On the Impact of Touch ID on iPhone Passcodes

Ivan Cherapau, Ildar Muslukhov, Nalin Asanka, Konstantin Beznosov
University of British Columbia, Vancouver, Canada
{icherapau,ildarm,nalin,beznosov}@ece.ubc.ca

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 before granting access to applications and data on the phone. iPhone's unlocking secret (a.k.a., *passcode* in Apple's terminology) is also used to derive a key for encrypting data on the device. Recently, Apple has introduced *Touch ID*, that allows a fingerprint-based authentication to be used for unlocking an iPhone. The intuition behind the technology was that its usability would allow users to use stronger passcodes for locking their iOS devices, without substantially sacrificing usability. To this date, it is unclear, however, if users take advantage of Touch ID technology and if they, indeed, employ stronger passcodes. It is the main objective and the contribution of this paper to fill this knowledge gap.

In order to answer this question, we conducted three user studies (a) an in-person survey with 90 participants, (b) interviews with 21 participants, and (c) an online survey with 374 Amazon Mechanical Turks. Overall, we found that users do not take an advantage of Touch ID and use weak unlocking secrets, mainly 4-digit PINs, similarly to those users who do not use Touch ID. To our surprise, we found that more than 30% of the participants in each group did not know that they could use passwords instead of 4-digit PINs. Some other participants indicated that they adopted PINs due to better usability, in comparison to passwords. Most of the participants 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 their passcodes provide.

1. INTRODUCTION

Smartphones have become our primary devices for accessing data and applications. 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 [15]. Smartphones are already used for online banking, accessing corporate data, operations that used to be only in the domain of desktops and laptops. This results in sensitive and confidential data being stored and accessed on smartphones. High mobility and small size of smartphones alter the common threat model we 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].

Adopted by all mobile OS developers, the state of the art in protecting data-at-rest is to encrypt it. In order to avoid the problem of storing an encryption key together with the encrypted data, the key encryption key is commonly derived from the secret used for unlocking the device. Unfortunately, users employ weak unlocking secrets (a.k.a., "passcodes" in Apple's terminology), mainly due to usability-related considerations [32]. Being most common unlocking secretes, personal identification numbers (PINs) are not only susceptible to shoulder surfing attacks, but can also be easily bruteforced [34]. At the same time, PINs 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 such users unprotected [31].

Several device manufactures, such as Apple and Samsung, have recently introduced biometric authentication for unlocking smartphones. As a case in point, with the release of iPhone 5S in 2013, Apple has introduced a fingerprint sensor integrated into the "home button". Branded as Touch ID, the sensor authenticates a user, once she touches the button. As stated in the iOS security white paper [4], the key advantage of 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 appear to be based on the assumption that the usability of a password largely depends on the frequency of its usage and that users will use stronger passwords, as a result of the decrease in usage frequency. Recent research, however, casts doubts on this assumption. In particular, several findings suggest that users tend to create low-entropy passwords, regardless of how frequently they have to input them [8, 18, 35]. Thus, it is unclear if and how Touch ID impacts the choice of users' passcodes. It is the main focus and the contribution of this paper to fill this knowledge gap.

In order to understand the impact of Touch ID sensor on users' passcode selection, we focused on testing our main hypothesis (H_1^{alt}) – *"There is a difference in passcode entropy between those who use Touch ID and those who do not."* For assessing passcode's strength, we used *zero-order entropy*, which estimates the search space of a secret, assuming that each character is chosen randomly and independently. Zero-order entropy served the purpose of comparing the strength of two passcode groups, without having access to actual passcodes. The results of our study revealed that even

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

with zero-order entropy, which overestimated the real complexity of passcodes, the strength of the participants' passcodes was such that made brute-force attacks practical. For brevity, throughout this paper we refer to zero-order entropy as "entropy".

To test H_1^{alt}, we performed three user studies. First, we conducted an in-person survey with 90 iPhone owners in shopping malls and other public places in Vancouver, Canada. We opted for an in-person survey in order to verify accurately the self-reported data, such as the passcode length and the method of the phone unlocking. Results of the survey did not reveal statistically significant difference in the passcode entropies between those who did and who didn't use Touch ID. Furthermore, the 95% confidence interval suggested that if, hypothetically, there were a difference, then its absolute value could not be larger than 3.35 bits.

In order to understand why users are not adopting stronger passwords when Touch ID is available, we followed up with an interview study of 21 participants. Its results led us to identify possible reasons for users to stick with 4-digit PINs. Finally, to corroborate findings of the first two studies, we conducted an online survey with 374 Amazon Mechanical Turks. Overall, we confirmed statistical results of the first study and measured prevalence of reasons for using 4-digit PINs. In particular, more than 30% of the participants were unaware that passwords are available on iPhones, 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 theoretical difference in passcode entropies between the two groups down to 1.91 bits.

Overall this paper makes the following contributions:

- We question the validity of the assumption that such phone unlocking methods as Touch ID would nudge users to use higher-entropy passcodes. We did not find any significant difference in passcode strengths between the two groups. Furthermore, the 95% confidence interval for the differences in mean entropy shows that even if there were a statistically significant difference, it would not be greater than 1.91 bits. In the light of observed average entropy (approximately 16 bits), such a difference would result in passcodes of 18 bits of entropy, translating to about 4.5 hours of extra work for an adversary performing an on-device brute-force guessing attack on an iPhone [4].

- We investigate why Touch ID has not resulted in stronger passcodes. In particular, we find that more than 30% of users do not know that they can use passwords, rather than PINs. Others use PINs due to the usability benefits over passwords, e.g., easy to remember or faster to type.

- Finally, we find a significant mismatch between the desires for protection the majority of iPhone owners report and the actual strength of their passcodes. In particular, the preferences of only 12% of participants matched the provided level of protection, while others preferred significantly higher protection. For instance, 48% desired their passcodes to protect the data for more than 40 years, which is far from reality.

The rest of the paper is organized as follows. We first provide background and discuss related work in Sections 2 and 3. Next, we present our research question and our approach at answering it in Section 4. Then we describe our studies: in-person survey in Section 5, interviews in Section 6, and MTurk survey in Section 7. We discuss results in Section 8 and conclude in Section 9.

2. BACKGROUND

We begin this section with a description of a practical brute-force attack on iOS device passcode. Then, we explain how Touch ID works. We conclude by describing zero-order entropy.

2.1 Data Protection and Brute-force 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., on the first unlock after booting. These class keys are protected with a combination of the user's passcode and the *device key*, a unique per-device key embedded in the crypto-chip. In order to extract this device key, an adversary can attempt to reverse engineer the crypto chip, which is an expensive task in terms of time and resources required. An alternative option for an adversary would be to mount an *on-device* guessing attack on the passcode. An adversary uses the crypto-chip directly in an *on-device* attack, in order to try passcode candidates and eventually to decrypt class keys. To decrease the effectiveness of such attacks, the crypto-chip in iPhones and iPads is calibrated to take at least 80 ms for each passcode attempt.

In order to mount an *on-device* attack, an adversary needs to run arbitrary code on the target device. This can be achieved by compromising the *boot-chain* [1], which would allow bypassing iOS kernel's limitation on the number of available passcode guessing attempts [42]. For example, the current version of iOS (8.3), if configured so, would limit the number of guesses to 10, and wipeout the device afterwords. It takes some time, effort, and luck to find an exploitable bug in the boot-chain. While no flaws are known in the current iOS, such flaws have been found in earlier versions.

To summarize, due to the feasibility of on-device unlimited guessing attacks, the protection of the data-at-rest on iOS devices could any day end up hinging on the security of their passcodes.

2.2 Touch ID

Touch ID is a biometric authentication sensor based on a high definition fingerprint scanner embedded into *"home button"* on iPhones and iPads. 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 passcode, users are still required to set passcodes on their devices, before being able to use Touch ID. The main reason for such a strict requirement lays in data-at-rest encryption, which needs a source of entropy that is not stored on the device itself. User's device unlocking secret serves this purpose.

A passcode can be either (1) a simple 4-digit PIN[1] or (2) a longer one, with up to 37 characters selected from the alphabet of 77 symbols, to which we refer in this paper as "password". The user can chose to set up either a PIN or a password as her unlocking secret. We use term "passcode" as a general reference for an unlocking secret, unless we want to distinguish between PINs and passwords.

When a device with Touch ID enabled boots, it prompts the user to provide the correct passcode. At this stage, the internal memory of Touch ID is clear, i.e., immediately after reboot users are not able to use Touch ID sensor. Once the user provides the correct passcode, the iOS is able to recover actual data encryption keys and uses them to decrypt and encrypt data. If the device is locked, OS erases certain types of keys from RAM, which will require either the correct passcode or successful unlocking with Touch ID, in order to recover these keys on unlock. The unlocking flow with Touch ID enabled is shown in Figure 1.

When a user locks the device that has Touch ID enabled, iPhone's

[1]Apple security white paper defines it as a "simple passcode".

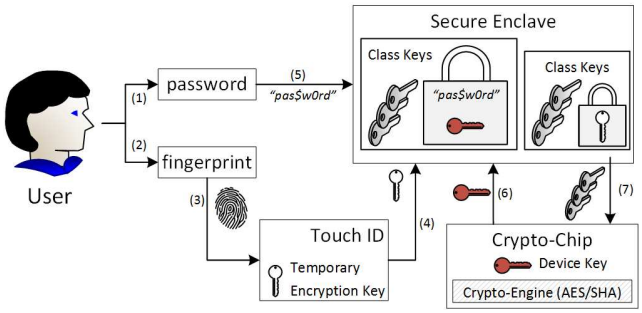

Figure 1: Unlocking flow with Touch ID enabled. When the user locks the device, the class encryption keys are wrapped by a random temporary encryption key (TEK). To unlock the device, the user has two options, she can either (1) type in her passcode, or (2) use Touch ID. When the user uses Touch ID, it authenticates the user by matching her fingerprint with saved fingerprints (3). If the authentication is successful, the sensor releases the TEK to the Secure Enclave (4), which allows decrypting class keys and sending them to the crypto-chip (7). If, the user fails to authenticate for five times with Touch ID, or does not unlock device for 48 hours, the Touch ID sensor flushes the TEK, which leaves typing in the passcode as the only option for unlocking the device. Without Touch ID, the user types her passcode (1), which is sent to the Secure Enclave (5). The combination of the device key (6) and password (5) are used to decrypt class keys and send them to the crypto-chip (7).

CPU generates a random *temporary encryption key* (TEK), which protects certain class keys by "wrapping" them (a cryptographic operation somewhat similar to encryption). It then sends the TEK to Touch ID and deletes class keys from RAM. After that, there are two options for the iOS to recover the wrapped class keys (1) receive the TEK from Touch ID once the user successfully authenticates to the sensor, or (2) receive the correct passcode from the user, then derive the correct encryption key from a combination of the passcode and the device key, and then "unwrap" class keys. When the user touches the Touch ID sensor, the sensor tries to authenticate the user based on the fingerprint. If the authentication attempt is successful, the sensor releases the TEK to the Secure Enclave, which is located in the CPU. If, however, the user fails to authenticate with the fingerprint for five times, or has not unlocked the device for 48 hours, the Touch ID sensor flushes the TEK, which leaves passcode as the only option for unlocking an iPhone.

We decided to focus on Touch ID, because it is deployed on an existing and popular mobile platform, adopted by millions of users worldwide. We did not study Android fingerprint and face recognition because the former is a new technology that first appeared in April 2014 [20] and the latter has not become widely adopted by the users, probably due to usability [7] and security issues [16].

2.3 Zero-order Entropy

The strength of an authentication secret is defined by the effort an attacker needs to spend on guessing it. In simple terms, this effort is assumed to be proportional to the size of the search space the attacker needs to check in order to find the secret. One such metric is *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. For example, the length of iPhone's PIN in iOS 8.3 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 secrets of a given length and the size of a given alphabet, with the assumption that each character is selected randomly and independently from all other characters.

Of course, zero-order entropy, as a metric, suffers from several limitations, when it's applied to human-chosen secrets, like passwords and PINs. The most important one is that it does not measure the secret strength accurately. Recent research has shown that users tend to select highly predictable passwords and often use dictionary words as ones [9, 17]. 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 attacker's work. In other words, it overestimates the actual work.

3. RELATED WORK

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 [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.* [40] analyzed a set of leaked passwords. The 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]. Such a policy might require users to use a password that contains non-alphanumeric symbols, lower and upper case letters, and numbers. Using a password policy that is too strict, 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 phones [21]. Egelman et al. also found a strong correlation between locking behaviours and risk perceptions, but the authors believe that users underestimate actual the risks [14]. In contrast, we focused on studying the effect that Touch ID makes on users unlocking password selection and the reasons for such an effect.

Biometrics-based authentication modality has also received considerable attention from the research community in recent years [2, 30, 38]. Although usability of a biometric system is still an important factor in adoption [33, 37], such authentication methods could potentially remedy common drawbacks of text-based passwords. For example, users do not need to remember anything [7]. Indeed, recent studies showed that the usability of biometric-based phone unlocking is important for users [13]. Crawford and Renaud [12], however, have showed that users are willing to try biometric authentication mainly for its usability benefits. In addition, Breitinger *et al.* [10] suggest that 87% of users are in favour of fingerprint authentication. Others have found that the presence of a biometric factor in a two-factor authentication system can lead users to picking weaker credentials, in comparison with a password-only authentication system [41]. In contrast, we focus on how Touch ID impacts users' choice of iPhone passcodes 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 [39]. Fingerprint sensor can improve the security and the

convenience for users, if used in smartphones [19], because there are many limitations of smartphones' screens and keyboards [19, 25] that make password-based authentication/unlocking undesirable. For instance, 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 for desktops [28]. In addition, Bao *et al.* [6] found that the average typing speed for an 8-character alphanumeric password on mobile devices is three times slower than on desktop computers.

Finally, recent research suggests that users tend to use weak 4-digit PINs over alphanumeric passwords in smartphones [24, 32]. Users justify such choice by ease of use of PINs, in comparison to passwords, especially in cases when one has to unlock their device with high frequency for day-to-day activities [31]. Unfortunately, it is clear today that a 4-digit PIN provides virtually no security for data-at-rest [4, 36]. To make the matter worse, even within the search space of 4-digit PINs, users make highly predictable choices. For example, Amitay [3] analyzed over 200,000 iPhone PINs and discovered that "1234" is the most common PIN, followed by "0000" and "2580". Considering the software limitation on the number of allowed unlocking attempts (i.e., 10 attempts in iOS) through the user interface, one can try the top 10 PINs and still achieve 15% success rate without the need to go for an *on-device* brute-force attack.[2] That is, one in seven iPhones can be unlocked by just trying the top 10 PINs. It seems that the main intuition behind the design of Touch ID was to reduce the number of times the 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 by using stronger passcodes.

4. METHODOLOGY OVERVIEW

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

- H_1^{null} – *Use of Touch ID has no effect on the entropy of passcodes used for iPhone locking*.
- H_1^{alt} – *Use of Touch ID affects the entropy of passcodes 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*.

We conducted three user studies, starting with a study based on in-person surveys. This study allowed us to test our hypotheses. In addition, it allowed us to clarify areas with the lack of understanding and refine our follow-up studies. We followed the first study with an interviews, in order to gain deeper insights into passcode selection by users. In particular, we focused on understanding why users do not take advantage of Touch ID, i.e., understanding users' reasoning for not adopting stronger passcodes when Touch ID is available. Finally, to corroborate our data from the first study and to measure the prevalence of the reasons for using weak passcodes, 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 provided descriptive statistics on reasons for using weak passcodes.

In the first and third studies, we chose zero-order entropy for estimating the strength of participants' passcodes, even though it has limitations, as discussed in Section 2.3. There were several reasons for this choice. First, evaluation of the passcode's guessability would require access to plaintext passcodes, which we chose not to obtain 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 overestimated the passcodes strength, the actual workload for a brute-forcing attacker is still practical.

We obtained ethics approval from our university's behavioural research ethics board for all three studies.

5. STUDY I: IN-PERSON SURVEY

5.1 Methodology

In our first study, we chose to use an in-person survey of iPhone users for several reasons. First and foremost, this choice allowed us to verify answers related to participants' unlocking behaviour and the authentication secret being used. In addition, an in-person nature of the study allowed us to follow-up unforeseen answers with additional questions. We strived to recruit a pool of diverse participants, hence we approached people in public locations, such as shopping malls and coffee shops. Each participant 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 used an iPad with our own survey app. All answers were stored locally on the iPad, and for some of the questions we also validated participants' answers by asking participants to show us some elements of their unlocking process and other relevant data. In particular, we validated the type of the unlocking method used, by asking them to show the locked screen. We also validated the length of the password (for those who used it) by asking participants to show us the unlocking screen after the password has been typed but before they clicked on the *enter* button. This allowed us to validate their answer about the password length by our researcher counting the number of stars in the password field. In addition, participants were asked to navigate to the settings of the auto-lock screen on their iPhones and show us the value of the auto-lock timeout. Finally, by asking each participant who claimed to use Touch ID to unlock their device with a fingerprint, we were able to confirm that they, indeed, used it.

Most of the survey questions were either open-ended or contained option "other", which allowed participants to provide their own answer if needed. The questionnaire guide is provided in Appendix A.1 and consists of the following parts:

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

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

Part 3 Questions on the experience participants had so far with their smartphones, including if they locked their previous smartphones.

[2]This is a simpler approach that does not require execution of arbitrary code on the device.

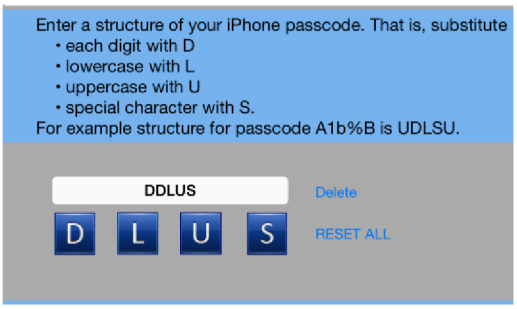

Figure 2: Passcode structure question in Study I.

Part 4 Passcode metrics questions. In this part, we asked participants to provide us a structure of their unlocking passcodes. In order to preserve confidentiality of their passcodes, we asked participants to substitute each character in their passcodes with the mnemonic of the character type: **D** - digits, **L** - lower-case letters, **U** - upper-case letters, **S** - special characters. We refer to such encodings of passcodes as "masks". The screenshot of this question is shown in Figure 2. We chose this approach for two reasons. First, it allowed us to assess entropy. Second, this approach did not require participants to reveal their passcodes to us.

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

Part 5b This section was only relevant to the owners of iPhone 5 and older models. Here, we asked 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 several questions in the questionnaire and added an attention check question (#28 in Appendix A.1). Most of the changes we made were aimed at improving questions' clarity and 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 invited them to participate in our study. We chose this recruitment method mainly because we were interested in the general population of iPhone users. We recruited participants who were iPhone users and 19 years old or older. Although the main focus of our study were owners of Touch ID (iPhone models 5S, 6, and 6 Plus), we also recruited owners of older models. Participants that used Touch ID were assigned to Touch ID group, while the rest to non-Touch ID group. Note, that those iPhone 5S, 6 and, 6 Plus owners who did not use Touch ID, were assigned to the non-Touch ID group.

5.2 Results

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

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

Out of 90 participants, 30 were female. The minimum and maximum age was 19 and 71 years, and the average age was M = 29 (SD = 12). Among all participants, 41 used Touch ID sensor and 49 did not. The majority of our participants was experienced iPhone users, i.e., they owned an iPhone for more than two years. Only 12 participants owned iPhones for less than a year. Almost all of the participants (81) had owned another smartphone before the current one. Most of our participants (69) stated that they unlock their iPhones at least once per hour. In addition, we found that 32 participants had lost their smartphones before, and 15 participants were victims of smartphone theft. On average, participants 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 2 (column "Study I").

Reasons To Lock Or Not To. Overall the participants use various reasons for locking or not locking their iPhones. Some of the reasons were driven by *a possible attacker*, e.g., 58 participants locked their devices to prevent strangers from access, and four participants locked their devices to protect data if they get mugged, 23 participants used locked their iPhones to control access by their family and/or friends. In addition, we found that some participants used social norms to rationalize locking, e.g., 12 participants locked their devices because their friends did the same.

Other reasons could be attributed to either (1) *usability problems* of device locking, voiced mainly by those who did not lock their device, or (2) the *necessity to have certain features* that were either enabled or prevented by device locking. The four participants 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 (c) unlocking process takes too much time. Only two participants, out of the four who did not lock their iPhones, stated that they did not care about security of their data.

Use of PINs and Passwords. Out of the 90 participants, 86 locked their phones, with 66 employing 4-digit PINs, and 20 using passwords. Third of the participants (36) used the same passcode for their iPhones as in their previous smartphones. In addition, 52 participants stated that they shared their passcode with someone else, and 53 stated that they knew passcodes for smartphones owned by others.

Touch ID Group. The Touch ID group included 41 participants, with 29 of them using 4-digit PINs. The 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 participants stated that the use of Touch ID was easy or very easy (see Appendix A.2 for more details). The majority of the participants (30) had never had any issues with Touch ID, and, overall, Touch ID participants considered Touch ID as a convenient, secure, quick, and easy to use unlocking mechanism.

Touch ID participants 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 the device, while the owner is sleeping (e.g., P9 "... [I] might be sleeping and someone might use my finger to unlock [my iPhone] ..."). [3] Some participants were even afraid that an attacker might fake their fingerprints, in order to access the 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

[3] Exactly the same story has happened in December 2014, when a boy unlocked the iPhone of his sleeping father with his father's thumb [11].

Table 1: Passcode average entropies for Touch ID and non-Touch ID groups in Study I. While non-Touch ID group had 49 participants, four of them did not use any passcode to lock their phones and were excluded in computing entropies.

	Touch ID	Non-Touch ID
Mean	15.88 bits	15.61 bits
SD	6.93 bits	7.45 bits
N	41	45

participants (P11) stated that she was afraid about "Apple leaking my fingerprint and someone can impersonate me" and "fingerprint being used for purposes other than to just unlock my phone."

Non-Touch ID Group. The non-Touch ID group included 49 participants, where 37 participants used PINs and eight used passwords to unlock their iPhones. Four participants did not lock their phones and were excluded from computing average entropy of passcodes in this group. While 13 in this group had Touch ID available, they 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), "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" (P89), "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 the 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.

5.2.1 Hypothesis Testing

To test H_1, we first compared proportions of participants that used PINs 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). For computing entropy of participants' passcodes, we obtained the length of the passcodes and the alphabet size from the masks our participants provided (Figure 2). The results of Mann-Whitney U test did not reveal any statistically significant difference between mean values of entropies in Touch-ID and Non-Touch ID groups (W = 15708, p = 0.70), see Table 1. 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 find it due to small size of the participant pool, and considering the observed mean entropy value of 15.88 bits, we can assess that the possible maximum entropy with 95% confidence is 19.23 bits. Taking into account the design of the data encryption in iPhones, i.e., that each passcode guessing attempt takes at least 80ms, we can show that 19.23 bits of entropy corresponds to roughly 14 hours. In comparison, it would take only 1.1 hour to brute-force passcodes in non-Touch ID group with average entropy of 15.61 bits.

We tested H_2 hypothesis with Chi-squared test (χ-squared = 0, p = 1.0). We were unable to reject H_2^{null}, and hence we conclude that Study 1 failed to show an effect of Touch ID on users' preference to lock their iPhone.

5.3 Limitations

There were several limitations that might have negatively impacted our ability to find a statistically significant difference between passcodes of Touch ID and non-Touch ID groups. First, we might not have obtained large enough sample size. Second, our participant pool had a fairly large bias towards the 19-34 age group. Third, since we obtained only passcode exact length and the types of the characters in each position, but not the characters themselves, this coarse granularity of the data did not allow us to observe the difference. Fourth, as we did not control for or collect data on how technically and security savvy our participants were, we might have had one of the two groups with participants heavily skewed on these traits. In order to address these limitations and gain a deeper insight into why users are sticking with 4-digit PINs we decided to proceed with an interview-based study.

While we included an attention check question (see question 28 in Appendix A.1), we realized after running the survey that the question was poorly worded. So, we have decided not to exclude participants based on their response to this question, because most of those who failed the question likely did not understand it. We paraphrased the question and used it in Study III (see question 36 in Appendix C.1).

6. STUDY II: INTERVIEWS

We followed the in-person survey with an interview study in order to gain a better understanding of users' reasoning to stick with weak passcodes. Our main objective was to answer research question (RQ_1) "Why Touch ID users do not employ stronger passcodes for smartphone locking?"

6.1 Methodology

We designed our study with the focus on qualitative data collection. We used semi-structured interviews since they gave us the freedom to explore new topics, as they emerged. We used theoretical sampling, rather than random sampling, because (as common with explorative enquiries) we were interested in the diversity and richness of the participants' answers, rather than in the generalizability of the findings. A pilot study with eight participants revealed the necessity for real life scenarios in several questions, and we revised the interview guide accordingly. We randomized the order of interview questions, in order to reduce bias due to the order of the questions. Two first interviews were conducted by two researchers together in order to ensure that all important questions were asked and well understood by the participants. Each participant was compensated $10 for a 20-minute interview. We audio recorded all interviews and two researchers coded each interview independently. After each coding session, the coders discussed any disagreements 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%.

6.1.1 Participant Recruitment

We recruited participants by directly approaching them in public places such as shopping malls, libraries, and coffee shops in Vancouver. Our inclusion criteria were participants of age 19 years and older who used Touch ID on their iPhones. After the 17th interview, we did not observe any new codes and decided not to schedule new participants, hence we stopped interviewing after 21 participants. Saturation analysis of new concepts with each additional interview is shown in Figure 3.

Table 2: Participants' demographics for the three studies.

		Study I		Study II	Study III	
Parameter	**Value**	**#**	**%**	**#**	**#**	**%**
Gender	Female	30	34	10	220	59
	Male	60	66	11	154	41
Age	19 to 24	43	48	7	110	29
	25 to 34	29	32	4	195	52
	35 to 44	8	9	2	49	13
	45 to 54	2	2	2	17	5
	55 to 64	6	7	3	2	1
	65 or older	2	2	3	1	0
	Mean	29		30	N/A	
	Median	30		27	N/A	
Education	High school	30	34	5	19	5
	College degree	22	24	5	129	35
	Bachelor	28	31	8	151	40
	Master or PhD	7	8	3	75	20
	Other	3	3	0	0	0
Income	Less than 20K	25	28	2	67	18
	20K-50K	29	32	3	97	26
	50K-80K	16	18	7	70	19
	80K-120K	8	9	6	99	26
	Above 120K	5	6	0	41	12
	Prefer not to answer	7	8	3	0	0
Industry	Construction	2	2	2	1	0
	Trade	2	2	3	8	2
	Transportation	3	3	1	6	2
	Finance and real estate	7	8	3	23	6
	Professional services	5	6	6	67	17
	Business and building	11	12	0	18	5
	Educational services	4	4	2	51	13
	Health care and social	5	6	2	52	13
	Inform./culture/recreation	3	3	0	16	4
	Accommodation and food services	6	7	3	19	5
	Public administration	1	1	0	9	2
	Other	45	41	3	104	27
Role	Individual Contributor				122	33
	Team Lead				35	9
	Manager				46	12
	Senior Manager				7	2
	Management / C-Level				9	2
	Partner				5	1
	Owner				18	5
	Volunteer				4	1
	Intern				12	3
	Student				57	15
	Other				59	16
Locking method	PIN	66	73	19		
	Password	20	22	2		
	None	4	5	0		
Locked with PIN/Password/None	non-Touch ID				177/6/18	
	Touch ID				166/7/0	

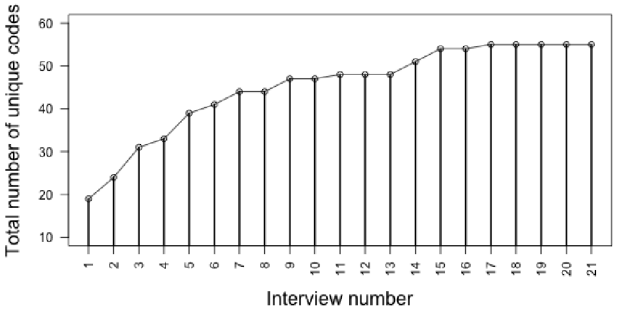

Figure 3: The total number of unique codes for each additional interview in Study II. We reached saturation around 17th interview.

6.1.2 Procedure

After agreeing to be interviewed and showing us their iPhone 5s, 6, or 6 Plus, each participant was asked to read and sign 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:

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.

Locking Behaviour: 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 why they chose to use PIN or password. We also asked participants about their passcode sharing behaviour.

iPhone Data: Then we asked participants about the most valuable data in their iPhones, what data they considered to be confidential or sensitive, and who they cared protecting it against.

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** participants, out of which 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 a year. Almost all participants had owned another smartphone before the current one. In addition, 16 participants lost their smartphones before, including the six participants who also were victims of smartphone theft. Participants' demographics are summarized in column "Study II" of Table 2.

6.2.2 Reasons for using PINs

The most common reason for using 4-digit PINs was a 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 led to confusion about the relationship between passcode and Touch ID. They believed 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.

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

Another evidence of participants' confusion was that they incorrectly understood how Touch ID and passcode work together. That is, they assumed that using Touch ID, in addition to having a passcode, increases security of data-at-rest, while in reality it does not. In addition, some participants thought that Touch ID provides higher security, compared to passcode. They justified such an answer by stating that users tend to use dictionary words as passwords, while random digits are usually used for PINs. For instance:

> *"Touch ID is more secure than PIN or password because it's unique for the owner" [P3]*

> *"people often choose their dogs' names or middle names or something similar as their passwords" [P11]*

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

> [After the participant was explained what a passcode is and how to use it.] *"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" [P4],*

Two participants stated that they used PINs because the sales staff who helped with setting up their iPhones in Apple Stores, showed only the PIN option to the participants. As a result, they believed that this was the only option available:

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

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

Also, five participants admitted that they got habituated to use PINs from their previous devices, and continued to use PINs on the new iPhones. In addition, participants stated that they did not want to remember a new password, so they just decided to use the old PIN on the new device:

> *"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." [P1]*

Unsurprisingly some participants stated that they decided to use PINs because it is easier to use, faster to type and easier to remember in comparison to passwords. Indeed, similar results have been shown in previous research, e.g. [31]. In addition, five participants stated that they did not store any sensitive information on their iPhones, thus, they did not care about the extra level of security a password can provide. They believed that PINs are good enough to protect their phones and did not see a good reason to switch to passwords:

> *"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" [P15]*

Finally, seven participants reused their PINs across multiple devices or accounts in order to reduce the amount of information they needed to remember. Several participants stated that, because they shared their iPhones with others, PINs were easier to share for them than passwords, for instance:

> *"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" [P8]*

In summary, participants provided various reasons for sticking with 4-digits PINs. In particular, some participants did not know that they can use alphanumeric passwords, others were only shown how to setup and use PINs, when they were assisted by the salespeople when purchasing their iPhones. Other participants justified the use of PINs by the fact that they had low requirements for the security of data-at-rest on their iPhones. Some participants were habituated to use PINs from previous devices or wanted to reuse PINs across various devices and accounts. Understandably, participants stressed the usability benefits of PINs over passwords, as one of the reasons to use the former. In particular, they stated that PINs are faster, easier to use and memorize. More critically, our participants misunderstood how Touch ID works and how it impacts the security of data-at-rest, in cases when an iPhone is lost or stolen. Finally, PINs were more convenient than passwords for sharing iPhones with others.

6.2.3 Passcode Sharing Behaviour

Eight participants shared their passcodes with others for several reasons. First, some participants were pressed to share:

> *"I share [PIN] with my girlfriend because she forced me to!" [P2]*

Second, participants trusted others with their data, and, thus shared their passcode:

> *"I share with my boyfriend because I trust him and sometimes he uses my phone, too" [P19]*

> *"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" [P10]*

Finally, participants shared their passcodes with others because of concerns with emergency situations, when someone close needs access to the phone or its data. For instance:

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

To summarize, the participants shared their passcodes to enable emergency access to their phones, or because they trusted others with the data on their phones, or because they were pressed to share their phones.

6.3 Limitations

Our interview study has several limitations. As with most qualitative enquiries, the results of the interviews are not generalizable. The results of the analysis might have been impacted by our biases. We strived to minimize this bias by using separate coders and discussing the disagreements. Finally, the participants might have misunderstood some questions. To reduce chances of such misunderstanding, we conducted a pilot study with eight participants, with the main purpose of testing the interview questions. We alleviated some of these limitations by conducting our third study.

7. STUDY III: ONLINE SURVEY

The results of the first study suggest the lack of any practically significant impact of Touch ID on passcode selection, prompting us to investigate why users don't choose stronger passcodes, provided that they need to type them rarely if they use Touch ID. While the findings from the second study offered possible reasons for sticking with 4-digits PINs, the study did not allow us to assess the prevalence of these reasons in a representative sample of the iPhone users. Our third study aimed at addressing exactly this limitation. We designed it in a form of an online survey, so that we could recruit a larger and more representative sample in order (a) to corroborate statistical results from the first study, and, (b) to measure qualitatively the prevalence of reasons for iPhone users not employing stronger passcodes.

7.1 Methodology

The online survey closely resembled in its structure our in-person questionnaire (Section 5.1). We just added questions for collecting descriptive statistics about the reasons for not using stronger passcodes. Appendix C.1 provides our online survey.

We recruited participants on Amazon Mechanical Turk (MTurk) [23] between February and March 2015. We limited MTurk workers to the US participants with HIT approval rate at 90% and above. Before running the study, we conducted a pilot with 149 MTurk participants to test the data collection in general and the survey questions in particular.

In comparison with the first two studies, which were conducted in-person, the online survey made it challenging to validate whether or not a participant had an iPhone and used the unlocking mechanism as she claimed to. To mitigate this concern, the participants were asked during the survey to submit two photos: (1) a photo of their iPhone reflection in a mirror taken with the front-facing camera, and (2) a screenshot of the unlocking interface. Examples of verification photos that our participants submitted are shown at Figure 4. We later used these photos to validate the claimed iPhone model (i.e., iPhone 4, 4S, 5S) and the locking mechanism. In addition, we also asked participants to provide us with the model number, e.g., ME302C/A,[4] which has one-to-one correspondence with the marketed model, e.g., iPhone 5S. We excluded responses from all those participants who 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 one we used in Study I, in order to check if the participant read instructions carefully. This time, it was revised to improve the wording (see question 36 in Appendix C.1). We paid $1.00 to all the participants, including those who failed the attention check question or iPhone model verification or unlocking mechanism verification.

7.2 Results

7.2.1 Demographics

Overall, we recruited 1,219 participants and assigned them to Touch ID and non-Touch ID groups, depending on whether they reported using Touch ID or not. At the end, responses from 374 participants were taking into account during the data analysis, 31% of the ones who were recruited.

Non-Touch ID group. 698 participants have started the survey in the non-Touch ID group, and 550 finished it. On average it took each of them about 16.3 minutes (SD = 7.5 minutes) to finish the survey. Note that we excluded seven participants that spent more

[4]Device model can be found in the Model field of iPhone's Settings in `General->About` section.

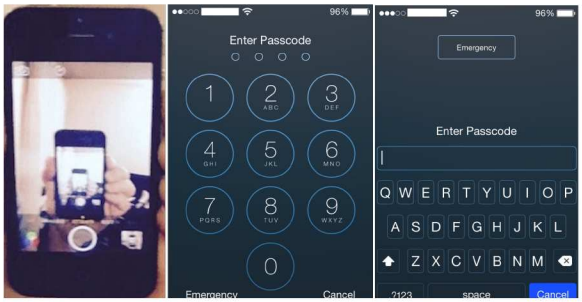

Figure 4: Examples of verification photos that participants sent us. From left to right, (1) a photo of an iPhone taken with front facing camera in a mirror, (2) a screenshot of PIN based iPhone unlock interface, and (3) a screenshot of password-based iPhone unlock interface.

than an hour finishing the survey. 317 participants failed to submit correct photos of the iPhone and screen shots of the locking interface, which left us with 226 eligible participants. Finally, 25 out of 226 participants failed the attention check question, which reduced the non-Touch ID group size to **201** participants, i.e., 37% of all participants that finished the survey.

Touch ID group. 521 participants have started the survey, and 445 finished it. On average it took about 15.7 minutes (SD = 6.2 minutes) for participants to answer the questions. Similarly to non-Touch ID group, we excluded unqualified participants. In particular, we excluded five participants that spent over an hour to finish the study, and all the participants who failed to submit a proper proof of an iPhone and locking mechanism screenshot. We also excluded all the participants who failed the attention check question, which reduced our participant pool down to **173** participants, 39% of those who finished.

The participants' demographics are shown in column "Study III" of Table 2. We recruited participants from various occupations, ranging from agriculture to public administration. The participants' job titles also included various positions, such as managers, students, team leaders and others. Our participants had diverse education levels, including 75 participants with Ph.D. or Masters degrees. More than 50% of the participants were between 25 and 34 years old. Finally, our participants had various income levels.

7.3 Testing Hypotheses

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

The 95% percentile confidence interval for the difference between the means of passcode entropies in two groups was [-1.91, +0.95]. That implies that in case if, hypothetically, there is a difference and we just failed to reveal it, due to small sample size, then with 95% confidence we can state that the difference between mean entropies of passcodes in Touch ID and non-Touch ID groups would be 1.91 bits at most. Analysis 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. Due to the results of these statistical tests, we could not reject H_1^{null}.

Similarly to Study I, we estimated the amount of work an attacker will need to do, on average, in order to brute-force the whole passcode space for Touch ID group, assuming the best case scenario for defenders, i.e., iPhone users. Considering the observed average passcode entropy in Touch ID group (14.61 bits) and the maximum possible difference between the groups (i.e., 1.91 bits), we can easily obtain the maximum possible average entropy in the Touch ID group (with 95% confidence), which is 16.52 bits.[5] Considering that for testing each passcode candidate on iPhones, an attacker must spend at least 80ms, they can brute-force the whole search space of 16.52 bits in size in about 2 hours.

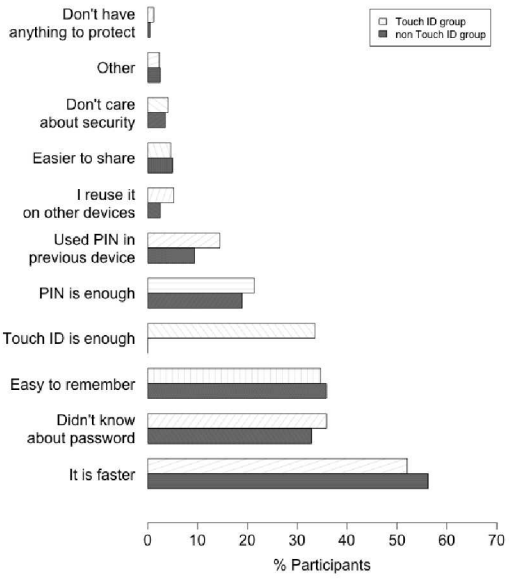

Figure 5: Reasons for using PIN instead of password for each group.

In order to test H_2 hypothesis, we split all 18 participants in the non-Touch ID group who did not lock their device on those who had Touch ID (4) and 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 in the two groups. Thus, we could not verify the correlation between the presence of Touch ID on the phone and the user's willingness to lock their device with a passcode.

7.4 Reasons for using PIN

In both groups, we asked users for reasons why they used a PIN rather than a password. A summary of participants' answers is shown in Figure 5. Note, that for this analysis we excluded the last option, i.e., "Touch ID is enough", from both groups, since it was only present in Touch ID group. Our analysis did not reveal any statistically significant difference in distributions of answers between the two groups (χ-squared = 4.88, p = 0.85).

The results of the statistical analysis suggested that users in both groups use similar reasons for using PINs. We found that the top most three reasons were either related to usability of PINs, 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 participants stated that Touch ID was

[5] As with Study I, this was an overestimation and real difference of search spaces is likely smaller. We chose to overestimate the search space to show the upper bound, i.e., the maximum work an attacker needs to do on average.

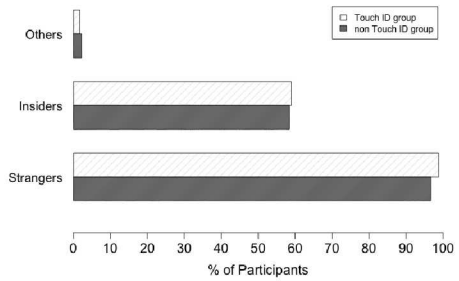

Figure 6: Distribution of actors (insiders and strangers) who our participants locked their iPhones against.

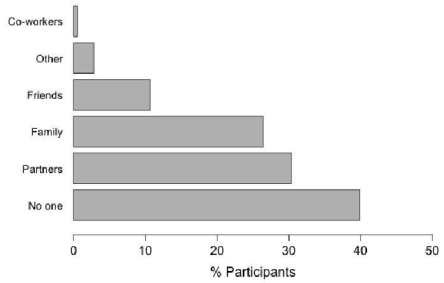

Figure 7: Distribution of passcode sharing with various groups of people (N = 374).

good enough for them from the security perspective.

7.5 Reasons for using Touch ID

Participants selected speed, convenience, and ease of use as the top three reasons for using Touch ID. Furthermore, more than 50% of participants stated that *security* provided by Touch ID was one of the reasons to use it. This suggests that the key factors that drive the adoption of Touch ID are due to its usability and perceived security. The summary of participants' answers is provided in Figure 10.

7.6 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 9 in Appendix C.2. Our analysis did not reveal any statistically significant difference between Touch ID and Non-Touch ID groups (χ-squared = 9.98, p = 0.13). Interestingly, almost all participants in both groups stated that they wanted to protect their device against *strangers* (see Figure 6). At the same time, participants 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. These results are in line with previously reported findings [32].

We also asked participants for how long they would want their data to be protected in case if someone steals their iPhone and tries to brute-force the passcode, in order to decrypt data. See question 27 in Appendix C.1.1 for the options that we gave to choose from. Note that for the observed average passcode entropy (i.e., about 15 bits, see Section 7.3 for details), we can show that it takes less than 44 minutes to search through the whole password space. Comparing the results with what users desired, we found, surprisingly, that the preferences of only 12% of our participants matched the strength of the actual protection. The remaining 88%, however, preferred the data to be protected for more than an hour. Even more, 48% of participants wanted the data to be protected for 40 years or *indefinitely*.

7.7 Passcode Sharing Behaviour

We asked our participants who they shared their iPhone passcodes with (Figure 7). We did not find 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. Overall, we found that 40% of participants did not share their passcodes with anyone. Others shared with different categories of related people. In particular, more than 25% of participants shared their passcodes with a partner or other family members. About 10% shared their passcodes with friends, while almost no one shared their passcodes with co-workers. In addition, 61% of all participants stated that they knew unlocking secret of someone else's smartphone.

7.8 Limitations

Online surveys have several limitations. First of all, in this study we asked Amazon Mechanical Turk participants to take a picture of their phone and send us a screenshot. This requirement introduced a bias in our survey toward more technically savvy users. We tried to mitigate this limitation by providing detailed instructions on how to make a screenshot. Second, Mechanical Turk users do not necessarily represent general iPhone users, thus, any generalization of the results from this study should be done carefully.

8. DISCUSSION

We first discuss the main result of the work, that is, the lack of correlation between the use of Touch ID and passcode entropy. We then proceed with a discussion of reasons why users do not take advantage of Touch ID and continue using weak passcodes. Finally, we conclude with a discussion of possible approaches to address the low adoption of stronger passcodes.

8.1 No Effect

Surprisingly, we did not find any statistically significant difference between the entropies of passcodes of those users who use Touch ID and those who do not. In addition, the results of our study suggest that the availability of Touch ID does not increase the ratio of users who lock their devices. At least, the effect is so small that we could not measure it. Under the assumption that use of Touch ID does result in the increase of passcode entropy by 1.91 bits (cf. see Section 7.3), our estimates show that, on average, an attacker would need to spend around 2 hours to brute-force the whole space of passcodes in an on-device attack. For the observed average entropies in both groups, i.e., around 15 bits, the attacker would only need 44 minutes to search through the whole space, which would meet desires of only 12% of our participants from Study III.

8.2 Reasons for Using 4-digit PINs

The second and the third studies allowed us to get a better understanding of reasons for users to stick with PINs. In particular, the results suggest that the main factors are (a) the lack of awareness that one can use password, and (b) usability considerations, e.g., ease of remembering, sharing, and typing. For instance, we found that more than 30% of our participants did not know that they can use passwords instead of PINs. Currently, during device initialization with iOS 8.3, one can setup only a PIN, even if Touch ID sensor is turned on. If the user wants to switch from PIN to password, she must do so by navigating to the corresponding settings, and only

after her iPhone setup is finished. Even more, our interview study revealed that some users have been guided by salespersons with setting up the device lock, hence, have not explored the passcode setup options. These findings suggest that currently the password option lacks visibility. First, this option should be made available during the setup process. Second, users should be told about this option, if they are assisted by a salesperson at the time of setup.

The remaining participants, approximately 70%, used PINs due to their higher usability. For example, more than 50% of participants stated that they used PINs, as they are faster to type than passwords. Furthermore, about 45% used PINs because they are easier to remember. This suggests that more research is needed to find a usable authentication method that allows users to create secrets that are stronger than PINs yet just as memorable. In addition, new methods should have speed and accuracy comparable to PINs. For instance, an investigation of passcode-composition policy affects, similar to the one by Komanduri et al. [27], can be conducted with a focus on smartphone unlocking. Also, an option of providing users with feedback on passcode strength might be a promising direction for future research.

Finally, we found that over 55% of participants share their passcodes with someone else, such as family members, friends, partners, etc. Participants stressed that they did so in order to enable those people to access their devices in case of emergencies. Given that Touch ID allows registering up to five fingers, it would be interesting to see if Touch ID could actually facilitate such sharing, possibly in a more secure way. In addition, our participants indicated that they were concerned that locking an iPhone makes it impossible to call from it a dedicated number, specified by the owner, when a lost phone is found. This suggests that certain features are still missing from the current mobile OSs.

8.3 Recommendations

We envision several approaches for improving the current state of passcode selection, when Touch ID available. First, considering that the user can only use a PIN during the setup of a new iPhone, Apple should allow or request users to create stronger passcodes when they set Touch ID. Also, if sales personnel helps users to setup their iPhones, they should explain to the customers the weaknesses of PINs and let them know about the password option.

Second, the results of our study suggest that most users do not understand how Touch ID works and how it impacts the security of the data-at-rest. In particular, our participants did not understand that Touch ID is just another path 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 better system image that facilitates the development of an adequate mental model. For example, showing that the time span of the data-at-rest protection depends only on the passcode might be one such improvement.

Third, the feedback on passcode strength can also be improved. Results of our investigation suggest that currently the preferences of only 12% of users roughly match the strength of the actual protection provided by their passcodes. It would be interesting to see if feedback on passcode strength might help users to choose appropriate passcodes.

Fourth, persuasion might be an effective option. For example, iPhone can show statistics to the Touch ID user on how often they actually use their passcode and suggest choosing a stronger passcode. Also, in order to alleviate the difficulty of retaining infrequently used passcodes in long-term memory [5], the OS can ask the user to type their passcode once every 2-3 days, in locations where it is easy to do so, e.g., at home or in office, but not on a bus, or in a car, or while the user is walking. Finally, one can employ gamification methods to motivate the choice of stronger passcodes, e.g., the user can get something (app, music, game, iCloud storage) for free as a reward.

Last but not least, our findings suggest that current mobile OSs miss important features that could impact users' choice with regards to locking their devices. In particular, the owner should be able to specify another phone number that can be called from a locked phone if someone finds it, in order to facilitate a return.

In addition, the ability to share device in a usable and secure fashion appears to be another important factor that impacts users' choice of passcodes. By providing a secure and usable way to share a smartphone, developers can enable users to pick stronger passcodes, yet being able to share their devices easily.

9. CONCLUSION

In this paper, we presented our investigation of Touch ID's impact on passcodes used for unlocking iPhones. 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 correlation between the use of Touch ID and the strength of users' passcodes. In particular, we observed that the average entropy was 15 bits, which corresponds to 44 minutes of work for an attacker to brute-force the whole search space, in order to find the correct password. Surprisingly, the preferences of only 12% of our participants matched the strength of the actual protection provided by passcodes. We also found that more than 30% of participants 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 passcodes on data-at-rest security and to increase the visibility of the password option. We plan to investigate the proposed research directions in future work.

10. ACKNOWLEDGMENTS

We would like to thank our reviewers and our colleagues for their help and constructive feedback on earlier versions of this paper. Constructive suggestions of our SOUPS shepherd Simson Garfinkel were very helpful in improving the paper.

11. REFERENCES

[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, GjÃÿvik University College*, 2012.

[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.

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

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

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

[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.

[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.

[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.

[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.

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

[11] CNN. iPhone encryption stops FBI, but not this 7-year-old. http://money.cnn.com/2014/12/01/technology/security/apple-iphone-encryption-fingerprint, December 2014. last accessed June 13, 2015.

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

[13] 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.

[14] 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.

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

[16] 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.

[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.

[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.

[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.

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

[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.

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

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

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

[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.

[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.

[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.

[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.

[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/. last accessed August 18, 2011.

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

[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.

[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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

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

[38] 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.

[39] T. Trimpe. Fingerprint basics. http://sciencespot.net/Media/FrnsScience/fingerprintbasicscard.pdf, June 2009. last accessed March 5, 2015.

[40] 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.

[41] 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.

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

APPENDIX

A. STUDY I: SUPLEMENTAL MATERIALS

A.1 Questionnaire

A.1.1 Inperson Interaction Script

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.1.2 Questions for both conditions

1. What is your age? [6]
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] Questions that does not have suggested possible answers are open-ended questions

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.

28. 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

A.1.3 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.1.4 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.1.5 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.2 Additional Results

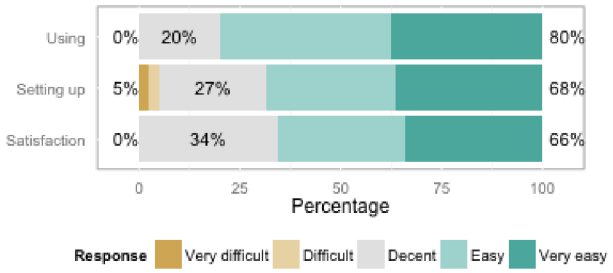

Figure 8: Touch ID participants' answers for questions "How hard was it to set up Touch ID?", "Is it easy to use Touch ID?" and "Overall, how satisfied are you with using Touch ID?" (n = 41).

B. STUDY II: INTERVIEW GUIDE

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?

C. STUDY III: SUPLEMENTAL MATERIALS

C.1 Survey Questions

C.1.1 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.

For PIN participants: 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

For password participants: 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:

26. 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-2d-3d-1w-2w-1m-2m-6m-1y-2y-5y-10y-20y-40y-indefinitely]

27. What is your gender?

(a) Female
(b) Male
(c) Prefer not to answer

28. What is your age?

(a) 19-24
(b) 25-34
(c) 35-44
(d) 45-54
(e) 55-64
(f) 65 or older

29. What is your highest level of completed education?

(a) High school
(b) College degree
(c) Bachelor
(d) Master or PhD
(e) Other, please specify

30. 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

31. What is your job title?

32. 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

33. Have you ever lost your smartphone?

(a) Yes
(b) No

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

(a) Yes
(b) No

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

(a) Yes
(b) No

36. 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.1.2 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.1.3 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.2 Additional Results

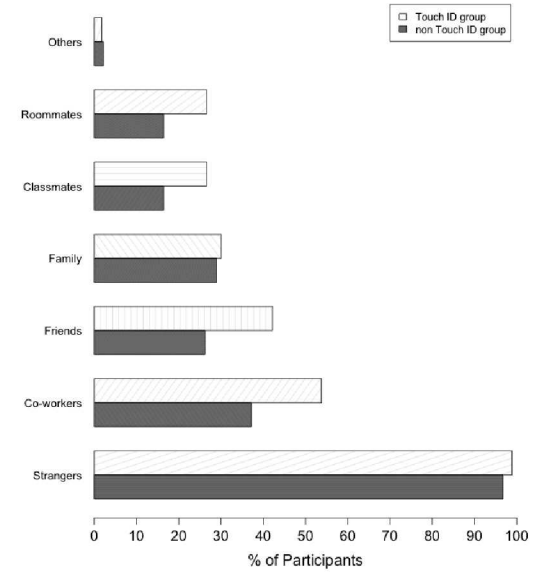

Figure 9: Actors who users lock their iPhones against, for Touch ID (n = 173), and non-Touch ID (n = 201) groups.

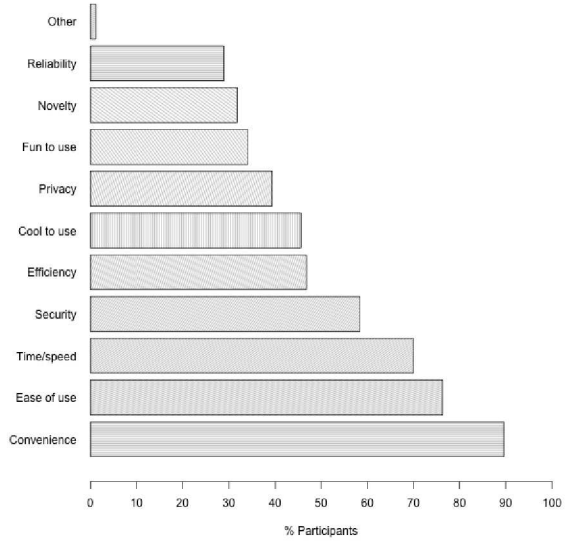

Figure 10: Reasons for using Touch ID (n = 173).