IMPLICIT AUTHENTICATION

Inventor(s): Bjorn Markus Jakobsson, Mark J. Grandcolas, Philippe J.P. Golle, Richard Chow, and Runting Shi

BACKGROUND

Field

[0001] This disclosure is generally related to user authentication. More specifically, this disclosure is related to a method and system for implicitly authenticating a user to access a controlled resource based on contextual data indicating the user's behavior.

Related Art

[0002] A Mobile Internet Device (MID) is a multimedia-capable handheld computer providing wireless Internet access. MIDs are designed to provide entertainment, information and location-based services for personal use. As the market of MIDs expands, mobile commerce (also known as M-commerce) is experiencing rapid growth. There is a trend toward hosting applications and services on the Internet. This results in increased demand for Internet

authentication – whether of devices, computers or users. Moreover, the use of digital rights management (DRM) policies will likely increase the need for frequent authentications. Some of such authentications may happen simultaneously due to the increased use of mashups.

[0003] On the other hand, the shift toward greater market penetration of MIDs complicates password entry due to the limitations of MID input interfaces. Typing passwords on mobile devices, such as an iPhone™ or a BlackBerry™, can become a tedious and error-prone process.

[0004] Single sign-on (SSO) is an authentication mechanism to control the access of multiple, related, but independent software applications and services. With SSO, a user logs in once and gains access to all applications and services without being prompted to log in again at each of them. SSO addresses the problem of frequent authentications. However, SSO does not defend against theft and compromise of devices because it only vouches for the identity of the device, not its user.

SUMMARY

[0005] One embodiment provides a system that implicitly authenticates a user of a Mobile Internet Device to access a controlled resource. The system first receives a request to access the controlled resource. Then, the system determines a user behavior score based on a user behavior model and recent contextual data, wherein the user behavior score facilitates identifying a level of consistency between one or more recent user events and a past user behavior pattern. The user behavior model is derived from historical contextual data of the user. The recent contextual data are recent data of the user collected from one or more user mobile devices indicating the user's recent behavior or one or more recent user events.

The recent contextual data can be collected without prompting the user to perform an action explicitly associated with authentication. Further, the recent contextual data include multiple data streams, which provide basis for the determination of the user behavior score. However, a data stream alone provides insufficient basis for the determination of the user behavior score. Next, the system provides the user behavior score to an access controller of the controlled resource, thereby making an authentication decision derived from the user behavior score for the user to access the controlled resource based at least on the user behavior score. In addition, the system can be used in combination with another form of authentication.

[0006] In some embodiments, the system also collects contextual data of the user periodically from one or more user devices, and updates the user behavior model based on the collected contextual data of the user.

[0007] In some embodiments, the system also determines an action based on the user behavior score. The action can be a demand for a further authentication.

[0008] In some embodiments, the system also determines whether the user behavior score is higher than a predetermined threshold value, and if so, authenticates the user to access the controlled resource using the authentication decision derived from the user behavior score.

[0009] In some embodiments, the system also uses the authentication decision derived from the user behavior score to increase or decrease an assurance associated with another form of authentication.

[0010] In some embodiments, the system also:

- observes the recent event associated with the recent contextual data of the user;

- calculates a quality measure associated with the recent event;
- calculates a weight associated with the type of observation;
- determines whether the observed event is consistent with the user behavior model; and
- increases (if consistent) or decreases (if inconsistent) the user behavior score based on the quality measure and the weight.

[0011] In some embodiments, the system also determines that the user behavior score is lower than a predetermined threshold value, and requests the user to provide a user credential, thereby explicitly authenticating the user to access the controlled resource.

[0012] In some embodiments, the system collects the contextual data with a number of measurements. The user behavior model describes the past user behavior pattern by a combination of one or more measurements.

[0013] In some embodiments, the recent contextual data of the user are data from at least one of the following sources:

- device data that are available on a user device;
- carrier data that are available to a network carrier; and
- third-party provider data that are available to a third-party provider providing an application to the user.

[0014] In some embodiments, the recent contextual data of the user comprise one or more of: GPS data, accelerometer data, voice data, sensor data, application usage data, web browser data, authentication attempts, connection attempts, network traffic pattern, DNS requests, typing pattern, biometric data, social group membership information, and user demographics data.

[0015] In some embodiments, the user behavior model is stored in a user model look-up table. The user model look-up table comprises historical

information on whether a condition is satisfied, and information on a plurality of user events. Each event is associated with a probability distribution and a score distribution.

[0016] In some embodiments, the system collects historical contextual data via one or more of a survey of contextual information about the user entered by a representative of the user, an accumulation of periodically transmitted contextual data of the user from one or more mobile devices, or an inheritance of the contextual information about the user from another device associated with the user.

[0017] In some embodiments, the system derives the user behavior model from a second model of a group of users sharing similar characteristics.

[0018] In some embodiments, the recent event belongs to one of a plurality of categories. The plurality of categories comprise one or more of: (1) a very positive event; (2) a positive event; (3) a neutral event; (4) a negative event; and (5) a very negative event. The determination of increasing or decreasing the user behavior score and the amount of increment or decrement are associated with the category to which the recent event belongs.

BRIEF DESCRIPTION OF THE FIGURES

[0019] FIG. 1A shows a diagram of the usability and security of different authentication techniques.

[0020] FIG. 1B shows a schematic diagram of a system for implicitly authenticating a user to access a controlled network resource in accordance with an embodiment.

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.