



(51) International Patent Classification:

G06F 21/31 (2013.01) G06F 21/34 (2013.01)
G06F 21/32 (2013.01)

(21) International Application Number:

PCT/US2016/018578

(22) International Filing Date:

19 February 2016 (19.02.2016)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

62/176,485 19 February 2015 (19.02.2015) US

(71) Applicant: **CARNEGIE MELLON UNIVERSITY**
[US/US]; 5000 Forbes Avenue, Pittsburgh, PA 15213
(US).

(72) Inventors: **HAYASHI, Eiji**; 5030 Centre Avenue, #851,
Pittsburgh, PA 15213 (US). **HONG, Jason**; 5329 Darling-
ton Road, Pittsburgh, PA 15217 (US).

(74) Agent: **CARLETON, Dennis, M.**; Fox Rothschild LLP,
997 Lenox Drive, Bldg #3, Lawrenceville, NJ 08648 (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).

Published:

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

(54) Title: UNIFIED AUTHENTICATION MANAGEMENT SYSTEM

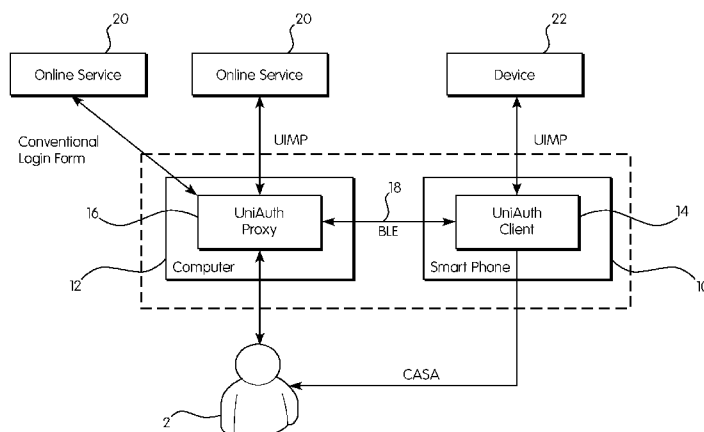


FIG. 1

(57) Abstract: A system for automatic authentication of a user to allow access to websites and physical devices which provides tiered levels of security and defines an API protocol for exchange of authentication credentials.

UNIFIED AUTHENTICATION MANAGEMENT SYSTEM

Related Applications

- [0001]** This application claims the benefit of U.S. Provisional Patent Application Serial No. 62/176,485, filed February 19, 2015.

Background of the Invention

- [0002]** Reliable authentication is an essential requirement for secure systems. Passwords are the most common form of authentication today; however, a great deal of past research has shown that people have difficulties in memorizing and managing their passwords in a reliable and secure manner. For instance, people tend to choose simple passwords, re-use passwords among multiple accounts, and fall for phishing attacks.
- [0003]** When passwords were first introduced in the 1960s, computers were a scarce resource, and experts only had to manage a few passwords. However, the security landscape has changed dramatically: there are far more users, each managing numerous passwords, using systems with different security requirements, and facing new kinds of attacks. Given this context, there are people claiming that passwords are fundamentally broken. However, it is argued that passwords are still good enough if used appropriately. If passwords are, for instance, long, randomly generated, unique among multiple accounts, and updated periodically, we can address many of the problems described above. Better tools that can help people manage and use passwords securely and appropriately are needed.

- [0004]** The computing landscape is also changing as well. More and more physical objects are equipped with computation, storage, sensing, and network capabilities. These smart devices often need some sort of user identification/ authentication; nevertheless, many physical objects do not have input capabilities suitable for password-based authentication (e.g. typing and pointing).
- [0005]** There are many password management applications. For example, all major web browsers have a built-in password management feature storing account information and automatically filling in this information later. There are also many standalone apps for computers and smartphones for managing credentials. While these apps help users store credentials, users often still have to do many steps manually to keep information in password managers consistent with that in online services.
- [0006]** There are also many research systems that manage passwords. For example, PassPet and PwdHash are browser extensions that dynamically generate site-specific passwords from a single master password and additional information such as user-chosen name for web sites or a domain name. While these systems do not store passwords, it is challenging to accommodate site-specific password composition policies. WebTicket embeds a credential in an encrypted QR code that can be printed or stored on smartphones. Some systems utilize mobile devices in the context of user authentication. Phoolproof Phishing is an authentication scheme designed to prevent phishing attacks, key loggers, and other kinds of malware. Gray is a physical access control system using smartphones. Nymi announced a wearable device that can manage authentication to physical devices, however, it requires other devices to support their own communication protocol. This makes its wide adoption challenging.

[0007] Other authentication systems depend on physical devices. RSA SecurID is a device for two-factor authentication. Users type their personal identification number as well as a number shown on the a hardware token to be authenticated. However, the tokens require server-side modifications. Furthermore, the deployment cost of the tokens is relatively high. As a result, the tokens tend to be used only for accounts with very high security requirements such as bank accounts. Single sign-on systems also try to address authentication problems. OAuth is one of the most commonly used single sign-on standards. With OAuth, a user can log into third party websites using an account at OAuth service providers such as Facebook and Google. However, involving multiple parties makes the system difficult to understand for users.

[0008] The FIDO alliance is a group of companies seeking to replace password-based authentication with public-private key pair based authentication. To log into an online account, a user first authenticates himself to his FIDO device with biometrics. Then, the device and a service complete authentication using a pre-shared public-private key pair. Although this approach could be more secure than password-based authentication, it requires server-side modifications and adoption of FIDO devices at the same time. Additionally, it has to meet a critical mass to be useful in practice.

[0009] There are many known password alternatives. It has been found that most schemes do better than passwords on security, however, every proposed scheme did worse than passwords on deployability, which is the biggest barrier for adoption.

Summary of the Invention

[00010] The present invention was designed to address these challenges. There are two core components. The first is that a single primary device (the “authenticator”) can be used to manage all of the procedures related to user authentication, including account creation, logging in, sharing accounts, etc. Recent changes in technology make this possible. In the United States, for example, smartphone penetration broke 65% in mid-2014, and it is very likely that in the future, everyone will have some kind of smart device that can be used as an authenticator. Second, smart devices can use onboard sensors to help strengthen authentication by using multiple factors to check that it is indeed the legitimate user who is trying to login, as well as improve the user experience by making authentication fast in safe situations, and making it more reliable in riskier ones.

[00011] The approach presented herein could help mitigate well documented problems with passwords. For example, people would no longer have to create passwords, memorize them, or type them in. In addition, it offers new kinds of protection through sensors and behavioral models, offers a transition path for stronger authentication, allowing the use of passwords in early stages of adoption, and be transparently replaced with stronger methods once a large fraction of users and services adopt. Lastly, the invention facilitates authentication for the “Internet of Things.”

[00012] The present invention describes the design and evaluation of a unified authentication management system to streamline credential management in password-based authentication to devices and web services. This system stores all credentials (e.g. user names and passwords) on users’ smart devices (including, but not limited to smartphones such as the iPhone) and provides credentials to laptops/desktops seamlessly. In one

embodiment, an authenticator for iPhone and Mac was designed and implemented, allowing the evaluation of user interactions and experiences in ecologically valid conditions.

[00013] In the system presented herein, a user first authenticates himself to a client, typically a smartphone or other smart device. The client can then authenticate to other services and devices on the user's behalf. The present invention was implemented with an example iPhone prototype and embodies features not supported in existing password managers, such as tiered and location-aware lock control, authentication to laptops via a physical knocking, and seamless storage of credentials on smartphones.

Brief Description of the Drawings

[00014] Fig. 1 is a top-level block diagram of one embodiment of the invention.

[00015] Fig. 2 is a block diagram showing the interaction between a user device and a computer.

[00016] Fig. 3 is a smartphone screen shown the tiered access approach.

[00017] Fig. 4 shows a smartphone screen allowing the entry of a password to unlock a secured tier of accounts.

[00018] Fig. 5 shows a smartphone screen allowing the saving of access information for an online service.

[00019] Fig. 6 shows a smartphone screen allowing viewing and editing of account access information.

[00020] Fig. 7 shows a screen on the computer of the user allowing viewing and editing of account access information.

[00021] Fig. 8 shows a smartphone screen providing the user a status message that account information has been accessed.

Detailed Description of the Invention

[00022] The goal of the present invention (referred to herein as the “unified authentication framework” or the “framework”) is to remove users from the credential management processes by offering machine-readable interfaces for authentication. Using these interfaces, the framework authenticators can handle all tasks related to credential management, such as account creation, authentication, password updates, and account termination with minimum intervention by the user. Furthermore, the framework provides features not supported in existing password management systems, such as streamlined credential management and authentication to physical devices.

[00023] Users need only authenticate themselves to their authenticators (with the assistance of sensors) to access their accounts for both online services and physical devices. This invention describes the process of managing account information with one device.

[00024] The system consists of three components: a universal identity management protocol (UIMP), clients, and proxies. UIMP is a set of application programming interfaces (APIs) that enables the clients to communicate with services to complete tasks related to credential management. For online services, UIMP is implemented as a set of RESTful APIs. The observation here is that many aspects of authentication are only human-readable or require manual intervention. Examples include password composition policies, password reset mechanisms, account creations, and logins. UIMP creates a protocol that machines can understand and support. When websites and other devices

implement UIMP, then any clients can interact with supported websites and devices with minimum human intervention. Because UIMP is intentionally designed in the same way as online services interact with users via html forms, a thin wrapper can be implemented on existing servers to make online services compatible with UIMP.

- [00025]** UIMP Clients (or “clients”) are authenticators that manage users’ credentials using UIMP. The client can be implemented on many different types of smart devices, e.g., smartphones or wearables, such as a smart watch. While the invention will be explained using a smartphone as the primary example, the invention is not meant to be limited to implementations using a smartphone.
- [00026]** The client communicates with services through UIMP on behalf of users. For instance, when a user wants to sign up for a service, the client can create an account by generating a strong and unique password that complies with any required password policies, providing requested user information (such as email addresses), and storing the credentials in a secure manner. When the user wants to authenticate to a service (or a physical device), the client automatically provides a credential. To address the bootstrapping problem, the client should also work with services that do not support UIMP (e.g. using heuristics to find the password field in a web page). Their functionalities are limited to ones that are feasible without UIMP. Nevertheless, users can get immediate benefit by using the client with services that do not support UIMP.
- [00027]** By having a smart device manage authentication, the burden of authentication from end-users to their devices can be shifted. However, there is a security risk in having one’s smart device stolen. To address this, the client will protect the user’s credentials using a set of onboard sensors. For example, for places with reasonable physical security (e.g.,

physical locks) like work and home, the client can operate focusing more on convenience, while for places that the user rarely or never goes to, or for situations that the system deems risky, the client can operate in a high security mode. Similarly, the New York Times web site may only need a low level of assurance, whereas the user's bank account may warrant a high level of certainty that the user is indeed the legitimate owner of the account.

[00028] UIMP Proxies (or “proxies”) are applications typically running on the user's computer(s) that mediate the communication between browsers and the client (since web browsers cannot directly communicate with clients).

[00029] Although the system attempts to let one device (i.e., the device running the client) handle various tasks related to credential management, its underlying user authentication is based on user IDs and passwords. The invention describes this design choice for backward compatibility with existing services, as well as to allow partial adoption of in its early adoption stage. That is, users can use clients, without servers having to change anything. However, as servers adopt the system, clients can gain more functionality and security (e.g. using approaches stronger than passwords).

[00030] The present invention describes a client and a proxy that allows using them with existing online services. This is essentially equal to the early adoption stage, where clients and proxies are deployed without UIMP-compatible services.

[00031] An exemplary embodiment is shown in Fig. 1. A combined suite is comprised of client 14 running on an smartphone 10 and a proxy 16 on a computer 12, All account information is stored in a database in client 14. Proxy 16, as shown in Fig. 2, consists of extensions 16a for whichever browser 13 user 2 chooses to use and an application 16b

that mediates communication between the browser extension 16a and the client 14, as well as provides an interface that allows users to manage account information stored in their smartphones 10 using computer 12.

[00032] Proxy 16 running on computer 12 connects with the client 14 running on smartphone 10 via a low energy link 18, preferably a Bluetooth Low Energy (BLE) link, and connects with the browser extensions 16a using a local web server 13. For security, user 2 can set the smartphone's BLE 18 to have a range of 1 to 15 meters. For both connections, mutual authentication is performed using a pre-shared key to prevent illegitimate connections. Once connection 18 is established, it is kept until smartphone 10 goes out of range or the application 16b running on computer 12 stops. All data exchanges after the mutual authentication are encrypted using AES-128. Because online services 20 do not, at the time of this writing, support UIMP, current implementations only support storing/auto filling credentials for online services 20 and computer 12.

[00033] Note that proxy 16 may also run on user device 10, for instance, when the user accesses a web site using a web browser running on user device 10 and desires automatic authentication.

[00034] **Tiered and Location-Aware Access Control** - In terms of access control, most existing password management systems have all-or-nothing access, i.e., allow access to all accounts or do not allow access to any accounts stored in the systems. However, it is difficult to satisfy different security and usability requirements for different accounts with this approach. To address this challenge, a tiered access control system was adopted.

[00035] Each account, is stored in one of several tiers 30, shown in Fig. 3 as Secure, Standard, and Quick. Each tier has a lock state and can be locked or unlocked independently. Thus, unlocking the Secure tier does not unlock the Standard or Quick tiers. To access account information in a tier, the tier should be in an unlocked state. For instance, if user 2 saved their Amazon account access information in the Standard tier, the Standard tier must be unlocked first to let the invention fill his credential for Amazon on computer 12. One of skill in the art would realize that the number of tiers 30 is a design choice, or may be a user-settable parameter.

[00036] In the preferred embodiment, three tiers have been chosen. In the preferred embodiment, the Standard and Quick tiers are automatically locked and unlocked based on whether users are at *trusted locations* to make account accesses easier. Users can register trusted locations such as homes and workplaces using client 14 in smartphone 10. In the current embodiment, a location is a 100 meter radius from a registered geolocation. Entering a trusted location unlocks the Quick tier automatically. This lets user 2 log into accounts in the Quick tier on their computer 12 without touching their smartphone 10. Exiting a trusted location locks the Quick tier automatically. The Standard tier can be unlocked by typing a master password on smartphone 10, as shown in Fig. 4. Alternatively, a biometric, such as the touch ID on an iPhone, can be used. If this happens at a trusted location, the Standard tier is unlocked until an iPhone exits from the trusted location. The Secure tier can be unlocked for one-time access by typing a master password regardless of location. It gets locked after one of the accounts in that tier is accessed from computer 12. In addition to these options, a user can unlock any tier for a specified period (from five minutes to one day), also as shown in Fig. 3, by typing his master password or

otherwise providing an identification via a biometric, regardless of location. Finally, a user can lock a tier manually at any time.

[00037] Storing and Managing Credentials - When user 2 logs into an account on a web site for the first time, the invention pops up a dialog asking if he wants to save his credentials, as shown in Fig. 5. User 2 can edit the name of the entry and its tier. When “OK” is clicked, the account information is sent to client 14. The account information consists of a user-configured name of the account, a URL, a user ID, a password, and IDs of a user ID field and a password field in a login form. After storing the information client 14 automatically fills the credentials when user 2 accesses the same website later. User 2 can also open a main screen by typing his master password to browse and edit stored account information, as shown in Fig. 7. This allows users to view their user IDs and passwords to log into accounts manually if needed (e.g., when logging into their accounts on foreign computers or when sharing an account with others). User 2 can also browse and edit account information using proxy 16 computer 12, as shown in Fig. 6. To access account information on computer 12, categories that the account information belongs to should be in an unlocked state.

[00038] Logging into Web Accounts and Devices - When user 2 opens a web page with a password field, browser extension 16a, sends the URL to client 14, which then looks up whether a corresponding account is stored for the domain. If an account is stored and its tier is unlocked, client 14 sends a credential to browser extension 16a, which then changes the colors of text fields in the login form to green, indicating that an account was

found in the system. User 2 can double click on one of these fields to fill the credential. If the tier is locked, a dialog asking the user to unlock the tier appears when user 2 double clicks the text fields.

[00039] Users can also log into a device 22, as shown in Fig 1. by physically knocking on the device 22 twice, as if knocking on a door. Alternatively, users can double click the command button. Note that device 22 may be the user's computer 12. This login will typically happen when a user wakes up computer 12 from sleep mode or from a password-protected screensaver. This feature is implemented to let participants experience logging into physical devices with authenticators. When proxy 16 detects either of these cases, it requests that the appropriate client 14 send a password for computer 12. If the credential for computer 12 is stored in client 14 and its tier is unlocked, client 14 sends a password back to proxy 16, and proxy 16 generates key type events to fill a password field and log into computer 12 automatically. Because a pre-shared key is required to establish a connection between smartphone 10 and computer 12, attackers cannot launch replay attack on this process without knowing the pre-shared key.

[00040] When a credential is accessed from proxy 16, client 14 shows a notification message to user 2, as shown in Fig. 8. This notification helps lets a user know that someone accessed the account if user 2 is still in BLE range but not in front of the computer, for example, right after user 2 leave his computer 12.

[00041] The authentication to physical devices 22 can be expanded to any one of a number of devices commonly grouped together under the term "Internet of Things", for example, office doors, bike locks, copy machines, smart appliances, smart lighting systems, smart cars, etc., which have implemented the UIMP protocol.. A user can indicate their desire

to be authenticated by these devices through physically knocking them or by some other means, such as pressing buttons on them or via voice commands.

[00042] Furthermore, this authenticator can be implemented in wearable devices, such as, but not limited to, smart watches. This opens up new potential in user-system interactions. For instance, smart watches can have sensors that detect whether the watches are worn or not. A client 14 on the watch can request a master password when a user wears the watch and keep a tier unlocked until the user takes off the watch in addition to (or instead of) location-based access control implemented in the application and discussed herein. Furthermore, it is also possible to do mutual authentication between devices 22 and client 14 on watches using knocking gestures. Because the knocking pattern can be measured by both device 22 and the watch, we can verify whether user 2 wearing the watch is actually knocking the device by comparing the patterns.

[00043] Additional Features

[00044] *Unified Account Creation* - The system may include a unified account creation feature which provides a way for users to easily create their accounts. When a user visits a UIMP-enabled website for the first time, the system can ask if the user wants to create an account. If so, it displays a dialog with input fields for all information requested by the website such as a name and an email address. These fields are prepopulated with personal information stored in client 14, along with a randomly generated password. Also, if the user prefers, the password can be overwritten with a manually created, user-generated password. Then, when the user clicks the OK button, the system communicates with the website to create an account and store the account information in client 14. This is useful

because in existing account creation procedures, a user has to take extra steps to save credentials in password managers after creating an account. However, with UIMP, password managers can create accounts and save credentials seamlessly.

Managing Password Updates - Users can receive a reminder after a specified time since their last password update. Users can select the period (e.g., 3 months), or it can be specified by a service if periodic password updates are enforced. When receiving a reminder, users can manually update a password in the invention via UIMP, or let the invention automatically update a password and notify afterward.

[00045] The invention has been presented using exemplary hardware and software implementations, but it should be realized by one of skill in the art that alternate implementations may be used without deviating from the intended scope of the invention, which is outlined in the claims below.

We Claim:

1. A system for providing automatic user authentication, comprising:
 - a user device running an authentication client;
 - a database of authentication credentials, accessible by said client;
 - wherein said authentication client:
 - receives requests for authentication credentials;
 - retrieves the requested authentication credentials from said database; and
 - returns said requested authentication credentials to the requester.
2. The system of claim 1 wherein said authentication credentials are secured and further wherein said authentication client verifies, via a security protocol, that said authentication credentials may be returned.
3. The system of claim 2 wherein said if said user device is within a predetermined distance of pre-set geolocation.
4. The system of claim 3 wherein said pre-set geolocation is settable by a user of said user device.
5. The system of claim 2 wherein said security protocol allows authentication credentials to be returned after a user enters a password or a biometric.

6. The system of claim 5 wherein said security protocol disallows returning of authentication credentials after one set of authentication credentials has been returned.
7. The system of claim 4 wherein said security protocol disallows returning of authentication credentials when said user device is travels a predetermined distance from a pre-set geolocation.
8. The system of claim 1 further comprising a wireless link between said user device and a second computer making a request for authentication credentials.
9. The system of claim 8 wherein said security protocol disallows returning of authentication credentials when said wireless link with said second computer is lost.
10. The system of claim 2 wherein said security protocol disallows returning of authentication credentials a pre-determined time after said authentication client verifies that said authentication credentials may be returned.
11. The system of claim 10 wherein said pre-determined time is settable by a user of said user device.
12. The system of claim 8 wherein said authentication client accepts requests for authentication credentials when a web site requiring authentication of the user is accessed

from said second computer.

13. The system of claim 12 wherein software, running on said second computer, receives requests from a website for authentication credentials via a predefined protocol and makes said request via said wireless link to said authentication client for said authentication credentials for said website.

14. The system of claim 12 wherein software, running on said second computer, recognizes when a website accessed by a user of said second computer requires authentication credentials and makes said request via said wireless link to said authentication client for authentication credentials for said website.

15. The system of claim 1 further comprising a wireless link between said user device and a physical device making a request for authentication credentials.

16. The system of claim 15 wherein said physical device is any device requiring user authentication and capable of communicating with said user device via said wireless link.

17. The system of claim 16 further wherein said authentication client receives requests for authentication credentials from said physical device via a predefined protocol.

18. The system of claim 16 wherein said request from said physical device is initiated via an action of a user.

19. The system of claim 18 where said action is a knocking motion on said physical device.

20. The system of claim 18 wherein said knocking motion may be in a pre-defined pattern recognized by said physical device.

21. The system of claim 19 wherein said physical device is a second computer.

22. The system of claim 1 wherein said requests for authentication credentials and return of authentication credentials are embodied in a defined API.

23. The system of claim 1 wherein said database stores said authentication credentials in an encrypted form.

24. The system of claim 1 wherein said authentication credentials are returned in an encrypted form.

25. The system of claim 1 wherein said authentication client can generate new passwords:
when a request to update an existing authentication credential is received, or
when a request to add a new authentication credential is received.

1/8

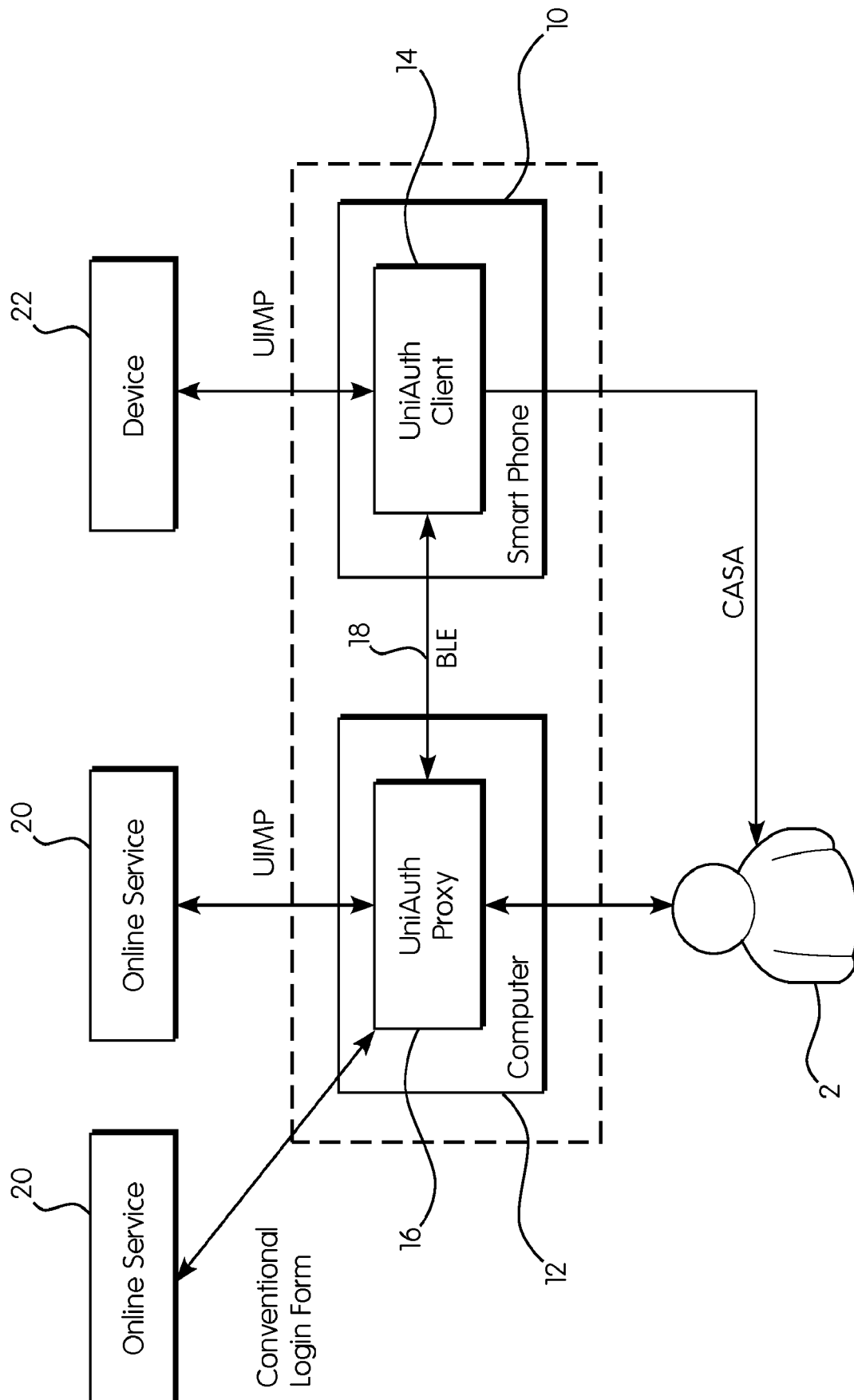


FIG. 1

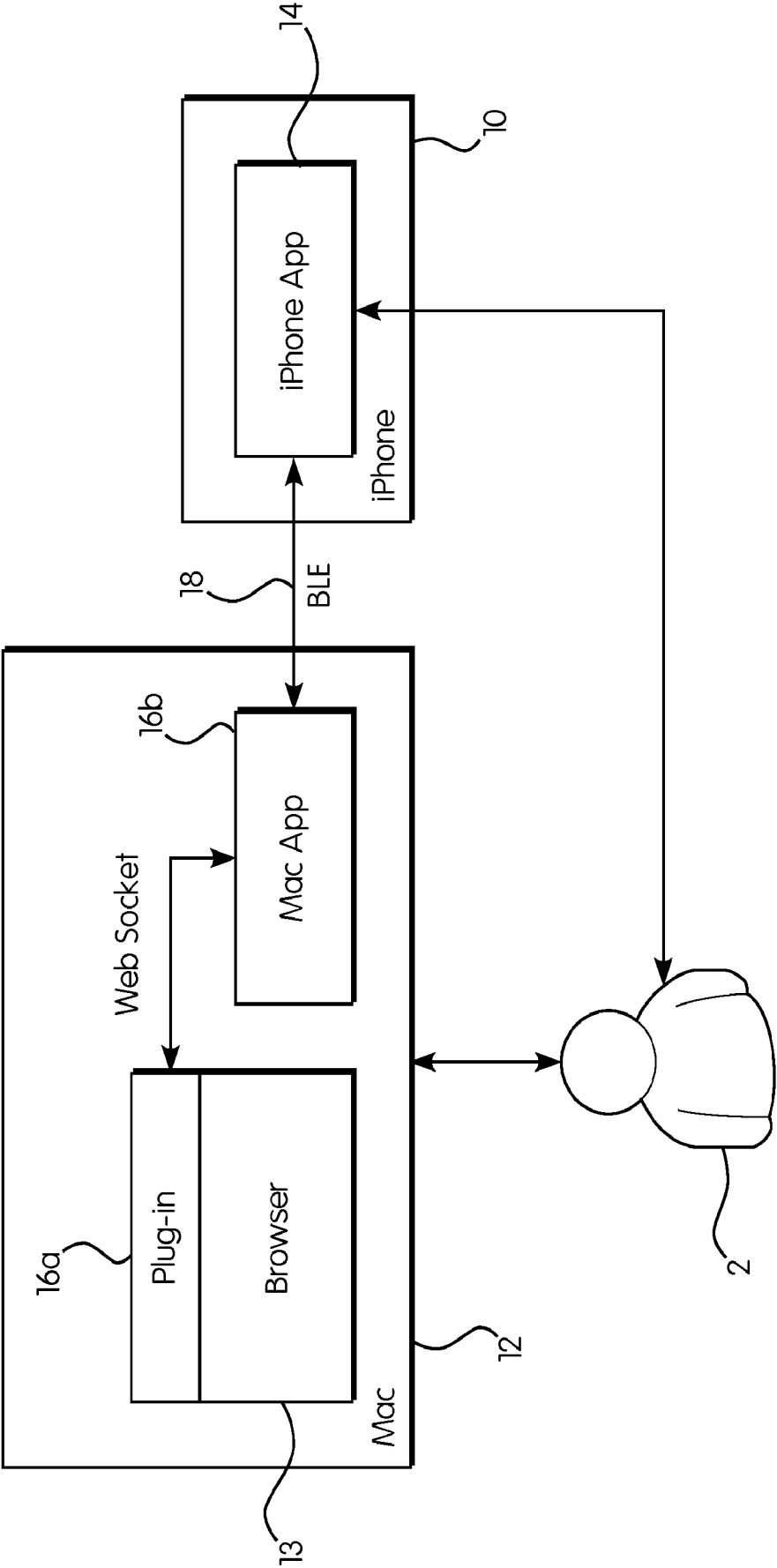


FIG. 2

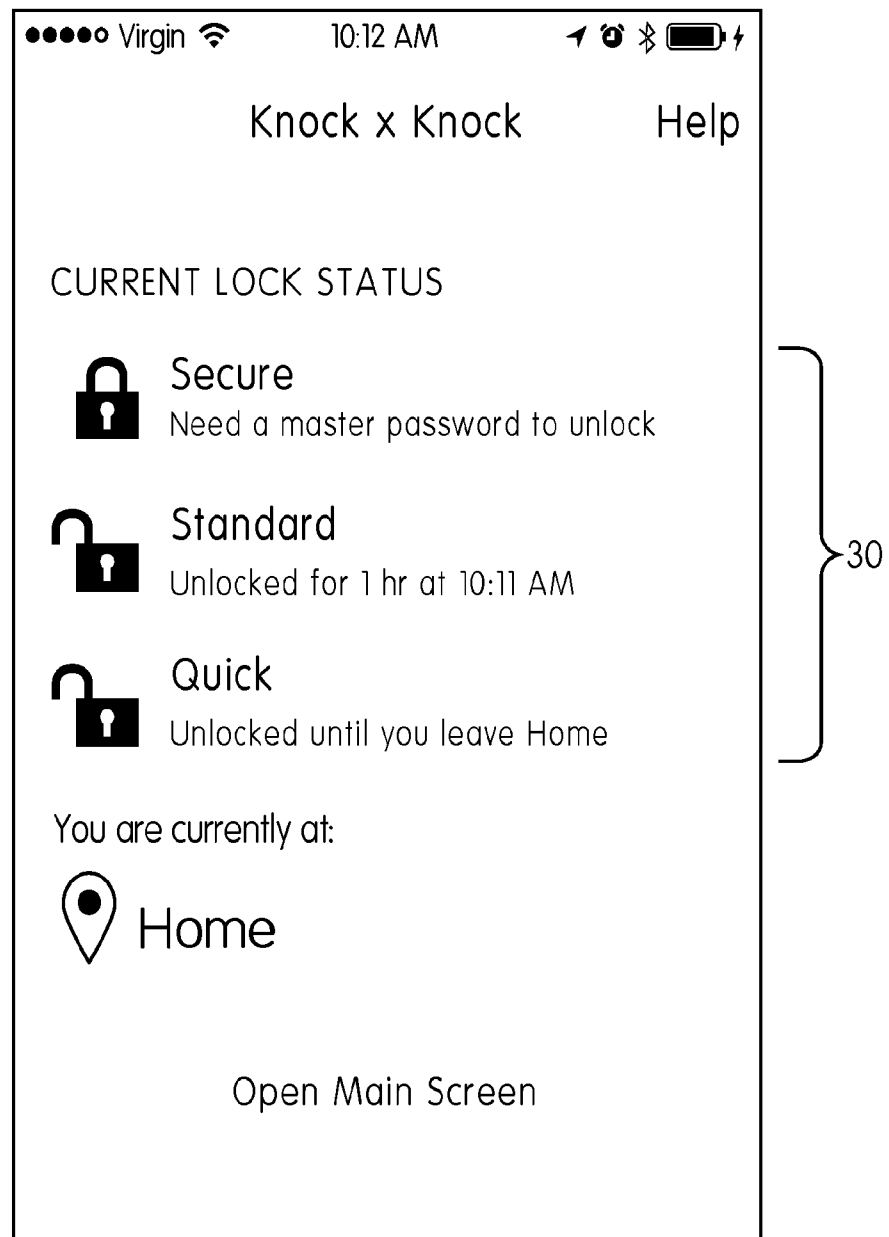


FIG. 3

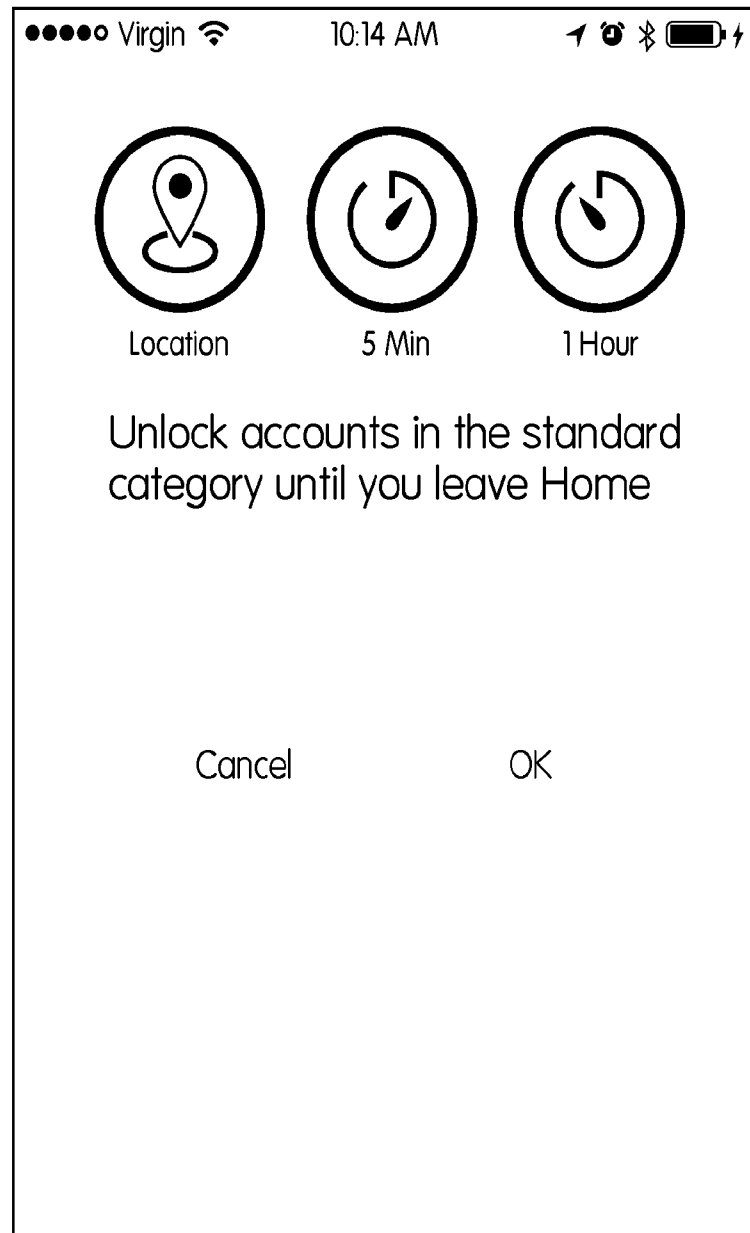


FIG. 4

○ ○ ○ Knock x Knock

Store the login to your iPhone?

Amazon.com Sign In

Category Secure **Standard** Quick

Never Not for Now Save

FIG. 5

6/8

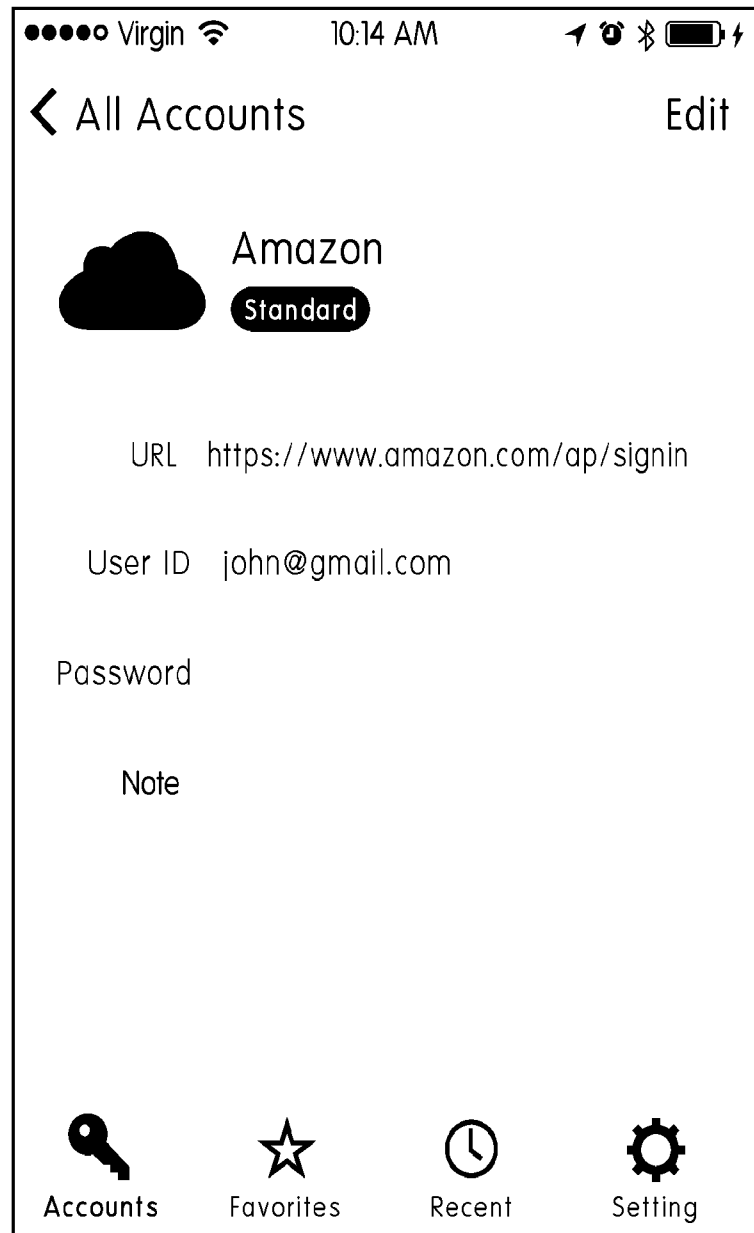


FIG. 6

7/8

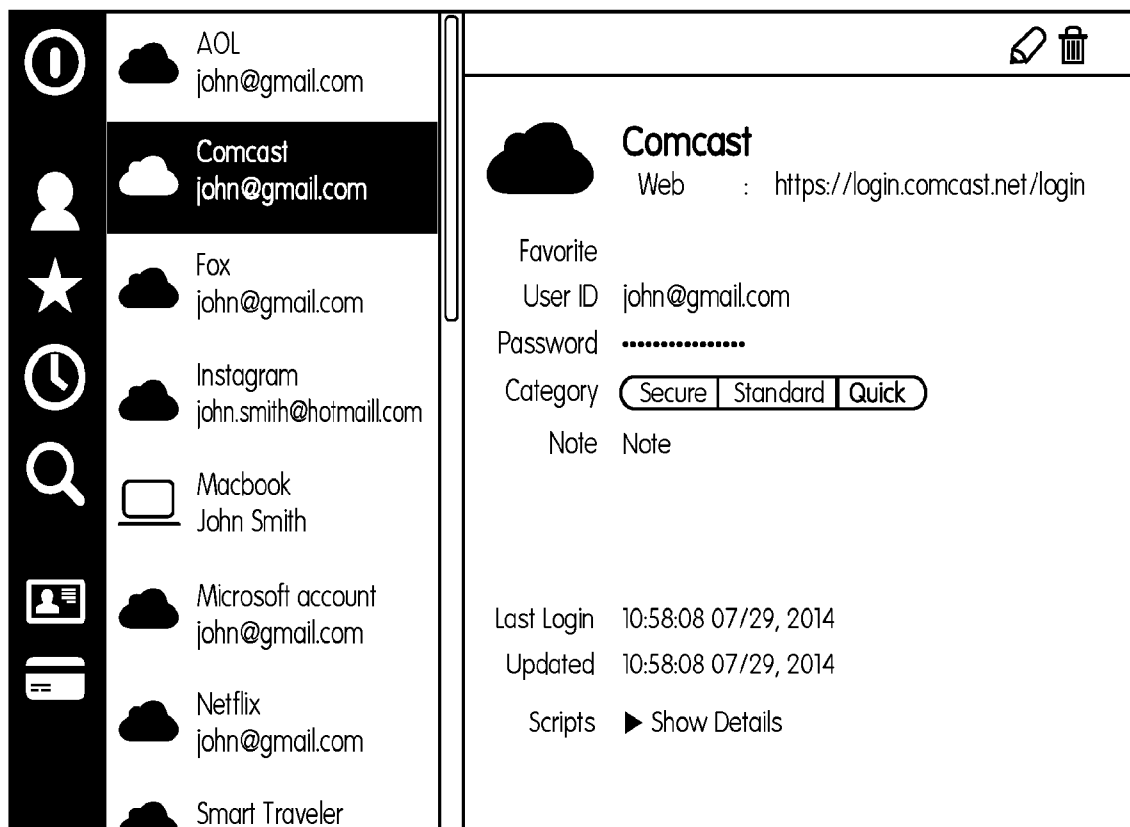


FIG. 7

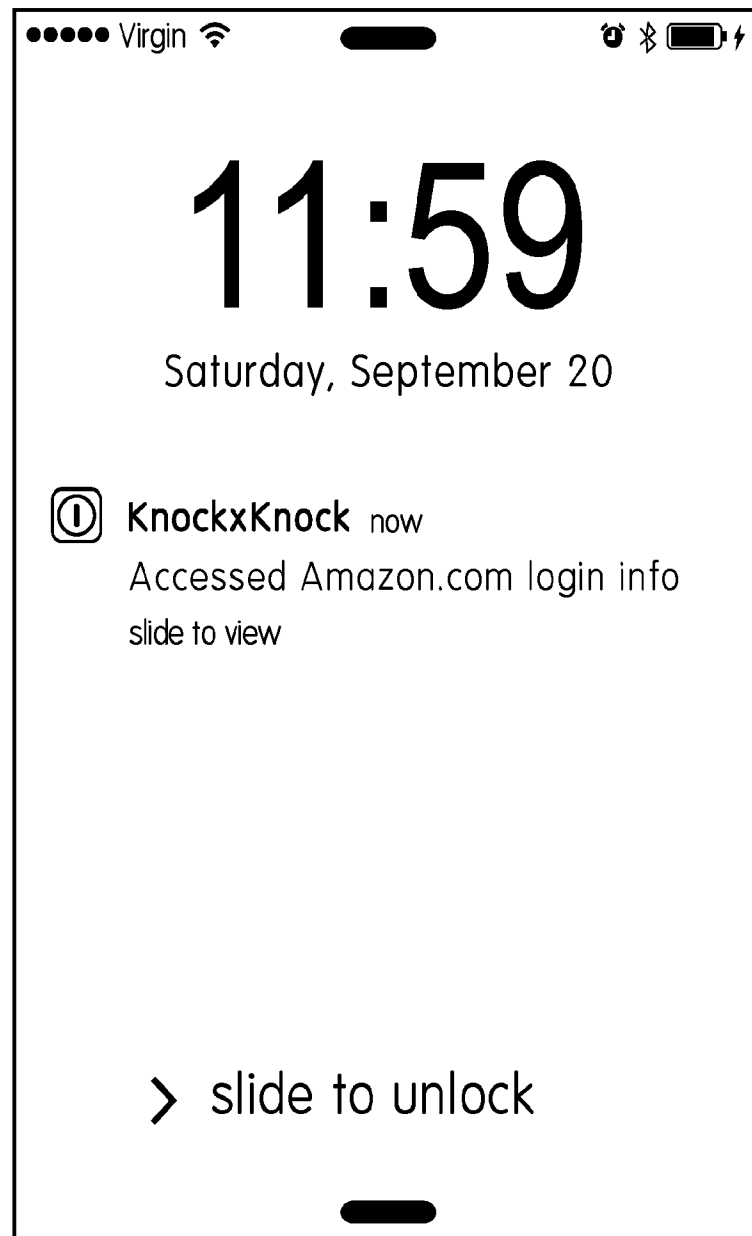


FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US16/18578

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - G06F 21/31, 21/32, 21/34 (2016.01)

CPC - G06F 21/31, 21/32, 21/34

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(8) - G06F 21/30, 21/31, 21/32, 21/34 (2016.01)

CPC - G06F 21/30, 21/31, 21/32, 21/34; H04L 29/06; H04W 12/06, 12/08

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)

PatSoor (US, EP, WO, JP, DE, GB, CN, FR, KR, ES, AU, IN, CA, RU, AT, CH, TH, BR, PH, SE, NO, DK, FI, BE, NL, LU, Other Countries (INPADOC)); EBSCO; IEEE/IEEEExplore; Google/Google Scholar; Keywords: configure, setting, password, passcode, mobile, phone, authenticate, authorize, manager, wireless

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2013/0268767 A1 (SCHRECKER, S.) 10 October 2013; Paragraphs [0011], [0012], [0019], [0028], [0029], [0049], [0076]	1-10, 12-25 ----- 11
Y	EP 2498529 A1 (TRUSTED LOGIC MOBILITY SAS) 12 September 2012; Paragraphs [0023], [0027]	11
A	US 2012/0266220 A1 (BRUDNICKI, D. et al.) 18 October 2012; Entire Document	1-25
A	EP 2355028 A1 (SECURENVOY LIMITED) 10 August 2011; Entire Document	1-25



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

5 April 2016 (05.04.2016)

Date of mailing of the international search report

02 MAY 2016

Name and mailing address of the ISA/

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-8300

Authorized officer

Shane Thomas

PCT Helpdesk: 571-272-4300
PCT OSP: 571-272-7774