Automatic Authentication of Smartphone Touch Interactions using Smartwatch

Juhi Ranjan
University of Virginia
Charlottesville, USA
juhi@virginia.edu

Kamin Whitehouse
University of Virginia
Charlottesville, USA
whitehouse@virginia.edu

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.
Copyright is held by the owner/author(s).
UbiComp/ISWC' 16 Adjunct, September 12-16, 2016, Heidelberg, Germany
ACM 978-1-4503-4462-3/16/09.
http://dx.doi.org/10.1145/2968219.2971370

Abstract
In this demo, we will display a smartphone authentication system that can automatically validate every touch interaction made on a smartphone using a smart watch worn by the phone's owner. The IMU sensors on a smart watch monitor the motion of the hand for specific signal characteristics, which is relayed to the phone. If the signal features match certain criteria then the touch is authenticated and the phone responds appropriately. If not, the phone's screen remains locked/unresponsive to the touch action. The challenge here is to be able to validate every touch gesture within acceptable limits of human perception.

Author Keywords
Phone Security; Touch Authentication; Wearables; IMU sensor

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous

Introduction
The ubiquity of smartphones is undoubted; by 2020, it is estimated that 70% of the global population will be using a smartphone [3]. This in turn has made sensitive and personal information more easily accessible in a way that it has become important to secure a smartphone with a locking

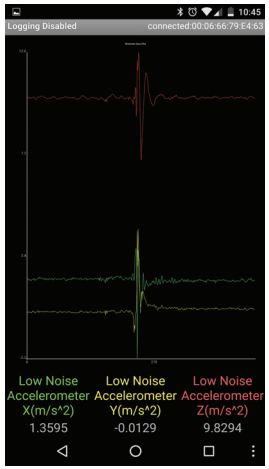

Figure 1: Sensor Datastream: Users will be able to visualize the sensor data stream while interacting with the phone

mechanism. According to a study, [1], an authentication procedure is seen as cumbersome by as many as 30% of smartphone users who leave their phones unlocked.

Most of the commercially available authentication mechanisms unlock once and then keep the phone unlocked until the screen is switched off the user. There are mainly two types of authentication methodologies present in smartphones -
1.Automatic and Implicit authentication - for e.g., using presence of a nearby bluetooth device, or a known location, such as home, to unlock the phone. In this, easier the unlocking mechanism, higher the security risk.
2. Manual and Explicit Authentication - for e.g. patterns or pin. In this, once the device is unlocked, it is not locked until the user shuts the screen off. Sharing phone with friends, for e.g., can allow them access all the data on the phone.

In this demo, we aim to answer a different authentication question - *how to continuously and automatically authenticate every touch gesture on a smartphone?*. We propose to do so by using a person-independent authentication mechanism, which assumes that the smartphone's owner wears a smartwatch. The intuition behind our system is that a smartwatch is usually present on the hand which either holds the smartphone or interact with the phone. IMU sensors present on-board the smart watch can detect specific signal behaviors which indicate that the phone's actual user is interacting with it.

Related Work

Commercial smartphone manufacturers have included a wide range of device unlocking mechanisms [2]. Some of these are - patterns, pin code, facial recognition, etc. Some LG devices even have a unique knock code to unlock the device. Android has released a new SmartLock feature [6] that does not lock the phone when it is within range of another bluetooth device, e.g. a smart watch. While this is convenient, any other person in the same location can also unlock the phone.

Researchers have been exploring ways to make unlocking of a phone more intuitive and automatic, while maintaining the security aspect. Nickel et al. propose a biometric gait based authentication system, in which they claim to identify the phone owner's walking pattern using on-board accelerometer [4]. In another work, Riva et. al proposed a system that uses factors such as biometric, continuity, possession of a phone, to determine that it is still with its owner [5]. This work assumes that if the phone is moving then it is in your hand, pocket, or purse, but it doesn't account for the possibility that the owner could have handed the phone to somebody.

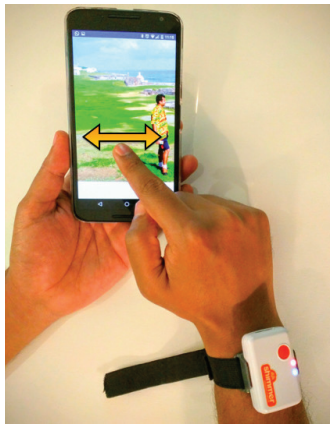

Figure 2: User Interaction Snapshot: Only the person wearing a smart watch paired with the phone can interact with the photograph on the screen

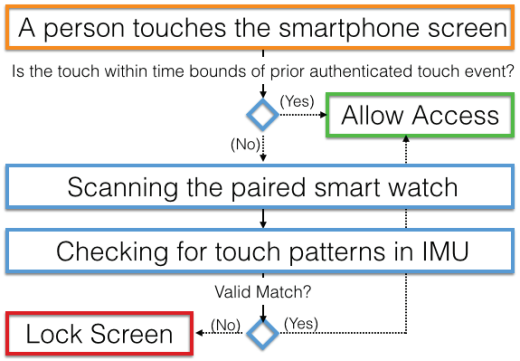

Figure 3: System flowchart of the authentication app

System Design

There are mainly two types of touch interactions on a smartphone that we consider in this demo - a. clicks (short taps), and b. scrolls (dragging motion). The smart watch currently samples the IMU data (accelerometer+gyroscope+magnetometer) at 100 Hz and streams it continuously to the smartphone, as shown in Figure 1. The phone app performs feature extraction on the received data. As shown in the Figure 3, when the person wearing the smart watch (presumably the phone's owner) interacts with the phone (shown in Figure 2), the app temporally correlates the touch activity with the motion sensed by the watch. First the system check if the touch event is within short time span of a previously authenticated touch. If it is, then it validates the current touch without further checks. If not, then it searches the smart watch sensors for certain features to determine if the watch registers a touch gesture. If a touch gesture is detected, then the touch event is authenticated and the system responds to the gesture appropriately. If the touch event is not authenticated, then the phone's screen remains unresponsive.

We have implemented this system using only off-the-shelf hardware systems: a Nexus 6 Android phone, and a Shimmer wearable device.

Demo Application

Our system interacts with the user via an Android App. The user wears a smart watch, and interacts with photographs and text on the app. For a person wearing the smart watch, the interactions should be smooth and uninterrupted. If a person who is not wearing the smart watch tries to click or scroll anywhere on the screen, the phone's screen freezes. The users will be able to use the devices in different combinations of - A. hand holding the phone, B. hand wearing the smartwatch, and, C. hand interacting with the phone. There are eight combinations of (A,B,C) - (L,L,L), (R,R,R), (L,L,R),

(R,R,L), (R,L,L), (L,R,R), (L,R,L) and (R,L,R), where 'L' stands for Left Hand and 'R' stands for Right Hand. Participants can try out any of these combinations to except for (L,R,L) and (R,L,R) in which the phone is held in the same hand which is interacting with it, while the wearable is on the other hand. In these two cases, the wearable is not able to sense the hand using the phone and therefore cannot validate the touch of the user. Users at the demo are free to experiment in interacting with the app's contents in different ways to validate the robustness of the system.

Conclusions

Smartphones are widely used by people all over the world now. These phones are often linked with their user's personal email account, and contain sensitive personal information. While password protected screen locks are one way to guard the data in the phone, many people don't use any security mechanisms as they consider them inconvenient. In this demo, we present a new implicit smartphone security mechanism for users who own a smart watch as well. The proposed security mechanism aims to implicitly validate whether every touch made on the screen as belongs to the owner of the phone or not. To do so it uses orientation independent features of the smart watch sensors, which can discern the fine motions of a person's hands.

Acknowledgement

This work was funded in part by NSF awards 1305362, 1038271, and 0845761 and NSF Graduate Research Fellowship Program 0809128.

REFERENCES

1. 2011. People Do Not Secure Phones. (2011). http://www.bullguard.com/news/latest-press-releases/press-release-archive/2011-06-21.aspx.
2. 2014. 10 Ways to Secure Your Smartphone. (2014). http://www.androidcentral.com/10-best-ways-secure-your-smartphone.
3. 2015. Smartphone Usage Predictions. (2015). http://www.pcmag.com/article2/0,2817,2485277,00.asp.
4. Claudia Nickel, Tobias Wirtl, and Christoph Busch. 2012. Authentication of smartphone users based on the way they walk using k-NN algorithm. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on*. IEEE, 16–20.
5. Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive authentication: deciding when to authenticate on mobile phones. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)*. 301–316.
6. smartlock 2016. Android Smart Lock. (2016). https://support.google.com/nexus/answer/6093922?hl=en.