Obfuscator Overlay for Fingerprint Sensor

David Ogutu
ABSTRACT

Fingerprint authentication is a convenient technique for authentication on consumer devices such as smartphones, tablets, laptop computers, etc. However, some users have concerns regarding privacy of their fingerprint data. This disclosure addresses such privacy concerns while retaining the ability for users to utilize fingerprint authentication. Per this disclosure, an obfuscating capacitive layer along with a capacitive sensor is placed on a fingerprint sensor, or is integrated in a fingerprint sensor. The layer generates a random pattern at the time of creation of the layer. This pattern along with the user’s fingerprint is recognized and used to authenticate a user. In this manner, a user’s fingerprints are not used directly, which enhances user privacy. Since the layer does not change over time, the sensor generates deterministic patterns in response to the user’s fingerprints and makes authentication possible.

KEYWORDS

- Fingerprint sensor
- Fingerprint obfuscator
- Capacitive overlay
- Biometrics

BACKGROUND

Many users are hesitant to use fingerprint sensors for authentication purposes. For example, such hesitancy may be due to a desire to avoid storage and use of their fingerprints on a device, or by an authentication provider. For example, manufacturers of computing devices such as smartphones, tablets, laptops, etc. and providers of software applications that execute on those
devices may store or access fingerprint data for user authentication. However, fingerprint authentication is a convenient way to authenticate users.

**DESCRIPTION**

![Fig. 1: Sensor with obfuscating overlay](image)

This disclosure enables a fingerprint sensor that protects a user’s privacy. A thin capacitive overlay (104) is placed above a capacitive sensor (102). The overlay has a random pattern (106) at the time of its creation. The pattern is useful to protect the user’s fingerprint details.

In operation, when a user places the finger on top of the overlay, a pattern is generated that the fingerprint sensor picks up. The generated pattern is a combination of the pattern (106) and the user’s fingerprint. Since the generated pattern is different from the user’s fingerprint, the layer ensures that the user’s fingerprint is never captured or stored directly. Further, since the layer doesn't change over time, the capacitive sensor can provide authentication is still possible due to the generated pattern being deterministic. Therefore, the disclosure enables authentication via fingerprint sensors.
The capacitive layer as disclosed herein is easy to deploy, unobtrusive, and protects user privacy, while retaining authentication capability. Moreover, it can be deployed without any changes to conventional fingerprint sensors, since the layer does not affect the sensing ability of such sensors. Alternatively, the obfuscating overlay can be directly incorporated into a fingerprint sensor, or the capacitive sensor shown in Fig. 1 itself can detect fingerprints. Different techniques may be used to generate and apply capacitive layers, based on the material used for the sensor.

The techniques can be deployed by manufactures of computing devices that include fingerprint sensors, by software application providers that utilize fingerprint authentication, and by business entities that utilize fingerprint data for various purposes.

In situations in which certain implementations discussed herein may collect or use personal information about users (e.g., user data, information about a user’s social network, user's location and time at the location, user's biometric information, user's activities and demographic information), users are provided with one or more opportunities to control whether information is collected, whether the personal information is stored, whether the personal information is used, and how the information is collected about the user, stored and used. That is, the techniques discussed herein collect, store and/or use user personal information specifically upon receiving explicit authorization from the relevant users to do so.

For example, a user is provided with control over whether programs or features collect user information about that particular user or other users relevant to the program or feature. Each user for which personal information is to be collected is presented with one or more options to allow control over the information collection relevant to that user, to provide permission or authorization as to whether the information is collected and as to which portions of the
information are to be collected. For example, users can be provided with one or more such control options over a communication network. 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. As one example, a user’s identity may be treated so that no personally identifiable information can be determined. As another example, a user’s geographic location may be generalized to a larger region so that the user's particular location cannot be determined.

CONCLUSION

This disclosure describes a practical and unobtrusive solution to protect user fingerprint data during authentication by fingerprint recognition. A thin capacitive obfuscating layer is included atop a fingerprint sensor. The capacitive overlay has a random pattern. At the time of recognizing a fingerprint, the sensor detects a combination of the user’s fingerprint and the random pattern. The layer is permanent over the lifetime of the sensor, and provides deterministic patterns that are usable for authentication.