Smartphone Fingerprint Authentication versus PINs: A Usability Study

Shri Karthikeyan, Sophia Feng, Ashwini Rao, Norman Sadeh

July 31, 2014

CMU-CyLab-14-012

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213
Smartphone Fingerprint Authentication versus PINs: A Usability Study

Shri Karthikeyan, Sophia Feng, Ashwini Rao, Norman Sadeh
Carnegie Mellon University, Pittsburgh, United States
{skarthik, ffeng}@andrew.cmu.edu, arao@cmu.edu, sadeh@cs.cmu.edu

ABSTRACT

Today’s smartphones store a variety of sensitive information and provide access to sensitive functionality. Despite an abundance of features to secure one’s phone, many users leave their devices unprotected putting themselves and their organizations at risk. Over the past year, several vendors have started to offer fingerprinting functionality in an effort to increase the number of people who protect their phones. We present the results of a study conducted to determine whether fingerprint-based authentication functionality is likely to gain greater levels of adoption than today’s PIN-based solutions. Our study utilizes a task-based method in which participants complete a set of ten tasks. The study compares the usability of Apple’s iPhone 5S Touch ID fingerprint-based authentication with more traditional PIN-based authentication. Our results suggest that, from a usability standpoint, fingerprint-based authentication is better than PIN-based authentication and could contribute to reduce the dismal number of people who do not have locking functionality in place to protect access to their phones.

1. INTRODUCTION

As smartphones dominate the mobile phone market, it is becoming commonplace to use them for sensitive tasks such as mobile banking, social networking, and online shopping. For example, 19% of the participants in our study used their phones for mobile banking (see Fig. 1). Although people carry such important information on their phones, as many as 40% of smartphone users fail to protect their valuable data with a security mechanism such as a PIN-code[1]; using a PIN would make it harder for unauthorized users to access data on the phone. The situation is even more worrisome given that one in 10 smartphone users in the United States were victims of phone theft[2]. A recent bill introduced by California state senate mandating a kill switch for smartphones[5], which would wipe data from a smartphone upon theft, underscores the importance of this issue.

One of the common reasons for not using PIN-codes is the PIN-code entry burden, that is, the frequency of entering PIN-code on a smartphone. For example, on an iPhone, users may set their phone to automatically lock after one minute of inactivity. Although locking a phone as soon as possible may provide maximum protection, it also decreases usability by increasing PIN-code entry burden. As a response to this issue, in 2013, Apple launched the iPhone 5S with Touch ID fingerprint reader feature. This feature was marketed as allowing users to “easily and naturally unlock an iPhone without typing a passcode, just by placing a finger on the Home button.” Since then, fingerprint technology has become more popular, and, as of 2014, other mobile phone manufacturers such as Samsung have incorporated similar features into their products, for example, Samsung Galaxy.

In our study, which we conducted as part of a course project in Fall of 2013, we tested the claim related to usability of fingerprint readers. We focused on the usability aspects, but we note that it is important to understand other aspects such as privacy and security. For example, using fingerprints may be a privacy issue as they are personally identifiable. Further they cannot be changed as easily as a PIN-code, and it may be possible to lift fingerprints either from a phone or somewhere else.\footnote{As part of a sister project conducted in the same course, another group of students worked on cracking Touch ID. While the team of students was eventually successful, their study also showed that the likelihood of lifting a fingerprint of high enough quality to crack Touch ID from the phone itself was very low. This is not to say that a determined attacker could not easily find another source for such a fingerprint.}

We compared the usability of the new Touch ID fingerprint reader to the old PIN-code security system. Our study involved 40 smartphone users. We gave participants a set of ten tasks to complete five of which were to be done using Touch ID and five using PIN-code. These tasks tested different capabilities of Touch ID and PIN-code. Our objective was to examine both quantitative and qualitative data from participants’ reactions to the given tasks, and get a holistic picture on the usability of the two systems. We videotaped participants’ actions to calculate the time taken to complete each task. Furthermore, we recorded the number of mistakes participants made while completing each task. We did not tell our participants that we were timing them or counting their mistakes in order to create as natural of a setting as possible. Our results show that participants find setting up and changing Touch ID tasks more difficult than setting up and changing PIN-code. However, they find unlocking their iPhone and downloading an app from the Apple store easier with Touch ID than with PIN-code. This result is encouraging from the perspective of usability of Touch ID system as users carry out unlocking and downloading more often than set up or change. Users most often have to lock and unlock a phone many times a day, and, hence, it is very more important to help users with this usability issue.

The rest of this article is organized as follows. Section 2 gives a summary of background and motivation for the study. Section 3 gives a detailed description of the usability study and the individual tasks. Section 4 details the data collected for the tasks in the study, and analyzes the data from the
individual tasks. Section 5 provides an overall analysis of the results. Finally, Section 6 discusses the final conclusions and our proposed future work in this field.

2. BACKGROUND AND MOTIVATION

Before delving into the details of the study, let’s examine the existing PIN code system in detail and look at some of its downsides that gave rise to the Touch ID. To begin, out of the 40% of users who actually secure their phone with a 4-digit PIN code[1], one can expect many of them to choose weak PINs such as PINs in geometric shapes, famous dates, or use repeated numbers. For instance, a study of similar 4-digit PINs conducted by Bonneau in the context of ATM cards showed such patterns[3]. Given such easy-to-find and easy-to-guess 4-digit PINs, a hacker could crack into a secured iPhone about 9.23% of the time with three attempts, and 12.39% of the time in six attempts[3]. Thus, along with the obviously group of users who do not secure their phones at all, even those who do secure their phones using some passwords are still susceptible to having their phones hacked into.

Unfortunately, more than 40% choose to not secure their phone with a PIN[1], which is likely due to the hassle that comes with typing the PIN, and perhaps making typos or forgetting digits along the way. Danger of password cracking is not new. Consider the Morris worm, one of the first computer worms distributed over the Internet. As his discussion of the Morris worm in his article “Password Cracking: A Game of Wits,” Donn Seeley emphasizes that the worm can easily exploit vulnerabilities such as weak passwords. He explains, “The worm’s password guessing is driven by a 4-state machine. The first state gathers password data, while the remaining states represent increasingly less likely sources of potential passwords[6]. It does not help that most passwords today are, as we have mentioned, influenced by typical number data such as birthdays and even login usernames. The Morris worm is a clear exemplary hacking method that can easily crack typical passwords and it “is aided by some unfortunate statistics about typical password choices”[6].

In both Seeley’s and Bonneau’s papers, we see the vulnerabilities of not securing our phones, and even if we do attempt to secure our phones with some sort of password mechanism provided by the phone’s software, we are still susceptible to security issues. In exploring more and more password cracking mechanisms, we find that there are countless intelligent algorithms and developing theories for cracking passwords. Besides the well-known Morris worm, there are also algorithms that specifically targets 4-digit PIN codes, one of which Markus G. Kuhn discusses in his “Probability Theory for Pickpockets – ec-PIN Guessing”[4]. This is what motivates us to study the usability of Apple’s new Touch ID feature, which could potentially replace the PIN/password security system as a new and improved security mechanism.

3. OVERVIEW OF THE STUDY

Our study consisted of a total of ten tasks to be completed by each participant. The first five tasks pertained to the traditional PIN-code security system with the remaining tasks pertained to the new Touch ID security system. After participants completed the tasks, they were given a post-questionnaire containing questions to elicit their preferences. The post-questionnaire also contained statistics for the participant to read. Our participant pool consisted of 40 Carnegie Mellon University students most of whom were in their early 20s. Twenty two participants owned an iPhone and 18 owned a smartphone other than an iPhone.

3.1 Setup

In Fig. 2, we show how the study was set up. Participants were asked to sit at the corner of a table where they were given an iPhone 5S. A camera for video recording the participant’s actions on the iPhone 5S was positioned in such a way that it did not obstruct the participant’s ability to use the iPhone 5S. We told the participants that they were allowed to hold the iPhone 5S in any way that they wanted and the camera would follow their hands if needed.

To ensure the participants’ comfort, they were told that videos were only for study purposes and would be discarded post the semester project completion. All participants were required to sign a waiver to allow us to record them, and they were given general background information regarding our study. In order to create as natural of a setting as possible, we did not tell our participants that we were timing them or counting their mistakes.

3.2 Tasks

For each task, we recorded, using a non-intruding video-recording camera as shown in Fig. 2, the time taken and the number of attempts made by participants to successfully complete a task. Time for completion was recorded and analyzed in seconds. Attempts made for a Touch ID task were recorded as the number of times user touched his finger to the home button before successfully setting up a fingerprint, unlocking a phone or downloading an application. Attempts made for a PIN-code task were recorded as the number of times user entered a PIN or Apple ID password before successfully setting up a PIN, unlocking a phone or downloading an application.

For each task, we also computed accuracy and ease of completing a task. We measured accuracy by summing the number of typos/mistakes a participant made in each failed attempt at completing a task. To analyze ease of each task, we used the participant preferences data collected as part of the post-survey questionnaire. The following details the ten tasks that participants were asked to complete.
Task 1 – Set up PIN-code.
Participant was asked to set up a brand new iPhone 5S with a PIN-code provided by the experimenter. Note that we reset the phone for each participant to ensure the settings were same for each participant.

Task 2 – Unlock phone using PIN-code.
Participant was asked to lock the phone (phone is set to lock after pressing power button) and then unlock the phone using his/her PIN-code.

Task 3 – Download application from iTunes store.
Participant was given an Apple ID and password. He was asked to look up a specific application and download the application by confirming with his PIN-code.

Task 4 – Unlock phone using PIN-code.
Repeat Task 2.

Task 5 – Change PIN-code and unlock.
Participant was asked to change the PIN-code to a new one provided by the experimenter. This required a participant to reenter former PIN-code, and unlock using the new PIN-code.

Task 6 – Set up Touch ID.
Participant was asked to set up a brand new iPhone 5S with a fingerprint from the index finger. Note that we reset the phone for each participant to ensure the settings were same for each participant.

Task 7 – Unlock phone using Touch ID.
Participant was asked to lock the phone (phone is set to lock after pressing power button) and then unlock the phone using Touch ID.

Task 8 – Download app from iTunes store.
Participant was asked to look up a specific application and download the application by confirming with fingerprint. Note that before this task the iPhone 5S was set up by the experimenter so that the iTunes store settings was set to allow Touch ID to purchase or download applications.

Task 9 – Unlock phone using Touch ID.
Repeat Task 7.

Task 10 – Change Touch ID.
Participant was asked to change the old fingerprint from the index finger to a new fingerprint from the thumb.

4. DATA COLLECTION
In this section, we discuss data collected for each of the tasks in our study. We also discuss data collected regarding participant practices regarding PINs, their perceptions of security of PIN and Touch ID, and preference for PIN or Touch ID. Further, we analyze the data collected.

4.1 Setting up PIN vs. Touch ID
For the initial task of setting up a PIN, we assigned participants the PIN, 8439, which is known to be one of the least frequently used PINs. We specifically picked this PIN based on our findings in Bonneau’s discussion of PIN codes.
in his paper, “A birthday present every eleven wallets? The security of customer-chosen banking PINs,” in which he remarks that most people tend to pick weak passwords that have some sort of graphical pattern on the display. Thus, we decided to pick a statistically “difficult” password for all participants to ensure normality throughout the experiment. Though we take care of the case of people all picking easy PIN codes, we understand that we are compromising the less “real-world” experiment setting since people tend not to pick difficult passwords in their daily lives.

Fig. 3 shows data to support the claim that it takes more time to set up a Touch ID than the 4-digit PIN code. As Fig. 3 reports, on average it takes 48 seconds to set up the Touch ID whereas the 4-digit PIN code only takes 18 seconds to set up. When asked in a post-survey, if participants prefer setting up the Touch ID or the 4-digit PIN code, it can be seen from Fig. 3 that 70% of participants reported that they prefer setting up the PIN whereas only 10% prefer setting up the Touch ID. This preference for setting up the 4-digit PIN code could be correlated with the fact that it takes three times less time to set up a 4-digit PIN.

4.2 Unlocking using PIN vs. Touch ID

Throughout the experiment we asked our participants to unlock the phone with either the 4-digit PIN code or Touch ID. As Fig. 4 shows, the second attempt at unlocking took less than the first time at unlocking the phone with both methods. This data makes sense because the participants became more comfortable with the task the second time around. We can also see that, on average, it took more time to unlock the iPhone 5S with a 4-digit PIN than Touch ID.

Participants made more unlocking attempts with a 4-digit PIN than Touch ID. Observe from Fig. 4 that 40 people who performed the task of unlocking the iPhone 5S using a PIN made a total of 58 attempts at unlocking. In theory, the ideal number of attempts is 40, where each person makes one successful attempt at unlocking the iPhone 5S. However, there were 18 failed attempts to log in on the first try using a PIN. Given the same 40 people who performed the task of unlocking the iPhone 5S using Touch ID, there were only 48 attempts. In this case, there were only 8 extra attempts made compared to the 18 extra attempts using a PIN.

As we can see from Fig. 4, when participants were asked their preference for unlocking with a 4-digit PIN vs. the Touch ID that 50% prefer unlocking the phone with the Touch ID whereas only 20% prefer unlocking with the PIN. This makes sense given that participants, on average, took more time and attempts to unlock their phone using a PIN than Touch ID.

4.3 Downloading an Application using PIN vs. Touch ID

Our participants were told to purchase an app using either the Touch ID or the Apple ID (note Apple ID is longer than the 4-digit PIN code). From Fig. 5 one can see that all participants downloaded an app faster using the Touch ID than with the Apple ID PIN. From Fig. 5, we can see that the average download time was less for Touch ID than PIN.

From Fig. 5, we can see that 60% prefer using the Touch ID to purchase an app compared to 15% who prefer to use PIN. One reason for this could be that it takes, on average, less time to download an app using Touch ID.

4.4 Changing PIN vs. Touch ID

We evaluated how much time it takes to change a PIN password compared to a Touch ID pattern. From Fig. 6, it can be seen that changing a 4-digit PIN takes less time than changing a Touch ID pattern. Recall that users also took more time to set up a Touch ID compared to a PIN. Given that PIN takes less time to change, it seems reasonable that 60% percent of participants prefer to change a PIN whereas only 10% of people prefer to change Touch ID (see Fig. 6).

4.5 Consumer Preferences

The final part of our study was to look into some of the behavior of our participants. When asked if they secured their phone with a security system such as a PIN, 40% of participants responded that they do not secure their phone (Fig. 7). This is similar to the national average of 40% [1]. We also asked them how often they changed their PIN. As Fig. 7 shows 58.3% of people never change their PIN, 33.3% change it once a year and only 8.3% change it more than once a year.

We asked our participants why they chose not to secure their phone. The number one reason (33%) people do not secure their phone, as seen from Fig. 7, is that it frustrates them to login with a password. The number two reason (21%) was that users felt that they were always near their phone, and, hence, there was no reason to use a security feature. Other reasons included time taken to set up a PIN password, the (often false) perception that their phone did not have any sensitive data that needed protection, and the need to share their phone with other people.

When asked what method people felt was more secure, it can be seen from Fig. 8 that the Touch ID beat the PIN code method in that 35% felt the Touch ID was more secure versus only 20% felt that the PIN code method was more secure. However 45% of the users believed that both methods were equally secure.

At the end of our survey we asked the participants which method they would use to secure their phone. From Fig. 8, we can see that a majority or 60% of people said that they would secure their phone with the Touch ID, 30% would secure their phone with PIN, and 10% would not secure their phone at all.

After we asked participants about their preferred method, that is, Touch ID, PIN or none, for securing their phones, we tried to sway their opinion by giving them some statistics. We told them that 9.23% of phones secured with the 4-digit PIN code could be hacked and that smart hackers have successfully lifted fingerprints off from phones and used them to trick the fingerprint sensors. Given these two statistics, we asked participants for the second time which method they preferred for securing their phones. This time, 65% of users stated that they would prefer the Touch ID, which is a 5% increase compared to the first time (see Fig. 8). As with the first time, 30% of the users chose PIN code system. Compared to the 10% of the users who chose not to secure their phone the first time, only 5% said that they would not secure their phone. We can see that users that initially preferred not to secure their phones were swayed to move to a Touch ID system rather than a PIN code system.

5. OVERALL ANALYSIS

With all the statistics gathered, we looked at the data as
Figure 3: Figures showing statistics related to set up task. Time (sec) taken by participants (n=40) for setting up Touch ID and PIN (left); average setup time (middle); participants’ preference for setting up PIN vs. Touch ID (right)

Figure 4: Figures showing statistics related to unlocking with PIN vs. Touch ID. Time taken (sec) by participants (n=40) for first unlock (upper left); time taken for second unlock (upper right); attempts taken for unlocking (lower left); participants’ preference for unlocking with PIN vs. Touch ID (lower right)

Figure 5: Figures showing statistics related to downloading an app task. Time (sec) taken by participants (n=40) for downloading an application using Touch ID and PIN (left); average download time (middle); participants’ preference for downloading app with PIN vs. Touch ID (right)
Figure 6: Figures showing statistics regarding changing PIN or Touch ID task. Time (sec) taken by participants (n=40) for changing PIN and Touch ID (left); participants’ preference for changing PIN vs. Touch ID (right).

Figure 7: Figures showing statistics related participants’ (n=40) PIN practices. Percent who secure their phone with a PIN (left). How often participants change their PIN (middle). Participants’ reasons for not securing their phone with PIN (right).

If we had to declare winners and losers for the usability of each task then the PIN clearly is the winner for setting up/changing the password whereas the Touch ID is the winner for unlocking the phone and downloading apps. The winning method always took less time to complete and reduced the number of user errors. Furthermore, from the data presented in Section 4, it can be seen that users liked downloading apps a lot more with the Touch ID than with the Apple ID. It should be noted that the reason for this is that the Apple ID is more than 4-digits long and takes longer to type as a result.

The last statistic to look at before recommending a security system is to look at Fig. 7, which shows that 58.3% of people never change their PIN, 33.3% change it once a year and only 8.3% change it more than once a year. Based on this behavior, it is easy to say that the Touch ID might be a better method for this group of consumers. Although Touch ID takes three times longer to set up and change compared to that of the 4-digit PIN code, many users are reluctant to change their PIN, so setup would be a one-time burden for these consumers. Furthermore, most users unlock their phones and download apps many times a day and by using the Touch ID, the time it would require them to complete these tasks would be reduced greatly in comparison to the PIN method of security.

6. CONCLUSIONS AND FUTURE WORK

As part of our study conducted in Fall 2013, we compared the usability of Touch ID fingerprint reader with that of PIN-code. Our study included a total of 40 smartphone participants. Twenty two of our participants owned an iPhone...
and 18 had a smartphone other than the iPhone. We asked participants to complete a set of ten tasks five of which were done using the Touch ID and five using the PIN-code method. We calculated the overall time and average time taken to complete a task. We also recorded the number of mistakes participants made while completing each task. Our results show that, on average, non-iPhone users took more time in completing the tasks than iPhone users. Overall, both iPhone and non-iPhone users preferred the same security technique, that is, PIN or Touch ID, for a given task. Participants often preferred the security system for a given task based on which system allowed them to complete the task faster. Overall, users struggled more to set up and change their Touch ID compared to PIN-code. However, they found it easier to use the Touch ID to unlock the phone and download apps compared to PIN-code. During the post-study survey of participant preferences, 60% of the participants expressed that they would secure their phone with the Touch ID whereas 30% said that they would secure their phone with a PIN. The results from our study and the post-study survey suggest that people prefer to secure their iPhone 5S with the Touch ID instead of the PIN-code security system.

Our study can be improved in several ways. Our participant pool consisted of 40 Carnegie Mellon University students, a well-known academic institute. Most of our participants were in their early 20s and likely more technology savvy than an average consumer. Hence, our results may be biased due to the background of our participant pool. In future, to get a broader view of consumers as a whole, we could expand our participant pool to a more general audience and see how that would affect our results. In our study, we asked both iPhone and non-iPhone users to complete tasks on an iPhone. Non-iPhone users took more time to complete the tasks, which may be natural as they are not familiar with an iPhone, but we feel that it should be investigated more. For the PIN-code related tasks, we provided participants with a PIN code. However, participants may perform better at PIN-code related tasks if they select the PIN-code themselves, or if we provide them with PIN-codes that are known to be used more frequently.

Our results suggest that user burden consideration have been a major impediment to the adoption of PINs on smartphones and that fingerprint authentication solutions such as Touch ID have the potential of gaining broader adoption. While fingerprint authentication has some limitations and shortcomings, these findings have to be looked at in light of the large number of smartphones stolen every year in the US and abroad and the fact that somewhere between 40 and 50% of smartphone users do not use PINs today.

7. REFERENCES

2Concurrently with this project, another group of students working in the class in the Fall of 2013 demonstrated how TouchID could be cracked.