Leveraging Movement, Posture, and Anthropometric Contexts to Strengthen the Security of Mobile Biometrics

Matthew Lombardo[1], Ariana LaCue[2], Moazam Abass Mir[3]
Kiran Balagani[3], Paolo Gasti[3], Rosemary Gallagher[3], Isaac Kurtzer[3]
[1]Johns Hopkins University, [2]Kean University, [3]New York Institute of Technology
mlombar7@jhu.edu, lacuea@kean.edu, mabass@nyit.edu,
kbalagan@nyit.edu, pgasti@nyit.edu, rgalla01@nyit.edu, ikurtzer@nyit.edu

Abstract

Behavioral biometrics are characteristics of human behavior (such as how a user swipes on their smartphone) that can be used to authenticate individuals in smartphone security applications. In this project, we investigate the effects a user's posture has on her smartphone behavior; e.g. does whether a person is sitting vs. walking significantly affect some of their behavioral biometrics? This question is very relevant to behavioral biometric authentication systems; if the way a user interacts with her smartphone changes significantly as her posture changes, the security system needs to be able to distinguish between these circumstances to always recognize her, regardless of her posture. To track this information, we developed two apps: one that records the user's swiping activity, and one that records the user's typing activity. Using these apps, as well as a motion capture system to monitor posture information, we ran data collection sessions to obtain behavioral biometric data, and began processing it to investigate whether posture has a significant effect on smartphone behavioral biometrics.

Background

Authentication:

In a security context, *authentication* is the process of verifying that a user is who they say they are. One common form of smartphone authentication is the passcode. The issue with security measures like passcodes is that anyone with the information can access the system; there is no check that it is actually the device's owner entering the correct passcode.

Biometric Authentication:

Using biometrics (physiological characteristics such as facial geometry and fingerprints) to verify users. With these systems, it is difficult to replicate an exact physical feature of someone. An example is Apple's Face ID, which scans your face to verify you are the owner.

Behavioral Biometric Authentication:

Using behavioral biometrics (see abstract) to authenticate user identities. The benefit this has is twofold:

- 1.) Authentication is *implicit* – the user does not need to take any inconvenient security steps (like reentering passcode), their identity can be authenticated automatically without their effort.
- 2.) Authentication is *continuous* – the user of the device can be continually verified. This is very relevant to intrusion, as even if an intruder accessed the device through a passcode, the device could still detect that it is an intruder using the phone.

Behavioral Biometrics & Posture

The objective of this project is to investigate whether behavioral biometrics change as a user's posture changes. For instance, a user leaning against the back of a chair may hold her phone differently than when she is walking down the street, leading to different swiping patterns. We hypothesize that posture will have an effect on smartphone interaction, and will investigate the extent that this affects authentication.

Data Collection Apps

These apps were developed to obtain phone usage information from the user during experiments. They both record accelerometer, gyroscope, and face-tracking data, as well as video from the front facing camera. They are native iOS apps, written using the Swift language in Xcode.

Typing App:

In this app, the user is prompted to answer basic questions, of which she must respond with a minimum of ten characters. Once she finishes responding, she hits the 'Next' button, and is brought to a new question. The questions are shuffled in a specific order based off the user's experimental ID, in order to ensure the same question never occurs more than once. This app also records all of the keystrokes entered by the user (characters, spaces, backspaces, etc.).

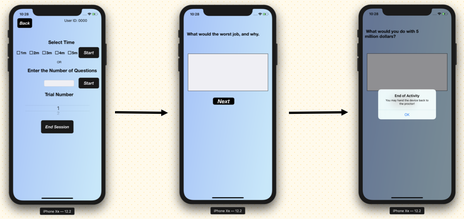

Figure 1. The UI of the typing app. The first screen (left) is only used by the proctor. The participant then hits 'Start', and answers questions until the trial is up, at which time the alert in screen 3 (right) appears.

Swiping App:

In this app, the user is presented with the name of a color (either Blue, Green, Red, or Yellow), whose font is also one of those four colors. Her task is to drag the word to the border corresponding to the color name, not the font color (e.g. if the word 'Blue' popped up in a green font, she would drag that word to the blue border). Once the word touches the correct border, it disappears, and a new word appears. This app also records all of the swipe data of the user, documenting where the user's finger is on the screen, and at what times, during all swipes.

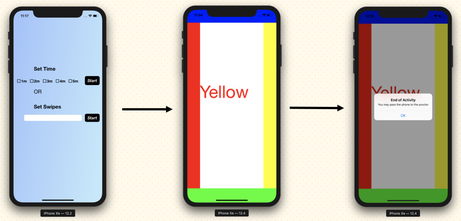

Figure 2. The UI of the swiping app. The first screen (left) is only used by the proctor. The participant then hits the 'Start' button, and drags words trial is up, at which time the alert in screen 3 (right) appears.

Experiment Setup

Figure 3. The Motion Capture Studio, as seen from the ground floor. The bright red lights are the IR illumination LEDs mounted on the Vicon cameras.

Figure 4. Another view of the Motion Capture Studio, as seen from above.

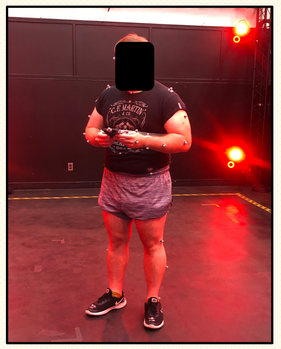

Figure 5. User set-up for data collection. The silver spheres taped to the subject are the sensors monitored by the cameras.

The experimental portion of this research was conducted at the Motion Capture Studio on New York Institute of Technology's campus in Old Westbury, Long Island. The studio is equipped with 36 cameras, which track sensors on the subjects as they move around the studio. This data is then fed to a computer, which produces the real-time video of the subject moving, as seen in Figure 6 (walking) and Figure 7 (sitting). The subjects wore 30+ sensors to be tracked by the motion cameras, as seen in Figure 5, and 3 sensors were placed on the phone as well. The users participated in 2 sessions (one on each of two different days), and during each session completed 12 1-minute trials of each app, 6 trials walking and 6 trials sitting.

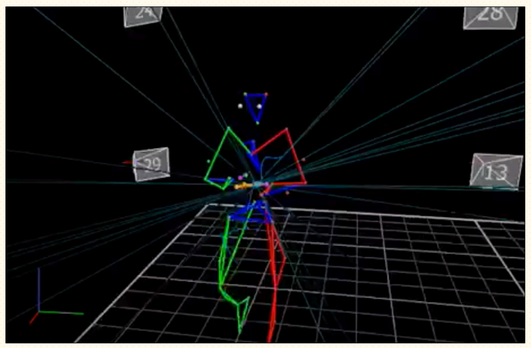

Figure 6. A visualization of the motion capture data during a walking trial. The lines connect 2 sensors on the body, and the numbered, gray squares in the background represent the cameras.

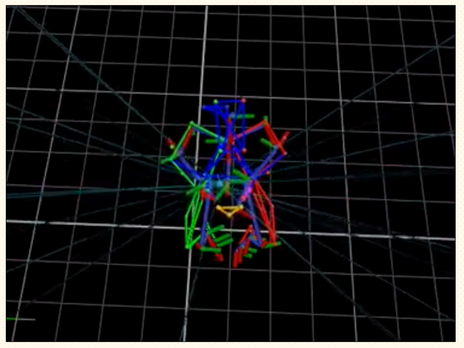

Figure 7. A visualization of the motion capture data during a sitting trial. As in Figure 10, the lines connect 2 sensors on the body.

Data Processing

When the data arrives from the phone and cameras, it is simply columns of numbers in spreadsheets, and hence has to be processed into meaningful information. *Feature extraction* is the process of "extracting" certain parameters of interest from those spreadsheets, such as reconstructing swipes from the raw swipe data or calculating the velocity of swipes. This analysis is done in MATLAB, and will be a major focus of the project moving forward (see "Future Work").

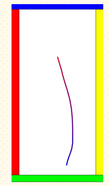

Figure 8. A reconstructed swipe. The color fades from red to blue over time.

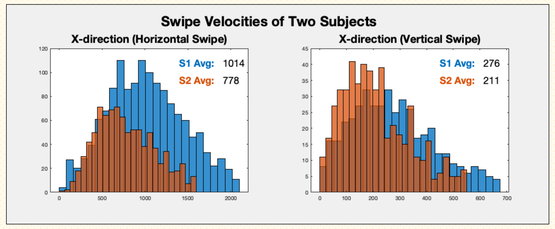

Figure 9. Average swipe velocities for two different users; this shows that swipes are distinguishable between people.

One data processing issue that will need to be addressed is that of *synchronization*. The phone data, phone video, and motion capture data all record the same events, but on different systems and with different timestamps. Thus, the data must be synchronized to a single timeframe, so that the video, phone, and capture data can all be accessed for any specific instance of time.

Future Work

There are two major focus areas for the future:

- 1.) Designing a take-home app: the experiments conducted during this research were test trials, to work out issues with the app and experiment setup. Now, the apps will be combined into a single app that users will take home on a phone, which will prompt them to complete activities over the course of several months.
- 2.) More feature extraction: more features, aside from swipes and velocity, need to be considered. Thus, more feature extraction tools must be built to process these.

Acknowledgement

This research was supported by the National Science Foundation (NSF) Research Experiences for Undergraduates (REU) program at the New York Institute of Technology (NYIT) and NSF grant nos. 1852316 and 1619023.

References

[1] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication," IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, pages 136 – 148, 2013.
[2] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, Jan. 2015.
[3] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," IEEE Transactions on Information Forensics and Security, Vol. 11, No. 5, May 2016.