View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Technical Disclosure Common

Technical Disclosure Commons

Defensive Publications Series

March 2020

Automatic Activation of Mobile Device Security Upon Detection of Theft

Peter Lewis

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Lewis, Peter, "Automatic Activation of Mobile Device Security Upon Detection of Theft", Technical Disclosure Commons, (March 06, 2020)
https://www.tdcommons.org/dpubs_series/2986

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Automatic Activation of Mobile Device Security Upon Detection of Theft

ABSTRACT

This disclosure describes techniques to reduce the risk of a data breach when a mobile device is stolen. In certain modes, e.g., augmented reality (AR) mode, selfie mode, etc., optimal use of a mobile device requires that the user hold the device out at an arm's length in a public location, leading to an increased likelihood of theft. With user permission, a potential risk state is activated upon detecting such use of the device. If sudden movement of the device, e.g., as detected by an on-board accelerometer, location sensor, or other sensor is detected, the device is automatically locked, requiring user authentication for data access. If the user permits, location tracking is also activated which can assist physical recovery of the device.

KEYWORDS

- Smartphone theft
- Mobile device theft
- Augmented Reality (AR)
- Street view
- Device locking
- Location tracking

BACKGROUND

In certain modes, e.g., augmented reality (AR) mode, selfie mode, etc., optimal use of a mobile device requires that the user hold the device out at an arm's length in a public location. In such a mode, mobile phones and other devices are at a high risk of theft, especially when owners use their phones in public places. As more applications become available that use augmented reality (AR), e.g., to aid users in navigating unfamiliar areas, to play AR games, etc., the risk of device theft increases.

When a device is stolen, there are several downstream consequences. For example, the stolen device can be subsequently sold, especially if it continues to work on cellular networks. Further, there is increased risk to the device owner's data, e.g., if the device is unlocked when taken. Further, the user suffers a monetary loss due to the loss of the device.

DESCRIPTION

This disclosure describes techniques to reduce the risk of a data breach when a mobile device is stolen. With user permission, it is determined if a mobile device is being used in a context that is associated with a likelihood of theft. Device sensors are activated to detect theft. If theft is detected, the device is automatically locked, and with user permission, device location is tracked and made available via the device user's online account.

Fig. 1: A user using a mobile device in selfie mode

Fig. 1 illustrates a user (102) using a mobile device (100) taking a selfie using the front camera of the device. In the selfie mode, the user's hand is stretched out at an arm's length. Similarly, a user may use their mobile device in augmented reality mode where an application engages the user in a public place in a way such that the user holds the phone out at a distance. For example, augmented reality maps or games may require such use of the device.

In such user contexts, where the user holds the mobile device at an arm's length, the likelihood of device theft is higher. Per techniques of this disclosure, with user permission to determine such context, a potential risk state is detected for the device and one or more of the on-board sensors are activated. In this heightened awareness state, sensors such as accelerometer, location sensor etc. are activated to detect sudden removal of the device. If sudden removal is detected, the device is automatically locked, requiring that the user's credentials be resubmitted in order to continue using the device. Further, if the user permits, location tracking is enabled on the device and the device location is reported to the user's online account at suitable intervals.

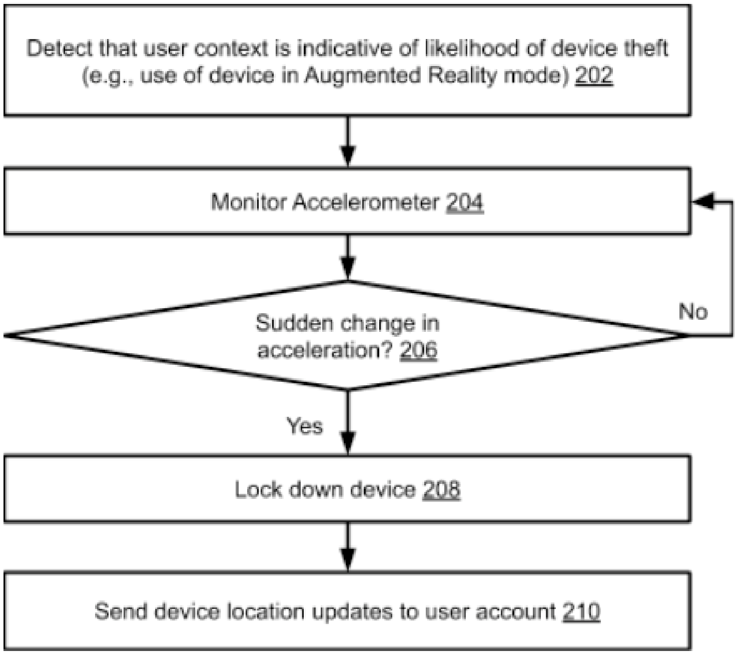
Detect that user context is indicative of likelihood of device theft (e.g., use of device in Augmented Reality mode) 202
Monitor Accelerometer 204
Sudden change in acceleration? 206
No
Yes
Lock down device 208
Send device location updates to user account 210

Fig. 2: Automatically detecting device theft and performing mitigating actions

Fig. 2 illustrates a flowchart of a method to automatically detect device theft and perform mitigating actions, per techniques of this disclosure. With user permission, it is detected that the context of use of a mobile device is associated with a high likelihood of theft (202). Upon detection of such context, device accelerometer readings are monitored (204). Based on the readings, it is determined if there is a sudden change in acceleration (206), which is indicative of sudden removal of the device from a user's hand. If sudden removal is detected, the device is locked down (208) and with prior user permission, the device location is tracked and updates of the location are sent to the user's online account (210) at suitable intervals. The location reporting rate can be set at a higher rate than in the user settings.

While Fig. 2 illustrates accelerometer-based detection, other sensors such as location sensor, gyroscope, camera, etc. can also be used, or a combination of sensors can be used to detect sudden device removal. In this manner, the techniques described herein can mitigate the risk of a data breach when a user's mobile device is stolen, and can enable recovery of the device through location tracking.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user's social network, social actions or activities, profession, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes techniques to reduce the risk of a data breach when a mobile device is stolen. In certain modes, e.g., augmented reality (AR) mode, selfie mode, etc., optimal use of a mobile device requires that the user hold the device out at an arm’s length in a public location, leading to an increased likelihood of theft. With user permission, a potential risk state is activated upon detecting such use of the device. If sudden movement of the device, e.g., as detected by an on-board accelerometer, location sensor, or other sensor is detected, the device is automatically locked, requiring user authentication for data access. If the user permits, location tracking is also activated which can assist physical recovery of the device.

REFERENCES

1. https://www.youtube.com/watch?v=TWilMUpEMEk
2. https://www.theguardian.com/uk-news/2018/jun/07/moped-enabled-crimes-london-police-called-to-430-a-week-in-past-year