LatentGesture: Active User Authentication through Background Touch Analysis

Premkumar Saravanan, Samuel Clarke, Duen Horng (Polo) Chau, Hongyuan Zha
College of Computing
Georgia Institute of Technology
{psaravanan, sclarke, polo}@gatech.edu, zha@cc.gatech.edu

ABSTRACT

We propose a new approach for authenticating users of mobile devices that is based on analyzing the user's touch interaction with common user interface (UI) elements, e.g., buttons, checkboxes and sliders. Unlike *one-off* authentication techniques such as passwords or gestures, our technique works *continuously* in the background while the user uses the mobile device. To evaluate our approach's effectiveness, we conducted a lab study with 20 participants, where we recorded their interaction traces on a mobile phone and a tablet (e.g., touch pressure, locations), while they filled out electronic forms populated with UI widgets. Using classification methods based on SVM and Random Forests, we achieved an average of 97.9% accuracy with a mobile phone and 96.79% accuracy with a tablet for single user classification, demonstrating that our technique has strong potential for real-world use. We believe our research can help strengthen personal device security and safeguard against unintended or unauthorized uses, such as small children in a household making unauthorized online transactions on their parents' devices, or an impostor accessing the bank account belonging to the victim of a stolen device.

Author Keywords

Active authentication; touch gestures; shoulder surfing; fraudulent transactions; classification model.

ACM Classification Keywords

D.4.6 Operating System and Protection: Access controls, authentication

General Terms

Security, Human Factors

INTRODUCTION

We propose a unique method of active authentication on mobile devices based on analyzing the user's touch interaction with common user interface (UI) elements, such as buttons, checkboxes and sliders. Current prevailing methods of authentication in mobile devices involve either entering an alphanumeric password or performing a sequence of gestures to interact with an image on screen. Both of these approaches are knowledge based and thus can potentially be learned and replicated by false users.

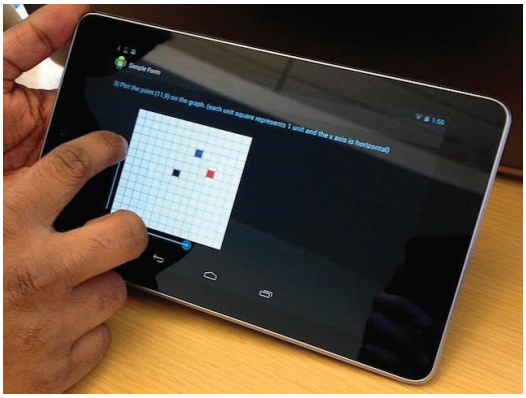

Figure 1: A user filling out an electronic form (an application) with simple aptitude questions on an Android tablet. Unknown to the user, his interaction traces (e.g., touch pressure and locations) are recorded by the application in the background. We build classifiers that differentiate users based on their interaction traces.

While these methods have been proven to be quite reliable and are thus prevalent today, they are vulnerable to fraud in certain scenarios. For example, these methods are susceptible to shoulder surfing wherein an aspiring intruder could observe the owner during authentication to gain access to the device. Furthermore, many current systems do not test if there was a change in user within the duration of the session. A PIN-based solution to this issue may involve periodically re-entering a PIN, but a survey revealed that as many as 41% of mobile device users find entering a PIN to be inconvenient [1]. The same survey also revealed that a similar proportion of mobile device users doubt the security of solely PIN-based authentication. Apple sought to address these shortcomings by incorporating a fingerprint scanner, called Touch ID, into the iPhone 5S, but this has also been shown to be vulnerable to physical replicas of fingerprints[9]. While no approach is completely invulnerable to intruders, our approach involves continuous authentication that depends on biometric behavioral aspects of a user, features that may be more diffi-

Chinese CHI '14, April 26-27, 2014, Toronto, ON, Canada
Copyright 2014 ACM 978-1-4503-2876-0/14/04 $15.00.
http://dx.doi.org/10.1145/2592235.2592252

cult to imitate. Furthermore, the Android 4.3 OS introduced the restricted profiles feature which enabled mobile devices to set different privileges for different users on a single shared device. This suggests that mobile devices are often shared among multiple users, so we also explored if our technique can help differentiate multiple users.

Our proposed method of authentication, LatentGesture, focuses on user interaction with common UI elements built into the Android framework. Thus, continuous intra-session authentication may be performed in the background while the device is in use. Furthermore, by using only built-in UI elements, we democratize and standardize our approach to be generalizable and more accessible to mobile app developers with minimal effort. This approach is capable of complementing existing methods and could be integrated with conventional authentication to form a hybrid system by offering an additional defense mechanism against an intruder who has already gained physical access to the device.

The technique employed by LatentGesture has the potential to benefit all users of touch-based mobile devices by adding a substantial level of security without changing the user-experience. Our major contributions include:

- We propose a continuous authentication technique based on the analysis of users' natural touch interaction with common UI elements, e.g., buttons, checkboxes, sliders.
- We demonstrate our idea is viable, through a 20-person user study where participants used mobile phones and tablets to fill out a simple digital form containing common UI elements. We achieved an accuracy of 97.78% when detecting 5 different users. We also achieved a true negative accuracy of 99.13% of detecting intruders while maintaining a true positive accuracy of 96.87% for detecting the true user through single-class or unary classification.

RELATED WORK AND OUR DIFFERENCES

Authentication techniques for mobile devices have generally been dominated by alphanumeric passwords, graphical methods [2], or gesture-based techniques [8]. More recently, biometrics-rich gestures were explored [6] as an alternative to the classical PIN or alphanumeric passwords. Users can select from an array of different multi-touch gestures involving the use of up to five fingers to unlock their device [10].

Similarly, researchers have been investigating whether gestures could be combined with passwords to provide another level of security. For example, a touch screen tapping characterization system was devised and shown to offer good resistance to mimic attacks [7]; while it is easy to mimic the timing of button presses involved in an alphanumeric password, other features such as touch pressure, size of touch (i.e., finger size), and acceleration are harder to reproduce simultaneously. A few other password systems also capitalize on this idea, such as the Pressure-Grid system [7], in which the user must touch multiple objects and apply a higher pressure on those objects in the correct sequence. Some such systems are compatible with PIN systems and graphical passwords[11].

Our work belongs to the new paradigm of *active* authentication, that has not been explored, until recently. In this form of authentication, the system continuously authenticates the user throughout the duration of use. The research team behind Touchalytics [4] and a group from the University of Munich [3] both independently investigated the feasibility of using features extracted from scrolling gestures for authentication. However, neither study generalized their approach for classifying gestures employed while using common UI elements, which is the focus of our investigation. In addition, we look into authentication on both mobile phones and tablets, whereas they only studied phone use.

OUR PROPOSED APPROACH

Overview

LatentGesture authentication was implemented by collecting touch features such as position on screen, time, frequency, and pressure through common sensors available on mobile devices today using the Nexus 4 phone and Nexus 7 tablet. We then used an array of machine learning classifiers to find the most appropriate model for our specific data set. We found the *LibSVM* and *BayesNet* classifiers to be the optimal choice for unary and multi-class classification respectively. The overarching objective was to be able to build a behavioral model with this feature set in order to determine the user of the device based on a trained classification model.

Authenticating One User

The fundamental goal was to determine if the current user using the device is in fact the owner of the device or an intruder. This would complement conventional authentication on personal devices. We accomplished this by using the LibSVM classifier and the meta OneClassClassifier wrapped around the Random Forests classifier performing unary classification. Overall, the Lib-SVM classifier was optimal for unary classification. We trained the models with only the instances of the true user of the device. The testing data consisted of both new instances of the true user and all other user data was used to form an intruder data set constituting the threat model, which we define below.

Threat Model. We assume an attacker is already in possession of the mobile device, and the password (can be PIN or gesture) to unlock the device. That is, the first security barrier has been breached. The attacker is free to use the applications on the device. With LatentGesture, the attacker will be subject to background authentication when he or she interacts with applications that use common UI elements (e.g., changing system settings) and will be flagged and reported to the central monitor to which the device has been registered (e.g., Apple, for iOS devices).

Authenticating Multiple Users

We strove to perform multi-class classification and pinpoint each user of the device with significant accuracy using a small training dataset reflective of a user using a new personal device. This would assist in authentication on shared mobile devices with multiple users. For example, children using a shared mobile device at home could be recognized, and certain features could be locked such as making online transactions.

This was accomplished by training an ensemble of classifiers including the classical Naive Bayes, J48 (java implementation of the C4.5 algorithm), Random Forests, and BayesNet classifiers. The optimum classification for every data set for variable number of users was selected from these classifiers. The best classifier was selected based on the training cross-validation accuracy. Overall, the BayesNet classifer was optimal for multi-class classification.

The features we obtained from the UI elements are indicated below. One other practical issue we faced was the inconsistent sample rate of Android devices that varies up to 14 microseconds. We tackled this issue by filtering touch events in time to reduce the sample rate variance to 2 microseconds.

- **Radio Buttons and Checkboxes**: we used the first two touch events, and for each event, we used its pressure, relative timestamp, and coordinates
- **Slider**: we used all touch events, and for each event, we used its pressure, relative timestamp, and coordinates

We used the first two touch events for button presses because that is the minimum information needed to distinguish if there was any sliding of the finger during the event. Using more than two events decreased classification accuracy. We formed the feature vector by concatenating all of the features listed above for all of the widgets to construct a single instance for every user. The multi-class classifiers were trained with multiple users up to ten users whereas the unary classifier was trained with only the true user's data. The true negative rate was tested with other users' data, i.e. an intruder dataset; the true positive rate was tested with the same user's data.

USER STUDY

We collected user interactions through the use of an electronic form containing simple aptitude questions. The users were involved in the high level task of filling out the form, unaware of the background analysis being performed. After collecting data, we trained classifiers with user data to test both multi-class classification and unary classification.

Participants

We recruited 20 participants from our university of which 5 were female. All participants were required to have used mobile devices prior to the study and were asked to follow the same procedure detailed below. However, only the interactions of 10 of the participants were used to build the multi-class classification models whereas all 20 participants were used to test for unary classification. We chose 10 users based on our prior experience of multi-class evaluation and its limits on classifying our specific type of data-set accurately. Furthermore, a need for more than 10 accounts on a shared device is analogously impractical in a common household setting.

Procedure

Each subject's interactions were collected through the use of built-in Android UI elements within the digital form. We conducted 9 trials for every user on both the Nexus 7 and Nexus 4 to get a multiple of the number of UI elements being tested. The UI elements on each page included radio buttons, checkboxes, sliders of both vertical and horizontal orientation.

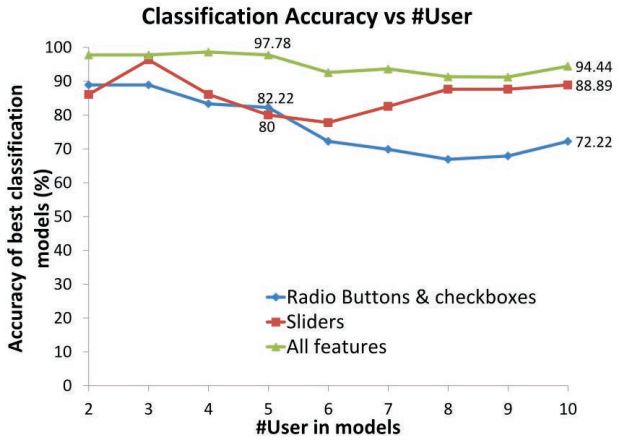

Figure 2: Multi-user authentication accuracy on a Nexus 4 phone with respect to number of users considered by the classification models

It was a challenge to incorporate these common UI elements into a digital form without creating an artificial setting. We decided to use the sliders as a means to transition from one page to the next. This emulates the common iPhone lock screen and the way pages are flipped when reading an ebook on a tablet. Radio buttons emulate common interaction such as opening apps and checkboxes emulate for example clicking image links and hyperlinks on a browser. We also incorporated slider inputs that required the user to position the slider at a specific location. The high level task involved for these sliders was to align two sliders which represented the two axes of the x-y coordinate plane in order to plot a specific point (see Figure 1).

The user was required to scroll vertically to submit all responses. The user's preferred positioning of the UI elements by free vertical scrolling was captured by taking the raw positions of interaction on the screen. Users were given the opportunity to test the application prior to data collection to allow the users to subconsciously find their preferred methods of interacting with the widgets on the device. Finally, subjects were asked to fill out a questionnaire which surveyed them on some biographical information such as gender and age group.

Results

We expected to find that gestures involving sliders would provide higher discriminatory information about the user than radio buttons and checkboxes. Also, we predicted that the tablet would provide more reliable discrimination than the phone as a larger screen space implied a higher possibility for variation among users, which could be used as distinguishing criteria.

Multi-User Authentication. After training the multi-class classifiers available under Weka 3 open source software [5] with the data set obtained from 10 of the users, we found that we were correct about the discriminatory power of the different types of UI elements as shown in Figures 2 and 3. We were also correct that interactions with the tablet would be better classified than those of the phone. We achieved an average multi-class classification accuracy of 100% on the

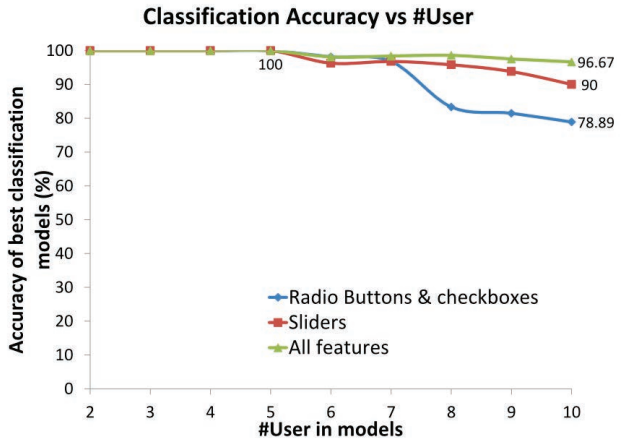

Figure 3: Multi-user authentication accuracy on a Nexus 7 tablet with respect to number of users considered by the classification models

Phone			Tablet		
TP rate	TN rate	Accuracy	TP rate	TN rate	Accuracy
96.67%	99.13%	97.9%	94.45%	99.14%	96.79%

Table 1: The average true positive (TP) and true negative (TN) rates of single-user authentication from the user study. TP is the rate of correctly identifying the legitimate user of the device; TN is the rate of correctly identifying illegitimate users.

tablet and 97.78% on the phone with the complete feature set by performing 10-fold cross validation for 5 users.

Single-User Authentication. With unary classification, we were able to achieve an average accuracy of 97.9% on the phone and 96.79% on the tablet. The unary classifier was tested with 81 intruder instances randomly sampled from the other 19 participants in the study.

Summary. We found that it is viable to authenticate up to 5 users on a mobile device with significant accuracy using background touch analysis. Furthermore, we also determined that it is possible to authenticate single users on personal mobile devices through unary classification.

CONCLUSIONS

We presented an active authentication technique based on analyzing the user's touch interaction with common user interface (UI) elements. We believe this authentication approach may be more resistant to attacks such as "shoulder surfing" and other threat models, since a successful intrusion of the device would require the intruder to interact with the mobile device the same way as the legitimate user would, *continuously*. We conducted a lab study with 20 participants, where we recorded their interaction traces on a mobile phone and a tablet while they filled out electronic forms. By using machine learning methods based on LibSVM and Random Forests, we achieved an average of 97.9% accuracy with a phone and 96.79% accuracy with a tablet for single user classification, demonstrating our technique has strong potential for real-world use. We plan to investigate how touch signatures are influenced by different external contexts (e.g., usage while walking, standing) to improve authentication.

ACKNOWLEDGEMENT

This work is supported in part by: NSF IIS-1116886, IIS-1049694 (REU program), and PURA from Georgia Tech.

REFERENCES

1. Clarke, N., Furnell, S., Rodwell, P., and Reynolds, P. Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security 21*, 3 (2002), 220 – 228.
2. Davis, D., Monrose, F., and Reiter, M. K. On user choice in graphical password schemes. In *USENIX Security Symposium*, vol. 13 (2004), 11–11.
3. De Luca, A., Hang, A., Brudy, F., Lindner, C., and Hussmann, H. Touch me once and i know it's you!: Implicit authentication based on touch screen patterns. In *Proc. CHI'12*, CHI '12, ACM (2012), 987 – 996.
4. Frank, M., Biedert, R., Ma, E., Martinovic, I., and Song, D. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *Information Forensics and Security, IEEE Transactions on 8*, 1 (1 2013), 136 –148.
5. Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., and Witten, I. H. The weka data mining software: an update. *ACM SIGKDD explorations newsletter 11*, 1 (2009), 10–18.
6. Khan, M. K., Zhang, J., and Wang, X. Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices. *Chaos, Solitons & Fractals 35*, 3 (2008), 519–524.
7. Kim, D., Dunphy, P., Briggs*, P., and Hook, J. Multi-touch authentication on tabletops. In *Proc. CHI'10*, ACM Press (2010), 1093–1102.
8. Liu, J., Zhong, L., Wickramasuriya, J., and Vasudevan, V. uwave: Accelerometer-based personalized gesture recognition and its applications. *Pervasive and Mobile Computing 5*, 6 (2009), 657–675.
9. Rosenblatt, S. Touch id hack verified as legit, 9 2013. `http://news.cnet.com/8301-1009_3-57604255-83/touch-id-hack-verified-as-legit/`.
10. Sae-Bae, N., Ahmed, K., Isbister, K., and Memon, N. Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In *Proc. CHI'12*, ACM Press (2012), 977–986.
11. Zheng, N., Bai, K., Huang, H., and Wang, H. You are how you touch: User verication on smartphones via tapping behaviors. ACM Press (2012), 1093–1102.