Behavioral Biometric Identification on Mobile Devices

Matt Wolff

University of Hawaii, Honolulu, HI 96813, USA
wolffm@hawaii.edu
http://www2.hawaii.edu/~wolffm

Abstract. We show that accelerometers, touch screens and software keyboards, which are standard components of modern mobile phones, can be used to differentiate different test subjects based on the unique interaction characteristics of each subject. This differentiation ability can be applied to authenticate individuals under a continuous authentication scheme. Based on six 15 minute data sets collected from the test subjects utilizing our data collection platform, we extract multiple features from the data and show an ability to accurately identify individuals at a rate of 83 percent using a simple normal distribution of each feature.

Keywords: identification, security.

1 Introduction

Determining the authenticity of the user of a computing device is always an issue when considering a system's security. Standard security practices invoke the use of some type of challenge/response pattern, including passwords, patterns, or biometrics such as a fingerprint. Typically the challenge/response pattern is presented to a user at initial access or at some interval. Initial authentication provides a level of defence at initial access to computing. Continuous authentication, the process in which a user in continually authenticated based on some metrics, can also be applied to authenticate the user during their interaction with a computational device. The use of continuous authentication improves the security of a device by verifying a user after the initial authentication, and continues to do so during the lifetime of user interaction.

Mobile devices are now starting to become the dominant model of human computer interaction. It is estimated that by 2015 over 5 billion devices will be in use worldwide [1]. This growth can be attributed to the low cost, ease of use, and innovative interaction models that are provided by these devices. Many of these mobile devices contain a set of sensors that are capable of tracking low level interaction characteristics of the device user.

In this paper, we look at the different sensors provided by mobile phones, and show that data collected from these sensors can distinguish mobile users by analyzing the user's interaction with the device. Our system observes the interaction characteristics of what we define as behaviormetric data - the subset

D.D. Schmorrow and C.M. Fidopiastis (Eds.): AC/HCII 2013, LNAI 8027, pp. 783–791, 2013.

of biometric data that can be used to express individual behaviors, such as gait, In particular, we collect information from the user/device acceleration, keystrokes, and touch interactions. The analysis engine then extracts key features from the data to support differentiation of users.

2 Related Work

The collection of behaviormetric data is a requirement for conducting any type of behaviormetric analysis on a system capable of collecting such information. Below we take a look at studies that included the collection of behaviormetric data on mobile devices, and the methodologies used in each study.

2.1 Gait-Based Collections

Gait-based classification of users has received recent attention in the field of behaviormetrics, mostly due to the accessibility of mobile devices that contain accelerometer sensors. Boyle et. al. [2] conducted a series of five data collection activities to generate a data set pertaining to sensor readings during the act of walking by test subjects. The authors place a Motorola A855 into the possession of each test subject to collect accelerometer and magnetometer data. In the first three series of data collection activities, the authors collected 33 samples of accelerometer and magnetometer data per experiment on two subjects, with each sample duration being under 60 seconds. The fourth experiment introduced two additional subjects with 28 samples collected per user. In the last experiment, 117 segments of data are collected on each user, with a variance in walking speed across each sample that was not present in previous experiments conducted by the authors.

Mantyjarvi et. al. [3] attached a three-dimensional accelerometer behind the waist of all test subjects. 36 test subjects walked a distance of 20 m at normal, fast and slow speeds. The test was repeated after five days, with 108 total segments of data collected.

Gafurov [4] attached an accelerometer to the leg of 21 study participants, who walked a distance of 35 meters in one direction, and 35 meters back to their original starting position. The data collected was divided into two section, the 35 meters before the turn around, and the 35 meters after the turn around. In a more comprehensive experiment [5], accelerometers were attached to the ankle, hip, pocket, and arm of test subjects while conducting the same walking test as in [4].

In additional gait-based studies, Marc et. al [6] place accelerometers on the ankle of test subjects. 5 subjects in the study walked for 1 minute 8 times a day for five days. Each 1 minute walk introduced different variables, either with different shoes or walking speeds. Over 200 minutes of walking data was collected from the 5 participants. [7] placed an iPhone into the pant pocket of 9 test subject to collect accelerometer and ambient audio data. The 9 participants walked for 2 minutes in indoor and outdoor environments on 3 separate days, with the additional requirement that participants wear different pants on each

day. In [8], 36 subjects placed an Android-based smart phone in the front leg pocket. Subjects were then asked to walk, job, climb up and down stairs for a specified period of time.

2.2 Other Accelerometer Collections

Another popular hand-held device, the television remote was also used for the collection of behaviormetric data. Chang [9] attached an accelerometer to the home remote control of five households. Accelerometer data was collected 24 hours a day for a period of one to three weeks per household.

2.3 Keystroke Collections

Clarke and Furnell [10], focused on the collection of keystroke dynamics based on the entry of telephone numbers and pin codes on a mobile keypad. In their first study, 16 subjects entered 11-digit phone numbers and 4-digit pins into a numerical pad that was typical of a cell phone keyboard input in 2003. In the second study, the authors recruited 30 participants and each participant completed 30 iterations of the entry of 11-digit phone numbers, 4-digit pins, and text messages. The authors collected data on the *inter-keystroke latency* and *hold-time* of the user keystrokes.

In the most comprehensive study of keystroke-dynamics on a mobile device, [11] has twenty-five users participate in a study that collected the press/release time of all keys over a diverse set of Nokia phones running the Symbian operation system over the course of 7 days. Between 2900 and 13713 key hits were recorded per user, correlating to the frequency of keypad use per subject.

[12] recruited 25 users to enter a 4-digit pin into a numeric pad. In this research, in addition to the natural entry method of the test subject, each subject was forced to enter a password with artificial pauses entered into the test entry. Each user created an enrolment set consisting of five password entry recordings, and an additional thirty password entry attempts per entry method. After the test subjects completed the task, they were then asked to pose as *imposters*, where they were given the pin of other test subjects and asked to enter the other subjects pin numbers twice.

[13] recruited forty test subjects, with each subject entering the same 6 password 20 times over four distinct sessions, with each session being a minimum of 10 minutes apart from another session into a alpha-numeric pad. Of note, to enter a character in this type of keyboard can require multiple presses of the same key to select the appropriate character.

[14] combined the use of a number pad with a touch screen to extract hold-time, inter-key duration, finger pressure, and finger position from 10 subjects. Each subject entered the ten digit number thirty times, in consecutive order. Pressure and position were recorded every 20 milliseconds.

3 Data Collection

We developed the software needed to collect readings from the accelerometer, software keyboard, and touch screen of a mobile phone running the Android operation system. Our data collection platform consisted of three major components; an ability to collect raw accelerometer readings across three dimensions, a custom software keyboard that allows for the capturing of keystroke information, and a modification to the android kernel that allows for the collection of touch screen interactions. We used this software to conduct a real-world data collection study of six individual test subjects.

4 Feature Selection

We identified three main areas to extract features from the data set: keystroke dynamics, touch dynamics, and accelerometer signals. For each feature that is selected from the data, we generate a normal distribution of the feature. The normal distribution takes the mean and variance of a feature over the course of the 15 minute test sample, and provides a representation of the probability of a given discrete data point occurring in the test sample. This allows us to compare the same feature across different test subjects to get a reasonable idea regarding the similarity of a feature between two test subjects.

4.1 Keystroke Dynamics

In our analysis of keystroke interaction, we identified several factors that provide a differentiation capability; inter-key duration, key hold time, key-to-key duration, and key press location. Inter-key duration is the measure of the time interval between the release of one key and the press of the next key in the time sequence. Key hold time is a measure of the amount of time a key is held by the user. Key-to-key duration is the inter-key duration between two specific keys. Key press location is the two-dimensional location inside the key where the user initially pressed a key.

4.2 Touch Dynamics

Touch dynamics refers to the extraction of features from the user interaction with a touch screen. In our data collection platform, we are able to determine the location, pressure, and size of each discrete touch event. Typically, multiple discrete touch events are combined to represent a single action. For example, the press of a button may generate a touch event for the down motion, a few events while holding the button down, and a final event when releasing the button.

We separated out touch actions into two distinct groups; taps and gestures. Taps are the collection of touch actions where the distance between the starting and ending point of the touch are below some minimum threshold, and gestures

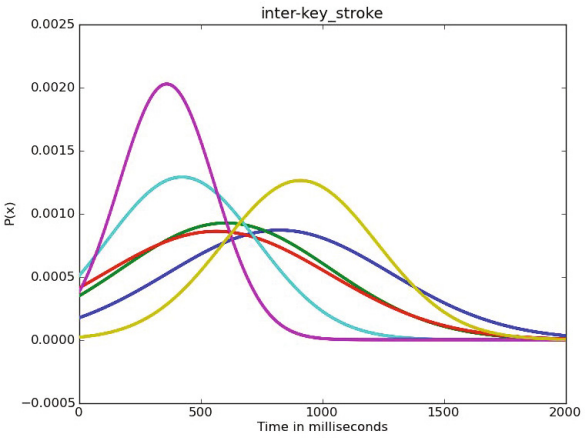

Fig. 1. Normal distribution of each of the six test subject's inter-key duration

consist of the group where the distance is above the same threshold. This separation provides the benefit extracting features from user gestures, such as swipes or scrolling, without being influenced by button presses or selections.

Features of interest identified from the collection of tap activities include the duration of a tap, the two-dimensional location of a tap, the overall pressure of a tap, and the size of a tap. For the collection of gestures, we extracted additional features, inducing the direction of a gesture, the end point, the distance between the start and end of a gesture, the speed of a gesture, and the lateral variance on a gesture. Lateral variance is a measure of the amount of non-direct movement in a gesture. This is calculated by drawing a direct line between the start and end points of a gesture, and calculating the distance between every discrete point that generated the gesture and the direct line between the start and end point.

4.3 Accelerometer Dynamics

Device accelerometers provide acceleration data across three dimensions. In our data collection platform, discrete acceleration events were captured at a rate of about 100 per second during the course of each test subject's interaction. Two main features were extracted from the acceleration data; stability, which is a measure on the variance in acceleration over distinct time periodd, and orientation, which provides an idea of the direction of the x, y, and z axis of the device relative to gravity.

5 User Identification

The main goal of this study is to determine if the behaviormetric data collected from a mobile phone can be used to identify the individual that generated the

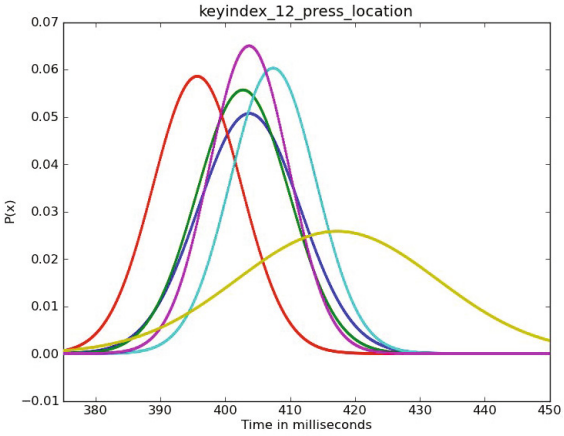

Fig. 2. Normal distribution of the X coordinate of each user's press when hitting key number 12 on the keyboard

data. To test this ability, we remove a random 90 second sample of data from a single user's 15 minutes of data. We then take the random sample, and compare it against the data of each user to find the user most likely to generate the sample.

For each test subject, we calculate a score representing the probability that the 90 second selected sample was generated by the test subject. The score is calculated as follows:

- For each feature (i.e. gesture pressure, z axis acceleration), a continuous normal distribution is generated representing the probability of a discrete event for the test subject and the 90 second sample
- For each feature, we determine the Bhattacharyya coefficient, which represents the amount of overlap between the two statistical samples
- For each feature, the Bhattacharyya coefficient of every test subject is normalized so that the sum of the coefficients for a single feature equal 1
- For each test subject, the normalized coefficient's are summed to generate a score representing the likelihood that the test subject generated the 90 second sample

Figure 5 compares the normal distribution of the 90 second test sample on the x coordinate ending point for a gesture feature to the same feature of each test user. In this figure, the black line represents the normal distribution of the 90 second sample. Based on this figure, one can determine that the purple and blue users have a high probability of having generated the 90 second sample, where as the other four test subjects have a low probability of having generated the 90 second sample.

Overall, for each test subject, we selected six random 90 second samples to test the ability to identify the test subject that generated the data. Using the

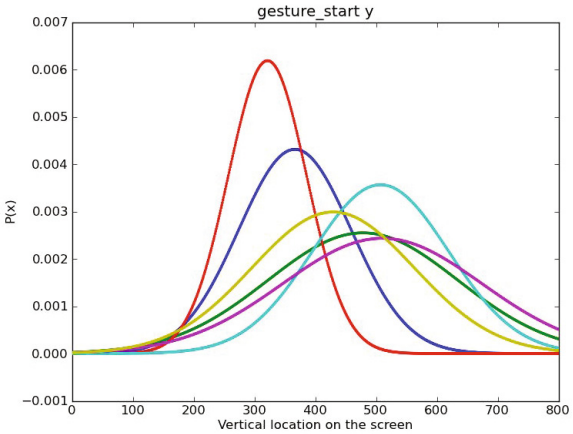

Fig. 3. Normal distribution of the Y coordinate for each user when a user starts a gesture

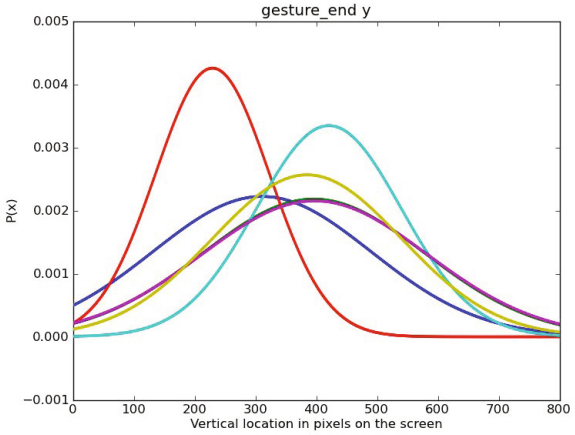

Fig. 4. Normal distribution of the Y coordinate for each user when a user ends a gesture

above technique to compare the selected sample against test subjects, we were able to correctly identify the test subject that generated the 90 second sample 83% of the time. We note that, due to the small sample size, we were not able to include keystroke dynamic features into the identification calculation. Many of the 90 second samples simply did not have enough keystroke information to make any type of determination.

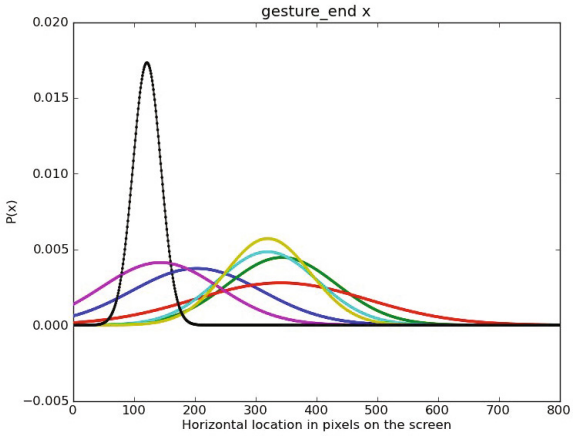

Fig. 5. Black line represents a normal distribution of the X coordinate of the ending point of a gesture of the 90 second sample, compared to all user's normal distribution

6 Conclusion

We have constructed a data collection platform to test the hypothesis that sensors on a mobile device, in particular the accelerometer, touch screen, and keyboard, can be used to differentiate between different users. Based on 15 minutes of real-world device interaction from six test subjects, we were able to correctly identify the test subject that generated a 90 second sample 83% of the time using a subset of features extracted from the data.

Although these findings are encouraging, a larger scale study incorporating more users and larger sample sizes is needed in order to make a more robust determination on the ability to identify users based on their behaviormetric data. In addition, more refined algorithms, as opposed to normal distribution of features as used in this preliminary research, will likely be more effective at user identification. Ultimately, these results provide a simple indication that further study in this area will likely lead to positive results.

References

1. Mcafee, McAfee Threats Report: Second Quarter 2011 (2011)
2. Boyle, M., Klausner, A., Starobinski, D., Trachtenberg, A., Wu, H.: Gait-based User Classification Using Phone Sensors. ipsit.bu.edu, pp. 395–396, `http://ipsit.bu.edu/documents/mobisys11.pdf`
3. Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S., Ailisto, H.: Identifying users of portable devices from gait pattern with accelerometers. In: IEEE International Conference on Acoustics, Speech, and Signal Processing, Proceedings(ICASSP 2005), vol. 2, pp. ii–973. IEEE (2005), `http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1415569`

4. Gafurov, D., Helkala, K., Søndrol, T.: Biometric Gait Authentication Using Accelerometer Sensor. Journal of Computers 1(7), 51–59 (2006), http://academypublisher.com/ojs/index.php/jcp/article/view/277
5. Gafurov, D., Snekkenes, E.: Gait Recognition Using Wearable Motion Recording Sensors. EURASIP Journal on Advances in Signal Processing 2009, 1–17 (2009), http://www.hindawi.com/journals/asp/2009/415817.html
6. Bächlin, M., Schumm, J., Roggen, D., Töster, G.: Quantifying gait similarity: User authentication and real-world challenge. Advances in Biometrics, 1040–1049 (2009), http://www.springerlink.com/index/WJ43150286835587.pdf
7. Ketabdar, H., Roshandel, M., Skripko, D.: Towards Implicit Enhancement of Security and User Authentication in Mobile Devices Based on Movement and Audio Analysis. Interactions, 188–191 (2011)
8. Kwapisz, J., Weiss, G., Moore, S.: Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), pp. 1–7. IEEE (2010), http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5634532
9. Chang, K.-h., Hightower, J., Kveton, B.: Inferring identity using accelerometers in television remote controls. In: Tokuda, H., Beigl, M., Friday, A., Brush, A.J.B., Tobe, Y. (eds.) Pervasive 2009. LNCS, vol. 5538, pp. 151–167. Springer, Heidelberg (2009)
10. Furnell, N.L.C.S.M.: Authenticating mobile phone users using keystroke analysis. International Journal of Information Security 6, 1–14 (2007)
11. Zahid, S., Shahzad, M., Khayam, S.A., Farooq, M.: Keystroke-based User Identification on Smart Phones. Technology, 1–18
12. Hwang, S., Cho, S., Park, S.: Keystroke dynamics-based authentication for mobile devices. Computers Security 28(1-2), 85–93 (2009), http://linkinghub.elsevier.com/retrieve/pii/S0167404808000965
13. Maiorana, E., Campisi, P., González-carballo, N., Neri, A.: Keystroke Dynamics Authentication for Mobile Phones. In: SAC, pp. 21–26 (2011)
14. Saevanee, H., Bhattarakosol, P.: Authenticating user using keystroke dynamics and finger pressure. In: Identity, pp. 1–2 (2009)