# Real Time Motion-Based Authentication for Smartwatch

Antwane Lewis*, Yanyan Li†, Mengjun Xie†
*Philander Smith College, Email: lewis.antwane@philander.edu
†University of Arkansas at Little Rock, Email: {yxli5, mxxie}@ualr.edu

***Abstract*—Smartwatches become increasingly powerful and popular. These personal devices carry multiple sensors that continuously measure, collect, and analyze various sensitive personal information. Therefore, a strong and user friendly authentication mechanism is much needed to prevent illegitimate accesses to those devices. However, traditional protection approaches are far from sufficient and desirable for smartwatches. In this work, we present our recent study on developing and testing a motion-based real time authentication system for smartwatch. Our system applies behavioral biometrics collected from a smartwatch to verify the person who wears the watch. We have developed a prototype application using Android Wear to authenticate users in real time. We tested our system against two types of attacks to evaluate its resilience to attacks. We recruited five volunteers in our preliminary evaluation, from which some interesting findings were discovered. Our preliminary experimental results indicate that real time motion-based authentication is viable and promising.**

***Index Terms*—Smartwatch; Authentication; Gesture**

## I. Introduction

Smartwatches become increasingly popular. These personal devices have many built-in sensors that can capture, record, and store a variety of sensitive personal data that should be well protected. However, traditional protection approaches on those devices are far from sufficient and desirable. For example, the small screen of smartwatches makes it challenging for users to use password or personal identification number (PIN) based authentication methods.

Inspired by the growing interest in applying behavioral biometrics to mobile authentication and the high sensing capability of smartwatches, in this work, we present our recent study on developing and testing a motion-based real time authentication system for smartwatch. Leveraging the experience accumulated through MotionAuth [6], we have developed an authentication prototype system using Android Wear to authenticate users in real time. Our system collects behavioral biometrics from a smartwatch to verify the person who wears the watch. The authentication process for our prototype system consists of two phases: a training phase and a testing phase. In the training phase, a user profile (or called template) is created using the sensory data collected from the smartwatch during the user performing a given gesture designed for authentication. In the testing phase, the sensory data captured during gesture performance is matched against the profile of the claimed user to verify the user's authenticity.

Our prototype system collects data from accelerometer and gyroscope and applies the dynamic time warping (DTW) method for template generation and matching. We included two types of attacks to evaluate our system's resilience to attacks. We recruited five volunteers in our preliminary evaluation, from which some interesting findings were revealed. The preliminary experimental results indicate that a real time motion-based authentication scheme is highly promising and practical for smartwatches with appropriately designed gestures.

## II. Related Work

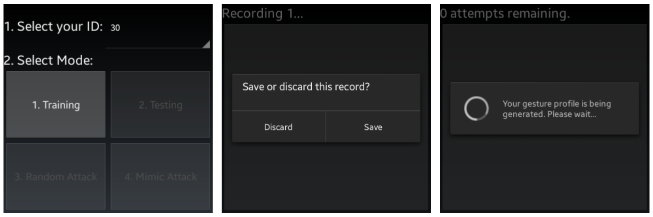
Authentication refers to a process in which provided credentials are compared to those already on file in a user database. If the credentials match, the user's identity is verified. Behavioral biometric authentication verifies users through their behavioral traits, e.g., touch gestures [3], [2]. Yang *et al.* presented MotionAuth in [6], which is a behavioral biometric authentication method applied on wrist-worn devices to verify the identity of the person wearing the device. MotionAuth focuses on offline data analysis and its tested gestures are predefined and the same for all participants. Xu *et al.* described how to measure motion energy in smartwatches and how to uniquely identify a user's hand and finger gestures in [5]. Sherman *et al.* discussed the security and memorability of free-form multitouch 2D gestures for mobile authentication in [4].

## III. System Design and Implementation

We use two motion sensors universally built in smartwatches, i.e., accelerometers and gyroscopes, to collect motion data for authentication. We assume that users perform custom free-form gestures using the arm wearing the smartwatch. During the training phase, a user first constructs a free-form 3D gesture and then performs it multiple times to create the template. The user's gesture performance is also recorded in video for later mimicry attack experiments. In the testing phase, a user is asked to perform the same gesture multiple times to examine the system's accuracy. Our smartwatch application decides whether to accept or reject the user in real time after each gesture performance. To assess the system's capability of countering attacks, we conducted two types of attacks: random attack and mimicry attack, which are explained as follows.

- Random Attack: The attacker has no knowledge of the legitimate user's gesture. The attacker randomly performs gestures in hope of passing the authentication. This type of attacks aims to reflect the scenario where a person tries to gain access to a lost or stolen smartwatch.

978-1-5090-3065-1/16/$31.00 ©2016 IEEE

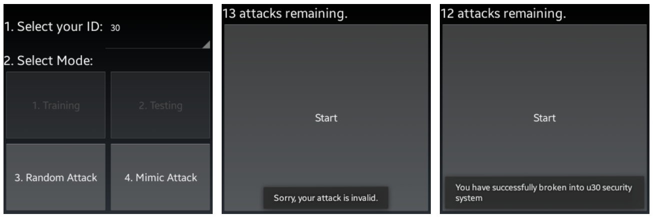


Save or discard this record?

Your gesture profile is being generated. Please wait...

(a) (b) (c)

Fig. 1: Screenshots of the prototype app for smartwatch



Sorry, your attack is invalid.

You have successfully broken into u30 security system

(a) (b) (c)

Fig. 2: Screenshots of performing attacks

- Mimicry Attack: The attacker knows the legitimate user's gesture (by watching the recorded videos) and pretends to be the user to gain the access. This type of attacks is much similar to shoulder surfing attacks.

DTW is applied as the method for matching given its popularity in biometric authentication and acceptable accuracy and computational cost. DTW has been used in many gesture authentication studies such as [1], [6] recently.

We implemented an Android prototype application. Some screenshots of the app's user interface (UI) are shown in Fig. 1. Each user is uniquely identified through an ID number. No personal information is recorded. To start the training, a user has to select the assigned ID number and then press "Training" button. The user can choose to save or discard each performed gesture (Fig. 1 (b)). After the user repeats the gesture for a given number of times, the gesture profile will be automatically generated using the DTW method (Fig. 1 (c)).

The app also allows for testing random and mimicry attacks. Fig. 2 displays some screenshots of the app when attacks are launched. Fig. 2 (b) shows the screen when an attack fails while Fig. 2 (c) shows the screen for a succeeded attack.

## IV. Evaluation

Five volunteers participated in the evaluation. All the participants are college students. They were asked to wear a Samsung Galaxy Gear smartwatch on the preferred arm for training, testing, and attack. Before training started, each participant was given time to make their desired gesture and practice it. The evaluation took two days with the first day for training (each participant performing a custom gesture 30 times) and first-round testing (30 times per user) and second day for second-round testing (30 times per user) and random and mimicry attacks. Each participant performed 15 random attacks and 15 mimicry attacks against every other participants. So each participant received 60 random attacks and 60 mimicry attacks in total.

TABLE I: Results of 2 rounds of testing and attacks. Format: #-of-successes/#-in-total

| | Round 1 Tests | Round 2 Tests | Random | Mimicry |
|---|---|---|---|---|
| U1 | 27/30 | 30/30 | 0/60 | 0/60 |
| U2 | 30/30 | 30/30 | 0/60 | 45/60 |
| U3 | 13/30 | 21/30 | 0/60 | 0/60 |
| U4 | 25/30 | 26/30 | 0/60 | 0/60 |
| U5 | 11/30 | 20/30 | 0/60 | 0/60 |
| Total | 106/150 | 127/150 | 0/300 | 45/300 |

All the participants' motion data were recorded for further in-depth offline analysis, which is still undertaken. Table I presents the online results for the two rounds of testing and attacks. We can clear see that personalized gestures can effectively defeat random attacks and most of mimicry attacks. Interestingly, the participant with ID 2 was vulnerable to the mimicry attack. By reviewing the video recording of his gesture, we found that his gesture is too simple (like banging his fist on the table twice) to withstand mimicry attacks. Some users did not get a high acceptance rate in the first round of testing partially due to insufficient practice. The false acceptance rate was significantly reduced in the second round of testing.

## V. Conclusion

In this work, we developed a gesture based real time authentication system for smartwatch and conducted a preliminary evaluation study. We not only measured the system's accuracy in accepting legitimate users based on their personalized free-form gestures but also examined the system's resilience to random and mimicry attacks. Our experimental results indicate that the proposed system is promising. Our future work includes more data collection and in-depth data analysis.

## Acknowledgment

This work was supported in part by the Research Experiences for Undergraduates (REU) Program of the National Science Foundation under Award Number 1359323.

## References

[1] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proc. CHI '12*, pages 987–996, 2012.

[2] P. Saravanan, S. Clarke, D. H. P. Chau, and H. Zha. Latentgesture: Active user authentication through background touch analysis. In *Pro. 2nd International Symposium of Chinese CHI*, pages 110–113, 2014.

[3] M. Shahzad, A. X. Liu, and A. Samuel. Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it. In *Proc. MobiCom '13*, pages 39–50, 2013.

[4] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos. User-generated free-form gestures for authentication: Security and memorability. In *Proc. ACM MobiSys '14*, pages 176–189, 2014.

[5] C. Xu, P. H. Pathak, and P. Mohapatra. Finger-writing with smartwatch: A case for finger and hand gesture recognition using smartwatch. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, pages 9–14. ACM, 2015.

[6] J. Yang, Y. Li, and M. Xie. Motionauth: Motion-based authentication for wrist worn smart devices. In *Proc. the 1st Workshop on Sensing Systems and Applications Using Wrist Worn Smart Devices*, pages 550–555, 2015.