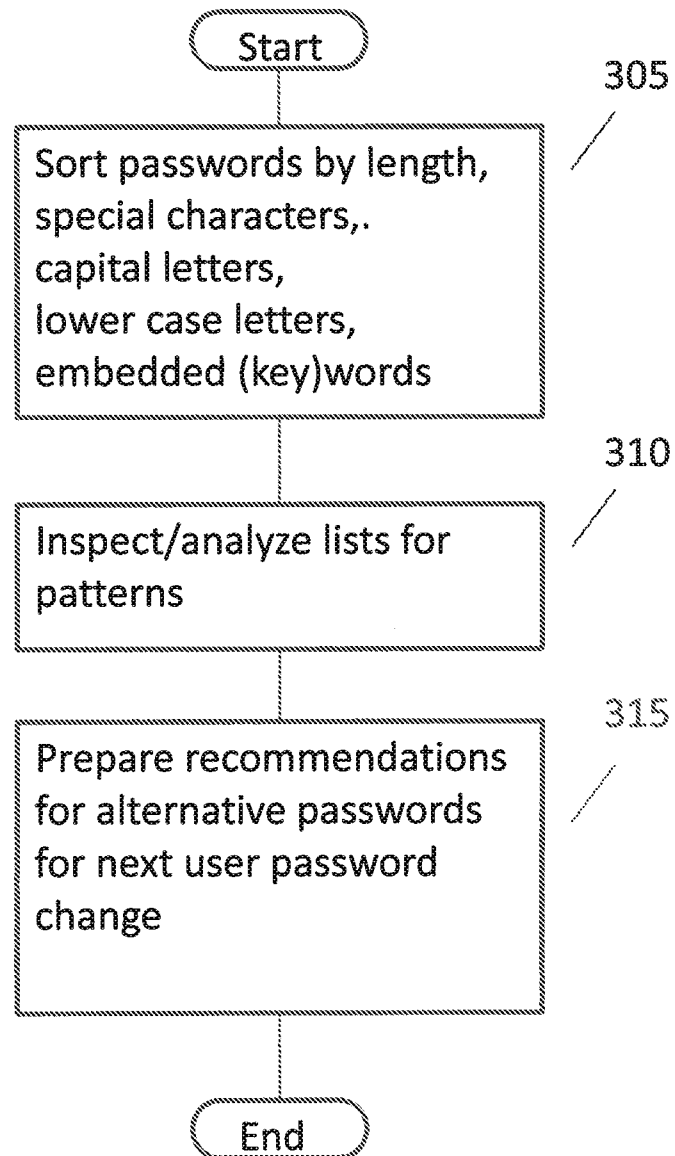


Fig. 3

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2012/065079

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/46 G06F21/31
ADD.

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)

G06F

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)

EP0-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2009/150677 A1 (VEDULA SRINIVAS [US] ET AL) 11 June 2009 (2009-06-11) paragraphs [0005], [0013] - [0027], [0031] - [0040], [0052] -----	1-3
A	US 2004/168068 A1 (GOAL PATRICK M [US] ET AL) 26 August 2004 (2004-08-26) paragraphs [0002], [0006], [0007], [0010], [0011], [0028] - [0037] figure 4 -----	1-3
A	EP 2 386 973 A1 (THOMSON LICENSING [FR]) 16 November 2011 (2011-11-16) paragraphs [0007], [0023] - [0027], [0032], [0035], [0038], [0054] - [0057] figures 2, 3 ----- -/--	1-4



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

19 June 2013

Date of mailing of the international search report

03/07/2013

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Volpato, Gian Luca

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2012/065079

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/177272 A1 (WALTERS GLEN R [US]) 9 September 2004 (2004-09-09) paragraphs [0008] - [0012], [0020] - [0022], [0026], [0028], [0029] figure 2 -----	1-3
X	US 2008/072283 A1 (RELYEA ROBERT [US] ET AL) 20 March 2008 (2008-03-20) paragraphs [0005], [0014], [0020] - [0029] figure 2 -----	4
A	US 2003/229791 A1 (DE JONG EDUARD [US]) 11 December 2003 (2003-12-11) paragraphs [0011], [0022], [0072], [0085] figures 3, 6 -----	4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2012/065079

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2009150677 A1	11-06-2009	NONE	
US 2004168068 A1	26-08-2004	NONE	
EP 2386973 A1	16-11-2011	CN 102884534 A	16-01-2013
		EP 2386973 A1	16-11-2011
		EP 2569725 A1	20-03-2013
		US 2013067554 A1	14-03-2013
		WO 2011141388 A1	17-11-2011
US 2004177272 A1	09-09-2004	NONE	
US 2008072283 A1	20-03-2008	NONE	
US 2003229791 A1	11-12-2003	AU 2003245304 A1	22-12-2003
		US 2003229791 A1	11-12-2003
		WO 03104951 A2	18-12-2003

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/065079

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-3

Method for performing password analysis

2. claim: 4

Method for performing a login procedure
