At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices

Zaire Ali and Jamie Payton
Department of Computer Science
University of North Carolina at Charlotte

Vincent Sritapan
Cyber Security Division
US Department of Homeland Security
Science and Technology Directorate

***Abstract*—Currently, the most prevalent approaches to authenticate smartphones involve either PINs, swipe patterns, or passwords. Few users enable these approaches. In order to encourage adoption, new authentication methods are needed. Emerging methods rely on the distinctness of a user's touch-based gesture for continuous authentication, providing an unobtrusive approach that simply monitors swipes and other input gestures as they are performed in the context of everyday smartphone use. However, existing methods do not consider the distinctness of a user's touch when different fingers are used. In this paper, we present the results of a small pilot study which suggests that a touch-based gesture performed by the same user with a different finger is indeed distinct. We present an approach that uses accelerometer data to identify the position of the phone and the finger that is being used in a touch-based gesture. Our results suggest that touch-based continuous authentication accuracies can be improved by considering accelerometer data and an individual's various fingers.**

***Index Terms*—Biometrics, mobile authentication, touch interaction, continuous authentication**

I. Introduction

To prevent unauthorized use of their mobile phones, most users typically rely on a feature that allows them to "lock" their smartphones using either PINs, swipe patterns or passwords. These authentication methods, though widely used, have several limitations [1]. First, all of these techniques are single-factor authentication methods. They all assume only authorized users will have knowledge of the PIN, password or swipe pattern. However, attackers can easily conduct a social engineering attack, like shoulder surfing, to steal these kinds of authentication codes [2]. Currently, mobile phone users have limited options for authentication outside of these methods. Second, almost half of users find these methods "annoying" [3]. This could be widely attributed to the frustration of having to authenticate the device each time that they want to access the phone's features after a (relatively short) timeout period has expired. As a result, only 36% of people lock their smartphones [3]. For users that do lock their devices, despite evidence showing that passwords are the most secure approach to authentication [4], most lock their devices with a PIN or pattern. This is likely because these kinds of inputs can usually be entered by the user in under two seconds. This highlights the importance of authentication methods that are tailored for use on the mobile platform which reduce frustration for the user.

In passive authentication, the user does not explicitly provide credentials for the purpose of authentication; rather, properties about the user are collected and used to identify the user. A promising direction for passive authentication is based on the observation that touch-based gestures can be used to uniquely identify an individual [5], [6]. In this paper, we show that touch-based gestures performed by different fingers of the same user are distinct as well. We propose an approach that uses the position of the phone to identify the finger used to perform a touch-based gesture. Our results show that such an approach increases the accuracy associated with identifying a particular user from a touch-based gesture by 6.67%.

II. Background

Interestingly, researchers have found that characteristics of touch-based gestures performed on a mobile device can identify a particular user [7], [8], [9]. Such gestures meet the criteria of biometric data [6]: universality, meaning every person possesses this data; collectability, meaning the data can be collected over a long period of time; distinctiveness, meaning that the data is distinct enough to identify between any two individuals, and permanence, meaning that individual's data will generally remain the same over a long period of time.

As device owners pinch, swipe, tap and write using touch screen interfaces, data such as pressure, size of the touch and the velocity of the gesture can be collected. To investigate how much touch data is required to authenticate users, a study was conducted by Frank et al. [5]. In this study, participants used an application to read Wikipedia articles (swipe up and down) and compare images (swipe right and left). Biometric data such as x-coordinate, y-coordinate, size and pressure were collected from the touchscreen and logged with a timestamp. Two classification approaches were applied to the set of features: k-nearest-neighbor (kNN) and support vector machine (SVM) with an RBF kernel. The authors found that 11 to 12 swipes per user were sufficient in the testing data set in order to achieve a classification error rate between 0% and 4%.

DOI 10.1109/SPW.2016.29

Building on this idea, the work in [6] included slide gestures, keystrokes, pinches and handwriting with a stylus. Again, a classification approach using an SVM was applied. Although the classification accuracy declined as the number of users increased, for data sets that included 32 users, the accuracy with which they were correctly identified in association with the performance of touch-based gesture remained above 80%.

While touch gestures provide a promising approach for adoption of authentication methods by users, there are limitations. For example, in [5], Frank et al. showed that there is a vulnerable time period between when the phone is activated to when the user is actually authenticated. A simple solution to this problem is to require the user to perform active authentication until enough training samples for creating a user-specific model of touch gestures have been collected from the user.

III. Experimental Study

As pointed out by Xu et al. [6], touch biometrics are distinct but do not display permanence over time. This could be due to numerous external factors such as fatigue, mood, and even the particular finger the user is using. For example, if a user used only their right thumb during the training phase and then began using their left thumb during the testing phase, the algorithm may not be able to correctly classify the user, resulting in a false negative for authentication.

(a) one handed (b) cradled (c) two handed

Fig. 1: How Users Hold Their Devices (a) one handed - 49% (b) cradled - 36% (c) two handed - 15%. Figure adapted from [10].

Such cases are likely, given how users typically handle their mobile devices. In a study performed by Hoober, users were observed on how they held their phones [11]. As shown in Figure 1, it was discovered that users either held and operated the phone in one hand, cradled the phone in one hand while using it with the other, or held it and used it with both hands. Hoober also observed that about 90% of users used their phone in portrait mode. We extend these findings in our pilot study with the observation that users typically operate their phones using either their right thumb, left thumb, right index finger or left index finger.

We hypothesize that touch-based gestures are not only distinct to a user, they are distinct to a particular finger (or thumb) of a user. As such, we expect that the accuracy of authentication will improve when training a per-user classifier with biometric data from the user's different fingers. Moreover, since users hold their phones in different ways to operate with different fingers, we hypothesize that we can improve classification by detecting the position and orientation of the phone; we do so by including features over the accelerometer data collected from the mobile phone in our classification approach.

As a first step, we conducted an initial pilot study of users as they performed touch-based swipe gestures on their mobile phones. Six participants were chosen (3 males; 3 females) using an online advertisement and snowball sampling. In order to collect a sufficient amount of data, participants were requested to perform the study multiple times over the course of 5 days.

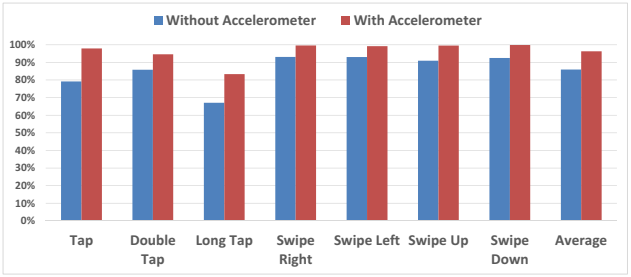
We collected accelerometer and touch-based data for our study with the use of an app we developed in Java for devices running on the Android OS. Since the majority of users were observed as portrait mode users, we forced portrait mode in our app to ensure consistency. Upon launch, the app begins by indicating which finger a user should use for the following activities. Then, participants were asked to perform real-world activities such as browsing through a collection of pictures (horizontal scrolling) and reading a document (vertical scrolling). In addition, the application prompted users to perform tasks that required gestures such as taps, double taps, long taps and swipes in various directions. This process would repeat until the app has collected data from the participant's left index finger, right index finger, left thumb and right thumb. For each initial and continuous contact with the touch screen, x-coordinate, y-coordinate, size, pressure, system time and accelerometer position were recorded by the app.

IV. Results

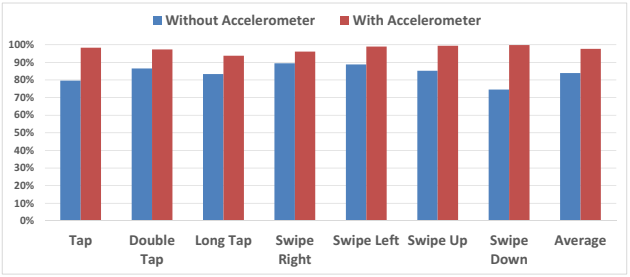
To provide a baseline for comparison, we implemented the passive authentication approach presented in [6], which uses a support vector machine with RBF kernel for classification of touch-based gestures. This is a representative approach for touch-based authentication and the authors made their touch-based gesture data sets publically available. Specifically, we used LibSVM 3.2 to implement scaling and classification; we chose the radial kernel type with gamma = 1. In order to analyze our results, we compute the accuracy of each classifier by comparing the number of test points that were correctly classified and the total number of test points provided.

A. Finger Distinctiveness

To begin, we first investigated the distinctiveness of an individual's fingers. For this analysis, we first only considered touch-based gesture data from an individual participant. The SVM classifier was applied on all the data collected from each gesture using the 10-fold cross-validation method. We then repeated this process with the data acquired from every user. On average, the classifier was able to differentiate between an individual's fingers, 86% of the time. Based on these findings, our hypothesis that touch-based gestures are distinct across the different fingers of a single individual is supported.



(a)



(b)

Fig. 2: (a) Accuracy for predicting a user's finger (b) Accuracy for predicting using 24 distinct fingers

We also observed that the distinctness of the touch-based gesture by finger differs based on the gesture performed. The difference between accuracy of certain gestures is likely due to the duration of (and therefore, amount of data collected for) each gesture. For a single gesture, only one data point is collected for both taps and long taps, two data points for double taps and an average of eight data points are acquired for any swipe. This accounts for being able to achieve 67.05% accuracy in distinguishing between fingers for long taps in comparison to achieving 92.38% accuracy in distinguishing between fingers for swipes.

B. Phone Position and Finger Usage

With the conclusion that touch-based gestures are distinct between the fingers of a single individual, we next investigated the possibility of exploiting the relationship between phone position and the finger used to perform the touch-based gesture; the goal is to increase the accuracy of classification of the user for passive authentication. Specifically, we used the data acquired from onboard accelerometers in conjunction with the touch-based gesture data. Again, a SVM approach using an RBF kernel was applied, and we performed 10-fold cross validation.

We observed that including accelerometer attributes increased the accuracy of classification. On average, the results of the previous analysis increased by 10.35% when considering data from the accelerometer. Fig 2a shows the comparison of classification accuracy for each gesture with and without accelerometer data. It should be noted that the classifier achieved average accuracies of over 99% for all swipe-based gestures. This further supports that a particular user's fingers are distinct but did not address whether they were distinct enough when compared to another user's fingers.

To investigate this matter, we compiled training sets for each gesture that consisted of all the data we acquired from each user. After creating the training sets, we assigned a unique class identifier to each finger, giving us a total of 24 class identifiers. The classifier then used the 10-fold cross-validation method on each training set. In addition, we also omitted the accelerometer data from the testing sets and analyzed the modified sets using the classifier. As shown in Fig 2b, the average cross validation accuracy while omitting accelerometer data was 83.93%. As expected, the resulting accuracies from including the accelerometer data with the training sets were higher, achieving an average accuracy of 97.67%.

If we considered each unique finger as a unique user, our implementation performed better than results from other studies, including Xu et al.'s [6]. The results from Xu et al.'s analysis on distinction shows for 24 distinct users, the average cross validation accuracy is approximately 82%. By including accelerometer attributes, our classifier had an average cross validation accuracy of 98.57% for swipes.

C. Finger Biometric Authentication

Upon observing higher accuracies after including accelerometer data, we investigated several other authentication cases. First, we wanted to observe how a classifier would respond to training with a) only the right index finger and testing with b) the right index finger, left index finger, right thumb and left thumb. Again, these fingers were chosen based on how users typically operate their devices. To begin, we created a training set using data only from the right index finger of each user. Then testing sets were created for each individual user and consisted of data from each of the four fingers we collected data for. These sets were then all labeled with the unique ID of each corresponding user. For this analysis, we extended the standard classifier to provide probability estimates that reflect how confident the classifier was in its predictions. After setting up the classifier, training and testing data sets were provided to receive a class identifier prediction for each vector in the testing set. This analysis was repeated for every user both including and omitting the accelerometer data.

	Tap	Double Tap	Long Tap	Swipe Average	Average
With Accelerometer	71.23%	67.57%	50.23%	59.84%	61.20%
Without Accelerometer	55.23%	57.54%	15.58%	65.74%	55.90%

TABLE I: Accuracies for training with right index fingers

As expected, the average prediction accuracies were lower than previously reported results for touch-based authentication when considering only the right index finger and testing with data from the index fingers and thumbs. For this analysis we

assumed users used their four fingers and even amount of time, which is supported by the low accuracies. However, in a real world environment, we expect users to use the same fingers at least 80% of the time. As detailed in Table 1, we also observed that the average accuracies for tap, double tap and long tap decreased without the accelerometer data, while the swipe average increased. This may be due to the low number of points in a single tap compared to the numerous points in a swipe. Secondly, the majority of the false positives were predicted with a confidence of ~18-22%. These findings suggest that touch-based authentication mechanisms should be carefully constructed to ensure that, for each user, training data is collected for each of the user's fingertips.

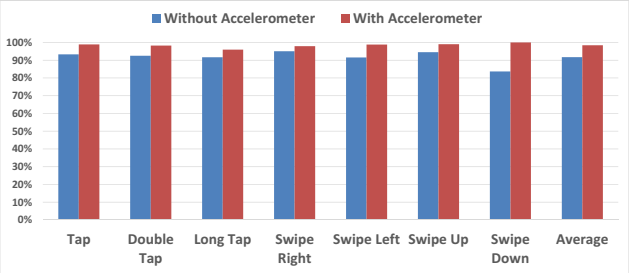


Fig. 3: Accuracies for predicting users

For a final look into touch-based authentication that considers finger distinctiveness, we applied the SVM-based approach for classification on training and testing data sets that considered both index fingers and thumbs. Again, we applied 10-fold cross verification on a training set consisting on all of the collected data for a particular gesture. For these training sets, users were given unique class identifiers in the training data set but we did not include labels for the user's separate fingers in the training data set. In addition, all of the training sets were supplied to the classifier with and without accelerometer attributes. The results of this analysis are illustrated in Fig 3.

For 6 distinct users, Xu et al. reported classification accuracies of 90-95% [6]. When omitting accelerometer data, our implementation follows the same approach as Xu, and accordingly, the classifier averaged similar results. However, when we included accelerometer attributes, the classifier gave an average accuracy of 98.42%.

V. Conclusions

Many smartphone users find current implementations of active authentication to be cumbersome and frustrating. As a result, most choose not to enable authentication methods on their mobile phones. Thus, interest in passive authentication methods using touch-based gestures has grown. In this paper, we presented an analysis of the distinctness of touch-based gestures for an individual's index fingers and thumbs. In addition, the results from our preliminary pilot study suggest that training data for touch-based authentication should include data from an individual's right thumb, left thumb, right index finger, and left index finger to increase accuracy. Finally, our preliminary pilot study suggests that including accelerometer data along with touch-based gesture data can help to improve the accuracy of touch gesture-based authentication methods.

One potential limitation is the size of our pilot study. However, an SVM approach, like that applied in our work, is suitable for relatively small data sets and we have applied standard measures to avoid overfitting, a common issue with small data sets. In the future, we plan to conduct a more expansive study that will include more users, a wider range of gestures, and will collect data over a longer period of time. Given the findings in [6], we expect that adding more users will cause classification accuracy to slightly decline before plateauing. However, it is unlikely that a large number of users (e.g., more than 5) would be using the same personal mobile device for authentication; as such, we would expect that our results would hold. Through the extended study, we also plan to evaluate the scalability of our implementation by analyzing how long users would need to train their devices and the latency of real-time classification on mobile devices for larger numbers of users.

Acknowledgment

This project is the result of funding provided by the Science and Technology Directorate of the United States Department of Homeland Security under contract number D15PC00160. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding agency.

References

[1] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *Security and Privacy (SP), 2012 IEEE Symposium on*, May 2012, pp. 538–552.

[2] Y.-L. Chen, W.-C. Ku, Y.-C. Yeh, and D.-M. Liao, "A simple text-based shoulder surfing resistant graphical password scheme," in *Next-Generation Electronics (ISNE), 2013 IEEE International Symposium on*, Feb 2013, pp. 161–164.

[3] N. Micallef, M. Just, L. Baillie, M. Halvey, and H. G. Kayacik, "Why aren't users using protection? investigating the usability of smartphone locking," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '15. New York, NY, USA: ACM, 2015, pp. 284–294.

[4] S. Gold, "Wireless cracking: there's an app for that," *Network Security*, vol. 2012, no. 5, pp. 10–14, 2012.

[5] 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," *CoRR*, vol. abs/1207.6231, 2012.

[6] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Symposium On Usable Privacy and Security (SOUPS 2014)*. Menlo Park, CA: USENIX Association, 2014, pp. 187–198.

[7] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones." in *NDSS*. The Internet Society, 2013.

[8] T. Feng, J. Yang, Z. Yan, E. M. Tapia, and W. Shi, "Tips: Context-aware implicit user identification using touch screen in uncontrolled environments," in *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '14. New York, NY, USA: ACM, 2014, pp. 9:1–9:6.

[9] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multi-touch devices," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '12. New York, NY, USA: ACM, 2012, pp. 977–986.

[10] J. Clark, *Designing for touch*. New York, N.Y: A Book Apart, 2015.

[11] S. Hoober, "How do users really hold mobile devices," *UXmatters*, 2013.