Exploring Games for Improved Touchscreen Authentication on Mobile Devices

Padmaja Scindia
New York Institute of Technology
Computer Science Department
pscindia@nyit.edu

Jonathan Voris
New York Institute of Technology
Computer Science Department
jvoris@nyit.edu

ABSTRACT

Mobile device theft is a growing problem. Yet due to usability issues and other concerns, people frequently choose not to use an authentication mechanism to protect their devices, putting the sensitive information that they store at risk. In order to provide mobile device owners with more usable authentication, we propose the study and development of mechanisms for authenticating users to mobile devices by modeling the manner in which they interact with games. We conducted an preliminary IRB approved study in which 12 users were asked to play 3 of the most popular games available in the Google Play Store on an Android device while their touchscreen interactions were logged. We then applied a Support Vector Machine to classify users based on 19 extracted touchscreen usage features. We were successfully able to classify over 90% of the samples for each game with a false reject rate of less than 1%. These results indicate that utilizing gameplay elements to encourage unique behavioral touchscreen features may be a promising direction of future research.

1. INTRODUCTION

Mobile device theft is a growing concern. In 2013, 3.1 million people in the U.S. were the victims of device theft and approximately $1.1 billion was spent replace them [6]. In light of these figures, it is imperative to provide device owners with strong options for authentication in order to protect the sensitive data stored on their devices. Mobile user authentication presents usability challenges, however. Passwords require either lengthy strings or unusual character combinations to provide sufficient levels of security against guessing attacks, both of which result in passwords that are difficult to enter on devices with small touchscreens [5]. Graphical passwords are better suited to a mobile setting, but in practice may result in low-entropy passwords [7]. Whatever the reason, users simply aren't using currently available authentication methods; 47% don't use a PIN, password, or unlock pattern, and 34% take no security precautions with their mobile devices whatsoever [6].

In order to address the challenges associated with performing authentication on mobile devices, we propose to utilize an activity that users already perform on their mobile devices on a regular basis: playing games. The average smartphone owner spent more than ten hours playing games in the fourth quarter of 2013 [3].

2. RELATED WORK

Recent research has shown that behavioral biometrics, which attempt to identify users based on how they interact with their devices, provide a promising solution to mobile user authentication. Examples include touchscreen usage [8] and application habits [4]. A goal of applying gameplay elements to the task of mobile authentication is to encourage users to rapidly make distinctive touch gestures, allowing judgements regarding feature classification, and therefore user identity, to be derived in a shorter time frame.

Games are a natural choice for behavioral authentication because of their widespread acceptance. While search and social applications are more frequently used, modeling these applications is complicated by the fact that they frequently involve sensitive personally identifiable information (quantifying precisely how much is leaked is an area of future work). Previous work has established that games have natural usability benefits when applied to other security tasks such as device pairing [1] and random number generation [2]. This work studies how these results can potentially be extended to the context of device authentication.

3. EVALUATION

We designed an IRB approved study to perform a preliminary assessment of the viability of game based touchscreen authentication. We installed our Touch Sensor software on a Samsung Galaxy mobile phone alongside three games from the Google Play Store: Angry Birds, FlowFree, and Fruit Ninja. These games were selected based on several criteria: There were among the most popular unpaid game applications at the time of selection and had relative simple gameplay mechanisms which would be appropriate for a broad audience. Further, each game required users to make touch gestures which were distinct from the others. Essentially we attempted to use games which were representative of those played by the typical Android device owner. We desired to determine which of these games, if any, caused users to interact with their mobile device in a way that was conducive to user authentication.

We advertised the study at our university via flyers and class announcements. 12 volunteers were recruited from the student body at our university. Each participant scheduled a session where they came to our usability lab to complete their study task. Users were presented with a brief overview of the study; care was taken not to discuss the security implications of the touchscreen task to avoid any security priming effects. The participants then played each of the three test games as they would naturally for a period of 5 minutes. While users played each game, the Touch Sensor logged their touchscreen interactions while silently running in the background.

4. RESULTS

We developed a Touch Sensor application for Android based devices which recorded low level touchscreen usage from the Android OS. These raw logs were processed in order to extract higher level features which better captured potentially distinctive touch screen mannerisms which could be modeled to achieve user authentication without requiring any specific touch pattern to be performed by users. The continuous output of the touchscreen state was parsed into discrete swipe gestures. We derived seventeen properties from each of these gestures, namely: 1) initial x coordinate, 2) initial y coordinate, 3) final x coordinate, 4) final y coordinate, 5) the amount of pressure applied during the gesture, 6) the area covered by the finger during the gesture, 7) finger width during the gesture, 8) the length of the gesture along the screen's x axis, 9) the length of the gesture along the screen's y axis, 10) the distance traveled during the gesture, 11) the direction of the gesture, 12) the speed of the gesture along the x axis, 13) the speed of the vector along the y axis, 14) the speed along the gesture's trajectory, 15) the velocity of the gesture, 16) the angular velocity of the gesture, and 17) finger orientation during the gesture. We selected these features because they had been studied in previous research, though it remained an open question whether they would be able to capture differences in user behavior for the more open ended task of playing a commercial game.

We randomly selected 300 gestures made by each of our 12 participants for a total sample of 3,600 gestures per game and 10,800 gestures across all three games. We utilized the Weka machine learning toolkit to apply a Support Vector Machine (SVM) to classify these samples according to the aforementioned features. We trained our SVM using the Sequential Minimal Optimization algorithm and performed 10-fold cross-validation on a game-by-game basis. Figure 1 displays the Area Under the Receiver Operator Characteristic (AUC) for each user and game, while Table 1 contains a comparison of classification statistics for each of the three tested games.

Game	TP Rate	FP Rate	Precision	AUC
Angry Birds	92.17%	0.70%	92.41%	0.983
Flow Free	98.86%	0.10%	98.87%	0.996
Fruit Ninja	99.45%	0.05%	99.46%	0.998

Table 1: Comparison of Classification Statistics by Game

All three tested games elicited touchscreen which was highly conducive to user authentication, particularly considering the expected 8.33% baseline for a 12 class problem. The game with the worst user classification performance, Angry Birds, had a 92.17% successful authentication rate and an AUC value of 0.983. Fruit Ninja was the best performing game, with a 99.45% true positive rate and an AUC of 0.998. Our hypothesis is that Fruit Ninja resulted in more accurate classification rates because it requires users to make many short swipe gestures in rapid succession, encouraging distinctive touchscreen habits to emerge rapidly in contrast to a game such as Angry Birds, which requires users to make slower, more deliberate gestures.

5. CONCLUSION

This paper proposes a novel research direction of applying gameplay to the challenge of authenticating users via touch-

Figure 1: Area Under the ROC Curve for each Combination of User and Game

screens on mobile devices. Including gaming elements has the potential to increase the usability of authentication while speeding up the authentication process by encouraging rapid bursts of discriminative interactions. The results of our initial study provide preliminary evidence of the viability of a game based approach to authenticating users on mobile devices, though additional data is required to draw significant conclusions. We intend to perform more comprehensive user studies involving more applications and a broader populations using a game based authentication mechanism on their own personal devices for extended durations as future work.

6. REFERENCES

[1] A. Gallego, N. Saxena, and J. Voris. Exploring extrinsic motivation for better security: A usability study of scoring-enhanced device pairing. In *Financial Cryptography and Data Security*. 2013.

[2] R. Halprin and M. Naor. Games for extracting randomness. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009.

[3] S. Perez. An Upper Limit For Apps? New Data Suggests Consumers Only Use Around Two Dozen Apps Per Month. TechCrunch, 2014.

[4] M. B. Salem, J. Voris, and S. Stolfo. Decoy applications for continuous authentication on mobile devices. In *1st Who Are You?! Adventures in Authentication Workshop (WAY) co-located with the 10th Symposium on Usable Privacy and Security (SOUPS)*, 2014.

[5] F. Schaub, R. Deyhle, and M. Weber. Password entry usability and shoulder surfing susceptibility on different smartphone platforms. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia*, 2012.

[6] D. Tapellini. Smart Phone Thefts Rose to 3.1 Million Last Year, Consumer Reports Finds. `http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm`, 2014.

[7] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013.

[8] 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)*, 2014.