Technical Disclosure Commons

Defensive Publications Series

December 2019

HEIGHTENED SECURITY MEASURES FOR MARKED APPLICATIONS

Rachel Hausmann

Collin Irwin

HEIGHTENED SECURITY MEASURES FOR MARKED APPLICATIONS

ABSTRACT

A system is described that enables a computing device (e.g., a mobile phone, a camera, a tablet computer, etc.) to associate an application with a security level (e.g., a high-sensitive level, a middle-sensitive level, a low-sensitive level, etc.), and provide additional security mechanisms (e.g., auto-lock, biometric authentication, password authentication, etc.) to the application based on the security level. A user may set a security level for an application, and the computing device may provide additional security mechanisms to the application based on the selected security level. For example, a user may associate a banking application with a high-sensitive security level, and based on the high-sensitive security level, the computing device may periodically (e.g., every second, every 10 seconds, every minute, etc.) require the user to provide biometric inputs to verify user identity.

DESCRIPTION

Existing application security mechanisms are set by application developers and may vary widely between different applications, even amongst applications of the same type (e.g., amongst banking or medical applications). A user may want additional security mechanisms for applications containing sensitive information, such as banking or medical applications. As such, it would be desirable for a computing device to be able to associate applications with a security level and provide additional security mechanisms based on the security level.

Figure 1 below is a conceptual diagram illustrating an example computing device configured to associate an application with a security level and provide additional security mechanisms based on the security level. In the example of FIG. 1, computing device 100 represents an individual mobile or non-mobile computing device. Examples of computing device 100 include a mobile phone, a tablet computer, a laptop computer, a desktop computer, a server, a mainframe, a set-top box, a television, a wearable device (e.g., a computerized watch, a computerized eyewear, a computerized glove, etc.), a home automation device or system (e.g., an intelligent thermostat or home assistant device), a personal digital assistant (PDA), a gaming system, a media player, an e-book reader, a mobile television platform, an automobile navigation or infotainment system, or any other type of mobile, non-mobile, wearable, and non-wearable computing device that contains a security module which configured to associate applications with a security level, and provide additional security mechanisms based on the security level.

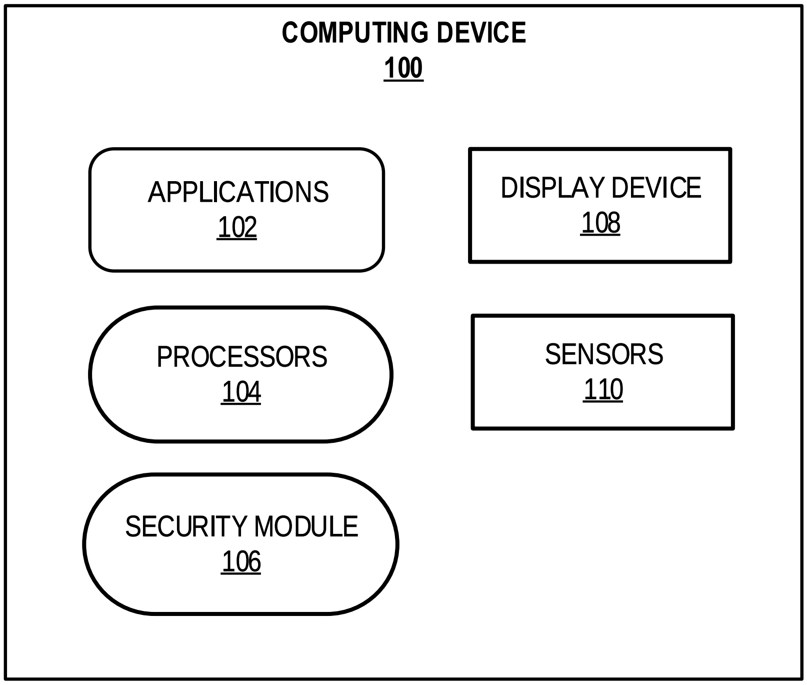

FIG. 1

Computing device 100 may include applications 102, processors 104, and security module 106. Applications 102 can be executed by processors 104 to provide various functionalities (e.g., accessing banking information, accessing medical records, etc.). Computing device 100 may include display device 108 (e.g., a liquid crystal display (LCD), thin-film transistor display (TFT), organic light emitting diode display (OLED), etc.) to utilize various applications, functions, and other features of computing device 100. Computing device 100 may also include one or more sensors 110 to detect various user inputs and may processed data received from sensors 110 to verify user identity. Examples of sensors 110 include, but are not limited to, a fingerprint sensor, a depth sensor, a radar sensor, an image capture device, and the like. Security module 106 may associate one or more applications 102 with a security level and may provide additional security mechanisms based on the security level. Additional security mechanisms may include one or more of biometric authentications (e.g., face authentication, fingerprint authentication, iris authentication, etc.), password authentication, or other suitable authentication technologies. These additional security mechanisms may be enforced at any point. As one example, after a pre-determined time (e.g., 5 minutes, 10 minutes, 20 minutes, etc.), computing device 100 may automatically close or cover one or more applications 102 with a lock screen, and face authentication may be used to unlock the one or more applications 102.

Computing device 100 may receive one or more detected user inputs from sensors 110 and may process data received from sensors 110 to verify user identity periodically. For example, computing device 100 may use sensors 110 (e.g., an image capture device) to capture a still image of a user periodically. Processors 104 may process the captured image to facial feature data and may compare the facial feature data with facial feature data of known users to authenticate the user of the device. Based on the comparison, computing device 100 may keep the user logged in to applications 102 or may send a notification to a trusted device to report the attempt to unlock applications 102 fails.

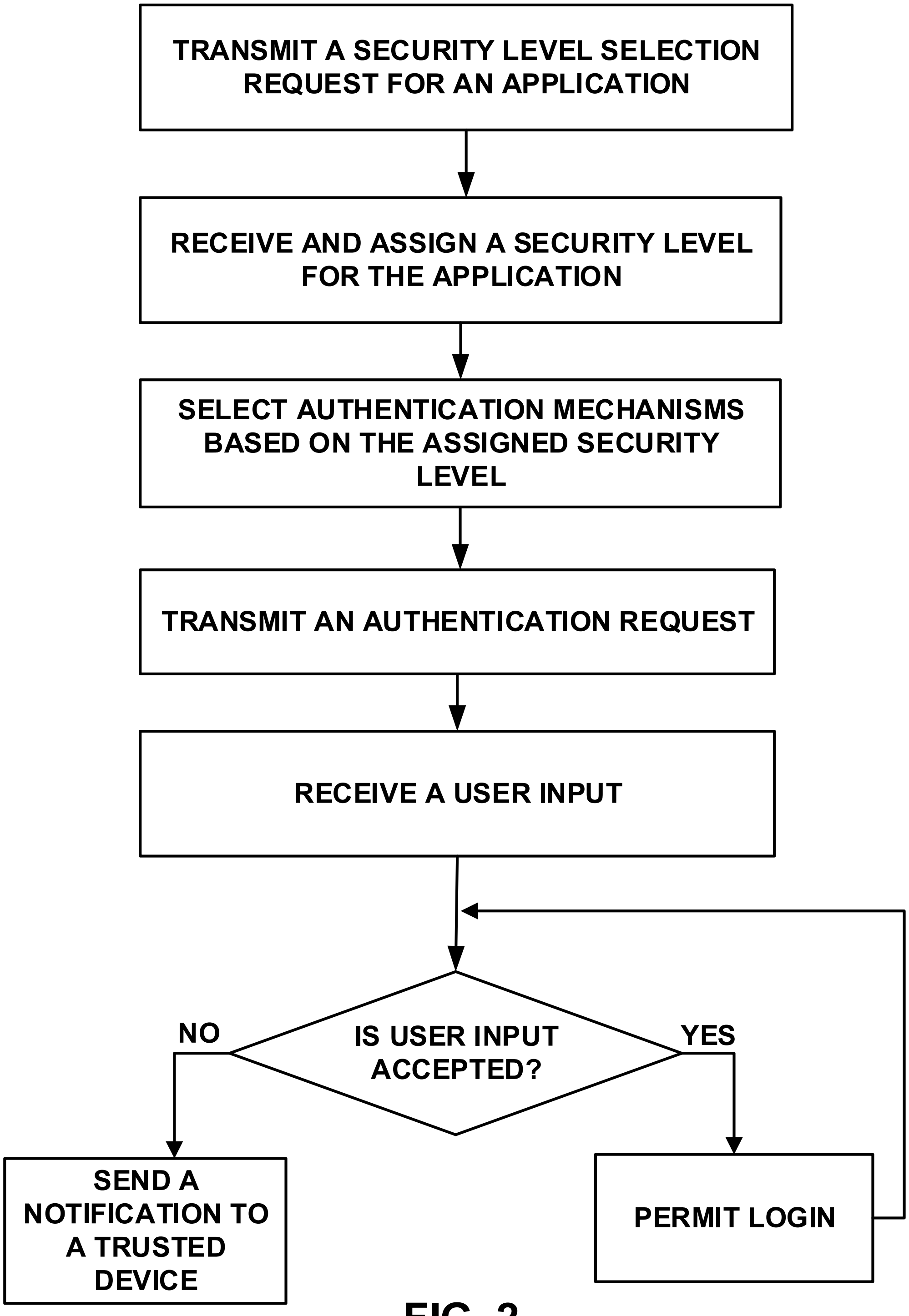
TRANSMIT A SECURITY LEVEL SELECTION REQUEST FOR AN APPLICATION
RECEIVE AND ASSIGN A SECURITY LEVEL FOR THE APPLICATION
SELECT AUTHENTICATION MECHANISMS BASED ON THE ASSIGNED SECURITY LEVEL
TRANSMIT AN AUTHENTICATION REQUEST
RECEIVE A USER INPUT
IS USER INPUT ACCEPTED?
NO
YES
SEND A NOTIFICATION TO A TRUSTED DEVICE
PERMIT LOGIN

FIG. 2

An example method to associate an application with a security level and provide additional security mechanisms based on the security level is shown above in Figure 2. As

Figure 2 is only an example, the steps shown in the figure may be carried out in a different order, carried out simultaneously, and/or omitted entirely.

As shown in Figure 2, a computing device may first transmit a security level selection request for an application to a user. A security level may indicate the type of additional security mechanisms to be added to the application. For example, when the user uses an application (e.g., a banking application, medical application, photo application, etc.) for the first time, the computing device may pop-up a window asking the user to associate the application with a security level (e.g., high-sensitive level, middle-sensitive level, low-sensitive level, etc.). Each security level may provide a set of additional security mechanisms to the application. For example, an application with high-sensitive security level may periodically (e.g., every millisecond, every second, every minute, etc.) authenticate the user of the application using biometric authentication technology (e.g., facial recognition, fingerprint recognition, iris recognition, etc.) and an application with a middle-sensitive security level may periodically authenticate the user of the application using password authentication.

The computing device may receive the user's biometric data through various sensors and may use the received biometric data to verify user identity periodically. For example, the computing device may periodically capture an image of the user, process the captured image to facial feature data, and compare the facial feature data with facial feature data of known users to verify user identity. If the computing device found a match, the computing device may keep the user logged in to the application. The computing device may also automatically lock the application after a pre-determined time (e.g., three minutes, five minutes, ten minutes, etc.) and request the user to provide the password of the application when the user attempts to log in to the application again. The computing device may cover the application with a lock screen, move the application to the background, or close the application to ensure the content of the application is protected.

If the computing device determines authentication fails, the computing device may send a notification to a trusted user device to report the attempt to unlock the application fails. For example, if the computing device does not find a match between the captured biometric data and the biometric data of known users, the computing device may send a notification to a trusted device. The notification may include a photo taken of the unauthorized user. In some examples, the computing device may track the number of failed attempts and may only send the notification after the number of failed attempts exceeds a pre-defined number. In some examples, the notification may include an option to allow the user of the trusted device to wipe out user data from the specific application on the computing device. This can protect the user from inadvertently deleting user data from other applications.

The computing device may update applications with high-sensitive security levels before other applications or may update applications with high-sensitive security levels irrespective of the availability of Wi-Fi ® connection. In some examples, the computing device may prevent the user from accessing applications with high-sensitive security levels when the applications are not up to date. Additionally, the computing device may sandbox applications with high-sensitive security levels and may prevent other applications from reaching user data from applications with high-sensitive security levels.

The security level of an application may be assigned by a user, a publisher, or automatically assigned by the computing device. For example, a publisher of an application (e.g., a banking application) may set a high-sensitive security level as the default security level. In another example, the computing device may automatically assign an application with a high-sensitive security level based on the title of the application. For example, the computing device may automatically detect a high-sensitive word (e.g., bank) contains within the title (e.g., mobile bank) of the application and may assign a high-sensitive level to the application based on the detected high-sensitive word.

Different users may be assigned with different authorization levels. For example, primary users (e.g., such as a device owner and the spouse of the device owner) may be assigned with a high-authorization level, which may allow the primary users to access all applications. A secondary user (e.g., such as a child of the device owner) may be assigned with a middle-authorization level, which may allow the secondary user to access applications with middle-sensitive and low-sensitive security levels. For example, a couple may be assigned with a high-authorization level, which may allow the couple to access applications with high-sensitive security levels (e.g., a banking application); a child may be assigned with a middle-authorization level, which may prevent the child from accessing applications with high-sensitive security levels.

A user may customize a security level by selecting a set of security features for the security level. For example, a user may name a security level as security level 10 and may customize security level 10 by associating a set of security features, such as facial recognition and iris recognition, with security level 10. In some examples, more than one security level (e.g., three levels, five levels, ten levels, etc.) may be customized by the user.

It is noted that the techniques of this disclosure may be combined with any other suitable technique or combination of techniques. Such a combination may be made for any suitable purpose, including, but not limited to, associate an application with a security level and provide additional security mechanisms to the application based on the security level. As one example, the techniques of this disclosure may be combined with the techniques of U.S. Patent Application Publication US20100322487A1.