US 20060020816A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2006/0020816 A1

Campbell (43) Pub. Date: Jan. 26, 2006

(54) METHOD AND SYSTEM FOR MANAGING AUTHENTICATION ATTEMPTS

(76) Inventor: John Robertson Campbell, Ottawa (CA)

Correspondence Address:
TORYS LLP
79 WELLINGTON ST. WEST
SUITE 3000
TORONTO, ON M5K 1N2 (CA)

(21) Appl. No.: 11/172,899

(22) Filed: Jul. 5, 2005

Related U.S. Application Data

(60) Provisional application No. 60/585,845, filed on Jul. 8, 2004.

Publication Classification

(51) Int. Cl.
H04L 9/00 (2006.01)

(52) U.S. Cl. 713/182

(57) ABSTRACT

The present invention provides, in certain embodiments, identification and management of authentication attempts using having a real time communication channel with the end user that is separate from the channel being used for authentication. An example is where Internet users are a) identified by their cell phone numbers and may b) access the internet from many different physical locations. Aspects of the invention allow for authentication issue detection to be extended, utilizing the separate communication channel to communicate directly with the user. This can allow the authenticating authority to take proactive action on a more automatic basis with the ability to distinguish fraud or abuse attempts from user problems aided by the separate communication channel.

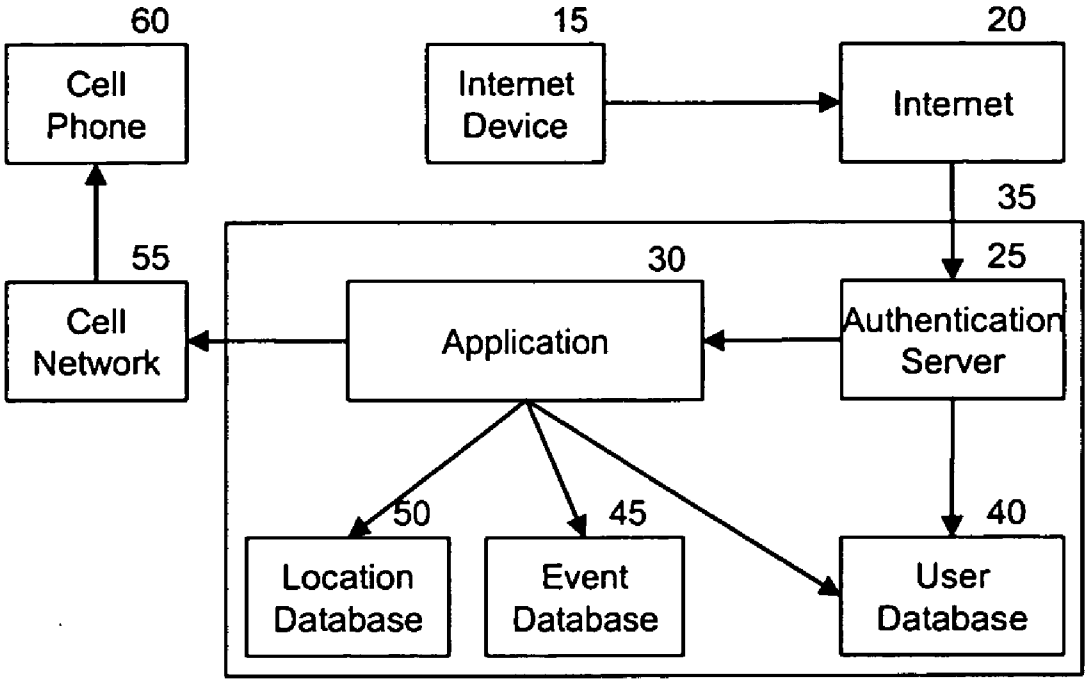


Figure 1

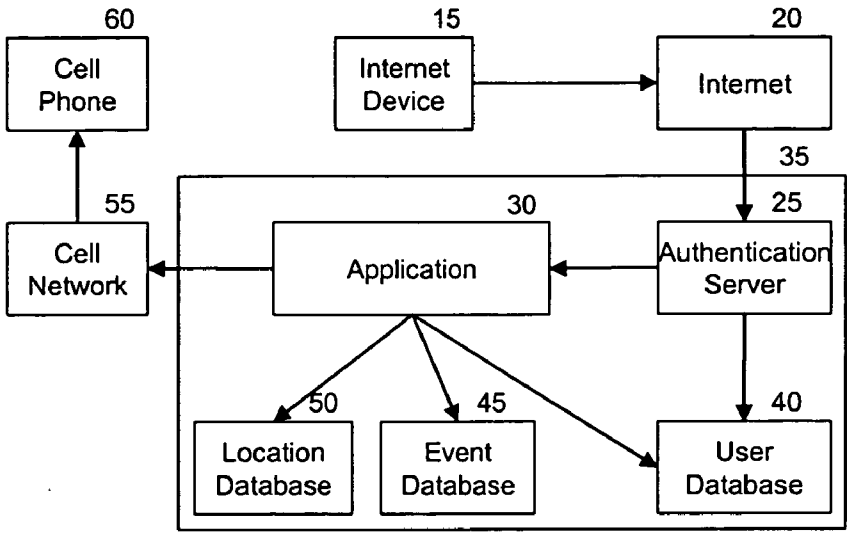


Figure 2

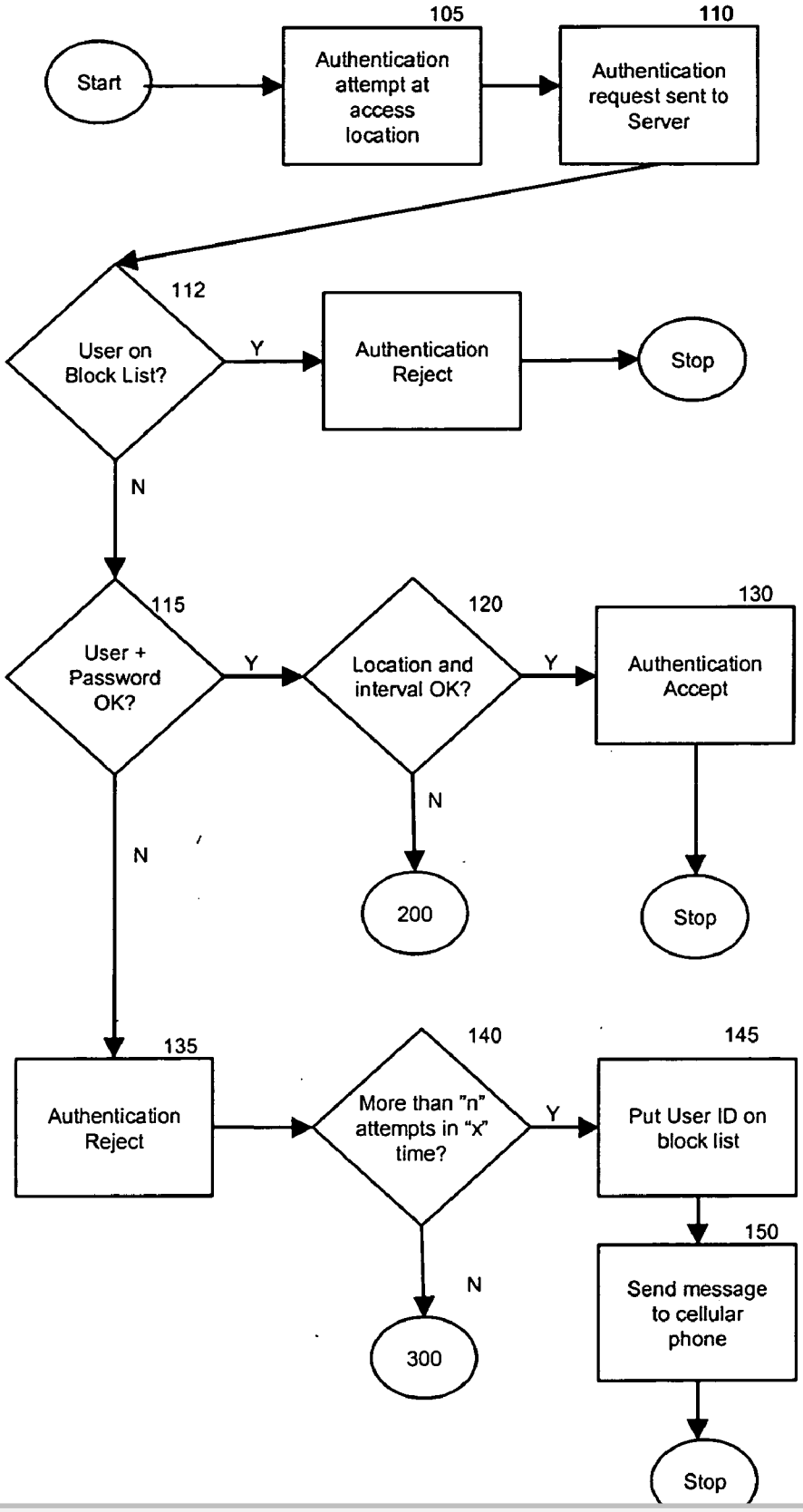
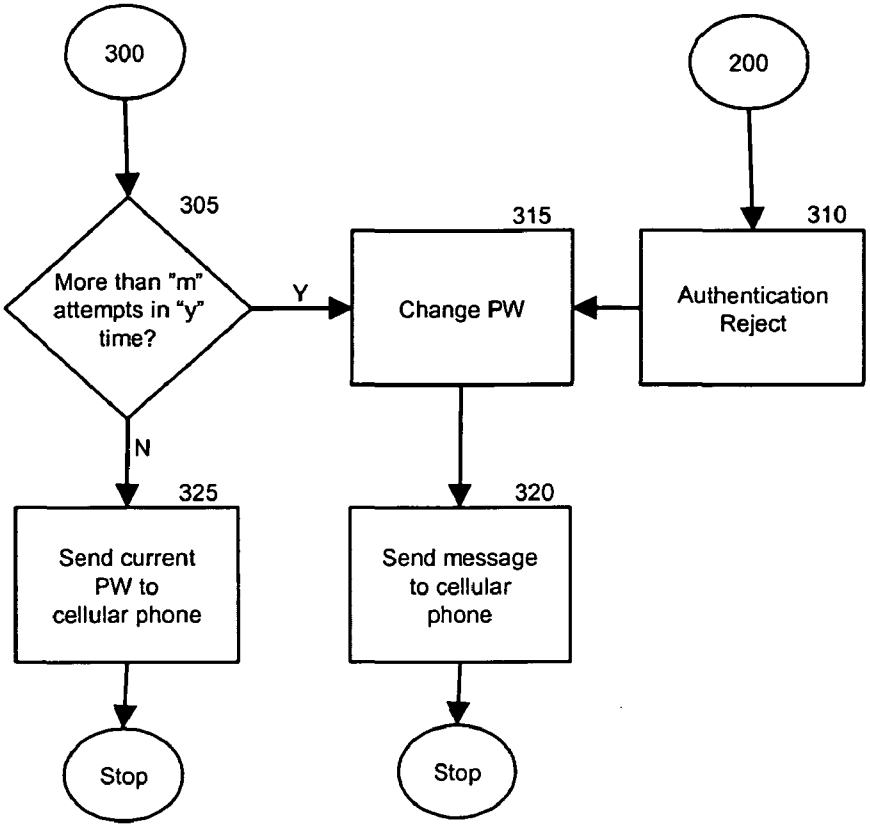


Figure 3



METHOD AND SYSTEM FOR MANAGING AUTHENTICATION ATTEMPTS

PRIORITY CLAIM

[0001] The present application claims priority from U.S. Provisional Patent Application No. 60/585,845, filed Jul. 8, 2004, the contents of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002] The present invention relates generally to computer authentication and more particularly relates to a method and system for managing authentication attempts.

BACKGROUND OF THE INVENTION

[0003] Authentication of users and the like in computing environments is an important aspect of providing secure computing environments. Such authentication should be rigid enough to provide reasonable assurance that only authorized users can access the computing environment, and yet should not be so onerous that the user finds it impractical to actually gain access to the computing environment.

SUMMARY OF THE INVENTION

[0004] Aspects of the present of this invention take effective action to manage invalid authentication attempts through pattern analysis and the use of a separate communication channel to communicate with Users in real time. Such invalid authentication attempts could include fraudulent or abusive situations as well as a lack of User knowledge.

[0005] The identification and management of authentication attempts can be improved in a unique way by having a real time communication channel with the end user that is separate from the channel being used for authentication. An example of this is where Internet users are a) identified by their cell phone numbers and may b) access the internet from many different physical locations. Aspects of the invention allow for authentication issue detection to be extended with superior action compared to prior art, utilizing the separate communication channel to communicate directly with the user. This can allow the authenticating authority to take more proactive action on a more automatic basis with the ability to distinguish fraud or abuse attempts from user problems aided by the separate communication channel.

[0006] Aspects of the invention involve managing access to the internet, or a network. Another aspects involve managing access to an application, such as an internet connected web application.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Embodiments of the present invention will now be described by way of example only with reference to the attached figures herein.

[0008] **FIG. 1** is a system block diagram of a system for managing attempted illegitimate authentication attempts in accordance with another embodiment of the invention;

[0009] **FIG. 2** is a flow chart of a method for managing

[0010] **FIG. 3** is a flow chart of a method for managing attempted illegitimate authentication attempts in accordance with another embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0011] Referring to **FIG. 1**, the system for managing authentication attempts is generally located at **35**. The System **35** includes an authentication application or Authentication Server **25**, which, for example, could be implemented with a RADIUS server. The System also includes a User Database **40**, which could be many different standards and products. The System also includes an Event Database **45** which is used to store information about authentication events such as User ID, location of authentication attempt, time of attempt, if password matched User ID. The Location Database **50** stores information about the geographic coordinates of access locations and the type of access location (e.g. airport). The System also contains an Application **30** which can interface with the databases, the Authentication Server and the Cellular Network **55**. The System may be contained in any kind of computer that has suitable processing power, RAM, Disc capacity and communications ports. The computer may run any OS that is compatible with the applications **25**, **30**, **40**, **45**, **50**.

[0012] Users requiring authentication are equipped with internet devices such as a computer, a notebook computer, a PDA or a WLAN enabled cell phone **15**. Such devices support internet communication protocols.

[0013] These devices are attempting to access the internet from various locations. The access could be via wireless or wired network. The internet equipment **20** at the location is able to block access to the internet until the device **15** has been authenticated. The Internet equipment communicates with the Authentication Server **25** to pass information about the User to the Authentication Server **25**. The Internet equipment will not permit the Device to access the network until it has been advised to do so by the Authentication Server. This often takes the form of an "authentication accept" message.

[0014] The Authentication Server interfaces to the User Database **40** to compare the User ID and password offered by the Internet Device **15** with that stored in the User Database **40**. The Authentication Server passes information about the authentication attempt to the Application and receives a message back from the application indicating if Authentication can proceed. If the authentication may proceed, the Authentication Server will communicate with the Internet equipment to inform the equipment that access may be permitted. This often takes the form of an "authentication accept" message.

[0015] The Application **30** receives information about authentication attempts, referred hereafter as "events", from the Authentication Server **25**.

[0016] The Application **30** may:

[0017] a) Record the event in Even Database (**45**).

[0018] b) Retrieve and analyse information about events when a new event occurs. The Application

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.