Poster: Usability Analysis of Biometric Authentication Systems on Mobile Phones

Chandrasekhar Bhagavatula [*]
Carnegie Mellon University
cbhagava@andrew.cmu.edu

Kevin Iacovino [*]
Carnegie Mellon University
kiacovin@andrew.cmu.edu

Su Mon Kywe [*†]
Singapore Management University
monkywe.su.2011@smu.edu.sg

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cmu.edu

Blase Ur
Carnegie Mellon University
bur@cmu.edu

1. INTRODUCTION

Despite decades of research into biometric authentication, few such systems have been deployed widely. Recently, however, popular smartphone platforms have offered average users the opportunity to use biometric authentication in the real world. Through two ongoing studies, we are investigating user perception of these systems, as well as their usability. We focus on Android's face authentication system and the iPhone fingerprint authentication system. In our first study, an online survey conducted on Amazon's MTurk, we ask users who have tried these biometric authentication systems on their own phones about the reasons for deciding to adopt, or not adopt, these systems. In our second study, a lab usability study, we compare the usability of these biometric authentication systems to standard PIN authentication under a variety of conditions we hypothesized might cause usability issues with these systems. Our initial findings have several implications for the future design of mobile biometric authentication systems.

2. ONLINE SURVEY

In order to ascertain how the iPhone 5s fingerprint authentication and the Android Face Unlock were being adopted in the real world, we launched surveys on Amazon's Mechanical Turk.

2.1 Methodology

Two Mechanical Turk surveys were launched for two groups of users: iPhone 5s and Android version 4.0. We were able to recruit 35 participants on the iPhone 5s survey, and 60 participants for the Android version 4.0 survey.

We start out with some general demographic questions and a verification question to see if the participant really has the desired phone. Participants first rank the phone's speed of authentication as well as the amount of errors it makes when authenticating, both relative to the other methods of authentication that they use. Then, they answer some open-ended usability questions, which garner concerns that the participants may have with the phone in certain scenarios, whether they think it is convenient or not, and if they think the biometric authentication is secure from anyone else trying to log-in to the phone.

2.2 Findings for Android Face Unlock

Out of 60 participants, who took the survey study, 36 of them (60%) correctly answered the verification question. There were a total of 28 males (78%) and 8 females (22%) with about 50 % having an undergraduate degree an average age of 28.

13 of the participants currently use the Face Unlock scheme and the most common reason given is that they feel it is more secure. This is contradictory to the fact that Google states the Face Unlock is a low security measure as it can be defeated. The most common reason given for not using the Face Unlock is that it does not work under certain lighting conditions. Many also stated that Android Face Unlock is not accurate enough and they fail to log-in or register. Multiple participants mentioned that unlocking while driving is much more convenient with the Face Unlock. This is quite surprising as the participants even acknowledge that it is illegal to type and drive but don't see a problem with using Face Unlock while driving. Since you have to look at the phone to unlock it, it is still very dangerous.

2.3 Findings for iPhone Fingerprint

Out of the 35 participants in the iPhone survey, only 23 correctly answered the verification question (77%), 11 males (47.8%) and 12 females (52.2%). The average age of the participants was 29. 16 (69.6%) of the 23 participants have college experience of some kind. 16 (69.6%) of the participants currently use the fingerprint authentication method as their unlocking scheme on their iPhone 5s with 12 using it because it is convenient and 4 using it because they perceive it as being secure. Many participants had issues with the reliability and the amount of time it takes to log in.

Most of the participants were unconcerned that the fingerprint authentication security may be compromised on their phone. Even though the fingerprint authentication has been defeated since the day of release, it seems as if many people are not aware of the potential security flaws. Given that most seem to be using the scheme for convenience, this may not be a problem for most people but it does underscore the divide between perception and reality of these systems.

3. LAB STUDY

A lab study was run to find out what specific scenarios cause problems with the biometric authentication systems and to find out how these affect a user's acceptance of the

[*] The first three authors contributed equally.

[†] This author did the project while she was an exchange student at Carnegie Mellon University.

system.

3.1 Methodology

Our within-subjects lab study investigated the usability of biometric authentication and traditional PIN authentication on both Android and iPhone. We asked participants to rate their basic perception of biometric systems on a 5-point Likert scale in order to get an idea of how the public views biometrics in general. We had participants try and use the PIN authentication systems on both the iPhone 5s and the Samsung Galaxy S4 as well as the fingerprint authentication on the iPhone 5s and the face unlock on the S4. We asked participants to set up the authentication method, providing help as needed. They were then asked to log into the phone in 5 different scenarios: sitting, sitting in a dark room, walking, walking while carrying a bag in one hand, and sitting after applying moisturizer to their hands. These scenarios were chosen to try and emulate some everyday situations in which a biometric authentication scheme may be more useful or fail. Participants rated the difficulty of each task on a 5-point Likert scale. Participants were then asked to rank the four schemes in order form their most favorite to least favorite and provide reasoning.

3.2 Findings for Usability Study

We had a total of 10 people take part in the lab study. 8 of the participants were male and 8 were under 30 years of age. We had 4 iPhone users and 6 Android users take part.

As in the online surveys, most participants said biometric systems are secure. People seem to think that the iPhone fingerprint registration is a little more difficult than the other schemes. The most common reason given by the participants was that the registration process for the iPhone fingerprint authentication did not have clear instructions. 7 out of the 10 participants gave this as a problem they saw with the fingerprint registration. We did notice that not one participant asked about the option to improve face recognition in the face unlock scheme which appears after the registration process is done. It seems it might be a possibility that actual users will not see this option which could lead to some of the frustration people may be having with the amount of failures from the face unlock scheme. The major difficulty in the scenarios was trying to unlock the phone in the dark using the face unlock. All the other authentication schemes worked well in both the seated and dark scenarios. The iPhone fingerprint authentication seemed a little more difficult when walking. This was due to having to hold the phone at the bottom and it being a little more awkward, especially with one hand. We found that the Face Unlock was most preferred when using the moisturizer since the screen did not need to be touched. The face unlock allows users to not be able to physically touch the phone.

The face unlock was mostly disliked by the participants as they found that holding the phone in front of them was awkward. However, the iPhone fingerprint authentication was also almost evenly split between most and least favorite. The interesting thing here is that nobody rated it anywhere other than the extremes. Those who did not like it cited the registration process as the main reason they did not want to use it. The process took too long or was unclear to them. By making these instructions clearer and shortening the enrollment process, the fingerprint authentication may gain more adoption. However, we don't know how much shortening the enrollment process would affect the accuracy of the authentication system.

4. RELATED WORK

While we are the first to study mobile biometric authentication systems that have been deployed widely in the real world, a number of researchers have investigated the usability of biometric systems in the lab. The perception and ease of use of biometric systems plays a large role in the acceptance of such systems. El-Abed et al. [2] have shown that user's perception can negatively affect the user's acceptance of the system. Both Braz et al. [1] and Lassmann et al. [3] perform a comparative analysis of general authentication methods, including biometric authentication methods. They also find that user acceptance affected the performance of the biometric authentication method. Sieger et al. [4] study the users' perception on the security and usability of mobile biometric authentication systems. They conclude that iris and fingerprint authentication systems are seen as highly secure and fingerprint authentication is also regarded as highly usable. Trewin et al. [5] also find out that mobile face and voice recognition were the fastest and had high performance in the memory task, but are not usable in all situations.

5. CONCLUSIONS

We plan on increasing the number of participants in order to confirm our findings thus far. However, from these participants, it seems as if one of the largest barriers to adoption of the biometric authentication schemes is the lack of clear communication between the users and the system. Unclear instructions lead to non-ideal enrollment scenarios and frustration for the user. Changing this may be the first step in gaining more adoption of these schemes.

6. ACKNOWLEDGMENTS

This research was supported by a Microsoft Research Award to Lorrie Faith Cranor at the Carnegie Mellon University

7. REFERENCES

[1] C. Braz and J.-M. Robert. Security and usability: The case of the user authentication methods. In *Proc. IHM*, 2006.

[2] M. El-Abed, R. Giot, B. Hemery, and C. Rosenberger. A study of users' acceptance and satisfaction of biometric systems. In *Proc. ICCST*, 2010.

[3] G. Lassmann. Some results on robustness, security and usability of biometric systems. In *Proc. ICME*, 2002.

[4] H. Sieger, N. Kirschnick, and S. Möller. Poster: Towards a user behavior model in computer security. In *Proc. SOUPS*, 2010.

[5] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David. Biometric authentication on a mobile device: A study of user effort, error and task disruption. In *Proc. ACSAC*, 2012.