August 2023

Smartphone Semi-unlock by Grip Authentication

Michael Xuelin Huang

Recommended Citation

Huang, Michael Xuelin, "Smartphone Semi-unlock by Grip Authentication", Technical Disclosure Commons, (August 14, 2023)
https://www.tdcommons.org/dpubs_series/6136

Smartphone Semi-unlock by Grip Authentication

ABSTRACT

Viewing notifications on a smartphone or other device either requires the user to unlock their device or allow notification delivery on the device lock screen. Delivery of notifications on the lock screen, while convenient, can potentially leak user information. However, biometric (face, fingerprint, etc.) or password/pattern based authentication can be cumbersome and/or unavailable in many situations. This disclosure describes the use of a user's grip style to semi-unlock an electronic device such as a smartphone, tablet, laptop, etc. without compromising privacy. Unlike biometric authentication (fingerprint, face, etc.), grip data alone does not contain sufficient personal characteristics to authenticate a user. Per techniques of this disclosure, to authenticate the user via grip, the user is instructed to perform a simple stimulated gesture. The sequential grip dynamics during the time the user performs the gesture are observed. For example, the gesture can be grasping the body of the device. Upon successful grip authentication, low confidentiality notifications can be displayed, or features such as a virtual assistant be made available to the user.

KEYWORDS

- Grip authentication
- Grip dynamics
- Stimulated gesture
- Semi-unlock
- Partial unlock
- Notification delivery
- Lockscreen

BACKGROUND

Notifications on smart devices such as smartphones, tablets, smartwatches, etc. can be displayed on the device lock screen (which is the user interface displayed when the device is locked). Such notifications provide convenience, but can leak user information, e.g., if notifications pop up when the device is held by a different user than the device owner, if the locked device is stolen, etc.

However, requiring formal authentication for the user to view notifications can be inconvenient and/or burdensome at times due to factors such as insufficient lighting for face authentication, wet or dirty fingers making the fingerprint sensor inaccessible, or the requirement to enter lengthy passwords and/or other authentication information (e.g., codes, patterns, etc.). Semi-unlock authentication, when enabled, allows users to access information that is associated with a low level of confidentiality. Some devices also implement automatic unlocking without explicit user authentication based on the device being present in a trusted location, being proximate to a trusted device, etc.

DESCRIPTION

This disclosure describes the use of a user's grip style to semi-unlock an electronic device such as a smartphone, tablet, laptop, etc. without compromising privacy. Unlike biometric authentication (fingerprint, face, etc.), grip data alone does not contain sufficient personal characteristics to authenticate a user. Per techniques of this disclosure, to authenticate the user via grip, the user is instructed to perform a simple stimulated gesture. The sequential grip dynamics during the time the user performs the gesture are observed. For example, the gesture can be grasping the body of the device. Upon successful grip authentication, low confidentiality notifications can be displayed, or features such as a virtual assistant be made available to the user.

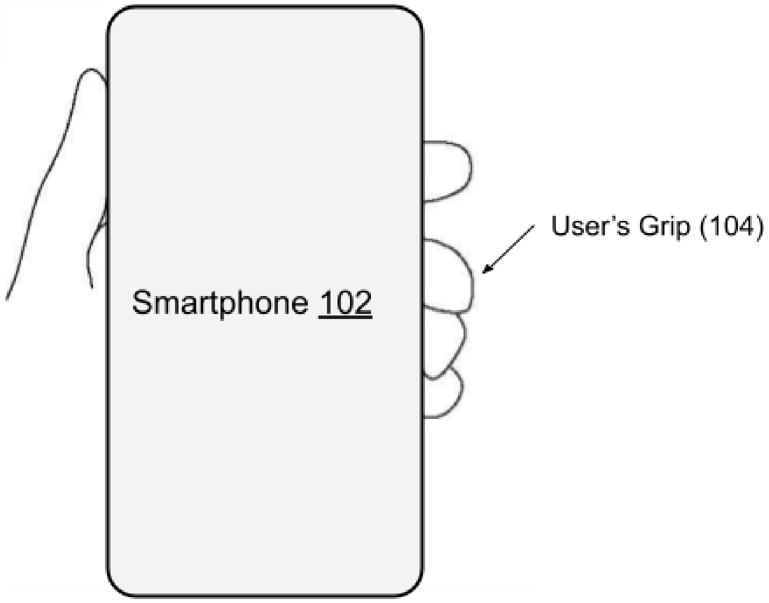

Fig 1: Smartphone Semi-unlock by Grip Authentication

Fig. 1 illustrates an example of how a user can semi-unlock their device by gripping it. A smartphone in a locked state (102) is gripped by the user in a way that is familiar and comfortable. The device sensors, e.g., the inertial measurement unit (IMU), barometer, etc. detect the user's gesture. The sensed values encode the amount of force applied to the smartphone housing and the amount of rotation it causes. This information can be used to model user-specific characteristics of grip dynamics, e.g., how the user's palm and wrist move during the performance of a stimulated gesture. These characteristics can be used for authentication. The stimulated gesture can be set as the input command to show notifications.

While such authentication does not contain strong biometric features that uniquely identify an individual user, it can be useful to identify a particular individual within a small group of users. The user effort to perform the authentication gesture is comparable to existing gestures such as "scroll down to see notifications" that the user performs on the lock screen and provides the added advantage of an extra layer of protection.

Grip authentication semi-unlock as described herein is a supplementary technique for existing unlocking techniques and can be used to show a class of notifications that correspond to the level of authentication. Grip authentication can also enable access to features and data that does not require strict confidentiality, e.g., interacting with a virtual assistant or chatbot. Sensitive notifications as well as full device features can be restricted such that these are available only on a fully-unlocked device using traditional formal authentication techniques.

CONCLUSION

This disclosure describes the use of a user's grip style to semi-unlock an electronic device without compromising privacy. Unlike biometric authentication, grip data alone does not contain sufficient personal characteristics to authenticate a user. Per techniques of this disclosure, to authenticate the user via grip, the user is instructed to perform a simple stimulated gesture. The sequential grip dynamics during the time the user performs the gesture are observed. For example, the gesture can be grasping the body of the device, etc. Upon successful grip authentication, low confidentiality notifications can be displayed, or features such as a virtual assistant be made available to the user.

REFERENCES

1. Mare, Shrirang, Reza Rawassizadeh, Ronald Peterson, and David Kotz. "Continuous smartphone authentication using wristbands." In *Proceedings of the Workshop on Usable Security*. 2019.