Investigating User Comprehension and Risk Perception of Apple's Touch ID Technology

Yousra Javed, Mohamed Shehab, and Emmanuel Bello Ogunu

November 6, 2016

Abstract

This paper investigates the user comprehension and risk perception of Apple's Touch ID technology. We conducted two user studies to assess perceptions in four domains: 1) security of Touch ID vs alternative unlock methods; 2) Touch ID authentication process for third party applications; 3) fingerprint access and storage; and 4) ease of circumventing Touch ID. We first conducted an in-person study with 30 participants. Our findings show that people perceive Touch ID to be more secure than other unlock/authentication methods, are unaware of the Touch ID authentication process for signing into applications, and have incorrect perceptions regarding the storage/access of their registered fingerprint before and after Touch ID authentication. We validated our findings from the in-person study through an online study over Amazon Turk on a more diverse and larger sample of 125 participants.

1 Introduction

Smartphones are being widely used today. Therefore, they contain massive amount of data about their users. They store all kinds of personal and business contacts, emails, and messages. Many users are now using their phones for banking and shopping as well, thereby storing credit card information on phones. This poses a serious threat to the security and privacy of user information if an adversary gets access to the device.

Many smartphone owners do not lock their devices with passcodes since they get in the way of their experience [11]. Fingerprint authentication on smartphones has been recently introduced as a fast and secure alternative to PIN/password. The first smartphone vendors to add fingerprint scanners to their handsets include Samsung, Huawei, and HTC. Apple introduced Touch ID in 2013, and was the first to implement the fingerprint authentication into the operating system. Apple's iPhone 5S is the first phone on a major US carrier since then to feature the Touch ID technology [10]. Touch ID is a seamless way to unlock the device by simply tapping a registered finger on the home button.

Touch ID not only enables users to unlock their devices, but also authenticates them in third party apps and authorizes purchases. The third party apps use the Local Authentication framework [1] to verify that the user is the owner of the device and, upon verifying, retrieve the username and password from the keystore. Due to the fact that a fingerprint is used during the authentication procedure, a misconception that Touch ID is used to authenticate the users in the apps is introduced. Moreover, since the app sits inside the phone, there is an assumption that app authentication using Touch ID is the same as the unlocking the phone.

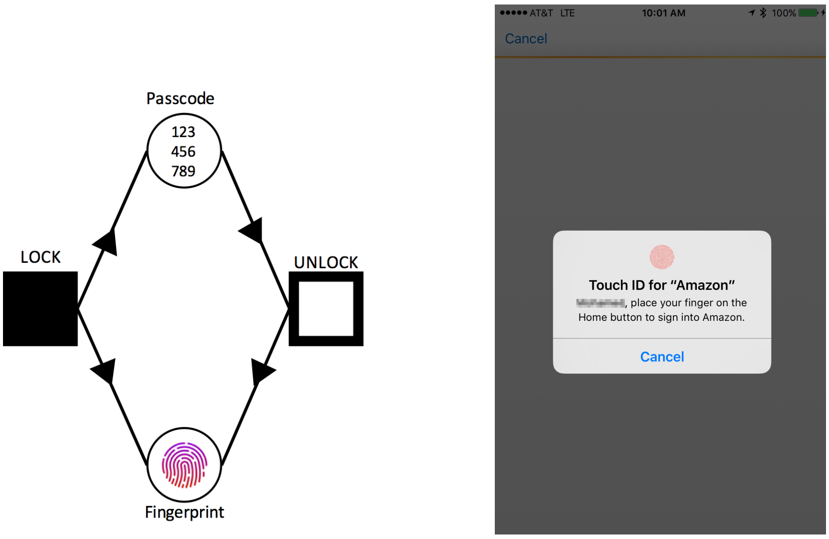
The Touch ID authentication takes place on the device. The fingerprint data is only stored on the Secure Enclave [2] of the device's chip, and is not stored on Apple servers or iCloud. The fingerprint data is never shared with or accessed by any application on the device, and it never leaves the device.

Touch ID adds a layer of security to the Apple device if PIN/password is not used. However, Touch ID can be bypassed using passcode. One way of achieving this is by leveraging the feature of multiple finger registration on the device. Multiple finger registration was added to improve the usability of Touch ID. However, if the adversary gets access to user's passcode, they can register their own fingerprint to allow them to unlock the device in the future, even if the PIN/passcode is changed. Similarly, the user's fingerprint can be photographed from a glass surface, to create a fake fingerprint that could unlock a Touch ID enabled device [6].

In this paper, we investigate the user comprehension and risk perception of Apple's Touch ID technology. We first conduct an in-person study with 30 participants. Our findings show that people perceive Touch ID to be more secure than other unlock/authentication methods, are unaware of the Touch ID based authentication process for third party applications, and have incorrect perceptions regarding the storage/access of their registered fingerprint before and after Touch ID authentication. To confirm our findings on a larger and more diverse sample, we performed another study over the crowdsourcing website, Amazon Mechanical Turk (MTurk) and tested our hypotheses on 125 participants. Our MTurk study findings corroborated with those of the in-person study.

2 Background

We begin this section with a description of Touch ID and how it is used. We then briefly explain the related hardware components and security design.



Touch ID for "Amazon"

[redacted], place your finger on the Home button to sign into Amazon.

Cancel

(a) Mechanisms of unlocking an Apple device

(b) Touch ID popup in the Amazon app

Figure 1

2.1 Using Touch ID

2.1.1 Device lock/unlock

Touch ID is Apple's biometric authentication mechanism that utilizes a fingerprint sensor built into the Home button of an Apple device. Its use is meant to increase security in Apple devices where a passcode (representing either a PIN or alphanumeric password) was formerly not used at all [3]. That is because configuring Touch ID requires setting a passcode. Using Touch ID is designed to minimize entering a passcode, thereby making the authentication process faster and easier, but a passcode is still required for additional security validation, such as when the device is restarted or when more than 48 hours have passed since unlocking the device. Therefore, entering a passcode and using a fingerprint are two independent mechanisms to unlock a device or be authenticated by a third party app (see Figure 1a). Enrolling a fingerprint with Touch ID involves placing the finger on the Home button repeatedly, making small adjustments to the position of the finger each time until a comprehensive fingerprint image has been captured. Up to five fingerprints can be stored by Touch ID.

2.1.2 User authentication in third party applications

In addition to device lock/unlock, Touch ID is being used by the third party developers to authenticate registered users into their application. Banks are using Touch ID based on the assumption that the Bank user's fingerprint is tied to the device, and only the user can unlock it. However, anyone whose fingerprint is registered on that device can essentially unlock the device and be authenticated as the owner of that Bank account. Touch ID based user authentication for applications works as follows:

- Step 1: User signs into the application for the first time using his username and password. The user's account credentials are then stored in the secure keystore

- Step 2: Once the user enables Touch ID for third party applications, all subsequent sign-ins to the application are done through Touch ID. The Touch ID pop up appears on the application's sign-in activity, (see Figure 1b), where the user taps a registered finger on the home button, and is verified by the third party application through the Local Authentication Framework as being the owner of the device.

- Step 3: If the user is verified as the owner of the device, their username and password is securely retrieved from the keystore and is used to authenticate the user

A similar procedure is performed to authenticate the user and make purchases in the iTunes Store, App Store, and iBooks Store, as well as to make Apple Pay purchases in physical stores.

2.2 Hardware & Security

The hardware components that contribute to Touch ID include a laser-cut sapphire crystal, built into the Home button, which acts as a sensor and protects the lens, along with a steel capacitative ring to detect the user's finger [2]. Upon contact with the ring, the sensor captures a high-resolution image from small sections of the fingerprint, which is then converted into a mathematical representation. This mathematical representation is encrypted, and carried over a hardware channel to a "Secure Enclave" on the chip in the device for authentication. This

Secure Enclave is the only location where the fingerprint data is stored, and not on any Apple servers or iCloud, nor within any application; additionally, the fingerprint authentication process only takes place locally on the device, and not within any application. During this process, the captured fingerprint data is compared with the stored fingerprint data to determine a match. If there is a match, a "yes" token is released, and authorization is enabled. Upto five unsuccessful fingerprint matches are allowed before the device prompts for a passcode in order to proceed.

3 Related Work

3.1 Locking behaviors in smartphones

Egelman et al. conducted a series of qualitative interviews and online experiments to examine why users choose to employ locking mechanisms, ranging from PIN/passcode and pattern to fingerprints [8]. They found a strong correlation between use of locking methods and risk perceptions, with a major reason for not locking smartphones including not believing there was any data worth protecting. This demonstrated that many users did not understand the extent to which their stored data could pervade their online and offline identity. Additionally, Van Bruggen et al. evaluated the ability to influence change in pattern-based and text-based locking mechanisms [13]. While two-thirds of those sampled secured their devices without prior interventions, any induced interventions had only limited impact, particularly when security was the intended source of influence. Karthikeyan et al. investigated locking behaviors specifically surrounding Touch ID as compared to PINs. This was done in order to determine whether fingerprint-based authentication is more likely to gain greater adoption than traditional PINs [9]. They found that the usability of fingerprint-based authentication over PIN-based could be a significant influencer to increased adoption of locking behavior, compared to the population of people who avoid locking at all. Cherapau et al. conducted a related study on the impact of Touch ID on iPhone passcodes[5]. While there is an expectation that using Touch ID allows users to employ stronger passcodes [3], results showed that they do not take advantage of this.

3.2 User perceptions of biometric authentication

There has been work on analyzing the usability, user perceptions, and decision factors regarding the adoption of existing authentication mechanisms on smartphones. Bhagavatula et al. studied the iPhone's Touch ID and Android's Face unlock [4]. They found that people perceive fingerprint as more secure than Face unlock and prefer it due to the difficulty of using Face unlock in certain scenarios. De Luca et al. conducted an Amazon Turk study on the decision factors behind using or discontinuing the use of biometric authentication on smartphones [7]. They focused on iPhone's Touch ID and Android's Face unlock mechanism and found that usability (convenience and ease of use over entering PIN) is an important factor in influencing the decision to choose which biometric authentication to use. On the other hand, privacy and trust were not considered as important factors. Trewin et al. examined facial, voice, and gesture based biometric authentication [12]. Their analysis showed that gesture was the most reliable and voice was the least usable.

4 Hypotheses and Methodology

Touch ID allows a fingerprint to be associated with a user's device, whereas a passcode is normally associated with a user's account on specific third party applications. When Touch ID is used to authenticate with these apps, however, it introduces this mental model that the fingerprint and passcode are interchangeable methods of authentication. Herein lies the root of the potential misconceptions regarding use and risk associated with Touch ID. While this might be considered a safe assumption due to the fact that the applications sit on the device, in reality the owner of the device is not necessarily always the user associated with all the applications on a device. Moreover, all of the fingerprints registered on the device may not belong to the actual owner of the device. Hence, we have observed that it is possible for a user, who may or may not be authorized to use the device, to be authenticated as an intended user of an application on the device if their fingerprint is registered with Touch ID. Consequently, we formulated the following hypotheses in order to drive our investigation of whether Touch ID users lack comprehension and risk perception of Touch ID technology:

H1 ***Users perceive that Touch ID is more secure than other smartphone authentication mechanisms***

H2 ***Users are not aware of how the fingerprint is being used during the Touch ID based authentication process for third party applications***

H3 ***Users are not aware of where their fingerprint is stored and how it is accessed during Touch ID authentication***

H4 ***Users perceive that it is not possible for someone other than the owner to unlock the Touch ID-enabled device and make a purchase with their fingerprint***

In order to evaluate our hypotheses, we first conducted an in-person study.

4.1 In-Person Study

4.1.1 Task 1 - Fingerprint enrollment and passcode creation

The participants were provided with an iPad mini 4 device running iOS 9.2.0 and were asked to configure Touch ID by creating a passcode and enrolling a fingerprint. They were then required to lock/unlock the iPad using their registered fingerprint to verify successful enrollment.

4.1.2 Task 2 - Perceptions about Touch ID based unlock/authentication, fingerprint access/storage, and ease of circumvention

After completing the first task, the participants completed a short survey, which comprised of questions assessing demographics, their security consciousness, and their familiarity with Touch ID. They were then asked to install the Amazon application (version 5.4.0 at the time of our study) which implements TouchID to allow users to be authenticated with their Amazon account. The participants signed up for or logged into their Amazon account, and performed the steps involved in an in-app purchase using Touch ID. We used the Amazon app to highlight the misconceptions surrounding authentication using Touch ID by third party apps. Once the prompt for Touch ID was displayed prior to making a payment on Amazon, as seen in Figure

1b, participants were asked to complete a post-survey comprising of questions directly related to the purchase scenario, which evaluated their understanding of how the Touch ID was used in device unlock and Amazon authentication, how the fingerprint was being stored/accessed during the purchase transaction, and how easy it is for an intruder to circumvent Touch ID to unlock the device and make purchase.

More specifically, the post-survey questions related to each of our four hypotheses are as follows:

Q-H1 For the first hypothesis, we posed four questions to study participants, regarding the security of Touch ID over other unlocking/authentication mechanisms. First, we asked participants to choose which method they believed to be the most secure from a list of the most common methods. We also asked participants to explicitly evaluate whether Touch ID was more secure than using a PIN/password, on a Likert-scale from Strongly Disagree to Strongly Agree. Then we asked them to evaluate on a Likert-scale from Very Difficult to Very Easy the feasibility of bypassing Touch ID. Lastly, we asked if they believed anyone could use his/her fingerprint to get into the participant's device using Touch ID.

Q-H2 For the second hypothesis, we posed two questions to the participants: (1) Is being authenticated by your fingerprint the same as by your username/password? and (2) Is your fingerprint being used by Amazon to authenticate you during this transaction? For both of these, the possible responses were "Yes," "No," and "I don't know".

Q-H3 The in-person study presented the participants with a scenario that involved using Touch ID to make a purchase in the Amazon App. Hence, the survey questions related to fingerprint storage were (1) Where is the fingerprint stored *before* the payment transaction? and (2) Where is the fingerprint stored *after* the transaction? Regarding fingerprint access, we asked participants (3) Who has access to your fingerprint *during* the payment transaction? For each question, the possible responses included iPhone, iCloud account, Apple server, and Amazon server; participants could select all that they believed applied.

Q-H4 For this hypothesis, we posed four questions regarding the feasibility of bypassing Touch ID, each with a slightly different variation as seen in Table 3. These questions dealt with who the device owner is, who the Amazon account holder is, and whose fingerprint is being used. For each question, the participant was asked whether it would be possible to make a purchase.

4.1.3 Task 3 - Fingerprint management

The third task was related to participant perceptions regarding fingerprint management. We told the participants that we were able to eavesdrop over their shoulder and figure out the passcode they created as part of Task 1. Therefore, we were able to unlock the iPad using their passcode and register a new fingerprint to allow us to use Touch ID. Based on this attack vector information, the in-person study participants were asked additional questions related to bypassing Touch ID (H4). Specifically, the participants were asked whether they believed (1) we could unlock the device and potentially make a purchase without their PIN/password if our fingerprint was registered, and (2) that by changing the PIN/password, they would be able to protect against a stranger completing this action with a fingerprint already registered.

Once the participants responded to the above questions, we enrolled our own fingerprint with Touch ID and demonstrated the unlocking action, asked them to change the PIN/ password, and then again demonstrated the attack by unlocking the device.

Participants received a $5 Amazon gift card for participating in the study. The study took approximately 20 minutes to complete. We recruited our participants through mass distribution emails and flyers around campus. Respondents were screened for eligibility based on ownership of a Touch ID enabled device.

4.1.4 Participant Demographics

A total of 30 participants completed the study. The participants were university students aged 18-35 years. 50% of the participants were male and 50% were female. A majority of the participants had used Touch ID for at least 6 months. Since our participant pool consisted primarily of students in the 18-35 age group, we conducted a second study to validate our results on a diverse and larger sample size.

4.2 Online Study

We conducted a second study over MTurk. Due to the study being conducted online, we modified some of our in-person study tasks.

4.2.1 Task

Each participant first answered a set of questions about demographics, security consciousness, and familiarity with Touch ID (similar to Task 2 of the in-person study). The participants then observed a short video demonstrating the same scenario that the in-person participants had to complete, i.e., logging into an Amazon app account, and making a purchase using Touch ID. After watching the video, the participants were asked to complete a post-survey related to the demonstrated scenario. The survey questions were the same as the ones in the in-person study, and evaluated participant understanding of how the Touch ID was used in device unlock and Amazon authentication, how the fingerprint was being stored/accessed during the purchase transaction, and how easy it is for an intruder to circumvent Touch ID to unlock the device and make purchase.

To ensure recruitment of valid owners of Touch ID enabled Apple devices, the participants were first asked to answer a set of questions to confirm their eligibility. In addition, they were required to complete another verification task at the end of the study to confirm that they owned a Touch ID-enabled iPhone. Similar to Cherapau et al., the verification task required each participant to provide (1) a picture of their iPhone, taken using the front-facing camera in front of a mirror, and (2) a screenshot of their iPhone's lock screen with the masked PIN/password entered [5]. We set up our study as an HIT. The HIT took approximately 10-15 minutes to complete, for which each worker was paid a fee of $0.50.

4.2.2 Participant Demographics

A total of 155 participants completed the HIT. However, after eligibility verification, we selected the responses of 125 participants based on their answers to the attention check questions and iPhone verification task. The male/female participant ratio was close to 50%/50%. Similarly, the participants fell in all three age groups, i.e.,18-35, 35-50, and >=50, as opposed to the in-person study. However, both samples had two ethnic groups in majority–i.e., asian/pacific islander and white/caucasian. The online sample was also more diverse w.r.t duration of Touch ID use.

5 Results

5.1 Hypothesis 1

Touch ID users perceive that Touch ID is more secure than other smartphone authentication mechanisms

We observed that 70% of the in-person study participants reported Touch ID to be more secure, over other unlock/ authentication mechanisms. Similarly, 57.6%, of the online study participants reported Touch ID to be more secure as compared to alphanumeric password, eye recognition, 4-digit and 6-digit PIN (See Figure 2a).

Regarding Touch ID being more secure than using a PIN/ password, 86.6% of the in-person participants Agreed or Strongly Agreed to Touch ID being more secure than using a PIN/password (See Figure 2b). Similarly, 71.2% of the online study participants responded with Touch ID being more secure than using a PIN/password.

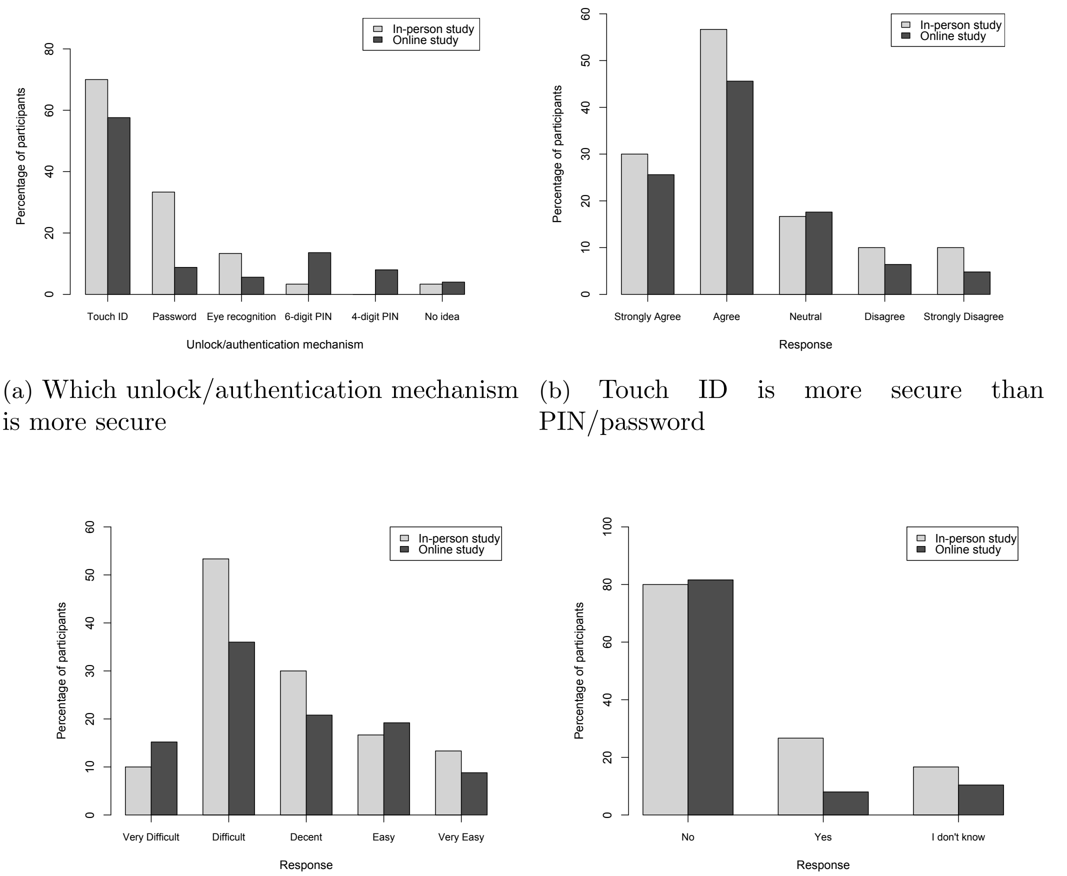
Our analysis of perception regarding the feasibility of bypassing Touch ID showed at least 50% participants in both in-person and online study perceived it to be Difficult or Very Difficult to bypass Touch ID (See Figure 2c). Lastly, we asked if the participants believed that anyone could use his/her fingerprint to get into the participant's own device using Touch ID. 79.3% of the in-person study participants reported 'No'. However, 81.6% of the online study participants perceived that a stranger could not use his/her fingerprint to get into the participant's own device using Touch ID (See Figure 2d) .

Overall, these statistics confirmed that user perception regarding Touch ID trends towards it being more secure than other authentication mechanisms.

5.2 Hypothesis 2

Touch ID users are not aware of how the fingerprint is being used in the Touch ID based authentication process for third party applications

To evaluate this hypothesis, we analyzed participant responses to two fingerprint authentication process related questions from the post-survey. Table 1 shows the participant responses to these questions. Since each of these questions could be considered a single categorical variable with two groups, this required a single-sample non-parametic test. Consequently, we used a Chi-square goodness-of-fit test to determine whether the distribution of cases for each question follows a known or expected distribution. We hypothesized that an equal proportion of participants would believe that fingerprint authentication was equivalent to PIN/password authentication, and also believe that Amazon used their fingerprint to authenticate. Since no standard or known proportion of Touch ID users exists for these cases, we believed the probability that at least half of users would hold incorrect assumptions about Touch ID authentication was a reasonable assumption. We use the same expected distribution for other Chi-square goodness-of-fit



(a) Which unlock/authentication mechanism is more secure

(b) Touch ID is more secure than PIN/password

(c) Feasibility of bypassing Touch ID

(d) Feasibility of a stranger unlocking participant's device using their fingerprint

Figure 2: Participant perceptions of the security of Touch ID over other unlocking/authentication mechanisms

tests conducted.

We hypothesized that approximately half of our participants would believe that fingerprint authentication was equivalent to PIN/password authentication, and also believe that Amazon used their fingerprint to authenticate them.

Chi-square goodness-of-fit test on perceptions regarding authentication with fingerprint being the same as username/password showed that 50% of the in-person study participants incorrectly perceive/or are unsure that being authenticated by fingerprint on a Touch ID enabled device is the same as being authenticated by username/password. Therefore, these perceptions do not differ significantly from the hypothesized (50%,50%) values that we supplied ($\chi^2(1) = 0.53$, p = 0.465). However, more than 50% of the online study participants had the incorrect perception ($\chi^2(1) = 9.8$, p = 0.001745).

Similarly, Chi-square goodness-of-fit test on perceptions of whether fingerprint was being used by Amazon to authenticate the participant during the purchase transaction showed that 50% of the in-person study participants incorrectly perceive/or are unsure that Amazon has

Questions & Responses		*% of participants (in-person study)*	*% of participants (online study)*
Is being authenticated by your fingerprint the same as by your username/password?	Yes No I don't know	56.6 30 13.3	61.6 27.2 11.2
Is your fingerprint being used by Amazon to authenticate you during? this transaction	Yes No I don't know	60 26.66 13.33	77.6 14.4 8

Table 1: Responses to survey questions regarding Touch ID authentication process perception for the in-person and online study.

access to their fingerprint in order to authenticate them during the purchase transaction. Therefore, these perceptions do not differ significantly from the hypothesized (50%,50%) values that we supplied ($\chi^2(1) = 1.2$, p = 0.273). However, more than 50% of the online study participants had this incorrect perception ($\chi^2(1) = 45$, p = 1.97e-11).

5.3 Hypothesis 3

Touch ID users are not aware of where their fingerprint is stored and how it is accessed during authentication

Question	*iPhone (%) In-Person*	*Other (%) In-Person*	*iPhone (%) Online*	*Other (%) Online*
Where is your fingerprint stored BEFORE purchase?	53.33	46.66	56	44
Where is your fingerprint stored AFTER purchase?	46.66	53.33	48	52
Who accesses your fingerprint DURING purchase?	46.66	53.33	41	58

Table 2: Participant perceptions of fingerprint storage before/after, and fingerprint access during the Touch ID-based Amazon in-app purchase transactions

To evaluate this hypothesis, we analyzed participant's recoded responses to two fingerprint storage/access questions from the post-survey (Table 2). We evaluated each set of responses as a single categorical variable with two groups, which required the Chi-square goodness-of-fit test. We also evaluated these sets of responses as two related groups (*before* and *after*) with the same dichotomous dependent variable (storage location). In other words, we sought to determine whether the proportion of participants who believed the fingerprint was stored on the iPhone only *before* the transaction significantly decreased *after* the transaction. This comparison required the use of McNemar test–a nonparametric test specifically for two related sample cases.

The Chi-square goodness-of-fit test result for the question regarding fingerprint storage *before* an Amazon transaction was not statistically significant for the in-person ($\chi^2(1) = 0.133$, p = 0.715) and online responses ($\chi^2(1) = 0.76923$, p = 0.3805), nor was the result significant for fingerprint storage *after* the transaction for the in-person ($\chi^2(1) = 0.133$, p = 0.715) and online responses ($\chi^2(1) = 0.2$, p = 0.6547). This means that for both of these, we do not reject the null hypothesis, and confirm that our estimated proportion of users who correctly understand where the fingerprint is stored compared to those who do not is accurate at 50%/50%. For the McNemar test conducted to determine if there was a significant change in that proportion from *before* to *after*, the transaction resulted in a p-value greater than 0.05 for both the in-person and online responses, and therefore deemed not statistically significant.

Lastly, for the question regarding fingerprint access *during* the transaction, the Chi-square goodness-of-fit test result was not statistically significant in the in-person ($\chi^2(1) = 0.133$, p = 0.715) or the online responses ($\chi^2(1) = 3.528$, p = 0.06034). Therefore, we were correct in assuming that the proportion of users who are unaware of how authentication with Touch ID works is approximately 50%; these are the users who perceive the fingerprint to be accessed by iPhone and/or other entities (Apple server, iCloud server, Amazon server).

Questions & Responses		*In-person (%)*	*Online (%)*
Can someone use HIS/HER fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone?	No Yes I don't know	80 16.66 3.33	84 5 11
Can someone use YOUR fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone?	No Yes I don't know	53.33 30 16.66	65 14 21
Can someone use YOUR fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?	No Yes I don't know	83.33 46.66 3.33	76 9 15
Can someone use HIS/HER fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?	No Yes I don't know	70 16.66 13.33	78 5 17

Table 3: Responses to survey questions regarding perceptions on the ease of getting into a Touch ID-enabled device and making a purchase

5.4 Hypothesis 4

Touch ID users perceive that it is not possible for someone other than the owner to unlock the Touch ID-enabled device and make a purchase with their fingerprint

We analyzed the participant responses to four questions shown in Table 3. Each of these questions were evaluated using the Chi-squared goodness-of-fit test, and we found that for all of them, the p-value was less than .05. This means that there was a significant difference between our expected proportion of 50%/50% and the actual proportion regarding users who responded accurately regarding the possibility of each of these.

Chi-square goodness-of-fit test on perceptions of whether a stranger could use their own fingerprint to make a purchase on the Touch ID enabled device owner's phone using the owner's Amazon account showed that more than 50% of the participants incorrectly perceive/or are unsure that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible. This was the case for both the in-person and the online study. Therefore, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied (for in-person: $\chi^2(1) = 13.33$, $p < 0.0001$; for online: $\chi^2(1) = 84.872$, p = 2.2e-16).

Similarly, Chi-square goodness-of-fit test on perceptions of whether a stranger could use the Touch ID enabled device owner's fingerprint to make a purchase using the owner's Amazon account on the owner's phone showed that more than 50% of the participants incorrectly perceive/or are unsure that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible. Therefore, once again, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied in both studies (for in-person: $\chi^2(1) = 4.8$, p = 0.028; for online: $\chi^2(1) = 60.552$, p = 7.166e-15).

Chi-square goodness-of-fit test on perceptions of whether a stranger could use the Touch ID enabled device owner's fingerprint to make a purchase using the owner's Amazon account on the stranger's phone again showed that more than 50% of the participants correctly perceive that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible or are unsure. Therefore, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied (for in-person: $\chi^2(1) = 16.13$, $p < 0.0001$; for online: $\chi^2(1) = 78.408$, p = 2.2e-16).

Similarly, Chi-square goodness-of-fit test on perceptions of whether a stranger could use their fingerprint to make a purchase using the participant's Amazon account on the stranger's phone again showed that more than 50% of the participants correctly perceive that a stranger cannot make a purchase in this scenario, while the rest perceive it to be possible or are unsure. Therefore, these perceptions differ significantly from the hypothesized (50%, 50%) values that we supplied (for in-person: $\chi^2(1) = 13.33$, p= 0.0002; for online: $\chi^2(1) = 84.872$, p = 2.2e-16).

Lastly, we conducted a Chi-squared goodness-of-fit test on the two separate set of responses related to the demonstrated attack vector. For the first question, regarding if we would be able to unlock the device and make a purchase on their account with our fingerprint, we found that the result was significant ($\chi^2(1) = 7.258$, p = 0.007), meaning it differed from the hypothesized proportion. This is what we expected, however, as we anticipated most participants would realize this was possible, and so our 50%/50 % proportion would not hold here. For the second question, however, the result of the goodness-of-fit was not significant ($\chi^2(1) = 1.581$, p = 0.209), meaning our expected proportion of those who would incorrectly assume a PIN change would help was indeed about 50%. We also conducted a McNemar test between the two sets of responses to determine whether the proportion of participants who believed we could bypass their Touch ID with our fingerprint would decrease based on the PIN change on the device. This test resulted in a p-value of 0.035, which confirmed that the proportion did decrease, meaning a larger proportion of participants incorrectly believed that changing the PIN would solve the demonstrated issue.

5.5 Limitations

While our results were significantly positive, our studies were not without a few limitations. For example, the sample of participants for both the in-person and online study were in the age range of 18-35, which arguably limits how generalizable our results are overall. Along those lines, the participants in the online study who completed the HIT might not necessary represent the general iPhone users. Additionally, we suspected that other data we collected, such as duration of Touch ID, technical expertise, or proficiency as iOS developers, may have had some influence on the perceptions that users have regarding Touch ID; for both studies, however, the homogeneity of our sample with respect to these variables was such that we were unable to make a proper evaluation of the impact that varying levels of these factors may have. Lastly, while our sample for the online study was sizable, we had anticipated an even greater amount of participants. It is possible that the additional verification requirement of uploading two iPhone photos could have been a deterrent to additional participants.

6 Discussion

In this section, we review the main findings of the work presented in this paper, and hypothesize why users' comprehension and mental model regarding risk perception may be as such.

Our results demonstrate that participants' comprehension of how Touch ID works is somewhat misguided, such that it may provide an undue sense of increased security. Users perceive that Touch ID is more secure than other authentication mechanisms, even without properly understanding how it works or where this data is stored. This perception of decreased risk could be dangerous, particularly for the many users who already underestimate the level of sensitive and personally identifiable information that is stored on their devices. Given that the notion of biometric authentication relies on something you are (in this case, your fingerprint), which is generally harder to spoof than something you have (like a smart card) or something you know (like a PIN or password), a plausible reason for users' assumption that Touch ID is secure enough could be based on the fact that they believe their fingerprint cannot be replicated by anyone else. However, the way Touch ID is designed, there is no association with a specific fingerprint and the actual original owner of a device. Hence, replicating a specific fingerprint is not necessary. To the device, all fingerprints stored on a device are considered authorized, whether they belong to one person or to many. Whether intended or not, multiple people could have the same level of privilege when it comes to accessing the device and using the features that require authentication. Hence, it may take more than user awareness, but also system-level changes to Touch ID in order to match users' mental model and ensure their security and privacy.

7 Conclusion

In this paper, we demonstrated that at least 50% of the Touch ID user base lacks the proper comprehension of Touch ID in relation to the fingerprint storage/access, authentication by third party applications, and the ease of bypassing the technology. We first performed an in-person study on 30 participants to test our hypotheses. Our findings show that people perceive Touch ID to be more secure than other unlock/authentication methods, are unaware of the Touch ID authentication process for third party applications, and have incorrect perceptions regarding the storage/access of their registered fingerprint before and after Touch ID authentication. We also demonstrated an attack vector showing how to bypass Touch ID. To validate the results of our in-person study on a diverse sample, we then conducted an online study on 125 participants. Our results from the online study matched those from the in-person study.

References

[1] Local authentication framework. `https://developer.apple.com/reference/localauthentication`.

[2] Apple. About touch id security on iphone and ipad, 2016. `https://support.apple.com/en-us/HT204587`.

[3] Apple. Use touch id on iphone and ipad), 2016. `https://support.apple.com/en-us/HT201371`.

[4] 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. *Proc. USEC*, 2015.

[5] I. Cherapau, I. Muslukhov, N. Asanka, and K. Beznosov. On the impact of touch id on iphone passcodes. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 257–276, 2015.

[6] C. C. Club. Chaos computer club breaks apple touchid, September 2013. `http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid`.

[7] 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 *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 1411–1414. ACM, 2015.

[8] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 750–761. ACM, 2014.

[9] S. Karthikeyan, S. Feng, A. Rao, and N. Sadeh. Smartphone fingerprint authentication versus pins: A usability study, 2014.

[10] C. Newton. Apple's new iphone will read your fingerprint, September 2013. `http://goo.gl/qDTtQL`.

[11] G. Smith. Fingerprints could be solution for half of iphone owners who don't lock their phones, September 2013. `http://www.huffingtonpost.com/2013/09/13/apple-locks-iphone_n_3908614.html`.

[12] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference*, pages 159–168. ACM, 2012.

[13] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy. Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 10. ACM, 2013.