MOBILE SECURITY COUNTERMEASURES

FIELD OF THE DISCLOSURE

The present disclosure relates to mobile device security.

BACKGROUND

Mobile devices, such as laptops, mobile phones, wearable computing devices, implantable devices, portable computing devices, etc., are susceptible to unauthorized users accessing data stored on the mobile devices. To illustrate, if an unauthorized user obtains (e.g., steals) a laptop that has information associated with an authorized user of the laptop, the unauthorized user may access the information and use the information for improper purposes. As a non-limiting example, the unauthorized user can steal identity information of the authorized user (e.g., identity theft).

SUMMARY

According to one implementation, a computer-implemented method includes generating, at a processor of a mobile device, a user profile for an authorized user of the mobile device based on behavior patterns associated with the authorized user. The behavior patterns are determined based on historical data indicating past user behavior of the authorized user. The computer-implemented method also includes detecting subsequent user behavior of a particular user during an attempt by the particular user to access the mobile device. For example, the subsequent user behavior may include a heart rate of the particular user, a time of day that the particular user attempts to access the mobile device, etc. The computer-implemented method also includes comparing the subsequent user behavior to the behavior patterns of the user profile to determine whether the particular user is authorized or unauthorized. In response to determining that the particular user is an unauthorized user, the computer-implemented method includes detecting activity by the unauthorized user and performing at least one countermeasure of a plurality of countermeasures in response to detecting the activity. Each countermeasure of the plurality of countermeasures has a security level and corresponds to a degree of the activity. Performing the at least one countermeasure includes determining that the activity satisfies a second security level, the second security level higher than a first security level, and performing a second countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the second security level. The second

countermeasure enables the mobile device to determine information associated with the unauthorized user. Performing the second countermeasure includes (a) prompting the unauthorized user to touch a particular portion of the mobile device, the particular portion of the mobile device comprising a hidden scanner integrated into an input device of the mobile device, and scanning a fingerprint of the unauthorized user while the unauthorized user touches the particular portion of the mobile device, and (b) providing false data in response to commands issued by the unauthorized user to engage the unauthorized user with the mobile device, the false data associated with the commands, and generating information about the unauthorized user while the unauthorized user is engaged with the mobile device, the information including a fingerprint of the unauthorized user, a voice signature of the unauthorized user, or both.

Different countermeasures may be performed for similar scenarios. For example, for a particular degree of activity, a first particular countermeasure or a second particular countermeasure may be performed. According to one implementation, a first countermeasure having a first security level protects

data stored at the mobile device from the unauthorized user. To illustrate, the first countermeasure may delete data stored at the mobile device. A second countermeasure having a second security level determines information about the unauthorized user. To illustrate, the second countermeasure may activate a camera of the mobile device to capture the surroundings of the mobile device, scan a fingerprint of the unauthorized user and compare the fingerprint to one or more fingerprint databases, etc. A third countermeasure having a third security level performs additional security measures or countermeasures. Each countermeasure is triggered by the degree of activity (e.g., improper activity) of the unauthorized user.

According to another implementation, an apparatus includes a memory that stores a user profile for an authorized user of a mobile device. The user profile is generated based on behavior patterns associated with the authorized user. The behavior patterns are determined based on historical data indicating past user behavior of the authorized user. The apparatus also includes a processor coupled to the memory. The processor is configured to detect subsequent user behavior of a particular user during an attempt by the particular user to access the mobile device. The processor is further configured to compare the subsequent user behavior to the behavior patterns of the user profile to determine whether the particular user is authorized or unauthorized. In response to a determination that the particular user is an unauthorized user, the processor is configured to detect activity by the unauthorized user and perform at least one countermeasure of a plurality of countermeasures in response to detecting the activity. Each countermeasure of the plurality of countermeasures has a security level and corresponds to a degree of the activity. The processor is configured to perform the at least one countermeasure by determining that the activity satisfies a second security level, the second security level higher than a first security level, and performing a second countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the second security level. The second countermeasure enables the mobile device to determine information associated with the unauthorized user. Performing the second countermeasure includes (a) prompting the unauthorized user to touch a particular portion of the mobile device, the particular portion of the mobile device comprising a hidden scanner integrated into an input device of the mobile device, and scanning a fingerprint of the unauthorized user while the unauthorized user touches the particular portion of the mobile device, and (providing false data in response to commands issued by the unauthorized user to engage the unauthorized user with the mobile device, the false data associated with the commands, and generating information

about the unauthorized user while the unauthorized user is engaged with the mobile device, the information including a fingerprint of the unauthorized user, a voice signature of the unauthorized user, or both.

Different countermeasures may be performed for similar scenarios. For example, for a particular degree of activity, a first particular countermeasure or a second particular

countermeasure may be performed. According to one implementation, a first countermeasure having a first security level protects data stored at the mobile device from the unauthorized user, a second countermeasure having a second security level determines information about the unauthorized user, and a third countermeasure having a third security level performs additional security measures or countermeasures. Each countermeasure is triggered by the degree of activity (e.g., improper activity) of the unauthorized user.

According to another implementation, a non-transitory computer-readable storage device includes instructions that, when executed by a processor, cause the processor to perform operations

including generating a user profile for an authorized user of a mobile device based on user behavior patterns associated with the authorized user. The behavior patterns are determined based on historical data indicating past user behavior of the authorized user. The operations also include detecting subsequent user behavior of a particular user during an attempt by the particular user to access the mobile device. The operations also include comparing the subsequent user behavior to the user behavior patterns of the user profile to determine whether the particular user is authorized or unauthorized. In response to determining that the particular user is an unauthorized user, the operations include detecting activity by the unauthorized user and performing at least one countermeasure of a plurality of countermeasures in response to detecting the activity. Each countermeasure of the plurality of countermeasures has a security level and corresponds to a degree of the activity. Performing the at least one countermeasure includes determining that the activity satisfies a second security level, the second security level higher than a first security level, and performing a second countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the second security level. The second countermeasure enables the mobile device to determine information associated with the unauthorized user. Performing the second countermeasure includes (a) prompting the unauthorized user to touch a particular portion of the mobile device, the particular portion of the mobile device comprising a hidden scanner integrated into an input device of the mobile device, and scanning a fingerprint of the unauthorized user while the unauthorized user touches the particular portion of the mobile device, and (b) providing false data in response to commands issued by the unauthorized user to engage the unauthorized user with the mobile device, the false data associated with the commands, and generating information about the unauthorized user while the unauthorized user is engaged with the mobile device, the information including a fingerprint of the unauthorized user, a voice signature of the unauthorized user, or both.

Different countermeasures may be performed for similar scenarios. For example, for a particular degree of activity, a first particular countermeasure or a second particular countermeasure may be performed. According to one implementation, a first countermeasure having a first security level protects data stored at the mobile device from the unauthorized user, a second countermeasure having second a security level determines information about the unauthorized user, and a third countermeasure having a third security level performs additional security measures or countermeasures. Each countermeasure is triggered by the degree of

activity (e.g., improper activity) of the unauthorized user.

One advantage of the above-described implementations is that a mobile device can detect that an unauthorized user has accessed the mobile device. Different countermeasures can be triggered at the mobile device based on levels of improper activity by the unauthorized user. For example, if the improper activity corresponds to a low-level security breach, the mobile

device can delete data to prevent the unauthorized user from accessing the data. If the improper activity corresponds to a higher-level security breach, the mobile device can actively collect data about the unauthorized user while the mobile device is in the unauthorized user's possession. The collected data may be used to identify the location of the mobile device (and thus the location of the unauthorized user) and the collected data may be used to determine an identity of the unauthorized user. As a non-limiting example, to determine the location of the mobile device, a camera of the mobile device may be activated to capture the surroundings of the mobile device. To determine the identity of the unauthorized user, a fingerprint scanner on the mobile device may scan a fingerprint of the unauthorized user and compare the fingerprint to one or more fingerprint databases. Thus,

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

generating, at a processor of a mobile device, a user profile for an authorized user of the mobile device based on behavior patterns associated with the authorized user, the behavior patterns determined based on historical data indicating past user behavior of the authorized user;

detecting subsequent user behavior of a particular user during an attempt by the particular user to access the mobile device;

comparing the subsequent user behavior to the behavior patterns of the user profile to determine whether the particular user is authorized or unauthorized; and

responsive to determining that the particular user is an unauthorized user based on the comparison:

detecting activity by the unauthorized user; and

performing at least one countermeasure of a plurality of countermeasures in response to detecting the activity, each countermeasure of the plurality of countermeasures having a different security level and corresponding to a degree of the activity,

wherein performing the at least one countermeasure comprises:

determining that the activity satisfies a second security level, the second security level higher than a first security level; and

performing a second countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the second security level, wherein the second countermeasure enables the mobile device to determine information associated with the unauthorized user,

wherein performing the second countermeasure comprises:

(a) prompting the unauthorized user to touch a particular portion of the mobile device, the particular portion of the mobile device comprising a hidden scanner integrated into an input device of the mobile device, and scanning a fingerprint of the unauthorized user while the unauthorized user touches the particular portion of the mobile device; and

(b) providing false data in response to commands issued by the unauthorized user to engage the unauthorized user with the mobile device, the false data associated with the commands, and generating information about the unauthorized user while the unauthorized user is engaged with the mobile device, the information including a fingerprint of the unauthorized user, a voice signature of the unauthorized user, or both.

2. The computer-implemented method of claim 1, wherein the historical data includes geographical locations where the authorized user accesses the mobile device, time periods when the authorized user accesses the mobile device, data indicating a heart rate of the authorized user, or a combination thereof.

3. The computer-implemented method of any one of claims 1-2, wherein the behavior patterns are determined using machine learning based on the historical data.

4. The computer-implemented method of any one of claims 1-3, wherein performing the at least one countermeasure comprises:

determining that the activity satisfies the first security level; and

performing a first countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the first security level, wherein the first countermeasure protects information stored at the mobile device from the unauthorized user.

5. The computer-implemented method of claim 4, wherein performing the first countermeasure comprises deleting data stored at the mobile device.

6. The computer-implemented method of any one of claims 4-5, wherein performing the first countermeasure comprises:

detecting a request for identity information from the unauthorized user, the identity information associated with the authorized user;

generating false identity information in response to detecting the request; and

providing the false identity information to the unauthorized user.

7. The computer-implemented method of claim 1, wherein performing the second countermeasure comprises activating a camera of the mobile device.

8. The computer-implemented method of any one of claims 1-7, wherein performing the second countermeasure comprises generating a voice signature of the unauthorized user while the unauthorized user speaks into a microphone.

9. The computer-implemented method of any one of claims 1-8, wherein performing the at least one countermeasure further comprises:

determining that the activity satisfies a third security level; and

performing a third countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the third security level.

10. The computer-implemented method of claim 9, wherein performing the third countermeasure comprises generating an electromagnetic pulse.

11. The computer-implemented method of any one of claims 9-10, wherein performing the at least one countermeasure comprises initiating a self-destruct processor to destroy a non-volatile memory.

12. The computer-implemented method of any one of claims 1-11, wherein the behavior patterns are weighted and comprise at least one of geographical location patterns of the authorized user, mobile device usage time patterns of the authorized user, typing speed patterns of the authorized user, or data-type patterns of the authorized user.

13. An apparatus comprising:

a memory storing a user profile for an authorized user of a mobile device, the user profile generated based on behavior patterns associated with the authorized user, the behavior patterns determined based on historical data indicating past user behavior of the authorized user;

a processor coupled to the memory, the processor configured to:

detect subsequent user behavior of a particular user during an attempt by the particular user to access the mobile device;

compare the subsequent user behavior to the behavior patterns of the user profile to determine whether the particular user is authorized or unauthorized; and

in response to a determination that the particular user is an unauthorized user based on the comparison:

detect activity by the unauthorized user; and

perform at least one countermeasure of a plurality of countermeasures in response to detection of the activity, each countermeasure of the plurality of countermeasures having a different security level and corresponding to a degree of the activity,

wherein the processor is configured to perform the at least one countermeasure by:

determining that the activity satisfies a second security level, the second security level higher than a first security level; and

performing a second countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the second security level, wherein the second countermeasure enables the mobile device to determine information associated with the unauthorized user,

wherein performing the second countermeasure comprises:

(a) prompting the unauthorized user to touch a particular portion of the mobile device, the particular portion of the mobile device comprising a hidden scanner integrated into an input device of the mobile device, and scanning a fingerprint of the unauthorized user while the unauthorized user touches the particular portion of the mobile device; and

(b) providing false data in response to commands issued by the unauthorized user to engage the unauthorized user with the mobile device, the false data associated with the commands, and generating information about the unauthorized user while the unauthorized user is engaged with the mobile device, the information including a fingerprint of the unauthorized user, a voice signature of the unauthorized user, or both.

14. The apparatus of claim 13, wherein the historical data is provided to a machine learning algorithm to determine the behavior patterns.

15. The apparatus of any one of claims 13-14, wherein the historical data includes geographical locations where the authorized user accesses the mobile device, time periods when the authorized user accesses the mobile device, data indicating a heart rate of the authorized user, or a combination thereof.

16. A non-transitory computer-readable storage device comprising instructions hat, when executed by a processor, cause the processor to perform operations comprising:

generating a user profile for an authorized user of a mobile device based on behavior patterns associated with the authorized user, the behavior patterns determined based on historical data indicating past user behavior of the authorized user;

detecting subsequent user behavior of a particular user during an attempt by the particular user to access the mobile device;

comparing the subsequent user behavior to the behavior patterns of the user profile to determine whether the particular user is authorized or unauthorized; and

responsive to determining that the particular user is an unauthorized user based on the comparison:

detecting activity by the unauthorized user; and

performing at least one countermeasure of a plurality of countermeasures in response to detecting the activity, each countermeasure of the plurality of countermeasures having a different security level and corresponding to a degree of the activity,

wherein performing the at least one countermeasure comprises:

determining that the activity satisfies a second security level, the second security level higher than a first security level; and

performing a second countermeasure of the plurality of countermeasures in response to determining the detected activity satisfies the second security level, wherein the second countermeasure enables the mobile device to determine information associated with the unauthorized user,

wherein performing the second countermeasure comprises:

(a) prompting the unauthorized user to touch a particular portion of the mobile device, the particular portion of the mobile device comprising a hidden scanner integrated into an input device of the mobile device, and scanning a fingerprint of the unauthorized user while the unauthorized user touches the particular portion of the mobile device; and

(b) providing false data in response to commands issued by the unauthorized user to engage the unauthorized user with the mobile device, the false data associated with the commands, and generating information about the unauthorized user while the unauthorized user is engaged with the mobile device, the information including a fingerprint of the unauthorized user, a voice signature of the unauthorized user, or both.

17. The non-transitory computer-readable storage device of claim 16, wherein the historical data is provided to a machine learning algorithm to determine the behavior patterns.