Towards understanding how Touch ID impacts users' authentication secrets selection for iPhone lock

by

Ivan Cherapau

B.Sc in Physics, University of Massachusetts Boston, 2010

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF

Master of Applied Science

in

THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES
(Electrical and Computer Engineering)

The University of British Columbia
(Vancouver)

June 2015

Abstract

Smartphones today store large amounts of data that can be confidential, private or sensitive. To protect such data, all mobile OSs have a phone lock mechanism, a mechanism that requires user authentication in order to access applications or data on the phone, while also allowing to keep data-at-rest encrypted with encryption key dependent on the authentication secret. Recently Apple has introduced *Touch ID* feature that allows to use a fingerprint-based authentication to unlock an iPhone. The intuition behind such technology was that its usability would motivate users to use stronger passwords for locking their devices without sacrificing usability substantially. To this date, it is not clear, however, if users take an advantage of Touch ID technology and if they, indeed, employ stronger authentication secrets. It is the main objective and the contribution of this work to fill this knowledge gap.

In order to answer this question we conducted three user studies (a) an in-person survey with 90 subjects, (b) an interview study with 21 participants, and (c) an online survey with 374 subjects. Overall we found that users do not take an advantage of Touch ID and use weak authentication secrets, mainly PIN-codes, similarly to those users who do not have Touch ID sensor on their devices. To our surprise, we found that more than 30% of subjects in each group did not know that they could use alphanumeric passwords instead of four digits PIN-codes. Others stated that they adopted PIN-codes due to better usability in comparison to passwords. Most of the subjects agreed that Touch ID, indeed, offers usability benefits such as convenience, speed and ease of use. Finally, we found that there is a disconnect between users desires for security that their passcodes have to offer and the reality. In particular, only 12% of participants correctly estimated the security PIN-codes provide while the rest had unjustified expectations.

Preface

Chapters 5, 6 and 7 of this thesis have been published. The author of this thesis performed the users studies mentioned in chapters 5, 6 and 7. He also analyzed the data from those studies. He authored the corresponding paper, under the supervision of Dr. Konstantin Beznosov who provided feedback and guidance throughout the research process. Details of the published paper are below:

- I. Cherapau, I. Muslukhov, N. Asanka, and K. Beznosov. Impact of Touch ID on Users Authentication Secrets Selection for iPhone Lock. In Proceedings of the Eleventh Symposium on Usable Privacy and Security, SOUPS 15, 2015.

Three user studies were conducted as part of the research. For the first study (explained in chapter 5), we submitted a human ethics application with the BREB number of H14-02759 to UBC Behavioural Research Ethics Board. For the second study (explained in chapter 6) and the third study (explained in chapter 7), we submitted amendments (with the same BREB number) to the first study application. The ethics application and its amendments were approved by UBC Behavioural Research Ethics Board.

Table of Contents

Abstract . . . . . **ii**

Preface . . . . . **iii**

Table of Contents . . . . . **iv**

List of Tables . . . . . **vii**

List of Figures . . . . . **viii**

Acknowledgements . . . . . **x**

1 Introduction **1**

2 Background **4**

2.1 Data Protection in iOS and Bruteforce Attack 4

2.2 Touch ID 5

2.3 Measuring Password Strength 7

3 Literature Review **8**

4 Research Question and Hypotheses **11**

5 Study 1 – In-person Survey **12**

5.1 Methodology 12

5.1.1 Study Design 12

5.1.2 Participant Recruitment 13

5.2 Results . . . 14
5.2.1 Participant Demographics . . . 14
5.2.2 Reasons To Lock Or Not To . . . 15
5.2.3 Use of PINs and Passwords . . . 15
5.2.4 Touch ID Group . . . 17
5.2.5 Non-Touch ID Group . . . 17
5.2.6 Hypothesis Testing . . . 18
5.3 Limitations . . . 19

6 Study 2 – Interviews . . . 20
6.1 Methodology . . . 20
6.1.1 Participant Recruitment . . . 21
6.1.2 Procedure . . . 21
6.2 Results . . . 22
6.2.1 Participant Demographics . . . 22
6.2.2 Reasons for Using PIN-codes . . . 22
6.2.3 Security Lock Sharing Behaviour . . . 25
6.3 Limitations . . . 26

7 Study 3 – Online Survey on MTurk . . . 27
7.1 Methodology . . . 27
7.2 Results . . . 28
7.2.1 Participant Demographics . . . 28
7.2.2 Testing H_1 . . . 29
7.2.3 Testing H_2 . . . 30
7.2.4 Reasons for Using PIN-code . . . 30
7.2.5 Reasons for Using Touch ID . . . 32
7.2.6 Who Users Lock Their iPhones Against . . . 33
7.2.7 Authentication Secret Sharing Behaviour . . . 33
7.3 Limitations . . . 35

8 Discussion **37**

9 Conclusion **40**

Bibliography **42**

A In-person Survey Guide and Questions **46**

A.1 Agenda 46

A.2 Questions for Both Conditions 46

A.3 Questions for Touch ID Group 53

A.4 Questions for Non-Touch ID 56

A.5 Final Instructions for Both Groups 57

A.6 In-person Survey Supplemental Graph 58

B Interview Guide and Questions **59**

B.1 Agenda 59

B.2 Questions 59

C Online Survey Questions **61**

C.1 Questions for Both Groups 61

C.2 Questions for Non-Touch ID group 71

C.3 Questions for Touch ID Group 72

C.4 Online Survey Supplemental Graph 74

List of Tables

Table 5.1 Demographics of In-person Survey Participants 16

Table 5.2 Average Entropies of Unlocking Authentication Secrets for Touch ID and non-Touch ID Groups. 18

Table 6.1 Demographics of Interviewed Participants 23

Table 7.1 Demographics of MTurk Participants and Distribution across Two Groups and Locking Authentication Method Used. 36

List of Figures

Figure 2.1 Overview of how Touch ID works. When Touch ID is enabled and user lock the device, the encryption key is wrapped by random wrapping key. A user has an option to type in his passcode (1b) or use Touch ID. When the user use his fingerprint to unlock the phone in step (1), Touch ID authenticates the user by matching his fingerprint with saved fingerprints. If the authentication is successful, the sensor release a wrapping key to the Secure Enclave in CPU (2) , so CPU can send Data Protection Keys to Crypto Engine (3). If, the user fails to authenticate for five times, or does not unlock device for 48 hours, the Touch ID sensor flushes the unwrapping key, which leaves typing in the passcode as the only option for unlocking an iPhone. 6

Figure 5.1 In-person survey's password structure question. 14

Figure 6.1 Number of unique codes for each additional subject. We reached saturation around 17th subject. 21

Figure 7.1 Examples of verification photos that subjects sent us. From left to right, (1) a photo of an iPhone taken with front facing camera in a mirror, (2) a screenshot of PIN-code based iPhone unlock interface, and (3) a screenshot of password-based iPhone unlock interface. 28

Figure 7.2 Reasons for using PIN-codes instead of passwords for each group. 31

Figure 7.3 Reasons for using Touch ID (n = 173). 32

Figure 7.4 Distribution of attackers who users lock their iPhones against. For Touch ID group (n = 173), and for non-Touch ID group (n = 201). 34

Figure 7.5 Distribution of authentication secret for iPhone lock sharing among different groups of people (n = 374). 35

Figure A.1 Study 1 (in-person surveys) Touch ID participants' answers for questions "How hard was it to set up Touch ID?", "Is it easy to use Touch ID?" and "Overall, how satisfied are you with using Touch ID?" (n = 41). 58

Figure C.1 Distribution of attackers (insiders and strangers) who users lock their iPhones against. For Touch ID group (n = 173), and for non-Touch ID group (n = 201). 74

Acknowledgements

First, I would like to thank my academic advisor, Konstantin Beznosov, for his kind support, guidelines and assistance during my graduate studies.

Second, this work would not have been possible without my smart colleagues and great friends. Thank you Ildar Muslukhov for a lot of help throughout the course of the project, Yazan Boshmaf for a great feedback and outdoor activities, Primal Wijesekera for intellectually stimulating conversations.

Third, I would like to thank all members of LERSSE for their feedback.

My heartfelt gratitude goes to my dear parents and my brother for their enormous support and constant encouragement.

To my parents for their endless love, support and encouragement.

Chapter 1

Introduction

Smartphones have become our primary devices for accessing data, applications and by extension the Internet. With more than a billion smartphones sold in 2014 and more than 2 billion active subscribers, global smartphone user base is expected to grow to 5.6 billion by 2019 [14]. Smartphones are already used for online banking, accessing corporate data, operations that used to be only in the domain of desktops and laptops. This transition results in sensitive and confidential data being stored and accessed on smartphones. High mobility and small size of smartphones alter the common threat model used for desktop and laptops devices. In particular, it is much easier to steal smartphones due to their size, and then to access data-at-rest [29].

The state of the art approach to protect data-at-rest, adopted by all mobile OSes, is to encrypt data, e.g., see [33]. In order to avoid the problem of storing an encryption key together with encrypted data, a user authentication secret is used to derive a key that protects the actual data encryption key. The common practice is to use smartphone lock authentication secret for such purpose. Unfortunately, users employ weak personal authentication secrets, i.e., personal identification number (PIN), mainly due to usability-related considerations [32]. PIN-codes are not only susceptible to shoulder surfing attack, they can also be easily bruteforced [35]. At the same time, 4-digit PIN-codes are considered unusable by more than 20% of smartphone users [32]. In particular, usability issues pushed these users to disable smartphone lock completely, which leaves hundreds of millions of smartphone users unprotected [31].

In recent years, several companies, such as Apple and Samsung, have introduced biometric authentication to smartphones lock. For example, in 2013, Apple has introduced a fingerprint scanner into the iPhone 5S "home" button, so-called Touch ID, which authenticates a user once she touches the *Home*

button. As it is stated in the iOS security white paper [4], the key advantage Touch ID is that it *"makes using a longer, more complex password far more practical because users won't have to enter it as frequently"* and *"the stronger the user password is, the stronger the encryption key becomes. Touch ID can be used to enhance this equation by enabling the user to establish a much stronger password than would otherwise be practical."*

These claims are based on the assumption that usability of the password largely depends on the frequency of its usage and that users will use passwords with higher entropy as a result of a reduced frequency . Recent research, however, casts doubts on this assumption. In particular, several studies have showed that users tend to create low-entropy passwords regardless of how frequently they have to type it in [8, 18, 36]. Thus, it's still unclear if and how Touch ID sensor impacts users' passwords selection. Thus, the main focus of the work presented in the thesis is to fill up this knowledge gap.

In order to understand the impact of Touch ID sensor on users' password selection, we focus on testing our main hypothesis (H_{Main}) – "There is a difference in password entropy between those who use Touch ID and those who do not". To measure password entropy we used zero-order entropy[1] as it (a) served the purpose of our study in terms of comparing two groups, (b) allowed us to do the comparison without having access to actual passwords. Furthermore, the results of our study revealed that even with zero-order entropy, which overestimates the real complexity of passwords, the strength of currently used passwords can not withstand brute-force attacks. Throughout this thesis we refer to zero-order entropy as entropy for brevity.

To test the H_{Main} we conducted three user studies. We received an approval for conducting the user studies from our university's office of research ethics. In order to get a first take at H_{Main}, we conducted an in person survey with 90 subjects. We opted for in person survey in order to able to verify reported data accurately. The results of the study did not reveal statistically significant difference between the average entropies of both groups. Meanwhile, the 95% confidence interval suggested that if there is a difference, hypothetically, then the absolute value of a difference should not be larger than 3.35 bits. In order to understand why users are not adopting stronger passwords when Touch ID is available we conducted a follow up qualitative study based on interviews. The results of the interviews with 21 subjects allowed us to identify the key reasons for users to stick with weak 4-digits PIN-codes. Unawareness of passcode availability is one such reason. Finally, to corroborate findings of the first two

[1]Zero-order entropy implies that each password character is selected independently of all previous characters.

studies, we conducted an online survey with 374 subjects. Final study confirmed the results of the in person survey and quantitatively measured the prevalence of found reasons. In particular, more than 30% of the participants were unaware that stronger passcodes are available, around 35% of the participants preferred PINs as they are easier to remember and more than half of the participants used PINs because they are easier to use (e.g., faster to type). In addition, we narrowed down the 95% confidence interval for a hypothetical difference in passwords entropies between the two groups (1.91 bits of difference at most).

Chapter 2

Background

In this chapter we give necessary background. We begin with discussion of the bruteforce attack on passcode in iOS device and how Touch ID sensor works. We conclude by explaining how we measured password entropy.

2.1 Data Protection in iOS and Bruteforce Attack

To protect data confidentiality, iOS encrypts each file with a unique per-file key. Per file key is then encrypted with one of four class keys. Each of the four class keys is available during various contextual settings, e.g., after the first unlock or when the device is unlocked. These class keys are protected with the user's passcode and a Device ID, i.e., a hardware embedded unique key. In order to extract hardware embedded key, an adversary can attempt to reverse engineer the crypto chip, which is expensive task in terms of time and resources required. If that key extraction operation fails, the adversary can still mount an *on-device* bruteforce attack, which uses the crypto-chip directly, in order to decrypt class keys. To decrease effectiveness of such attacks the crypto chip in iOS is calibrated to take at least 80 ms for each passcode attempt.

In order to mount an *on-device* attack an adversary needs to be able to run arbitrary code on the stolen device. This can be achieved by compromise of the boot-chain, which consists of the following steps (1) BootRom (non-updateable read-only firmware), which loads iBoot phase and verifies integrity before passing control to it, (2) iBoot - (updateable firmware), which checks integrity of Kernel, loads it and passes control to it, and (3) the Kernel, responsible for all the services in iOS and for loading users Apps [1]. To bypass Kernel's limitation on the number of available attempts, one needs to compromise

BootRom or iBoot [43]. The recent history of jailbreaking suggest that making iBoot and BootRom bug-free is quiet challenging [1]. Note that, it does not matter whether the phone is locked or not once the attacker can run arbitrary code on the device. That is, the attacker can use crypto chip directly in order to try all possible passcodes without restriction of 10 attempts enforced by the Kernel (i.e., iOS).

Of course, it takes some time, effort and luck to find an exploitable bug in BootRom or iBoot steps for new version of iOS. The history of security, however, has taught us that it is impossible to eliminate all bugs in complex systems. Even more, there are claims that these bugs are known to jailbreaking community for the most recent iOS version (i.e., 8.3)[2].

2.2 Touch ID

Touch ID is a biometric authentication sensor based on a high definition fingerprint scanner embedded into *home* button on iPhones. This sensor allows users to unlock their devices by simply touching the home button. Although Touch ID allows to unlock a device without typing in a password, users are still required to set a PIN-code or a password before being able to use the Touch ID sensor. The root cause for such strict requirement lays in data-at-rest encryption, which needs a source of entropy that is not stored on the device itself. Users' unlocking authentication secrets are used as such source.

A password can be a simple four-digit PIN-code[3] or a longer one, with up to 37 characters and with 77 possible symbols. When a locked device boots, it requires the user to provide the password or PIN-code, since the Touch ID internal memory is flushed on reset or shutdown, i.e., immediately after reboot users are not able to use Touch ID sensor. Once a user provides the unlocking secret, the OS is able to recover actual data encryption keys and uses them to decrypt and encrypt data. If the device is rebooted or locked, OS erases certain types of keys from RAM, i.e., a passcode will be needed to recover them on unlock.

When user locks the device and Touch ID sensor is enabled, iPhone's CPU generates a random wrapping key and "wraps" the encryption key derived from unlocking secret. It then sends the wrapping key to Touch ID sensor and deletes the key derived from unlocking secret from RAM. After that, a user has two options in order to unlock the device, either type in the unlocking secret or to use Touch ID to release the unwrapping key back to CPU. When the user touches the Touch ID sensor, the sensor tries

[1] http://blog.thireus.com/tag/iboot

[2] https://www.theiphonewiki.com/wiki/IBoot_(Bootloader)#Exploits

[3] Apple security white paper defines it as a simple passcode. We refer to such passwords as to PIN-codes.

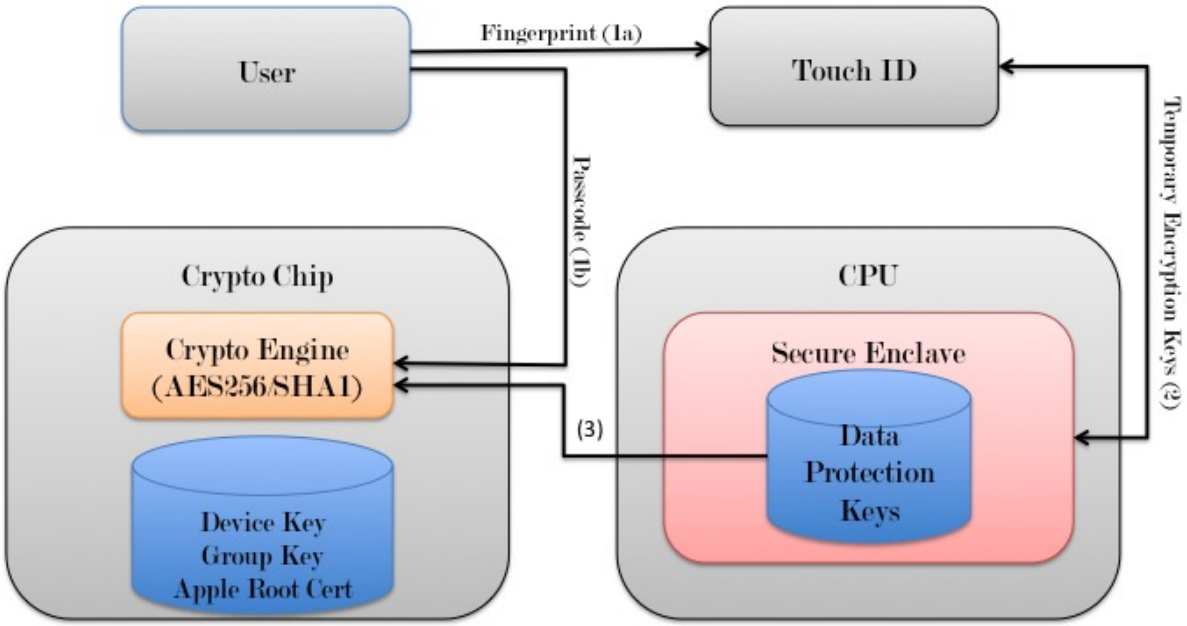

Figure 2.1: Overview of how Touch ID works. When Touch ID is enabled and user lock the device, the encryption key is wrapped by random wrapping key. A user has an option to type in his passcode (1b) or use Touch ID. When the user use his fingerprint to unlock the phone in step (1), Touch ID authenticates the user by matching his fingerprint with saved fingerprints. If the authentication is successful, the sensor release a wrapping key to the Secure Enclave in CPU (2) , so CPU can send Data Protection Keys to Crypto Engine (3). If, the user fails to authenticate for five times, or does not unlock device for 48 hours, the Touch ID sensor flushes the unwrapping key, which leaves typing in the passcode as the only option for unlocking an iPhone.

to authenticate the user based on the fingerprint. If the authentication attempt is successful, the sensor releases the unwrapping key to the CPU. If, however, the user fails to authenticate for five times, or does not unlock device for 48 hours, the Touch ID sensor flushes the unwrapping key, which leaves typing in the unlocking secret as the only option for unlocking an iPhone. The diagram of how Touch ID unlocks an iOS device is shown in Figure 2.1.

We decided to focus on Touch ID sensor mainly because it is implemented into an existing and popular operating system, which is widely adopted. We did not study Android fingerprint and face

scanners because the former is very new technology that first appeared in April 2014 [20] and the latter has several usability [7] and security issues [15].

2.3 Measuring Password Strength

The strength of an authentication secret is defined by the efforts an attacker needs to spend on guessing it. In simple terms, these efforts can be defined as the size of the search space the attacker needs to check in order to find the correct password. One such metric is the zero-order entropy, measured in bits and calculated as

$$L * log_2 N$$

where L is the length of the password and N is the character set size (e.g., the length of iPhone's PIN-code is four and the character set size is 10, hence, its zero-order entropy is 13.28 bits). That is, zero-order entropy measures the size of the whole search space of all possible passwords for a given length and a given alphabet set with the assumption that each character is selected independently from all previous ones.

Of course, zero-order entropy, as a metric, suffers from several limitations. The most important one is that it does not measure the password strength accurately. Recent research has showed that users tend to select highly predictable passwords and often use dictionary words as ones [9, 16]. Such predictability makes the search space smaller, i.e., the work of an attacker easier. This implies that the zero-order entropy measures the upper bound of the work for an attacker, i.e., overestimates the workload.

Even considering its limitations we decided to use zero-order entropy in our study for password strength comparison for several reasons. First, evaluation of the password's guessability requires access to plaintext passwords, which we did not have for ethical considerations. Second, zero-order entropy served well the purpose of our study in comparison of two groups, i.e., with and without Touch ID, in terms of work the attacker needs to do. Finally, the results of our study showed that even if we overestimate the password strength, the actual workload for a bruteforcing attacker is still practical.

Chapter 3

Literature Review

Authentication mechanisms have been studied extensively for many years [8, 26], however, text-based passwords remain the most commonly used authentication mechanism and the security's weakest link [9, 22, 27]. Florencio and Herley [16, 17] conducted a study on web password use and reuse with half a million users over a three months period. Their results suggest that web users employ and re-use low-entropy passwords on websites. Weir *et al.* [41] analyzed a set of leaked passwords. Authors showed that popular passwords were also weak and "123456" was very common among users. To prevent users from choosing passwords that are too easy for an attacker to guess, system administrators often enforce password-composition policies [27]. A policy might require users to use a password that contains non-alphanumeric symbols, lower and upper case letters, and numbers. Using a too strict password policy, however, might backfire and push users to write down passwords or store them on some other devices [27].

Two recent studies examined smartphone locking behaviours using conventional authentication mechanisms. Harbach et al. found that users activate their phones 85 times and unlock their phones 50 times per day on average and that most of users did not see any threat to the data on their phone[21]. Egelman et al. also found a strong correlation between locking behaviours and risk perceptions, but authors believe that user's risk perceptions underestimates actual dangers [13]. In contrast to these papers, we focused on the reasons for stronger passcodes not been used when TouchID is available.

A different authentication modality, such as biometrics-based authentication, has also received a lot of attention from research community [2, 30, 39]. If used, biometric authentication methods could remedy common drawbacks of text-based passwords. For example, users do not need to remember any-

thing [7]. Although, as it has been shown, the usability of a biometric system is still an important factor in adoption [34, 38]. The results of De Luca et al. study show that usability is one of the main factors that influences user's decision on whether or not to use smartphone biometric authentication [12]. Crawford and Renaud's [11] study revealed that users were willing to try biometric authentication mainly for its usability benefits. In addition, Breitinger *et al.* [10] showed that 87% of users were in favour of fingerprint authentication. Wimberly and Liebrock observed that the presence of the second factor in a two-factor authentication system caused users to pick weaker credentials than if only passwords were used to protect an account [42]. In contrast to our work, we focus on how Touch ID sensor impacts users' choice of iPhone unlocking authentication secret in a single-factor authentication system.

Indeed, there are many reasons to use fingerprint for authentication. To start with, it is unique to each individual, and it is almost impossible to find two people with an identical fingerprint pattern [4]. Individuals' fingerprint patterns never change during their life span [40]. Fingerprint sensor can benefit the security and the user convenience, if used in smartphones [19]. There are many limitations of smartphones' screen size and keyboards [19, 25]. Finally, text entry on constrained keyboards is prone to errors, time-consuming and frustrating. In particular, Lee and Zhai showed that error rate for typing on virtual keyboards, i.e., keyboards drawn on a screen, is 8% higher than on hardware keyboards on general purpose computers [28]. Furthermore, Bao *et al.* [6] found that the average typing speed for a 8-character alphanumeric password on desktop computers it was 17 words per minute (w.p.m), while on a mobile device it was 6 w.p.m., i.e., almost three times slower.

Recent research shows that users tend to use 4-digit PINs over alphanumeric passwords in smartphones [24, 32]. Users justified such choice by how easy it is to use PIN-codes in cases when one has to type them with high frequency for their day-to-day activities. Unfortunately, it is clear today that a 4-digit PIN provides virtually no security for data-at-rest [4, 37]. To make the matter worse, even within 4-digit PINs search space, users select highly predictable ones. For instance, Amitay [3] analyzed over 200,000 iPhone PINs and showed that "1234" is the most common PIN, followed by "0000" and "2580". Considering that iPhone allows up to 10 attempts for unlocking the device through user interface, before erasing the data, one can try the top 10 PIN-codes and still achieve 15% success rate. That is, one in seven iPhones can be unlocked by just trying the top 10 PIN-codes. The main intuition behind the design of the Touch ID sensor was to reduce the number of times a user must type her authentication secret to unlock the device [4]. Bhagavatula et al found that most Touch ID users perceive it as more

usable and secure than a PIN [7]. To the best of our knowledge, we are the first to assess whether users take an advantage of Touch ID sensor and increase entropy of their iPhone unlock secrets.

Chapter 4

Research Question and Hypotheses

The main research question (RQ_M) of our study is "How availability of Touch ID sensor impacts users' selection of unlocking authentication secrets". To answer this question we formulated the following hypotheses to be tested:

- H_1^{null} – *Use of Touch ID has no effect on entropy of authentication secrets used for iPhone locking*.
- H_1^{alt} – *Use of Touch ID affects entropy of authentication secrets used for iPhone locking*.
- H_2^{null} – *Availability of Touch ID has no effect on ratio of users who lock their iPhones*.
- H_2^{alt} – *Availability of Touch ID increases the ratio of users who lock their iPhones*.

To answer RQ_M we conducted three user studies. We started with a study based on in-person surveys. This study allowed us to get a first glance on our hypotheses, clarify areas with the lack of understanding and focus our future studies. Once we tested our hypotheses in the first study, we followed it with a focused interview-based study. The main focus of the second study was to fill our knowledge gap in users' reasoning for not adopting stronger authentication secrets with Touch ID. The results of this study allowed us to gain an insight into why users still use PIN-codes, even when Touch ID sensor is available. Finally, to corroborate our data and measure the relevance of different reasons for the use of weak authentication secrets, obtained from the second study, we conducted the third study in a form of an online survey. This study gave us a larger and diverse subject pool for testing our set of hypotheses and provide descriptive statistics on reasons for using weak unlocking authentication secrets.

Chapter 5

Study 1 – In-person Survey

5.1 Methodology

In our first study, we chose to use an in-person survey of iPhone users in order to get the first attempt at the set of hypotheses. An in-person nature of the study not only allowed us to follow-up unforeseen answers with additional questions, but also gave us an opportunity to validate most of the answers provided by subjects. We strived to recruit a pool of diverse subjects, hence we approached our participants in common public places, such as shopping malls and coffee shops. Each subject signed a consent form and received $10 as a compensation for participation.

5.1.1 Study Design

To facilitate faster data collection in public locations with limited and unreliable access to the Internet, we developed an iPad application, which showed survey questions to users and collected responses. All answers were stored locally, for some of the questions we also validated subjects' answers by asking participants to show us the item at question. For example, we validated the type of authentication method used, by asking to show us the locking screen, and we validated the length of the alphanumeric password by asking subjects to show us the unlocking screen after the password has been typed but the participant has not pressed the *Enter* button. This allowed us to count the number of stars in the password field, which validated the password length. In addition, subjects were asked to navigate to the settings of the auto-lock screen. This allowed us to validate auto-lock value. Finally, by asking subjects to unlock their device with a fingerprint we were able to confirm that they, indeed, used the Touch ID sensor.

Most of the survey questions were either open-ended or contained option "Other", which allowed subjects to provide their own answer if needed. The questionnaire guide is provided in Appendix A and consists of the following parts:

1. **Part 1** – Demographic questions (e.g., age, gender, education, income, occupation).

2. **Part 2** – Security and privacy concerns related questions, e.g., we asked subjects if they had any sensitive, private or valuable information on their iPhones.

3. **Part 3** – Questions on the experience subjects had that far with their smartphones, including if they used smartphone locks in previous smartphones.

4. **Part 4** – Password metrics questions. In this part, we asked subjects to provide us a structure of their unlocking passwords. In order to preserve confidentiality of the plaintext passwords, participants substituted each character in their passwords with character type mnemonic. For digits letter 'D' was used, for lower-case letters we used letter 'L', for upper-case letters we used character 'U', and finally, for special characters letter 'S' was used. For example, password "12pA@" would be presented as "DDLUS" string. The screenshot of this question is shown in Figure 5.1. We chose this approach for two reasons. First, it allowed us to assess entropy. Second, this approach did not require us to have access to plaintext unlocking authentication secret.

5. **Part 5a** – This section was only relevant for iPhone 5s, 6 and 6 Plus owners. In this section, we asked questions related to Touch ID's usability and reasons for its adoption.

6. **Part 5b** – This section was only relevant for the owners of iPhone 5 and earlier models. There, we asked subjects about their perception of biometric authentication methods such as Touch ID.

In order to test our questionnaire, we conducted a pilot study with 12 participants. Based on the results of the pilot study we revised the survey application and modified several questions in the questionnaire. Most of the changes we made were aimed at improving questions' readability.

5.1.2 Participant Recruitment

We recruited participants in public places such as shopping malls, libraries and coffee shops in the downtown area of Vancouver. We approached prospective participants who had iPhones with them and offered them to participate in our study. We chose this recruitment method mainly because we were

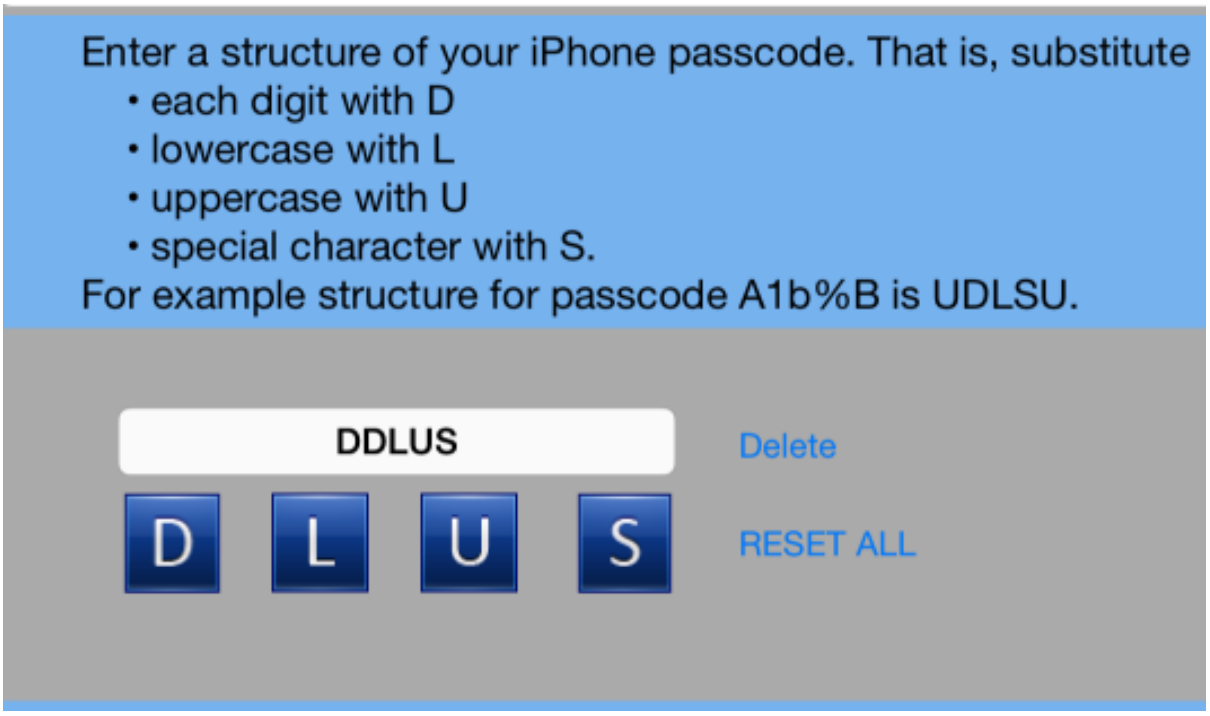

Figure 5.1: In-person survey's password structure question.

interested in the general population of iPhone users and. We recruited subjects who were iPhone users and 19 years old or older. Although the main focus of our study was Touch ID sensor (iPhone 5S, 6 and 6+ owners), we also recruited subjects with older models, such as iPhone 5 and older. Subjects that used the Touch ID sensor were grouped into Touch ID group while the rest were grouped into non-Touch ID group. Note, that even iPhone 5S, 6 and 6+ users were assigned to the non-Touch ID group if they did not use the Touch ID sensor.

5.2 Results

In this section, we report the results of an in-person survey study. We first report participants' demographics, then provide findings for all subjects and for each group separately. Finally, we report the results of statistical tests for H_1 and H_2.

5.2.1 Participant Demographics

Overall, we recruited 93 subjects. We, however, had to exclude 3 subjects who failed password length verification. Thus, the results presented in this section are based on **90** participants.

Out of 90 participants, 32 were female. The minimum and maximum age was 19 and 71 years, and

the average age was M = 29 (*SD* = 12). Among all subjects, 41 used Touch ID sensor and 49 did not. Majority of our participants were experienced iPhone users, i.e., they owned an iPhone for more than two years of experience. Only 12 subjects owned iPhones for less than a year. Almost all of the subjects (81) had owned another smartphone before the current one. Most of our subjects (69) have stated that they unlock their iPhones at least a once per hour. In addition, we found that 32 subjects had lost their smartphones before, and 15 subjects were victims of smartphone theft. On average, subjects completed survey in around 5.5 minutes (*SD* = 2 minutes) in non-Touch ID group, and in around 7 minutes (*SD* = 3 minutes) in Touch ID group. Demographics summary is provided in Table 5.1.

5.2.2 Reasons To Lock Or Not To

Overall we found that subjects use various reasoning to justify locking or not locking their iPhone. Some of the reasons were driven by *a possible attacker*, e.g., 58 subjects locked their devices to restrain strangers from using their iPhone and 4 subjects locked their phone to protect their data if they get mugged, 23 subjects used device lock to control access to their device by their family or friends. In addition, we saw that some subjects used social behavior to justify locking, e.g., 12 subjects said that they lock their device because their friends did the same.

Other reasons were focused either on *usability problems* of device locking, voiced mainly by those who did not lock their device, or *necessity to have certain features* that were either enabled or prevented by device locking. The four subjects who did not lock their device stated the following reasons: (a) locking a phone makes it impossible to use it in emergency cases, (b) locking iPhone makes it impossible to contact the owner in case the device is lost, and, finally, (c) unlocking process takes too much time. Only two subjects, out of the four, who did not lock their iPhones stated that they did not care about security of their data.

5.2.3 Use of PINs and Passwords

Out of the 90 subjects, 86 locked their phones, with 66 employing 4-digit PIN-codes, and 20 using alphanumeric passwords. Third of the subjects (36) used the same PIN or password for their iPhones as they used in their previous smartphones. In addition, 52 subjects stated that they shared their unlocking authentication secret with someone else, and 53 stated that they knew unlocking authentication secret from other smartphone users.

Table 5.1: Demographics of In-person Survey Participants

Parameter	Property	Participants	%
Gender	Female	30	34
	Male	60	66
Age	19-24	43	48
	25-34	29	32
	35-44	8	9
	45-54	2	2
	55-64	6	7
	65+	2	2
Education	High school	30	34
	College degree	22	24
	Bachelor	28	31
	Master or PhD	7	8
	Other	3	3
Income	Less than 20K	25	28
	20K-50K	29	32
	50K-80K	16	18
	80K-120K	8	9
	Above 120K	5	6
	Prefer not to answer	7	8
Industry	Construction	2	2
	Trade	2	2
	Transportation	3	3
	Finance and real estate	7	8
	Professional services	5	6
	Business and building	11	12
	Educational services	4	4
	Health care and social	5	6
	Inform./culture/recreation	3	3
	Accomm./food services	6	7
	Public administration	1	1
	Other	45	41
iPhone Ownership (years)	0-1	12	13
	1-2	18	20
	2-3	24	27
	3+	36	40
Frequency of unlocking	Once a day	3	3
	Few times a day	11	12
	Once per hour	12	13
	Few times per hour	57	64
	I have no idea	7	8
Locking method	PIN-code	66	73
	Password	20	22
	None	4	5

5.2.4 Touch ID Group

The Touch ID group included 41 subjects, with 29 of them using 4-digit PIN-codes. Majority of them agreed that they liked using Touch ID. In particular, 26 participants found that setting up Touch ID was easy or very easy and 29 subjects stated that use of Touch ID was easy or very easy (see Appendix A.6). Majority of the participants (30) had never had any issues with Touch ID. Overall Touch ID users thought of Touch ID as of convenient, secure, quick and easy to use unlocking mechanism.

Touch ID subjects also voiced their concerns with fingerprint scanning sensor. In particular, three participants had problems with sharing their iPhones. Others saw Touch ID sensor as a threat due to the ability of an attacker to unlock device while the owner is sleeping (e.g., P9 "... [I] might be sleeping and someone might use my finger to unlock [my iPhone] ...")[1]. Some subjects were even afraid that an attacker might fake their fingerprints, in order to access device later. Seven participants worried about privacy of their fingerprints, due to the lack of clarity on whether Apple stores their fingerprints somewhere else. For example, one of the subjects (P11) stated that she was afraid about "Apple leaking my fingerprint and someone can impersonate me" and "fingerprint being used for other purposes than to just unlock my phone".

5.2.5 Non-Touch ID Group

The non-Touch ID group included 49 subjects, where 4 subjects did not lock their phones and 37 used PIN-codes and eight used passwords as unlocking authentication secret. Out of 49 subjects, 13 had Touch ID available but did not use it.

We observed that participants perceived fingerprint authentication as a security improvement. For example, "anyone can figure out a password but people can't copy your fingerprint" (P69), "additional security", "for those with sensitive info on phones more security is desirable" (P78), "it is easy, accurate and secure" (P5), "it's safer" (P19), "more secure than 4 digit password" (P33), "no one can fake my fingers" (P98), "I will use Touch ID so my friends don't get in my phone" (P45). Although their iPhones did not have fingerprint scanners, more than one-third of participants believe that Touch ID is most secure unlocking method. Surprisingly, only three participants from non-Touch Group were willing to use a longer alphanumeric password alongside with the Touch ID.

[1] Exactly the same story has happened recently, when the son unlocked his father iPhone by his father's large thumb while the father was sleeping (http://money.cnn.com/2014/12/01/technology/security/apple-iphone-encryption-fingerprint).

Table 5.2: Average Entropies of Unlocking Authentication Secrets for Touch ID and non-Touch ID Groups.

	Touch ID	**Non-Touch ID**
Mean	15.88 bits	15.61 bits
SD	6.93 bits	7.45 bits
N	41	49

5.2.6 Hypothesis Testing

To test H_1 we first compared proportions of users that use PIN-codes and passwords in both groups. Then we compared mean values of entropies in both groups. Analysis of proportions did not reveal any statistically significant difference (χ-squared = 1.01, p = 0.32). In order to compare mean values of entropies in both groups we used masks that subjects provided in order to obtain the length of the authentication secret and the alphabet size, which later were used for entropy calculation. The results of Mann?Whitney U test for 2 samples (Touch-ID and Non-Touch ID groups) did not reveal any statistically significant difference between mean values of entropies in both groups (W = 15708, p = 0.70, see Table 5.2. Thus, we were unable to reject H_1^{null}.

In addition, statistical analysis of the mean values of entropies gave us a confidence interval, i.e., the possible interval of the difference. This allowed us to assess the biggest possible difference in entropies in case a statistically significant difference is found, by recruiting larger participant pool. In this case the 95% confidence interval for the difference between the means was from -3.35 up to 2.81, or 3.35 bits at most.

If we consider a hypothetical scenario in which the Touch ID group has a higher entropy, and we simply failed to determine that due to small size of the subject pool, and considering the observed mean entropy value of 15.88 bits, we can obtain the possible maximum entropy for the group, which is 19.23 bits of entropy. Taking into account the design of the data encryption in iPhones, i.e., that each password candidate check takes at least 80ms, we can estimate how long an average authentication secret would protect data-at-rest with password of 19.23 bits of entropy, which corresponds to roughly 14 hours. In comparison, the non-Touch ID group's passwords on average provide protection for only 1.1 hour.

We tested H_2 hypothesis with Chi-squared test (χ-squared = 0, p = 1.0). We were unable to reject H_1^{null}, and hence we conclude that our study did not show any effect of Touch ID on users' preference to lock their iPhone.

5.3 Limitations

Although we failed to find any statistically significant difference in password selection between Touch ID and non-Touch ID groups, there were several limitations, which might have impacted the outcome. First, we might not have obtained large enough sample size and there was still a fairly large bias towards the 19-34 age group. The U.S. Mobile Report found that over 43% of iPhone users are younger than 34[2]. Second, although we did not show any difference between two groups' selection of the unlocking password, we cannot explain that phenomena from data we collected in the survey. Third, we did not collect data on our participants' level of technical expertise or security knowledge. That is why we decided to proceed with a focused interview-based study, in order to improve our understanding of the reasons users choose to use 4-digit PIN-codes, which are usually weaker than passwords.

[2]The U.S. Mobile App Report'14 https://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report

Chapter 6

Study 2 – Interviews

We followed the in-person study with an interview study to gain a better understanding of factors that impact users' decisions on which authentication method to use in conjunction with Touch ID. Our main objective was to answer the following research question (RQ_1): "Why Touch ID users do not employ stronger authentication secrets for smartphone locking?" Answering RQ_1 gave us a better understanding of users' justification for using specific authentication method, i.e., password or a PIN-code.

6.1 Methodology

We designed our study with focus on qualitative data collection. We used semi-structured interviews since they gave us the freedom to deviate in cases when new topics emerge. We used theoretical sampling, rather than random sampling, because we were interested in the richness of the subjects' answers, rather than in demographic diversity of the participants. Each participant was paid $10 for a 20-minute interview. A pilot study with eight participants revealed the necessity for real life scenarios in several questions. We randomized order of interview questions, to mitigate question order bias

Two first interviews were conducted by two researchers together in order to ensure that all important questions were asked and well understood by the subjects. We audio recorded all interviews and two researchers coded each interview independently. After each coding, coders discussed their disagreement until they reached consensus. Overall, we coded 211 responses into 55 unique codes. Researchers disagreed on the coding of 5 responses, achieving inter-rate agreement of 91%[1].

[1]Many of questions had different codes. That is why we did not calculate Cohens Kappa for each question.

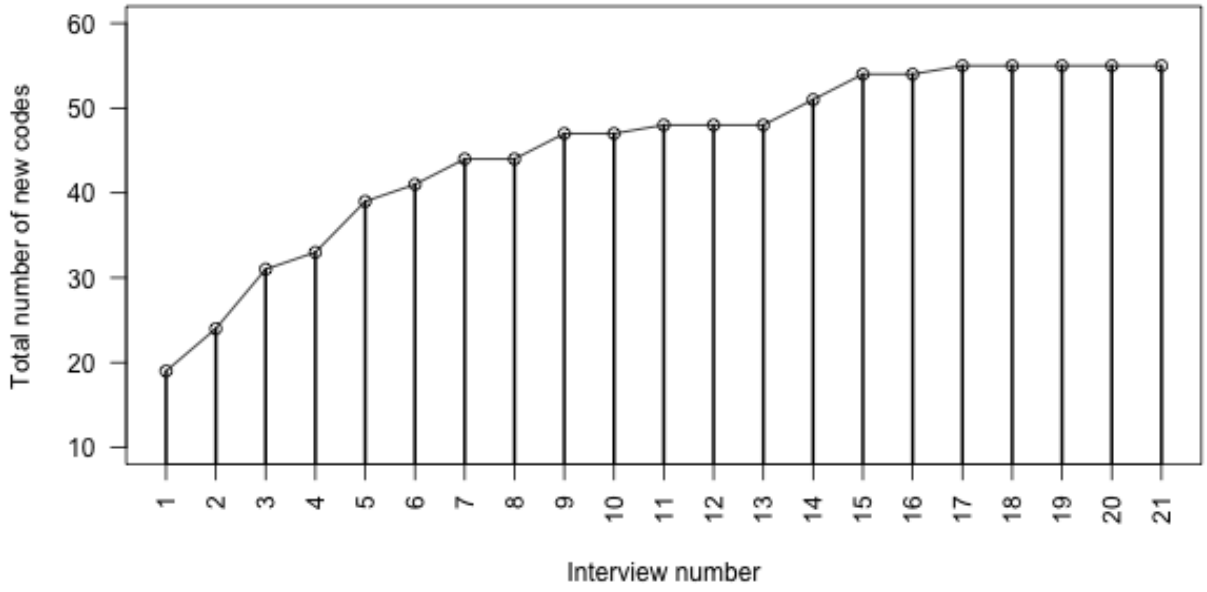

Figure 6.1: Number of unique codes for each additional subject. We reached saturation around 17th subject.

6.1.1 Participant Recruitment

We recruited subjects by directly approaching them in public places such as shopping malls, libraries and coffee shops in Vancouver. Our inclusion criteria were subjects 19 years or older who used Touch ID on their iPhones. After the 17th interview, we did not observe any new codes and decided to stop interviews after 21st. Saturation analysis of new concepts for each additional subject is shown in Figure 6.1.

6.1.2 Procedure

After agreeing to be interviewed and showing us their iPhone 5s, 6 or 6 Plus, each participant read and signed a consent form. The interviewer explained that the purpose of the interview was to investigate how users interact with their iPhones. Interviews followed the interview guide reproduced in Appendix B and consisted of the following parts:

1. **Using Touch ID:** In the first part of the interviews, we asked participants to describe why they use Touch ID, how they thought Touch ID works, whether it's possible to use Touch ID without setting up PIN or password, and why and how Touch ID impacts the iPhone security, in case the

phone gets stolen.

2. **Locking Behavior:** We asked participants whether they locked their iPhones or not and also, what method they used (PIN or password). We verified their answers by asking them to unlock their iPhones. We asked them why they chose to use PIN, not a password or why they chose to use a password, not a PIN. We also asked participants about their password sharing behavior.

3. **iPhone Data:** In this part of the interviews, we asked participants what the most valuable data in their iPhones was, what data they considered to be confidential or sensitive and who they cared protecting their data against.

4. **Data Protection:** We asked participants for how long they wanted their data to be protected in case their iPhones get stolen.

6.2 Results

6.2.1 Participant Demographics

Overall, we recruited **21** subjects. Out of 21 participants, 10 were females, and the average age was 29 (*SD* = 12.4). Only one participant used a password, while all others used a PIN. All participants had owned an iPhone for over one year. Almost all subjects had owned another smartphone before the current one. In addition, 16 participants lost their smartphones before, including six participants that were victims of smartphone theft. Participant demographics is summarized in Table 6.1.

6.2.2 Reasons for Using PIN-codes

The most common reason for using 4-digit PIN-codes was the wrong perception of Touch ID impact on data security when a device is lost or stolen. In particular, nine participants did not understand how Touch ID works, which lead to confusion on the dependency between PIN-codes or passwords and Touch ID. They assumed that Touch ID "somehow" protects data-at-rest when a device is stolen, i.e., would not allow to decrypt data without a correct fingerprint.

> *P1 – "I guess Touch ID will protect my phone. They cannot open my phone without my finger. So it [Touch ID] will definitely help."*

Table 6.1: Demographics of Interviewed Participants

Parameter	Property	Participants
Gender	Male	11
	Female	10
Age	19-24	7
	25-30	4
	31-35	2
	36-40	2
	41-45	3
	46-50	3
Education	High School	5
	Professional School or College Degree	5
	Bachelor	8
	Master or PhD	3
Household income	Less than 20K	2
	20K-50K	3
	50K-80K	7
	80K-120K	6
	Prefer not to answer	3
Occupation sector	Food and service	1
	Security	1
	Construction	2
	Non-profit	1
	Sale and Retail	3
	Parks and recreation	1
	Hospitality	2
	Banking	2
	Biotech	1
	Education	2
	Parking industry	1
	Fundraising	1
	IT industry	2
	Health research	1
	Software	2
	Student	2
	Unemployed	1
Lost smartphone	Yes	16
	No	5
Victim of smartphone theft	Yes	6
	No	15

Another evidence of subjects' confusion was that they wrongly perceived the combination of Touch ID and a PIN-code as providing higher security to data-at-rest in comparison to a PIN-code without Touch ID. Furthermore, some subjects ranked Touch ID even higher than a password in terms of security. For instance:

P3 – "Touch ID is more secure than PIN or password because it's unique for the owner"

Finally, some subjects were certain that PIN-codes provided higher security than passwords. For example:

P11 – "people often choose their dogs' names or middle names or something similar as their passwords"

The second most common factor for using a PIN-code was lack of knowledge of ability to use alphanumeric passwords. Six participants were not aware that they could use an alphanumeric password for unlocking their iPhones. For instance:

P4 – "Really? I even did not know that you could do this [use a password]. That is good to know. I will look at it today",

Several subjects (2) stated that they used PIN-codes because Apple representatives helped them to set up their iPhones and showed them only how to set up a PIN-code:

P5 – "When I bought my iPhone, they asked me to set up a PIN. That is why I am using PIN"

P14 – "They [Apple store customer service employee] only gave me a PIN code option"

Five subjects also admitted that they got habituated to use PIN-codes from their previous devices, so that continued to use PIN-codes on the new iPhone. In addition, subjects also stated that they did not want to remember a new password, so they just decided to use the old PIN-code on the new device:

P1 – "because on my old phone I was lazy to think about password back then so now I just stuck with PIN. There is really no major reason; it is just the way it is. I am just too used to this number and I am just too lazy to memorize a new set of numbers".

Unsurprisingly subjects also stated that they decided to use PIN-code because it is easier to use, faster to type and easier to remember in comparison to passwords. Five participants stated that they did not store any sensitive information on their iPhones, hence, they did not care about the extra level of security a password can provide. They believed that a PIN-code is good enough to protect their phones and did not see a reason to switch to passwords. Seven subjects reused their PIN-code across multiple devices or accounts in order to reduce the amount of information they need to remember.

P15 – "PIN is easier. I do not want to type the whole password in. If I lose my phone, it is not a big deal for me. There is nothing important on it"

Finally, subjected also stated that they share their PIN-codes with someone else, and PIN-codes are easier to share than passwords

P8 – "Simplicity I guess. As I said before, I am not the only person who uses my iPhone. So PIN is easy of access for other users. It is easier to give someone 1234 PIN than 'Charlie-unicorn' is weird, capitals, asterisks, etcetera"

In summary, subjects provided various reasons for sticking with PIN-codes. In particular, some participants did not know that they can use alphanumeric passwords, others stated that they been helped by Apple salespersons at the shop and were only shown how to use PIN-codes. Participants also did not understand how Touch ID works and how it impacts the security of data-at-rest in cases when a phone is stolen or lost. Other subjects were habituated to use PIN-codes from previous devices or wanted to reuse a PIN-code among various devices and accounts. Understandably, subjects stressed the usability benefits of PIN-codes over passwords as one of the reasons to use the former. In particular, they stated that PIN-codesa are faster, easier to use, share and memorize. Finally, some subjects justified the use of PIN-codes by the fact that they had low requirements to security of data on their iPhones.

6.2.3 Security Lock Sharing Behaviour

Eight subjects stated that they share their PIN-codes or passwords. They justified it by several reasons. First, a subject explained that they were pushed to share the unlocking secret:

P2 – "I share with my girlfriend because she forced me to!"

Second, participants trusted others with their data, and, thus shared the PIN-code or password:

P19 – "I share with my boyfriend because I trust him and sometimes he uses my phone too"

P10 – "I share it with my best friend because I trust her and if she has my phone and needs to look at it, she can do that"

Finally, subjects shared their unlocking authentication secrets with others because of concerns with emergency cases, where someone needs to use their phone.

P9 – "I share with my girlfriend because if something happens with me, at least she knows the code and can unlock the device"

To summarize, subjects shared their PIN-codes and passwords because of concerns about emergency cases when someone needs to use their phone, or because they trusted other people with the security of their data, or they were pushed to share their secrets.

6.3 Limitations

There are several limitations in this study. First, we used theoretical sampling and aimed for theoretical saturation rather than for random sampling and representative data, thus, we cannot make any conclusions on prevalence of different reasons among the general population. Second, the results of the study might have been impacted by researcher bias. We strived to minimize this effect by using separate coders and discussing the disagreements. Finally, subjects might have misunderstood some questions. To reduce chances of such misunderstanding we conducted a pilot study with eight subjects, with the main purpose to validate how understandable the questions are.

Chapter 7

Study 3 – Online Survey on MTurk

Although the interview study provided us with rich qualitative data, it did not allow us to measure the prevalence of the reasons subjects used to explain why they did not use stronger authentication secret for the device locking. That is why, in the final study, we decided to use an online survey in order to (a) recruit a larger and more representative sample, (b) improve the statistical power of the first study, and, finally, (c) measure the prevalence of reasons why users did not employ stronger authentication secrets.

7.1 Methodology

The methodology of the online survey study closely resembles the structure of the in-person survey that we conducted in study 1 (see Section 5.1 for more details). We extended the initial questionnaire by adding questions that allowed us to answer RQ_M. All questions that we asked in the online survey are provided in Appendix C. In contrast to the interview study, answering RQ_M through an online survey gave us the opportunity to collect descriptive statistics on reasons why users did not use stronger secrets for the device unlocking.

We recruited subjects on Mechanical Turk (MTurk) [23] between February and March 2015. We limited MTurk workers to the US subjects only with HIT approval rate above 90%. Before running the study we conducted a pilot study with 149 subjects in order to make sure that we collected data properly, and survey questions did not have any significant wording issues. We paid $1.00 to each subject.

In comparison with an in-person study, we were not able to validate whether a subject had an iPhone and used the locking mechanism she claimed to use. To mitigate this concern, as a part of the survey, the subjects were asked to submit two photos (1) a photo of an iPhone reflection in a mirror taken with the

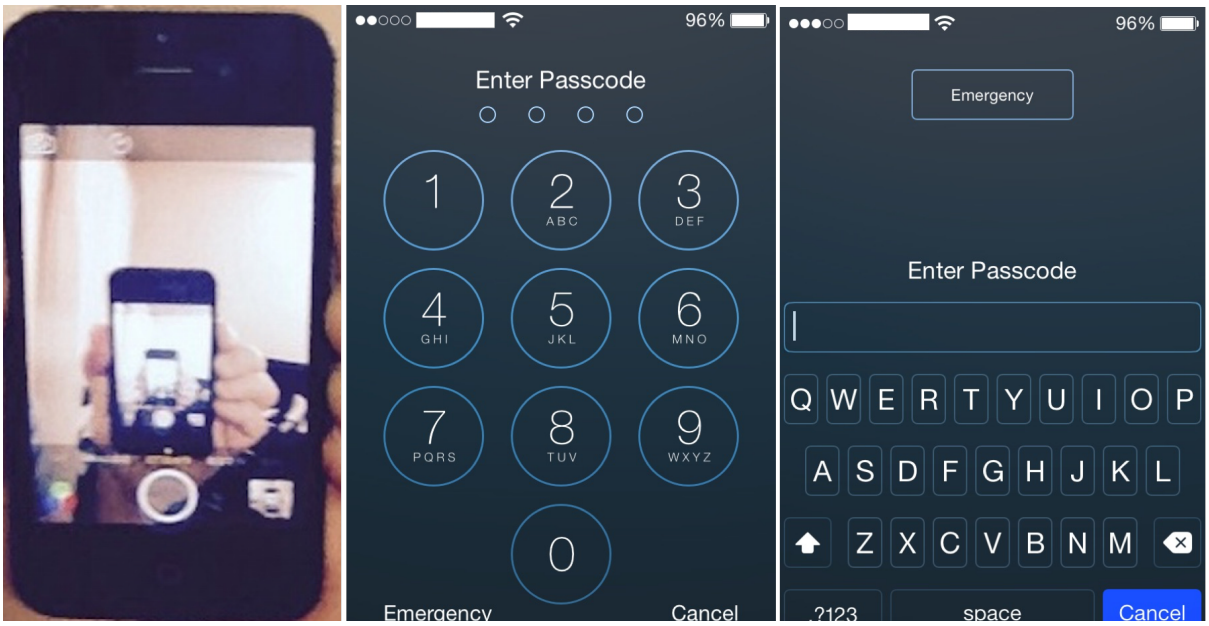

Figure 7.1: Examples of verification photos that subjects sent us. From left to right, (1) a photo of an iPhone taken with front facing camera in a mirror, (2) a screenshot of PIN-code based iPhone unlock interface, and (3) a screenshot of password-based iPhone unlock interface.

front-facing camera, and (2) a screenshot of the unlocking interface. Examples of verification photos are shown at Figure 7.1. We later used these photos to validate the claimed iPhone model (i.e., iPhone 4, 4S, 5S, etc.) and locking mechanism. In addition, we also asked subjects to provide us with the model number, e.g., ME302C/A[1], which has one-to-one correspondence with the marketed model, e.g., iPhone 5S. We excluded all subjects that either did not provide us with photos or who provided photos that did not match their choices in the survey. Finally, we also used attention check question, similarly to the in-person survey, in order to check if a subject read instructions carefully. We excluded all the subjects that failed the attention check question.

7.2 Results

7.2.1 Participant Demographics

Overall 698 participants have started the survey in the non-Touch ID group, and 550 has finished it. On average it took about 16.3 minutes to finish the survey for non-Touch ID subjects (SD = 7.5 minutes). Note, we excluded seven subjects that took more than an hour to finish the survey. 317 subjects failed to submit correct photos of the iPhone and screen shots of the locking interface, which left us with 199

[1]Such model can be found in an iPhone Settings General.About.Model field.

eligible subjects. Finally, 25 out of 225 subjects failed the attention check question, which reduced the non-Touch ID group size to **201** subjects or about 33% of subjects that finished the survey.

For the Touch-ID group, 521 subjects have started the survey, and 445 have finished it. On average it took about 15.7 minutes for subjects to finish the study (s = 6.2 minutes). Similarly, we excluded five subjects that took over an hour to finish the study, and all the subjects that failed to submit proper proof of an iPhone and locking mechanism screenshot, and all the subjects who failed the attention check question. This reduced our subject pool down to **173** subjects.

Participants' demographics, shown in Table 7.1, suggest that we recruited subjects from various occupations, ranging from agriculture to public administrations. The participants' job titles also included various positions, such as managers, students, team leaders and others. Our subjects had diverse education levels, including 75 participants with Ph.D. or Masters degree. More than 50% of subjects were between 25 and 34 years old. Finally, our subjects had various income levels.

7.2.2 Testing H_1

In H_1 we hypothesized that, due to the usability of Touch ID, users would switch from PIN-codes to passwords with a bigger search space, in order to increase the time required for brute-force attack. We first used Chi-square test to check if the proportions of users who used PIN-codes and passwords in both groups were different. The result of the statistical analysis did not reveal any statistically significant difference between proportions of users who use PIN-codes or passwords in both groups ($\chi = 0.01$, p = 0.92).

The 95% percentile confidence interval for the difference between the means of authentication secrets' entropies in two groups is [-1.91, +0.95]. That implies that in case there is a difference and we just failed to show it, due to small sample size, then with 95% confidence we can state that the difference between mean entropies in Touch ID and non-Touch ID would be 1.91 bits at most. Analysis of the difference between means entropy for authentication secrets between the non-Touch ID and Touch ID groups with t-test did not reveal any statistically significant difference (t= -0.66, p = 0.51) between the non-Touch ID (M = 14.13 bits, s = 5.04) and Touch ID (M = 14.61 bits, s = 8.20) groups. The results of the statistical tests suggest that we could not reject H_1^{null}.

Similarly to study 1 we estimate the amount of work an attacker will need to do on average in order to bruteforce the whole password space for Touch ID group in the best case scenario for defenders, i.e.,

users. Considering observed average password entropy in Touch ID group (14.61 bits) and maximum possible difference between the Touch ID and non-Touch ID group (1.91 bit) we can easily obtain the maximum possible average entropy in the Touch ID group, which is 16.52 bits[2]. Considering that for testing each password candidate on iPhones, an attacker must spend at least 80ms, we showed that an attacker can bruteforce the whole search space of 16.52 bits in size in about 2 hours.

7.2.3 Testing H_2

Considering that availability of Touch ID, gives an alternative and usable way of unlocking an iPhone, we hypothesized that the availability of Touch ID might nudge more people to lock their devices (H_2). In order to test this hypothesis, we split all 18 subjects in the non-Touch ID group who did not lock their device on those who had Touch ID (4) and those who did not (14). The results of Chi-square test did not reveal any statistically significant difference (χ = 3.78, p = 0.05) between the proportions of users who lock their iPhones when Touch ID is available and those who lock their iPhones when Touch ID is not available.

7.2.4 Reasons for Using PIN-code

In both groups, we asked users for reasons why they used a PIN-code rather than a password. Participants' answers summary is shown at Figure 7.2. Statistical analysis did not reveal any statistically significant difference in distributions of answers between the two groups (χ-squared = 4.88, p = 0.85). Note, that for such analysis we excluded the last option, i.e., "Touch ID is enough" from both groups since it was only present in the Touch ID group.

The results of the statistical analysis suggested that users in both groups use similar reasons for using a PIN-code. We found that the top most three reasons were either related to usability of PIN-codes, i.e., "It is faster" and "It is easier to remember", or to the gap in knowledge, i.e., "Did not know about the password". Finally, in Touch ID group, more than 25% of subjects stated that Touch ID was good enough for them from the security perspective.

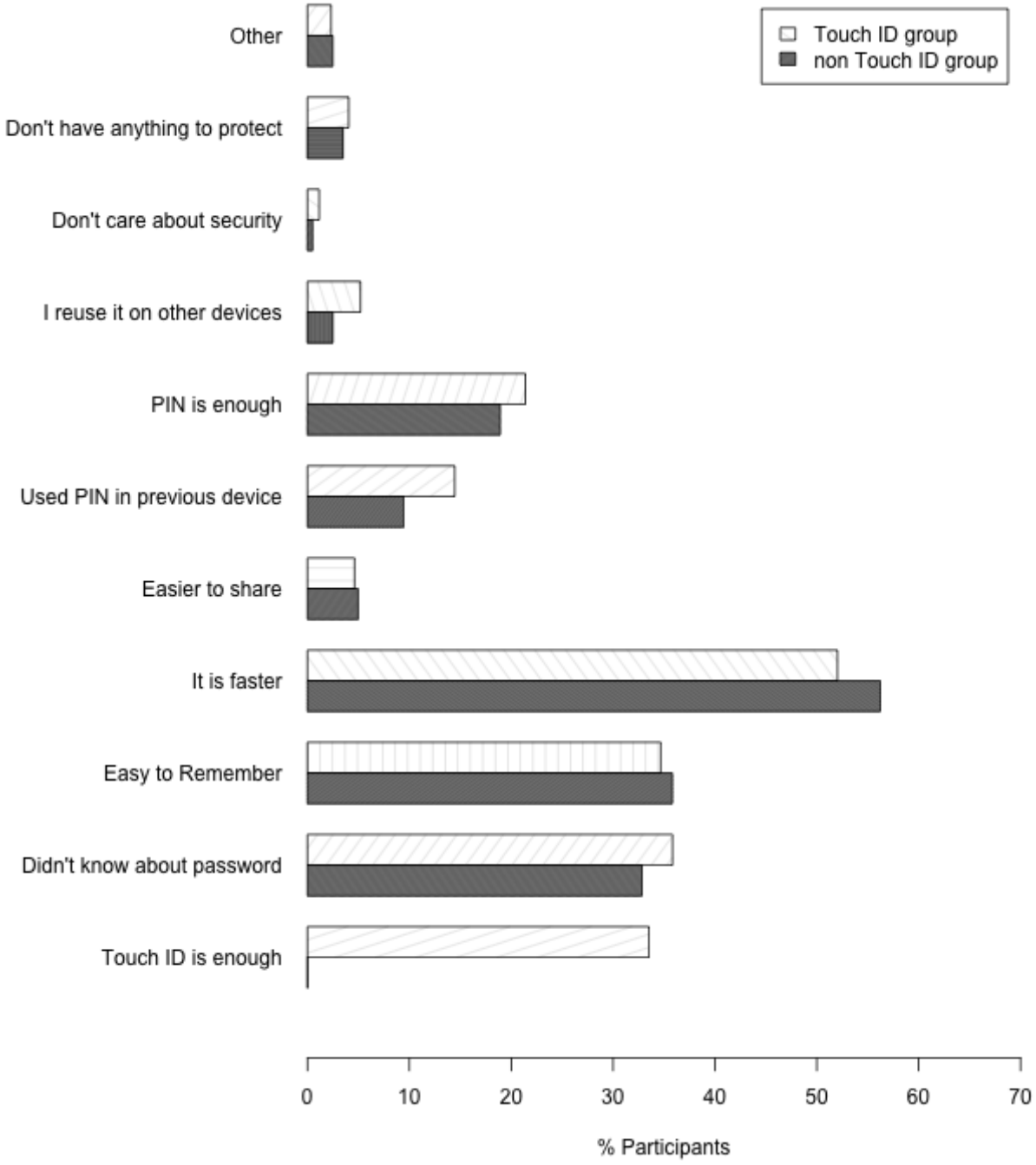

Figure 7.2: Reasons for using PIN-codes instead of passwords for each group.

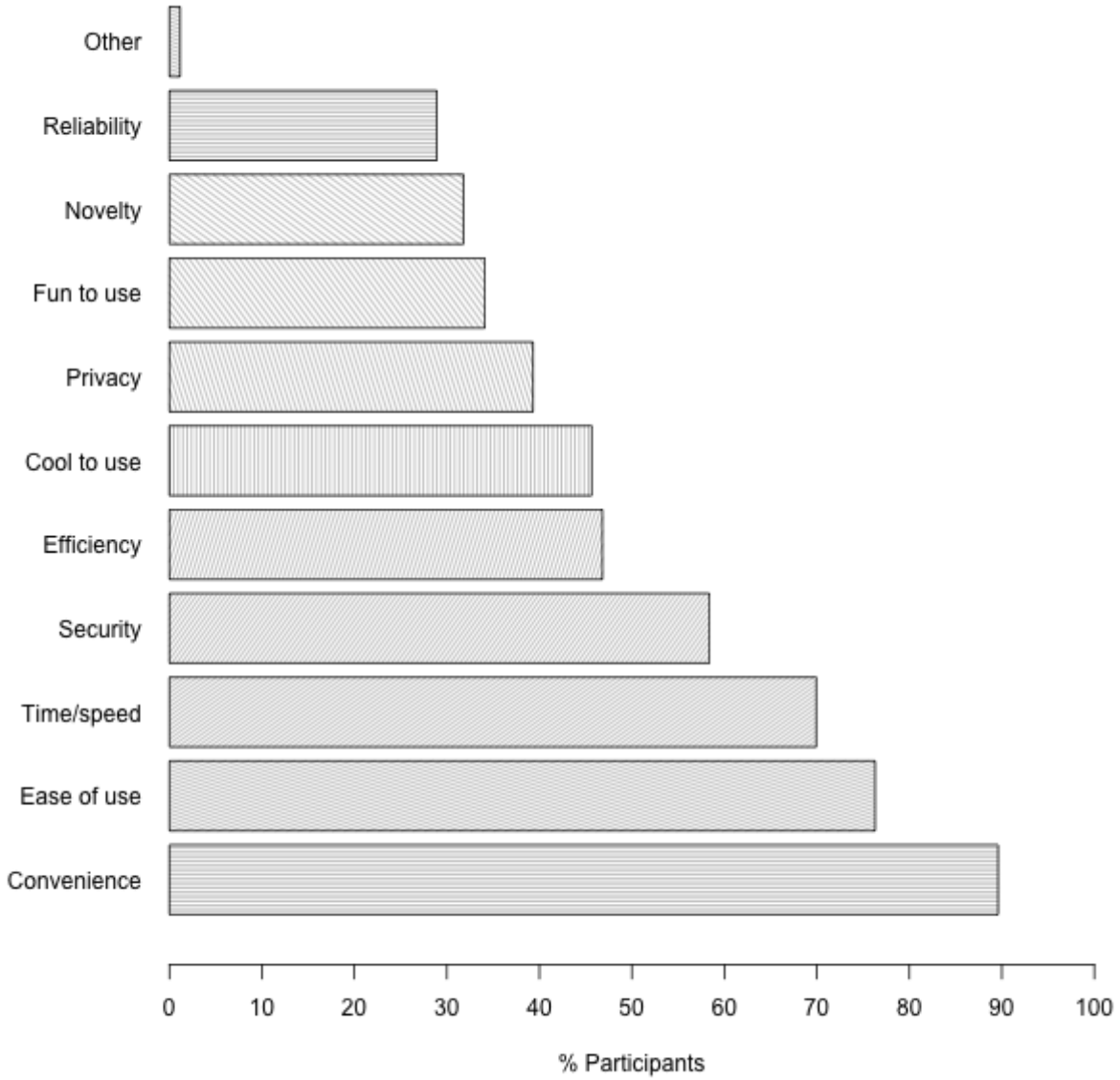

Figure 7.3: Reasons for using Touch ID (n = 173).

7.2.5 Reasons for Using Touch ID

The summary of subjects' answers is provided at Figure 7.3. Participants selected speed, convenience and ease of use as the top most three justifications for using the Touch ID. Furthermore, more than 50% of participants stated that *security* that Touch ID provides was one of the reasons to use it. This suggests that the key factors that drive adoption of the Touch ID originate in its usability. Security benefits that Touch ID provides to users are also important for the majority of the users.

[2]Again, this is an overestimation and real difference of search spaces will be smaller. We chose to overestimate the search space to show the upper bound, i.e., the maximum work on average an attacker needs to do.

7.2.6 Who Users Lock Their iPhones Against

The distribution of participants' answers to the question that asked who they locked their iPhone against is shown at Figure 7.4. Statistical analysis of distributions between the two groups did not reveal any statistically significant difference (χ-squared = 9.98, p = 0.13). Interestingly, almost all subjects in both groups stated that they wanted to protect their device against *strangers* (see Appendix C.4 for distribution between insiders and strangers). At the same time, subjects were also concerned with *insiders*. For instance, around 40% in both groups locked their device against co-workers, around 30% locked their phone against friends and family members, and around 20% locked their phones against classmates and roommates. The results are in line with previously reported findings [32].

We also asked subjects for how long they would want their data to be protected in case someone steals their iPhone and tries to bruteforce their passwords to decrypt data. See Appendix C.1 question 27 for all options that we gave to participants. Considering that (in Section 7.2.2) we showed that subjects entropy of authentication secrets used for iPhone locks is around 15 bits, this corresponds to 44 minutes required to search through the whole password space. Surprisingly, we found that such protection met expectations of only 12% of our participants, who did not expect data protection to last more than one hour. The remaining 88%, however, expected that data to be protected for more than an hour. In particular, 48% of subjects expected the data to be protected for at least 40 years or *indefinitely*. It shows that there is a discrepancy between the strength of participants' secrets and their expectations about the level of security that these secrets can provide.

7.2.7 Authentication Secret Sharing Behaviour

We asked our subjects who they shared their iPhone locking authentication secrets with. The summary of the results is presented at Figure 7.5. We did not observe any statistically significant difference in sharing habits between non-Touch ID and Touch ID groups (χ-squared = 3.00, p = 0.70), thus, in our report we combined both groups together.

Overall, we found that only 40% of subjects did not share their password with anyone. Others shared to some extent with different categories of related people. In particular, more than 25% of subjects shared their password or PIN-code with a partner or other family members. About 10% of participants shared their password or PIN-code with friends while almost no one shared their iPhone lock authentication secret with co-workers. In addition, 61% of all participants stated that they knew

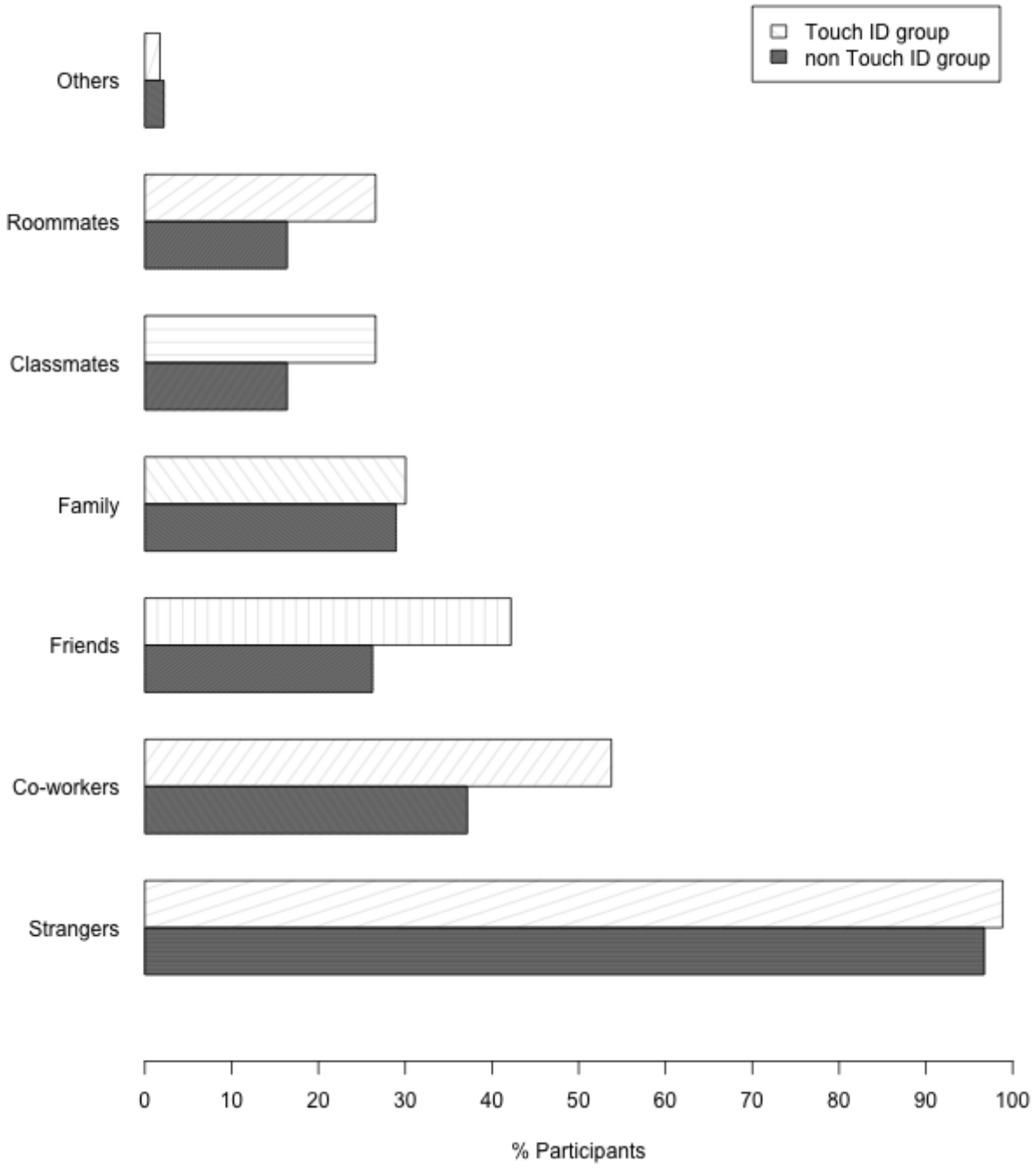

Figure 7.4: Distribution of attackers who users lock their iPhones against. For Touch ID group (n = 173), and for non-Touch ID group (n = 201).

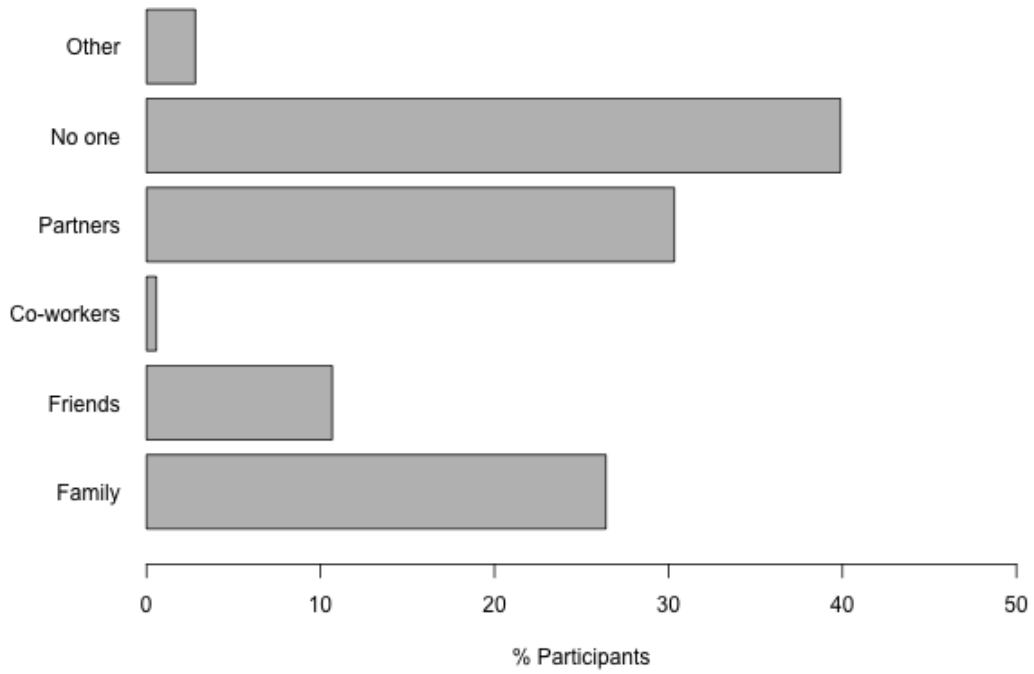

Figure 7.5: Distribution of authentication secret for iPhone lock sharing among different groups of people (n = 374).

someone's unlocking authentication secret.

7.3 Limitations

The main limitation of this study is having Mechanical Turk subjects take a picture of their phone and send us a screenshot. This requirement substantially biased our survey toward technical users. We tried to mitigate this limitation by providing detailed instructions on how to make a screenshot.

Table 7.1: Demographics of MTurk Participants and Distribution across Two Groups and Locking Authentication Method Used.

Parameter	Property	Participants	%
Gender	Male	154	41
	Female	220	59
Age	18 to 24	110	29
	25 to 34	195	52
	35 to 44	49	13
	45 to 54	17	5
	55 to 64	2	1
	65 or older	1	0
Education	Did not attend school	0	0
	Graduated from high school	19	5
	1 year of college	26	7
	2 years of college	68	18
	3 years of college	35	9
	Graduated from college	136	36
	Some graduate school	15	4
	Completed graduate school	75	20
Income	$0-$24,999	67	18
	$25,000-$49,999	97	26
	$50,000-$74,999	70	19
	$75,000-$99,999	65	17
	$100,000-$124,999	34	9
	$125,000-$149,999	17	5
	$150,000-$174,999	7	2
	$175,000-$199,999	3	1
	$200,000+	14	4
Industry	Agriculture	1	0
	Forestry, fishing, mining, quarrying, oil, and gas	1	0
	Utilities	2	1
	Construction	8	2
	Manufacturing	7	2
	Trade	8	2
	Transportation	6	2
	Finance and real estate	23	6
	Professional services	67	17
	Business and building	18	5
	Educational services	51	13
	Health care and social	52	13
	Inform./culture/recreation	16	4
	Accomm./food services	19	5
	Public administration	9	2
	Other	106	27
Role	Individual Contributor	122	33
	Manager	46	12
	Senior Manager	7	2
	Regional Manager	0	0
	Vice President	0	0
	Management C Level	9	2
	Partner	5	1
	Owner	18	5
	Volunteer	4	1
	Intern	12	3
	Student	57	15
	Other	59	16
Victim of smartphone theft	Yes	43	11
	No	331	89
Experienced unauthorized access	Yes	38	10
	No	336	90
Group	non-Touch ID	201	
	Touch ID	173	
Locked with PIN/Passw/None	non-Touch ID	177/6/18	
	Touch ID	166/7/0	

Chapter 8

Discussion

In this section we summarize our main findings. We first discuss the main result of the work, that is, the lack of impact of Touch ID on the entropy of unlocking authentication secrets. We then proceed with the discussion of reasons why users do not take advantage of the Touch ID and continue using 4-digit PIN-codes. Finally, we conclude with discussion of possible approaches to address the low adoption of stronger passwords.

No Effect. Surprisingly, we did not find any statistically significant difference in entropies of unlocking authentication secrets between users who use Touch ID and those who do not. In addition, the results of our study suggest that availability of Touch ID does not increase the ratio of users who lock their devices. In the best case scenario for defender, i.e., under assumption that use of Touch ID does increases the entropy by 1.91 bits (cf. see Section refsec:mturk:testingh1), our estimates show, that on average an attacker would need to spend around 2 hours to bruteforce the whole password search space. However, considering the observed average entropies for both groups, i.e., around 15 bits, the attacker would only need 44 minutes to search through the whole password space. Such a short protection time meets desires of only 12% of smartphone users.

Reasons to use 4-digit PIN-codes. The second and the third studies allowed us to get a better understanding of reasons for sticking with 4-digit PINs. In particular, the results suggest, that the main factors are lack of awareness that passcodes are available and usability considerations. For instance, we found that more than 30% of subjects did not know that they can use alphanumeric passwords instead of 4-digit PIN. Currently, iOS 8.3, one can only use 4-digit PIN code during device initialization, even if Touch ID sensor is setup. If user wants to switch 4-digit PIN to a passcode, she must go through settings

after an iPhone is setup. Even more, the interview study revealed that some users have helped by Apple store salespersons with setting up smartphone lock, hence, users have never explored the passcode setup options.

The remaining subjects, approximately 70%, used 4-digit PINs due to higher usability of PINs in comparison with alphanumeric passwords. For example, more than 50% of subjects stated that they used PINs as they are faster to type than alphanumeric passwords. Furthermore, approximately 45% of subjects used PINs since they are easier to remember. This suggests that more research is needed to find a usable password policy that allows users to create more memorable passwords, which they can type with acceptable speed and accuracy while increasing passwords entropy. For instance, a similar research to the one by Komanduri et al. [27] can be conducted with a focus on smartphone unlocking.

Finally, we found that over 55% of users share their unlocking secrets with someone else, such as family members, friends, partners, etc. Subjects stressed that they shared unlocking secret with someone to enable them to access their device in case of an emergency. In addition, subjects mentioned that they are concerned that locking a smartphone makes it almost impossible to call back to the owner when the device is lost and found by a person who is willing to return it.

Recommendations. Considering that the user can only use 4-digit PIN code during the setup on a new iPhone, including the latest models of iPhone, Apple can allow or request users to create stronger passcodes when they set Touch ID. We plan to investigate a better user interface during iPhone lock setup phase, which increases the visibility of available options for unlocking authentication secrets in future work.

The results of the interview study suggest that the origin of such misbalance lays in the lack of understanding of how Touch ID works and how it impacts the security of the data-at-rest. In particular, users did not understand that Touch ID is just a shortcut in the unlocking procedure and has no impact on the physical security of their iPhones. One possible way to address this lack of understanding is by providing a feedback to users during the authentication secret setup phase in terms of time it takes to bruteforce such a secret, in cases the phone gets stolen. We leave the investigation of improving the interface for choosing better authentication secrets for future work.

The second suggestion is to apply gamification methods, e.g., the user can get something (app, music, game, iCloud storage) for free as a reward for creating a better passcode. The third option is to show statistics to Touch ID users on how often they actually used their PINs and suggest them to

switch to the longer alphanumeric passcode. Also, in order to mitigate the problem of hard to remember infrequently used passwords[1], we can ask users to type the password once every 2-3 days, in locations where it is easy to do so, e.g., at home or in office, but not in a bus, or a car, or while walking outside.

Finally. users should be able to make some features of their phones available without requiring a password. For instance, one should be able access Health ID or to call designated numbers (e.g., home number of the owner or his/her partner's number) without unlocking the device.

[1] Items that are less frequently retrieved from human memory is harder to remember [5]

Chapter 9

Conclusion

In this work we presented our investigation of Touch ID's impact on iPhone unlocking authentication secrets selection by users. To characterize the impact we conducted three user studies (a) an in-person survey with 90 subjects, (b) an interview-based study with 21 participants, and (c) an online survey with 374 subjects. The results of user studies did not reveal any impact of Touch ID on unlocking authentication secrets selection. That is, users who use Touch ID and those users who don't use Touch ID tend to select authentication secrets of similar entropy. In particular, we observed that the average entropy was 15 bits, which corresponds to 44 minutes of work for an attacker to bruteforce the whole search space in order to find the correct password. Surprisingly, such short protection time satisfied only 12% of users. The unsatisfied portion of participants misunderstood the impact of Touch ID on data-at-rest protection. In addition, we found that more than 30% of subjects did not know that they can use alphanumeric passwords to lock their iPhones.

Based on the results of our investigation, we suggest research directions to improve the awareness of Touch ID users of the impact of stronger passwords on data-at-rest security and increase the visibility of the alphanumeric password option. We plan to investigate the proposed research directions in future research. There are several promising directions for future work. Considering that only 12% of users estimated the strength of their passcodes correctly, the feedback on passcode strength can help them to create a password that suits their preferences. One possible option for such feedback is to inform users how long it will take to brute force their password. Another approach is to provide users with an option to create a stronger password when they set up Touch ID i.e. suggest them to set 8-digits PIN or alphanumeric password instead of 4-digits PIN. Also, Apple customer service representatives may

educate their customers by informing them about possible risks of using weak authentication secrets. Finally. one can apply gamification methods, e.g., the user can get something (app, music, game, iCloud storage) for free as a reward for creating a better passcode.

Overall this work makes the following contributions:

- We show that the assumption that such authentication methods as Touch ID would nudge users to use higher-entropy passwords is questionable. Even the opposite, we did not find any difference in passwords strengths of both groups, and, the 95% confidence interval for the mean entropy difference shows that even if there were a statistically significant difference it would not be greater than 1.91 bits. For iOS platform this corresponds to two extra hours of work for an adversary during bruteforce attack [4].

- We investigate why Touch ID has not resulted in stronger authentication secrets. In particular, we showed that more than 30% of users did not know that they can use alphanumeric passwords. Others decided to use PIN-codes due to obvious usability benefits over alphanumeric passwords, e.g., easy to remember or faster to type.

- Finally, we found that almost all users did not know the actual level of security a 4-digit PIN-code provides. In particular, we showed that only 12% of subjects correctly guessed level of security a PIN-code can provide while others significantly overestimated it. For instance, more than 45% stated that it was desirable for them that 4-digit PIN code protects data for more than 40 years, which is far from reality.

Bibliography

[1] D. Abalenkovs, P. Bondarenko, V. K. Pathapati, A. Nordbø, D. Piatkivskyi, J. E. Rekdal, and P. B. Ruthven. Mobile forensics: Comparison of extraction and analyzing methods of ios and android. *Master Thesis, Gjvik University College*, 2012. → pages 4

[2] A. A. Al-Daraiseh, D. Al Omari, H. Al Hamid, N. Hamad, and R. Althemali. Effectiveness of iphone's touch id: Ksa case study. *(IJACSA) International Journal of Advanced Computer Science and Applications*, 6(1):154–161, 2015. → pages 8

[3] Amitay. Most common iphone passcodes. http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes, June 2011. URL http://danielamitay.com/blog/2011/6/13/most-common-iphone-passcodes. last accessed March 8, 2015. → pages 9

[4] I. Apple. iOS Security, 8.1 and up. http://www.apple.com/business/docs/iOS_Security_Guide.pdf, 2014. Accessed April 26, 2015. → pages 2, 9, 41

[5] A. D. Baddeley. *Human memory: Theory and practice*. Psychology Press, 1997. → pages 39

[6] P. Bao, J. Pierce, S. Whittaker, and S. Zhai. Smart phone use by non-mobile business users. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, pages 445–454. ACM, 2011. → pages 9

[7] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. *USEC '15*, February 2015. → pages 7, 9, 10

[8] J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 538–552. IEEE, 2012. → pages 2, 8

[9] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 553–567. IEEE, 2012. → pages 7, 8

[10] F. Breitinger and C. Nickel. User survey on phone security and usage. In *BIOSIG*, pages 139–144, 2010. → pages 9

[11] H. Crawford and K. Renaud. Understanding user perceptions of transparent authentication on a mobile device. *Journal of Trust Management*, 1(1):7, 2014. → pages 9

[12] A. De Luca, A. Hang, E. von Zezschwitz, and H. Hussmann. I feel like i'm taking selfies all day! towards understanding biometric authentication on smartphones. In *CHI'15*, Seoul, Korea, 2015. → pages 9

[13] S. Egelman, S. Jain, R. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? understanding user motivations for smartphone locking behaviors. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer & Communications Security, CCS*, volume 14, 2014. → pages 8

[14] Ericsson. Ericsson mobility report. http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf, June 2014. URL http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf. last accessed June 25, 2013. → pages 1

[15] R. D. Findling and R. Mayrhofer. Towards face unlock: on the difficulty of reliably detecting faces on mobile phones. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*, pages 275–280. ACM, 2012. → pages 7

[16] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666. ACM, 2007. → pages 7, 8

[17] D. Florencio and C. Herley. A large-scale study of web password habits. In *WWW '07: Proceedings of the 16th International Conference on World Wide Web*, pages 657–666, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-654-7. doi:http://doi.acm.org/10.1145/1242572.1242661. → pages 8

[18] D. Florêncio and C. Herley. Where do security policies come from? In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 10:1–10:14, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0264-7. doi:http://doi.acm.org/10.1145/1837110.1837124. URL http://doi.acm.org/10.1145/1837110.1837124. → pages 2

[19] M. Gao, X. Hu, B. Cao, and D. Li. Fingerprint sensors in mobile devices. In *Industrial Electronics and Applications (ICIEA), 2014 IEEE 9th Conference on*, pages 1437–1440. IEEE, 2014. → pages 9

[20] Google. Ice cream sandwich. https://developer.android.com/about/versions/android-4.0-highlights.html, March 2011. URL https://developer.android.com/about/versions/android-4.0-highlights.html. last accessed March 8, 2015. → pages 7

[21] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith. It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 213–230, Menlo Park, CA, July 2014. USENIX Association. ISBN 978-1-931971-13-3. URL https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach. → pages 8

[22] C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE*, 10(1):28–36, 2012. → pages 8

[23] https://www.mturk.com. Amazon Mechanical Turk. https://www.mturk.com/, 2005. → pages 27

[24] M. Jakobsson and R. Akavipat. Rethinking passwords to adapt to constrained keyboards. *Proc. IEEE MoST*, 2012. → pages 9

[25] M. Jakobsson, E. Shi, P. Golle, and R. Chow. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*, HotSec'09, Berkeley, CA,

USA, 2009. USENIX Association. URL http://dl.acm.org/citation.cfm?id=1855628.1855637. → pages 9

[26] S. Karthikeyan, S. Feng, A. Rao, and N. Sadeh. Smartphone fingerprint authentication versus pins: A usability study (cmu-cylab-14-012). *CMU-CyLab*, pages 14–012, July 31 2014. → pages 8

[27] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of passwords and people: measuring the effect of password-composition policies. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, CHI '11, pages 2595–2604, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0228-9. doi:http://doi.acm.org/10.1145/1978942.1979321. URL http://doi.acm.org/10.1145/1978942.1979321. → pages 8, 38

[28] S. Lee and S. Zhai. The performance of touch screen soft buttons. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 309–318. ACM, 2009. → pages 9

[29] I. Lookout. Lost and found: The challenges of finding your lost or stolen phone. http://blog.mylookout.com/2011/07/lost-and-found-the-challenges-of-finding-your-lost-or-stolen-phone/, 2011. last accessed August 18, 2011. → pages 1

[30] V. Matyáš and Z. Říha. Biometric authentication—security and usability. In *Advanced Communications and Multimedia Security*, pages 227–239. Springer, 2002. → pages 8

[31] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Understanding users' requirements for data protection in smartphones. In *Workshop on Secure Data Management on Smartphones and Mobiles*, 2012. → pages 1

[32] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Know your enemy: the risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, MobileHCI '13, pages 271–280, New York, NY, USA, 2013. ACM. ISBN 978-1-4503-2273-7. doi:10.1145/2493190.2493223. URL http://doi.acm.org/10.1145/2493190.2493223. → pages 1, 9, 33

[33] A. D. Portal. Encryption — android developers, May 2015. URL https://source.android.com/devices/tech/security/encryption/index.html. → pages 1

[34] M. A. Sasse. Red-eye blink, bendy shuffle, and the yuck factor: A user experience of biometric airport systems. *Security & Privacy, IEEE*, 5(3):78–81, 2007. → pages 9

[35] 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*, page 13. ACM, 2012. → pages 1

[36] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 2:1–2:20, New York, NY, USA, 2010. ACM. ISBN 978-1-4503-0264-7. doi:http://doi.acm.org/10.1145/1837110.1837113. URL http://doi.acm.org/10.1145/1837110.1837113. → pages 2

[37] A. Skillen and M. Mannan. On implementing deniable storage encryption for mobile devices. In *Proceedings of the 20th Annual Network and Distributed System Security Symposium*, NDSS Symposium'13, San Diego, CA, USA, 2013. → pages 9

[38] M. F. Theofanos, R. J. Micheals, and B. C. Stanton. Biometrics systems include users. *Systems Journal, IEEE*, 3(4):461–468, 2009. → pages 9

[39] S. J. Tipton, D. J. White II, C. Sershon, and Y. B. Choi. iOS security and privacy: Authentication methods, permissions, and potential pitfalls with touch id. *International Journal of Computer and Information Technology*, 03(03), May 2014. ISSN 2279 ? 0764. → pages 8

[40] T. Trimpe. Fingerprint basics. http://sciencespot.net/Media/FrnsScience/fingerprintbasicscard.pdf, June 2009. URL http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf. last accessed March 5, 2015. → pages 9

[41] C. S. Weir, G. Douglas, M. Carruthers, and M. Jack. User perceptions of security, convenience and usability for ebanking authentication tokens. *Computers & Security*, 28(1):47–62, 2009. → pages 8

[42] H. Wimberly and L. M. Liebrock. Using fingerprint authentication to reduce system security: An empirical study. In *Security and Privacy (SP), 2011 IEEE Symposium on*, pages 32–46. IEEE, 2011. → pages 9

[43] J. Zdziarski. Identifying back doors, attack points, and surveillance mechanisms in iOS devices. *Digital Investigation*, 11(1):3–19, 2014. → pages 5

Appendix A

In-person Survey Guide and Questions

A.1 Agenda

1. Introduce yourself, your affiliation and give an overview of the study: "The purpose of this study is to investigate how users interact with iPhones. We aim to investigate users' motivation for choosing passwords and using fingerprint unlock. You will be asked to answer the questionnaire on iPad. It will take approximately 15 minutes. Please feel free to provide any comments and feedback on the study".

2. Verify that the participant has iPhone.

3. After the participant read and agreed with the consent form, asked her to read and sign a payment receipt and hand her a honorarium payment of $10.

4. After a participant completed the survey, conduct short exit interview asking PIN users "Why do you use 4-digit PIN, not alphanumeric password?" and password users "Why do you use alphanumeric password, not PIN?".

5. Verify the length of the password and auto-lock time.

6. Debrief.

A.2 Questions for Both Conditions

1. What is your age? [1]

[1] Questions that does not have suggested possible answers are open-ended questions

2. What is your gender?

    (a) Female

    (b) Male

    (c) Prefer not to answer

3. What is your highest level of completed education?

    (a) High school

    (b) College degree

    (c) Bachelor

    (d) Master or PhD

    (e) Other, please specify

4. What industry have you worked for the past 6 months?

    (a) Agriculture

    (b) Forestry, fishing, mining, quarrying, oil and gas

    (c) Utilities

    (d) Construction

    (e) Manufacturing

    (f) Trade

    (g) Transportation and warehousing

    (h) Finance, insurance, real estate and leasing

    (i) Professional, scientific and technical services

    (j) Business, building and other support services

    (k) Educational services

    (l) Healthcare and social assistance

    (m) Information, culture and recreation

    (n) Accommodation and food services

(o) Public administration

(p) Other

5. What is the annual income of your household?

(a) Less than $20,000

(b) Above $20,000, below $50,000

(c) Above $50,000, below $80,000

(d) Above $80,000, below $120,000

(e) Above $120,000

(f) Prefer not to answer

6. Have you ever lost your smartphone?

(a) Yes

(b) No

7. Have you been a victim of smartphone theft?

(a) Yes

(b) No

8. In your opinion, what unlocking method is more secure?

(a) Multi-character password

(b) 4-digit PIN

(c) Fingerprint unlock (Touch ID)

(d) Eye recognition

(e) Face recognition

(f) None of them

(g) I have no idea

9. You are willing to use face recognition authentication

(a) Strongly disagree

(b) Disagree

(c) Agree

(d) Strongly agree

(e) I don't know

10. Please explain your answer to the previous question.

11. What is the model of your iPhone?

(a) 5s, 6 or 6 Plus

(b) 5c or earlier model

(c) I am not sure

(d) Other, please specify

12. Do you use the same password for your iPhone as you used in your previous smartphone?

(a) Yes

(b) No

(c) N/A

(d) Prefer not to answer

13. How often do you change your PIN or password?

(a) Weekly

(b) Monthly

(c) Every six months

(d) Once a year

(e) Never

(f) I don't know

14. Enter a structure of your iPhone password. That is, substitute each digit (single digit number) with D, lowercase with L, uppercase with U, special character with S. For example structure for password A1b%B is UDLSU.

15. For how long have you been using an iPhone during last 5 years?

    (a) Less than a year

    (b) 1 to 2 years

    (c) 2 to 3 years

    (d) Over 3 years

16. Does your iPhone store any sensitive or confidential information?

    (a) Yes

    (b) No

    (c) I have no idea

17. What is the worst thing that could happen to your iPhone?

    (a) My iPhone gets broken or stolen, but I recover my data, so nobody will get access to my data

    (b) Someone get access to the data on my iPhone

    (c) Someone misuses my apps and account

    (d) Other, please specify

18. On average, how frequently do you unlock your iPhone?

    (a) Once a day

    (b) Few times a day

    (c) Once per hour

    (d) Few times per hour

    (e) I have no idea

19. What is your iPhone auto lock time (how long the screen stays on if the device is not being used)?

    (a) Never

    (b) 1 min

    (c) 2 min

    (d) 3 min

    (e) 4 min

    (f) 5 min

    (g) I don't know

20. A simple password is a 4-digit number. Do you know how to turn simple password off in the settings?

    (a) Yes

    (b) No

21. Have you ever shared your iPhone password with anybody else?

    (a) Yes

    (b) No

    (c) Maybe

22. Do you know anybody else smartphone security lock?

    (a) Yes

    (b) No

    (c) Maybe

23. What motivates you to lock your iPhone? Select all that apply.

    (a) My friends lock their phones

    (b) Locking prevents strangers from using my iPhone

    (c) It's easy to lock

(d) Locking controls when my family or friends can use my iPhone

(e) Other, please specify

24. (alternative) Why do you choose not to lock your iPhone? Select all that apply.

(a) Information on my iPhone is useless

(b) In case of loss, I can easily be contacted

(c) It is too much effort

(d) In case of emergency, others can use my iPhone

(e) None of the above

(f) Other, please specify

25. What kind of smartphone did you own before iPhone?

(a) Android

(b) Windows Phone

(c) iPhone

(d) BlackBerry

(e) None of them

(f) Other, please specify

26. What security lock have you used for your old smartphone?

(a) Multi-character password

(b) 4-digit PIN

(c) Fingerprint unlock (Touch ID)

(d) Pattern Lock

(e) Face recognition

(f) I didn't use a lock

(g) I didn't have a smartphone

(h) Other, please specify

27. Enter a structure of your previous smartphone password. That is, substitute each digit (single digit number) with D, lowercase with L, uppercase with U, special character with S. For example structure for password A1b%B is UDLSU.

A.3 Questions for Touch ID Group

1. How hard was it to set up Touch ID?

   (a) Very difficult

   (b) Difficult

   (c) Decent

   (d) Easy

   (e) Very easy

2. Is it easy to use Touch ID?

   (a) Very difficult

   (b) Difficult

   (c) Decent

   (d) Easy

   (e) Very easy

3. Why do you use Touch ID?

   (a) Convenience

   (b) Novelty

   (c) Security

   (d) Time

   (e) Ease of use

   (f) Reliability

(g) Privacy

(h) Cool to use

(i) Fun to use

(j) Other, please specify

4. Have you ever had issues with using Touch ID?

   (a) Yes

   (b) No

   (c) I don't know

5. In your own experience, what situations are best suited for using Touch ID? Select all that apply. Answers are in random order for each survey.

   (a) Driving

   (b) Walking

   (c) Sitting

   (d) When using only one hand

   (e) When it's dark

   (f) When the owner is intoxicated

   (g) Other, please specify

6. What situations are NOT suitable for using Touch ID? Select all that apply. Answers are in random order for each survey.

   (a) Driving

   (b) Walking

   (c) Sitting

   (d) When using only one hand

   (e) When it's dark

   (f) When the owner is intoxicated

(g) Other, please specify

7. Does use of Touch ID affect your privacy?

   (a) Yes

   (b) No

   (c) I don't know

8. What is your major security or privacy concern about Touch ID?

9. What kind of limitations do you experience because of using Touch ID?

10. What kind of situations Touch ID should be temporarily disabled according to your own experience?

11. You feel that it is easy to circumvent Touch ID

    (a) Very difficult

    (b) Difficult

    (c) Decent

    (d) Easy

    (e) Very easy

12. Would you recommend using Touch ID to your friend?

    (a) Yes

    (b) Maybe

    (c) No

13. Please explain your answer to the previous question.

14. Overall, how satisfied are you with using Touch ID?

    (a) I hate it

    (b) I dislike it

(c) I'm OK with it

(d) I like it

(e) I love it!

A.4 Questions for Non-Touch ID

1. Have you ever used a biometric authentication system?

   (a) Yes

   (b) No

   (c) I don't know what is biometric authentication

   (d) I'm not sure I used biometric authentication

2. In general, what are your major security or privacy concerns about biometric authentication?

3. You are willing to use face recognition authentication

   (a) Strongly disagree

   (b) Disagree

   (c) Agree

   (d) Strongly agree

   (e) I don't know

4. Please explain your answer to the previous question.

5. You are willing to use fingerprint authentication

   (a) Strongly disagree

   (b) Disagree

   (c) Agree

   (d) Strongly agree

   (e) I don't know

6. Please explain your answer to the previous question.

7. Would you start using longer alphanumeric password alongside with using of fingerprint scanner?

   (a) Yes

   (b) Maybe

   (c) No

   (d) I don't know

A.5 Final Instructions for Both Groups

Please follow the instructions in the order given below:

1. Lock your iPhone.

2. Turn your iPhone on.

3. Swipe to unlock.

4. Enter your password (DO NOT PRESS 'DONE').

5. Show your masked password to the researcher (we just want to count number of characters).

6. Navigate to the 'Settings', 'General' and show the auto-lock interval to the researcher.

Thank you for your participation!

A.6 In-person Survey Supplemental Graph

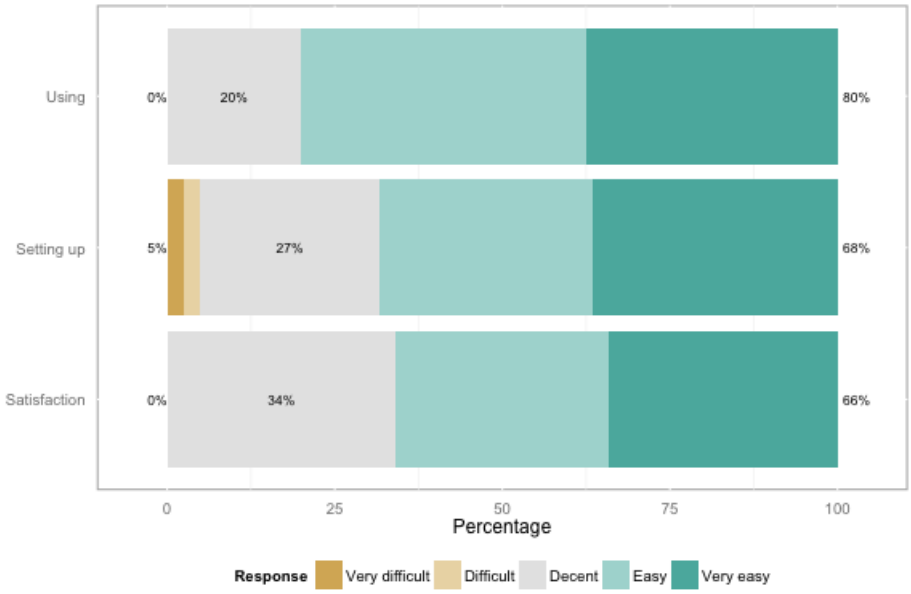

Figure A.1: Study 1 (in-person surveys) Touch ID participants' answers for questions "How hard was it to set up Touch ID?", "Is it easy to use Touch ID?" and "Overall, how satisfied are you with using Touch ID?" (n = 41).

Appendix B

Interview Guide and Questions

B.1 Agenda

1. Introduce yourself, your affiliation and give an overview of the study: "The purpose of the study is to investigate how users interact with iPhones. We aim to investigate users' motivation for choosing passwords and using fingerprint scanner. t will take approximately 15 minutes. Please feel free to provide any comments and feedback on the study".

2. Verify that a participant has iPhone 5S, 6 or 6 Plus with her.

3. Ask her to unlock her iPhone without using Touch ID.

4. Ask the participant to read and sign the consent form.

5. Turn on audio recording.

6. When interview is over, turn off audio recording.

7. Ask the participant to fill out a demographics form.

8. Ask the participant to sign a receipt form.

B.2 Questions

1. Lets talk about your use of Touch ID:

   (a) Why do you use Touch ID?

(b) How do you think Touch ID works?

(c) Do you know if you can use Touch ID without a password/PIN?

(d) How do you think Touch ID impacts the security of your device in case it gets stolen? [Ask to elaborate. Clarify that after Touch ID recognizes the fingerprint, it restores PIN or password and unlocks device using PIN or password]

2. Password vs. PIN code section:

   (a) Can I ask you if the password/PIN code that unlocks your iPhone is being used anywhere else? [Other Devices, Web-Sites, Credit Cards, other online services]

   (b) Do you share your password/PIN with anyone else, like family members, friends of colleagues? [YES] Why do you do that?

   (c) Do you know how to switch iPhone lock from PIN to password? [Please, show me how to do that]

   (d) Did you change your password/PIN after you started using Touch ID enabled iPhone? Why [for both cases]?

   (e) Why do you use PIN, not password? (OR Why do you use password, not PIN?)

3. Let's talk about how you use your iPhone:

   (a) What is the most valuable in your phone for you? How about your data? [Ask to elaborate on data types]

   (b) Is there any data that you consider to be confidential, private or sensitive? [Ask to provide some examples]

   (c) Who do you care protecting your private data against? [Strangers, Co-workers, Friends, Family]

4. Lets consider the following scenario: "Someone stole your iPhone. He is trying to get into it to get access to your data by guessing your PIN or password. Also, he is very careful, and removed SIM card so that your iPhone is not connected to the Internet." For how long would you like your iPhone to be able to protect your [sensitive, confidential, private] data in hands of such criminal?

Appendix C

Online Survey Questions

C.1 Questions for Both Groups

1. What is the model of your iPhone?

   (a) 3G, 3GS, 4, 4S, 5 or 5c

   (b) 5s, 6 or 6 Plus

   (c) I don't know

   (d) Other, please specify

2. What is the model number of your iPhone? You can find the model number in the About screen on your iPhone. Choose Settings, General, About.

3. How often do you change your PIN/password?

   (a) Hourly

   (b) Daily

   (c) Weekly

   (d) Monthly

   (e) Every six months

   (f) Once a year

   (g) Never

(h) I don't use either PIN or password

(i) I don't know

4. When did you change your iPhone PIN password last time?

(a) 1-2 hours ago

(b) 1-2 days ago

(c) 1-2 weeks ago

(d) 3-4 weeks ago

(e) 1-2 months ago

(f) 3-6 months ago

(g) 6-12 months ago

(h) More than 12 months ago

(i) Never

5. When did you change last but one iPhone PIN/password?

(a) 1-2 hours ago

(b) 1-2 days ago

(c) 1-2 weeks ago

(d) 3-4 weeks ago

(e) 1-2 months ago

(f) 3-6 months ago

(g) 6-12 months ago

(h) More than 12 months ago

(i) Never

6. For how long in total have you been using iPhone?

(a) Less than a year

(b) 1 to 2 years

(c) 2 to 3 years

(d) Over 3 years

7. What is the worst thing that could happen to your iPhone?

   (a) My iPhone gets broken, but I recover my data

   (b) My iPhone gets broken, but I do not recover my data

   (c) Someone steals my iPhone and gets access to my iPhone data, my apps or my accounts

   (d) Other, please specify

8. On average, how frequently do you unlock your iPhone?

   (a) Once a day

   (b) A few times a day

   (c) Once per hour

   (d) A few times per hour

   (e) I have no idea

9. What is your iPhone auto lock time (i.e. how long does the screen stay on if the device is not being used)? You can find iPhone auto lock time in Settings, General, Auto-Lock.

   (a) Never

   (b) 1 min

   (c) 2 min

   (d) 3 min

   (e) 4 min

   (f) 5 min

   (g) I don't know

10. Do you use 4-digit PIN or alphanumeric password for unlocking your iPhone?

(a) PIN

(b) Password. Please enter the structure of your iPhone password. That is, substitute each single digit number with D, lowercase with L, uppercase with U, special character with S. For example the structure for password A1b%B is UDLSU

(c) Neither

11. What motivates you to lock your iPhone? Select all that apply.

(a) My friends lock their phones.

(b) Locking makes my iPhone inaccessible in case I lose it.

(c) Its easy to lock

(d) Locking gives me control over when my family or friends want to use my iPhone

(e) Other, please specify

12. (Optional) Why do you choose not to lock your iPhone? Select all that apply.

(a) Information on my iPhone is not sensitive and I do not care if others look into it

(b) In case of loss, I can easily be contacted

(c) It is too much effort to lock

(d) In case of emergency, others can use my iPhone to call my family and friends

(e) I never lose sight of my iPhone, it's always with me

(f) Other, please specify

13. Do you use the same PIN/password for your iPhone as you used in your previous smartphone?

(a) Yes

(b) I did not use PIN/password in my previous smartphone.

(c) This is my first phone.

(d) No

14. Do you use your iPhone PIN/password anywhere else (for web sites, credit cards, other online services)?

(a) Yes

(b) No

15. Do you share your iPhone PIN/password with anyone else, e.g. family members, friends of colleagues?

    (a) Yes. Who do you share you iPhone PIN/password with? Family, Friends, Co-workers, Partners, No one, Other

    (b) No

    (c) Other, please specify

16. Do you know anybody else smartphone security lock?

    (a) Yes

    (b) No

17. Does your iPhone store any sensitive or confidential information?

    (a) Yes

    (b) No

    (c) I don't know

18. Who do you care protecting your private data against?

    (a) Strangers

    (b) Co-workers

    (c) Friends

    (d) Family

    (e) Classmates

    (f) Roommates

    (g) Other, please specify

19. What kind of smartphone did you owe or use right before your current iPhone?

(a) Feature phone

(b) Android

(c) Windows Phone

(d) iPhone

(e) BlackBerry

(f) None

(g) Other, please specify

20. What security lock have you used for your old smartphone? Select all that apply.

(a) Alphanumeric password. Enter the structure of your previous smartphone password. That is, substitute each single digit number with D, lowercase with L, uppercase with U, special character with S. For example the structure for password A1b%B is UDLSU.

(b) Long PIN (PIN with 5 or more digits)

(c) 4-digit PIN

(d) Fingerprints (Touch ID)

(e) Pattern

(f) Face recognition

(g) I didn't use a lock

(h) I didn't have a smartphone

(i) Other, please specify

21. In your opinion, what unlocking method provides the best security for your iPhone?

(a) Alphanumeric password

(b) 4-digit PIN

(c) Fingerprint scanner (Touch ID) + 4-digit PIN

(d) Fingerprint scanner (Touch ID) + alphanumeric password

(e) Other, please specify

22. Do you know that you can use alphanumeric password for unlocking your iPhone?

    (a) Yes. Please, provide exact steps how you can turn on alphanumeric password

    (b) No

23. Please, rate your agreement with the following statements. PIN is good enough for unlocking the iPhone

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly agree

24. My iPhone is more secure if I use Touch ID than PIN/password alone.

    (a) Strongly disagree

    (b) Disagree

    (c) Neutral

    (d) Agree

    (e) Strongly agree

25. Why do you use 4-digit PIN, not alphanumeric password?

    (a) Touch ID is enough to protect my iPhone, so I do not see a reason why I should use a password

    (b) I didn't know that there is an alphanumeric password option

    (c) PIN is easier to remember

    (d) PIN is faster to type

    (e) PIN is easier to share

    (f) I continue with PIN, because I used PIN in my previous smartphone(s)

    (g) PIN provides enough security for my iPhone

(h) I use the same PIN for multiple devices or accounts

(i) I do not care about security of my iPhone

(j) I do not have any sensitive data on my iPhone that I need to protect

(k) Other, please specify

alternative Why do you use alphanumeric password, not 4-digit PIN?

(a) Password is more secure than PIN.

(b) My company requires me to use password.

(c) I continue with password, because I used password in my previous smartphone.

(d) Other, please specify

26. What do you think the most common way for an attacker to break into your iPhone?

(a) Guessing (aka brute forcing) PIN/password to unlock your iPhone

(b) Using social engineering to learn your PIN/password

(c) Shoulder surfing

(d) Other, please specify:

27. Lets consider the following scenario: "Someone has stolen your iPhone. He is trying to get into your iPhone to get access to your data. She is doing so by guessing your PIN/password. Also, she is very careful, and removed SIM card so that your iPhone is not connected to the Internet. Thus, you can not remotely wipe or 'kill' your iPhone." For how long would you like your iPhone to be able to protect your data in hands of such criminal?

(a) SLIDEBAR [0-1h-3h-6-12-1d-2-3-1w-2w-1m-2m-6m-1y-2y-forever]

28. What is your gender?

(a) Female

(b) Male

(c) Prefer not to answer

29. What is your age?

30. What is your highest level of completed education?

    (a) High school

    (b) College degree

    (c) Bachelor

    (d) Master or PhD

    (e) Other, please specify

31. What industry have you worked for the past 6 months?

    (a) Agriculture

    (b) Forestry, fishing, mining, quarrying, oil and gas

    (c) Utilities

    (d) Construction

    (e) Manufacturing

    (f) Trade

    (g) Transportation and warehousing

    (h) Finance, insurance, real estate and leasing

    (i) Professional, scientific and technical services

    (j) Business, building and other support services

    (k) Educational services

    (l) Healthcare and social assistance

    (m) Information, culture and recreation

    (n) Accommodation and food services

    (o) Public administration

    (p) Other services, please specify

32. What is your job title?

33. What is the annual income of your household?

(a) Less than $20,000

(b) Above $20,000, below $50,000

(c) Above $50,000, below $80,000

(d) Above $80,000, below $120,000

(e) Above $120,000

(f) Prefer not to answer

34. Have you ever lost your smartphone?

(a) Yes

(b) No

35. Have you ever been a victim of smartphone theft?

(a) Yes

(b) No

36. Have you ever experienced a situation when somebody has unauthorizedly used your iPhone for data access or making a call?

(a) Yes

(b) No

37. You have almost completed the survey. We have to make sure that our data are valid and not biased. Specifically, we are interested in whether you read instructions closely. Please select the option 'no answer' for this question. How long did you feel this survey was?

(a) Very long

(b) Long

(c) Neither short nor long

(d) Very short

(e) No answer

C.2 Questions for Non-Touch ID group

1. Biometrics authentication is used in computer science as a form of identification and access control. Examples include fingerprint and face recognition Have you ever used a biometric authentication system?

   (a) Yes

   (b) No

   (c) I'm not sure I used biometric authentication

2. In general, what are your major security or privacy concerns about biometric authentication?

3. Please, rate your agreement with the following statements. I am willing to use face recognition authentication

   (a) Strongly disagree

   (b) Disagree

   (c) Neutral

   (d) Agree

   (e) Strongly agree

4. I am willing to use fingerprint authentication like Touch ID

   (a) Strongly disagree

   (b) Disagree

   (c) Neutral

   (d) Agree

   (e) Strongly agree

5. I am willing to use a longer alphanumeric password alongside the fingerprint scanner such as Touch ID

   (a) Strongly disagree

   (b) Disagree

(c) Neutral

(d) Agree

(e) Strongly agree

C.3 Questions for Touch ID Group

1. Why do you use Touch ID? Select all that apply.

   (a) Convenience

   (b) Novelty

   (c) Security

   (d) Time/speed

   (e) Ease of use

   (f) Reliability

   (g) Privacy

   (h) Efficiency

   (i) Cool to use

   (j) Fun to use

   (k) Other, please specify

2. Please, rate your agreement with the following statements. PIN is good enough for unlocking the iPhone

   (a) Strongly disagree

   (b) Disagree

   (c) Neutral

   (d) Agree

   (e) Strongly agree

3. My iPhone is more secure if I use Touch ID than PIN/password alone.

(a) Strongly disagree

(b) Disagree

(c) Neutral

(d) Agree

(e) Strongly agree

4. It was difficult for me to set up Touch ID

(a) Strongly disagree

(b) Disagree

(c) Neutral

(d) Agree

(e) Strongly agree

(f) I did not set it up

5. It is easy for me to use Touch ID

(a) Strongly disagree

(b) Disagree

(c) Neutral

(d) Agree

(e) Strongly agree

6. Overall, I am satisfied with using Touch ID

(a) Strongly disagree

(b) Disagree

(c) Neutral

(d) Agree

(e) Strongly agree

C.4 Online Survey Supplemental Graph

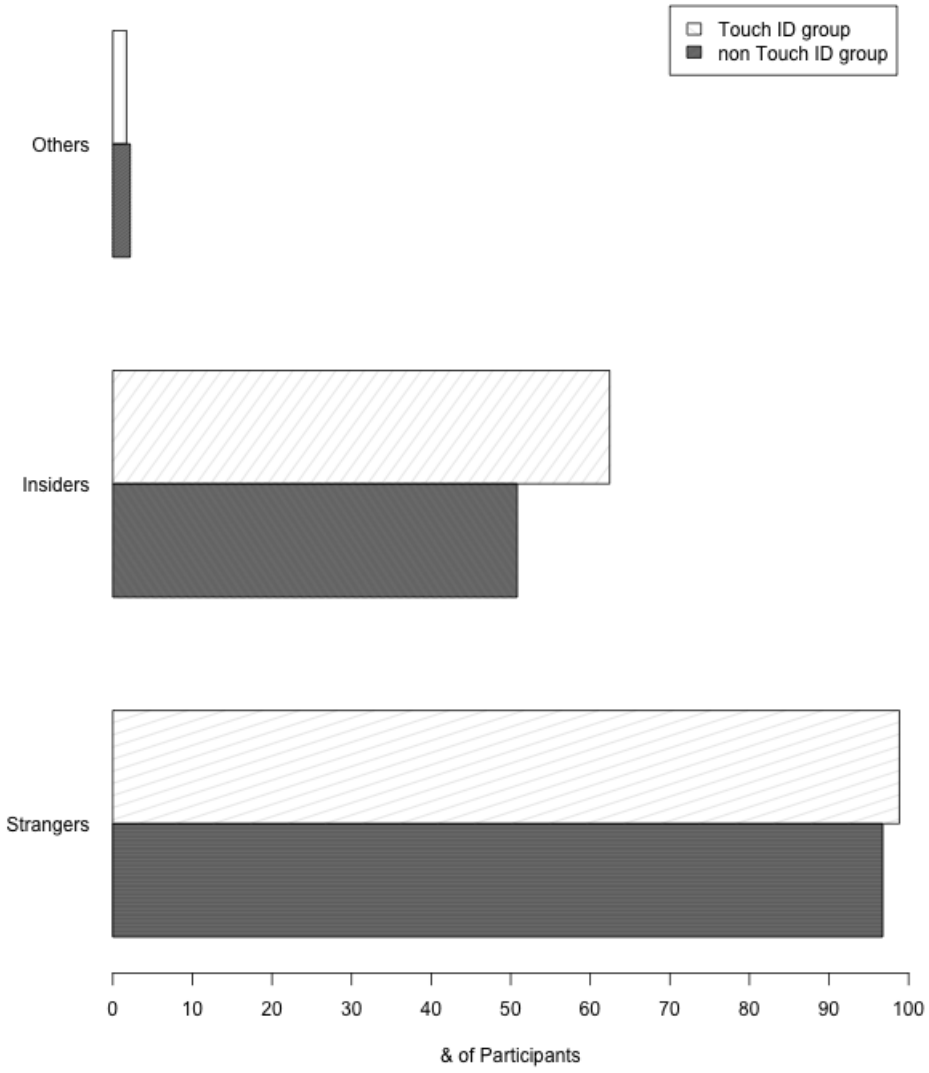

Figure C.1: Distribution of attackers (insiders and strangers) who users lock their iPhones against. For Touch ID group (n = 173), and for non-Touch ID group (n = 201).