Contact Information

Publications@ipcg.com

ipCapital Group, Inc.
400 Cornerstone Drive, Suite 325
Williston, VT 05495
United States of America
(802) 872-3200 x214

Title of Invention

Method for authenticating user identity using security questions based on prior operating system activity

Description of Invention

A module designed to record operating system activity by a given user can be used to generate security questions to verify the authenticity of the user. This method is effective for strengthening the security of the system because only the user should have knowledge of recent operating system activity.

Problem / Opportunity

Protecting sensitive material from unauthorized access is an ongoing issue for businesses and individuals. Though access to such material is typically password protected, the opportunity for unauthorized access remains if the password is compromised. In addition, if the rightful user is logged in but is temporarily absent from operating the system, an unauthorized user can easily access stored information.

In order to prevent a security breach, further safeguards may be necessary. In some cases, security questions must be answered correctly to gain access. Such questions could include the user's mother's maiden name or the make of the user's first car. While this process does increase the safety of the system from unauthorized users, this private information can also be subject to theft. What is needed is an improved means for authentication of users of computers

Detailed Description of the Invention

Using prior activity on an operating system as a basis for initializing security questions is one method to help prevent unauthorized access to a computing device. Such activity includes but is not limited to the saving of files, deleting files or programs, or sending emails. Knowledge of such activity is known only to the authenticated user and is continually changing, unlike static private information. While using the device, the user will be periodically prompted to answer a series of security questions based on the activities described above. For example, the question may provide a number of possible

file names and ask the user to select the last file that was saved. Access will be granted only if correct responses to a series of activity-based questions are given.

In order to highlight the importance of preventing unauthorized access to a computing device, consider the case of a financial services representative. The representative has access to sensitive financial information of clients such as account numbers and account balances. It is vital that only the representative have access to such information in order to protect the privacy and maintain the trust of the client.

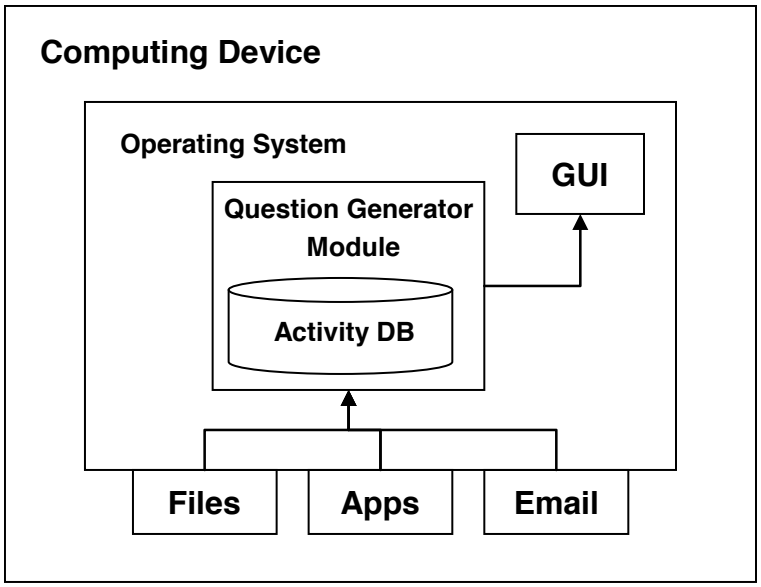

Figure 1 : User Authentication System

Description of Figure 1 Elements
Operating System: All file activity, applications, email activity, etc are performed by the software located in the OS (i.e. Linux).
GUI: Interface through which users interact with the operating system.
Question Generator Module (QGM): Tracks and stores OS usage details in the Activity Database. Using the stored operating system activity from the Activity Database, security questions are generated.
Activity Database: This stores all of the user's activity on the operating system to facilitate security question generation.
Computing Device: Any computing device such as a desktop computer, laptop, mobile device, etc.

The method begins when the user logs in to the computing device (**Figure 2**).

In step 1, the QGM tracks and stores operating system usage details for user of interest in the activity database.

In step 2, the QGM derives plausible correct answers based on knowledge of step 1.

In step 3, the QGM monitors usage and selects less disruptive moments to start AR.

In step 4, the QGM integrates steps 1 through 3 into an authentication routine as a question(s) to validate the authentication of the user.

In step 5, the Authentication Routine (AR) starts.
In step 6, the computing device is locked to prevent access to anything but the AR. This is necessary so the user cannot access sensitive material or attempt to mine the system for recent operating system activity.

In decision step 7, the user is prompted with question(s) related to recent activity. If answered correctly, the method continues to step 8. If answered incorrectly, the method proceeds to step 9.

In step 8, the system will unlock and return to normal functionality.

In step 9, the user will be returned to the primary login interface.

The method ends.

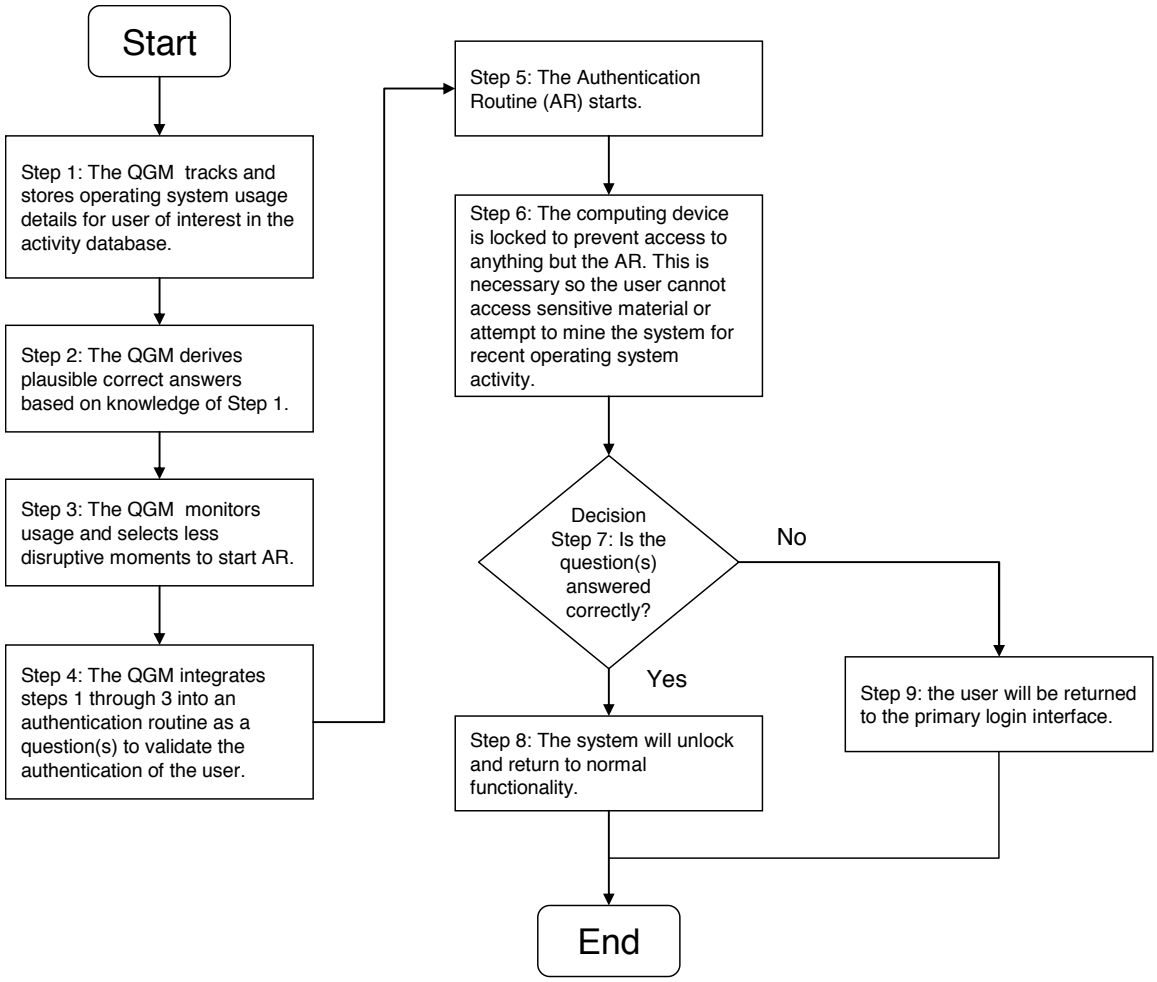

Figure 2: A flowchart for using OS activity to increase security on a computing device