

TOWARDS EFFECTIVE THIRD-PARTY APPLICATION DIALOGS:
SOLUTIONS FOR IMPROVED ATTENTION AND COMPREHENSION

by

Yousra Javed

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing and Information Systems

Charlotte

2017

Approved by:

Dr. Mohamed Shehab

Dr. Bei-Tseng Chu

Dr. Heather Lipford

Dr. Samira Shaikh

ABSTRACT

YOUSRA JAVED. Towards Effective Third-Party Application Dialogs: Solutions for Improved Attention and Comprehension. (Under the direction of DR. MOHAMED SHEHAB)

Computer security dialogs communicate important information to users. One avenue where such dialogs are presented are third-party applications, which play an important role in enhancing a user's experience and are popular in online social networks and smartphones. The first category presented by these applications are the permission authorization dialogs that request access to user information. The second category are the terms and conditions dialogs that describe the applications' policies regarding user information.

Research has demonstrated that users have a strong tendency to ignore security dialogs, resulting in uninformed decisions. Unlike physical warnings, whose design and use is regulated by law and based on years of research, computer security dialogs are often designed in an arbitrary manner. This research examines two human factors that cause users to ignore these dialogs. Habituation—a key factor behind users' inattention towards dialogs—is a form of learning in which an organism decreases or ceases to respond to a stimulus after repeated presentations. User mental models, the second factor, are an integral part of what drives their behavior. Based on their limited understanding, users form incorrect perceptions about how their information is accessed and used.

This dissertation proposes solutions that address human factors in third-party application dialogs and conducts user experiments to evaluate them. It makes three

contributions to improve third-party application dialogs regarding two information processing stages of the human in the loop framework: (1) attention switch and maintenance, and (2) comprehension.

The first contribution proposes two new dialog designs to improve attention and resist habituation towards permission authorization dialogs presented by third-party applications on a popular online social network, Facebook. The first design investigates the use of animation. It uses a real-life analogy and leverages the end-user's personal information examples to communicate the potential information disclosure in the event of permission authorization. The second design uses eye-gaze data from the eye-tracker as a mechanism of ensuring that the user reads the requested permissions before authorizing access to sensitive information.

The second contribution investigates advertisements as a potential environmental stimulus that can impede user attention towards the authorization dialog. A user experiment is conducted on the mockup of a popular gaming website to measure user attention in the presence and absence of advertisements comprising of four types of content, namely, food, shopping, politics, and sports.

The third contribution focuses on improving comprehension of the terms and conditions dialog, specifically the dialog displayed by Touch ID-enabled iOS applications. First, the potential misconceptions regarding Touch ID-based authentication with third-party applications are investigated. Second, four dialog designs are proposed to improve comprehension of the Touch ID terms and conditions dialog, specifically the information related to discovered misconceptions of fingerprint data access, application account access by others, and the role of fingerprint in Touch ID-based sign-in.

ACKNOWLEDGMENTS

Imagination is more important than knowledge. For knowledge is limited, whereas imagination embraces the entire world, stimulating progress, giving birth to evolution.

-Albert Einstein

If there is one trait that I have acquired over the course of my doctoral program, it would have to be imagination and thinking outside the box. This attribute together with persistence and perseverance has been crucial to this dissertation's success. Although this journey has been mine alone, many colleagues, friends, and family have walked it with me. Therefore, I would like to acknowledge those who have contributed directly or indirectly towards its completion.

First and foremost, I would like to express my indebtedness to my advisor, Dr. Mohamed Shehab. His continuous guidance and support has made this work possible. Each meeting taught me something new, be it problem solving, writing and presentation skills, analyzing data, or managing students. I was fortunate enough to work with such an enthusiastic and optimistic mentor; not only did he help me grow as an independent researcher and develop professional skills but also opened the doors for various opportunities at UNC Charlotte. I established collaborations with numerous researchers in and outside UNC Charlotte throughout my doctoral program. Moreover, he helped me gain the much needed teaching experience by serving as an instructor for courses such as introduction to information security, and mobile application development.

Furthermore, I would like to thank my dissertation committee members: Dr. Bei-

Tseng Chu, Dr. Heather Lipford, and Dr. Samira Shaikh. Their assistance, feedback, and guidance has been invaluable in preparing this work. I sincerely appreciate Dr. Lipford's helpful feedback in user study design and analysis.

The work in this dissertation would not have been possible without the funding I received from various sources, including the Graduate Assistant Support Plan (GASP) and the P.E.O. International Peace Scholarship (IPS) fund. This significant support allowed me to focus and continue my research without worrying about the financial demands of my program.

My sincere thanks goes to those who have collaborated with me on various research projects throughout the past few years. The list is long but I would like to particularly mention Dr. Boyd Davis, Dr. Heather Lipford, Dr. Emmanuel Bello Ogunu, Dr. Hakim Touati, Niranjan Ravichandran, Chad Ramsey, and Adharsh Desikan. The output of these collaborations has been crucial to my professional development. I learnt numerous skills while working with each one of these researchers.

I would also like to mention the efforts of UNC Charlotte staff whom I asked for help approximately a billion times either in-person or via email. I was always fascinated by how fast Kimberly Lord, and Sandra Krause would respond and resolve my problems be it related to paperwork or degree requirements. They will continue to impress me with there management skills.

My journey towards this dissertation has introduced me to several bright graduate students. The existence of this social circle has been vital to staying motivated all these years. I appreciate the efforts of these colleagues in helping me in anyway they could whenever I needed it. In no particular order, these colleagues include

Abeer AlJarrah, Malak Abdullah, Lida Safarnejad, Maryam Tavakoli, Dharashree Panda, Saneet Bonde, Fadi Mohsen, Hakim Touati, Mamoun Mardini, Babar Hussain, Fakhri Abbas, Ghaith Husari, Fida Hussain, Zeba Naqvi, Diana Joy, Fareeha Kanwal, Rahma Nawab, and Emmanuel Bello Ogunu. They all helped me at various occasions, sometimes with tasks as simple as cheering me up, going for coffee, restaurant, movie, or gym, and being a participant of my research study or helping me recruit more. I also received some of the best advices from these individuals. These include tips regarding gaining a healthy life-style during the stressful PhD life, consulting to the writing resource center for polishing my drafts, participating in the graduate research symposium, and attending professional development workshops in the center for graduate life. Moreover, I cherish all that I learnt from them by being exposed to their cultures. I got to try and learn wonderful cuisines from various countries. I got introduced to their music and languages. Many of these connections turned into close friendships. I would particularly like to mention Abeer and Malak who are a family away from home and have always been there for me through the thick and thin. We pulled all-nighters together in the lab to catch deadlines, proofread each other's paper drafts and posters, provided moral support to each other upon receiving rejected paper notifications, celebrated each other's paper acceptances, travelled to research conferences together, and explored various venues and coffee shops that would be a good fit for paper writing. Lastly, my deepest gratitude goes to my family for believing in me and giving me the courage to embark upon this journey. My parents' infinite support, encouragement, patience and unconditional love has been invaluable to me. My father's kind words to boost my morale and ensure my health,

and my mother's countless prayers have kept me going. My love goes to my sister and best friend Mubeen for her instant help and feedback whenever I needed it. A born writer and counselor, she has always helped with proof-reading my write-ups and making decisions in difficult times. Finally, my thanks and love goes to my sisters Iqra, and Sana, and my brother Talha for their continuous good wishes and care.

TABLE OF CONTENTS

LIST OF FIGURES	xii
LIST OF TABLES	xv
CHAPTER 1: INTRODUCTION	1
1.1. Statement of Hypothesis and Approaches	4
1.2. Summary of Contributions and Dissertation Organization	6
CHAPTER 2: BACKGROUND	9
2.1. Computer Security Dialogs	9
2.2. Third-Party Application Dialogs	10
2.2.1. Facebook Application Authorization Dialog	10
2.2.2. Touch ID Terms and Conditions Dialog	12
2.3. The Communication-Human Information Processing Model	14
2.4. Human In The Loop Security Framework	18
2.4.1. Communication delivery	19
2.4.2. Communication processing	21
2.4.3. Application	21
CHAPTER 3: RELATED WORK	22
3.1. Problems with Security Dialogs	22
3.2. Design Guidelines for Security Dialogs	23
3.2.1. Improving Attention: Attractors and Warning Designs	23
3.2.2. Improving Comprehension: Dialog Readability and Risk Signal Communication	25

CHAPTER 4: INVESTIGATION OF ANIMATION ON APPLICATION AUTHORIZATION DIALOGS	28
4.1. Animated Authorization Dialog Design	29
4.1.1. Design Elements	30
4.1.2. Dialog Prototype	32
4.2. Pilot Study	33
4.2.1. Design	33
4.2.2. Participants	37
4.3. Study Results	38
4.3.1. Attention Switch and Maintenance	38
4.3.2. Permission Comprehension	43
4.3.3. Permission Authorization Behavior	46
4.3.4. Ease of Use and Learnability	46
4.4. Discussion	48
4.5. Conclusion	49
CHAPTER 5: INVESTIGATION OF ACTIVE EYE-TRACKING ON APPLICATION AUTHORIZATION DIALOGS	50
5.1. Eye-Activated Permission Authorization	51
5.1.1. Overview	51
5.1.2. Design and Implementation	52
5.2. Evaluation	54
5.2.1. Experiment 1: Attention	55
5.2.2. Experiment 2: Habituation	65

	xi
5.3. Discussion	73
5.4. Conclusion	74
CHAPTER 6: IMPACT OF ADVERTISEMENTS ON USER ATTENTION AND DECISION ON AUTHORIZATION DIALOGS	76
6.1. User Study	78
6.1.1. Methodology	79
6.1.2. Participants	82
6.1.3. Study Results	83
6.2. Conclusion	88
CHAPTER 7: IMPROVEMENT OF USER COMPREHENSION OF TOUCH ID USE WITH THIRD-PARTY APPLICATIONS	90
7.1. Potential User Misconceptions	91
7.1.1. In-Person Study	92
7.1.2. Online Study	94
7.1.3. Results	95
7.1.4. Discussion	105
7.2. Proposed Solution for Resolving These Misconceptions	106
7.2.1. Proposed Designs	109
7.2.2. Evaluation	110
7.3. Conclusion	130
CHAPTER 8: CONCLUSION	132
REFERENCES	137

LIST OF FIGURES

FIGURE 1: Proposed Solution	6
FIGURE 2: Different types of computer security dialog boxes	10
FIGURE 3: Facebook Application Authorization Flow	12
FIGURE 4: Touch ID-based user authentication in third-party applications	15
FIGURE 5: Communication-Human Information Processing Model	17
FIGURE 6: Human In The Loop Security Framework	19
FIGURE 7: Animated Dialog Design Elements	32
FIGURE 8: Animated Dialog Design	32
FIGURE 9: Control and Checkbox-based Dialog Designs	34
FIGURE 10: Experimental Setup and Eye-Gaze Fixations/Saccades on the Animated Dialog	36
FIGURE 11: Eye-gaze Fixations On Permission Descriptions	39
FIGURE 12: Eye-gaze Fixations On Information Examples	41
FIGURE 13: Participants Eye-gaze Saccades	42
FIGURE 14: Heatmaps of eye-gaze fixations on the three dialog designs	44
FIGURE 15: Usability scores of the three dialogs	47
FIGURE 16: Heatmap of eye-gaze fixations on Facebook application authorization dialog (as of early 2015)	52
FIGURE 17: System Architecture	54
FIGURE 18: Eye-Select Facebook application dialog used in my experiment	55

FIGURE 19: Number of participants who identified one or both permissions (Attention)	60
FIGURE 20: Participant permission identification precision and recall during the attention experiment	62
FIGURE 21: Average eye-gaze fixation counts on application permissions area of interest for the control, control with time constraint, and treatment group (Attention)	63
FIGURE 22: Eye-gaze fixations of participants on the application installation dialog permission area of interest (Attention)	64
FIGURE 23: Number of participants who identified one or both permissions (Habituation)	70
FIGURE 24: Participant permission identification precision and recall during habituation experiment	70
FIGURE 25: Eye-gaze fixations of participants on the application installation dialogs area of interest during habituation and test period	71
FIGURE 26: Average eye-gaze fixation counts on the application permissions for the control, control with time constraint, and treatment groups (Habituation)	72
FIGURE 27: Banner and product placement advertisements in and around <i>Zynga</i> games on Facebook [28]	77
FIGURE 28: Heatmaps from an eye-tracking study on three websites. The areas where users looked the most are colored red; the yellow areas indicate fewer views, followed by the least-viewed blue areas. Gray areas didn't attract any fixations.	77
FIGURE 29: Static advertisements with four types of content	80
FIGURE 30: Mockup of the gaming website <i>Zynga</i> used in my experiment	81
FIGURE 31: Effect of advertisement's presence on user attention and decision on authorization dialog	85
FIGURE 32: Effect of advertisement content type on user attention and decision	88

FIGURE 33: Touch ID prompt for authentication in Amazon Application	93
FIGURE 34: Touch ID terms and conditions dialogs inside Banking applications	111
FIGURE 35: Screenshot of Touch ID popup appearing during sensitive tasks inside my user study applications	114
FIGURE 36: Normality assumption for factorial ANOVA in Hypothesis#1	119
FIGURE 37: Average time (ms) spent on each dialog design	120
FIGURE 38: Normality assumption for factorial ANOVA in Hypothesis#2 (decision on dialog)	125
FIGURE 39: Participants dialog rating on Likert Scale	128

LIST OF TABLES

TABLE 1: Average participant ratings for the effectiveness of permission layout and information examples in each dialog	45
TABLE 2: Average visit duration on each dialog	47
TABLE 3: Participant demographics for the attention experiment	59
TABLE 4: Participants demographics for the habituation experiment	68
TABLE 5: Descriptive statistics for the demography of the in-person and online study	96
TABLE 6: Responses to survey questions regarding Touch ID authentication process perception for the in-person and online study	98
TABLE 7: Participant perceptions of fingerprint storage before/after, and fingerprint access during the Touch ID-based Amazon in-app purchase transactions	100
TABLE 8: Responses to survey questions regarding perceptions on the ease of getting into a Touch ID-enabled device and making a purchase	102
TABLE 9: Participant demographics	118
TABLE 10: Percentage of participants in each group who answered a pre-test and post-test question correctly	122

CHAPTER 1: INTRODUCTION

Today, a majority of our daily tasks are conducted online. A significant percentage of these tasks are accomplished through the use of third-party applications on smartphones and online social networks (OSNs). Third-party applications, developed by entities other than the owner of a platform using its application programming interface (API), are used to provide such services as rides, shopping, food delivery or banking. As of 2017, there are over two million applications in the Android and Apple stores [5]. According to another report, 63% of US smartphone owners use 1 to 5 smartphone applications daily [3].

The plethora of user information shared and stored on OSNs and smartphones has made these platforms a lucrative target for information theft and malware. Malicious applications can request access to a large amount of personal information and compromise a user's privacy and security [38]. For example, the *Most Used Words* is a quiz application on Facebook that creates a word cloud of the user's most frequent words using their timeline posts. During authorization, this application requests access to the user's information including their current location, education history, and photos. This application was accused of stealing user data since the application was requesting many more permissions than required for its functionality [4]. Chia et al. [18] showed that free and lookalike applications request more permissions than is typical, such as the publish stream permission. Similarly, there has been a 23% increase

in malware attacks on Android devices. A majority of these attacks are attributed to third-party application downloads [8].

Third-party applications present security dialogs to users. These dialogs are windows that alert the user about important information along with a subsequent action that needs to be taken. The first category of dialogs presented by these applications are the authorization dialogs that request permissions to access user information. Third-party developers require user permissions to acquire read or write access to user data in accordance with the application’s functionality. These permissions are presented to the user (through the scope parameter) on the login dialog as part of the authorization flow. The user authenticates and approves these permissions. Once the permissions are granted and the authorization flow is completed, the third-party developer receives an access token to make API calls on behalf of the user and to retrieve user data.

The second category of security dialogs presented by third-party applications are the terms and conditions dialogs. These describe a legally binding agreement between the user and the application developer/company. These dialogs specify the application’s policy regarding user information and are presented during application installation or configuration phases. Both these dialogs are crucial to control information access to the application and to minimize the associated risks.

Unfortunately, computer security dialogs are disregarded by users everyday [6, 7]. Anderson et al. [12] observed a dramatic drop in the visual processing centers of the brain (using functional magnetic resonance imaging) after only the second exposure to a warning. Felt et al. [26] found that only 17% of smartphone users paid attention

to permissions during application installation. The reasons users ignore these dialogs can be grouped into the following categories:

1. Failures in communication delivery: Security dialogs fail to capture a user's attention. Attention switch and maintenance is the first information processing stage of the human in the loop (HITL) framework [19]. Failures in attention switch and maintenance can occur when the user has been conditioned to ignore the warning, a phenomenon known as habituation. When non-compliant behavior does not cause harm over time, users may develop an automated response, habituation, that does not take into account changes in the security dialog's context or message. Habituation decreases dialog effectiveness when users become less alert to the information presented in dialogs [21, 22, 46]. This amplifies the risk associated with third-party application usage because users authorize all requested permissions without reading them. In addition, external factors and environmental stimuli can divert a user's attention away from the dialog content.
2. Failures in communication processing: This is the second information processing stage in the HITL framework. Mental models are an integral part of user behavior. Due to their limited understanding and the dialog's poor wording/technical jargon, users form misconceptions about the message being communicated or the options available in the dialog [29, 41, 45, 30, 22, 20].
3. Lack of intention: Users may be unmotivated to respond to a security dialog because they believe that the dialog is irrelevant compared to their primary

task, that it is not urgent to respond to the dialog, or that it does not apply to them.

Numerous efforts have been attempted to improve security dialog communication delivery and processing. While a large volume of this research focuses on risk communication and design of software warning and update messages [15, 14, 12], only a handful of prior work have investigated the challenge of designing effective third-party application dialogs. Among these are permission authorization dialog designs to improve user comprehension of the dialogs [43, 23]. A few researchers have proposed risk signals to inform users about the threats associated with application installation to influence their decision. These include the use of personal information examples and social navigation cues [31, 13, 39]. Since the problems of habituation, lack of attention and dialog content comprehension continue to prevail, there is need for innovative techniques that can resist habituation and improve user attention and understanding of the message communicated by these dialogs.

1.1 Statement of Hypothesis and Approaches

This dissertation hypothesizes that:

Third-party application dialogs' effectiveness with respect to attention switch, attention maintenance, and comprehension can be improved by 1) incorporation of design heuristics such as animation, eye-tracking, risk signals/examples, and simplified text and 2) by investigation of potential misconception avenues and environmental stimuli that impede user attention.

To achieve this goal, first new techniques are investigated that can be leveraged to

ensure user attention. Moving elements are a powerful tool to attract users' attention [37]. The use of computer animations is increasingly becoming popular for creating security awareness among the users and helping them understand information security. However, the use of animation to attract user attention towards permissions and to create awareness about them has not been explored in the context of application permission dialogs. Therefore, animation is explored together with personal information examples as a potential design heuristic that can improve attention switch and maintenance. Next, active eye-tracking is explored as a mechanism to resist habituation. Since eye-tracking technology is becoming affordable and will be soon embedded in laptop and mobile devices, it can be leveraged to ensure user attention on application permissions. Along with this, advertisements, are analyzed as a potential environmental stimulus that can divert user attention from the authorization dialog and influence their decision. Since third-party application providers rely heavily on advertising-based revenues and display various advertisements in and outside the application in areas where users look the most, it is important to analyze their impact on user attention towards application permissions. Finally, to improve user comprehension of the dialog content, potential misconception avenues regarding the related technology are investigated. To resolve these misconceptions, various design heuristics are explored that can present the content in a simplified form. These include the use of bullet list-based text [23, 43], animation to explain a phenomenon, and visual cues to communicate whether the content represents a risk or a benefit. Figure 1 shows our proposed approach with respect to the communication impediment module and the two information processing stages of the HITL framework.

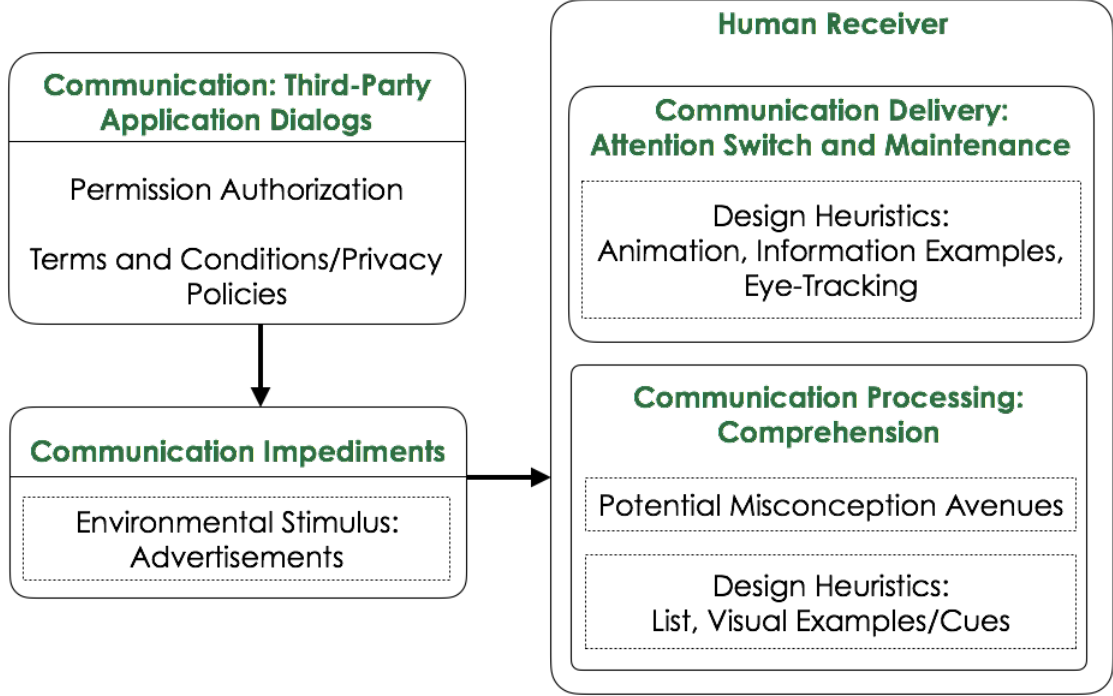


Figure 1: Proposed Solution

1.2 Summary of Contributions and Dissertation Organization

This dissertation specifically focuses on two types of third-party application dialogs: (1) permission authorization dialogs presented by Facebook during application installation and (2) terms and conditions dialogs presented by iOS banking applications while setting up Touch ID-based authentication. The contributions of this research are as follows:

1. Two dialog designs are proposed to increase user attention towards requested permissions on Facebook authorization dialogs. User experiments are conducted to validate the effectiveness of each design.

- First is an animated dialog design that leverages a real-life analogy of

luggage screening at airport security checkpoints. It incorporates the end-user's personal information examples to attract user attention and to communicate the potential information disclosure associated with each permission.

- Second is an eye-activated dialog design that deactivates the decision buttons on the authorization dialog initially and uses feedback from the eye-tracker to ensure that the user has looked at the permissions. After determining user attention, the decision buttons on the dialog are activated.
2. The impact of advertisement's presence above an application's authorization dialog on user's attention and decision is analyzed through a user experiment on a mockup of a popular gaming website. The control group is presented with no advertisements above the application authorization dialog, whereas the treatment groups are presented with static and animated (GIF-based) advertisements. The advertisements contain four types of content, namely, food, shopping, politics, and sports.
 3. User misconceptions regarding Touch ID-based authentication with third-party applications are investigated. Four dialog designs are presented to improve user comprehension of the terms and conditions dialog specifically presented by Touch ID-enabled iOS applications. The proposed dialog designs (1) simplify the information text and present it in bullet format with visual cues to aid the comprehension of the presented information, and (2) resolve discovered misconceptions of fingerprint data access, application account access by others, and

role of fingerprint in Touch ID-based sign-in. User experiments are conducted to validate the effectiveness of these designs.

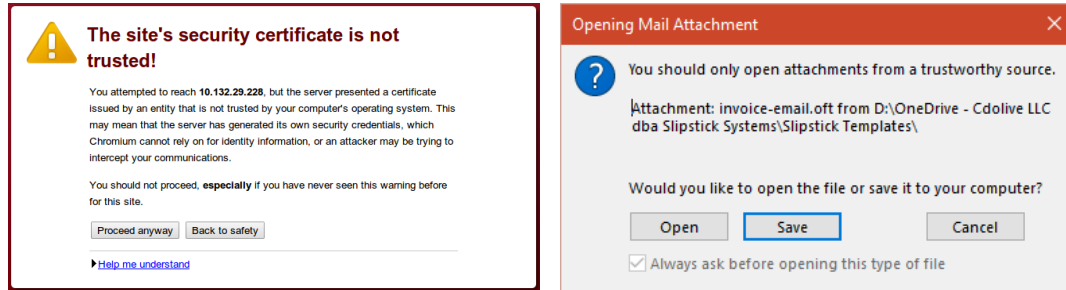
The remainder of this dissertation is organized as follows: Chapter 2 discusses the background information related to this research. Chapter 3 reviews the literature most relevant to this work. Chapter 4 describes the animated dialog design that leverages the use of animation with personal information examples to improve user attention towards Facebook application authorization dialogs. Chapter 5 discusses the eye-activated dialog design that utilizes eye-gaze information from the eye-tracker to ensure user attention. Chapter 6 discusses a user experiment focused on analyzing the impact of advertisements around application authorization dialogs on user attention. Chapter 7 first discusses a user study that investigates misconceptions that users have about the use of Touch ID authentication with third-party applications. It then discusses proposed dialog designs to improve user attention and comprehension of terms and conditions dialogs related to Touch ID use in iOS applications. Chapter 8 concludes this dissertation and discusses potential future paths for extending this research.

CHAPTER 2: BACKGROUND

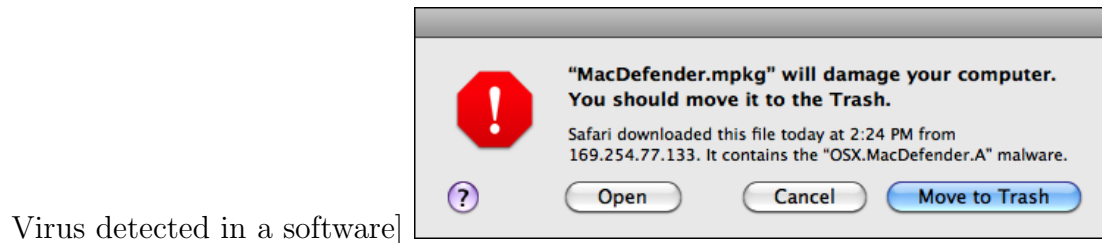
This chapter summarizes the background information relevant to the context and significance of this research. First, a brief introduction of computer security dialogs is provided. Second, third-party application dialogs—the specific type of security dialogs that are the scope of this work—are described. Third, a general model for warning effectiveness, known as the communication-human information processing (C-HIP) model, is explained. Fourth, the HITL security framework based on this C-HIP model is explained to understand the behavior of humans who are expected to perform security-critical functions and the reasons why users disregard these security dialogs.

2.1 Computer Security Dialogs

Warnings in computer systems are usually displayed on the brink of an impending danger to users' information or to their identity credentials. Unlike physical warnings, computer security dialogs are not permanently displayed: They are dynamic dialogs, triggered whenever the conditions set by software developers are met. The dialog's content is decided based on those conditions. In this sense, a computer dialog is a template: Part of its content and appearance is fixed, and the remainder corresponds to placeholders that are filled out with information before displaying the dialog. Figure 2 shows three examples of computer security dialogs.



(a) Server with SSL certificate that is either self-signed, or is signed by an untrustworthy authority (b) Opening an email attachment from untrustworthy source



Virus detected in a software]

Figure 2: Different types of computer security dialog boxes

2.2 Third-Party Application Dialogs

This section describes two third-party application dialogs that are the focus of this dissertation. First is Facebook’s application authorization dialog, and second is the Touch ID terms and conditions dialog.

2.2.1 Facebook Application Authorization Dialog

Third-party developers require user permissions to acquire read or write access to user data in accordance with a Facebook application’s functionality. These permissions are presented to the user (through the scope parameter) on the login dialog as part of the authorization flow. The user authenticates and approves the permissions. Once the permissions are granted and the authorization flow is completed, the third-party developer receives an access token, which is utilized to make API calls on behalf of the user and to retrieve data [9].

By default, a third-party application has access to the underlying user’s public profile information. This includes ID, name, link, username, gender, location, age range, and other information shared as public. If an application requires access to other user information, it needs to request permission from the user. These permissions are presented on two separate dialogs during application authorization:

1. Required Permissions Dialog: This dialog shows the permissions necessary for the application to function properly. These permissions cannot be revoked in the dialog during installation, i.e., they are not optional for users when installing the respective application. The dialog requests read access to extended profile properties. The information asked for can either be the authorizing user’s information or friends’ information. Figure 3(a) shows the *Fortune Cookies* application’s required permission dialog. In addition to the user’s information, this application requests access to friends’ information, which consists of birthday, work histories, status updates, check-ins, events, current cities, photos, and likes. For a detailed description of each permission, please refer to the “Permissions” section in [2].

2. Optional Permissions Dialog: This dialog appears after the required permissions dialog and displays permissions for access to sensitive information and for the ability to publish or delete data. Figure 3(b) shows the optional permissions dialog for the *Fortune Cookies* application. In addition to the optional permissions that request read or write access to user’s profile items, there are open graph and page permissions:

Open Graph Permissions: Open Graph lets an application publish stories on Facebook. The permissions under this category request read access to the Open Graph to



Figure 3: Facebook Application Authorization Flow

retrieve actions published by other applications, or write access to allow the application to publish actions to the Open Graph. There are a total of 6 permissions under this category.

Page Permissions: These permissions allows the developer to administer any Facebook page that the user manages.

2.2.2 Touch ID Terms and Conditions Dialog

Fingerprint authentication in smartphones was recently introduced as a fast and secure alternative to entering PIN/passcode. 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 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.

Apple recently released Touch ID to third-party applications, giving third-party developers the ability to utilize the Touch ID fingerprint sensor for user sign-in and for authorization of sensitive tasks, such as money transfer and purchase completion.

An iOS application presents the Touch ID terms and conditions dialog during Touch ID setup process for the application. This dialog informs the user about the risks and benefits of enabling Touch ID with the application.

Touch ID-based user authentication in an application works as follows:

Touch ID setup - The user first needs to enable Touch ID for the application. During this phase, the application presents the user with the Touch ID terms and conditions dialog. This dialog presents information in the following three areas:

1. Fingerprint use in Touch ID-based authentication: This information explains that using Touch ID removes the need to enter the account password.
2. Application account access: This information explains that anyone whose fingerprint is registered on the device can access the device owner's application account.
3. Fingerprint data access: This information explains that the application does not have access to a user's fingerprint data.

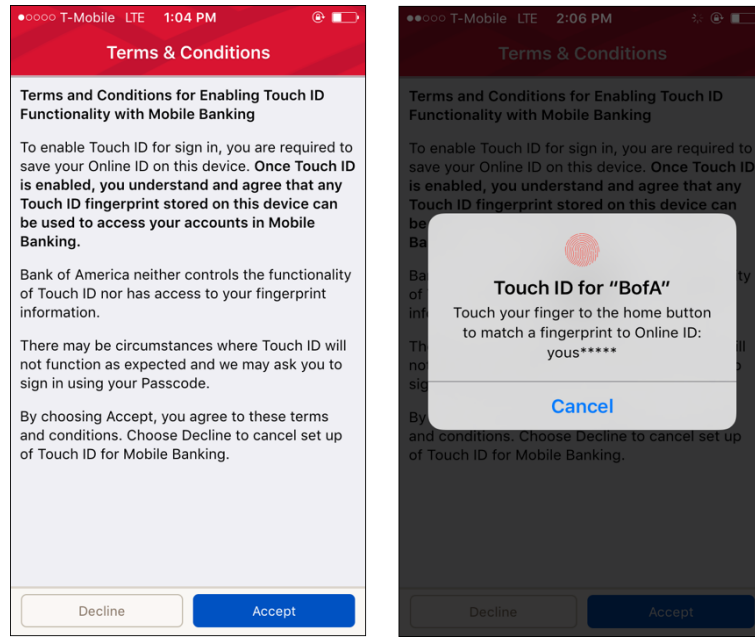
Figure 4(a) displays the Touch ID terms and conditions dialog. The first paragraph in the text informs the user that both a fingerprint and an account password are used in Touch ID-based authentication. This information is followed by text related to application account access by other people who have their fingerprint registered on the current user's device. The second paragraph shows information about fingerprint data access by the application. The user authorizes this dialog by accepting these terms and conditions. The user is then presented with a dialog popup window that requests the user to place a registered fingerprint on the home button in order to

associate a fingerprint with their application account ID (See Figure 4(a)). Once the provided fingerprint is verified, the Touch ID setup is complete.

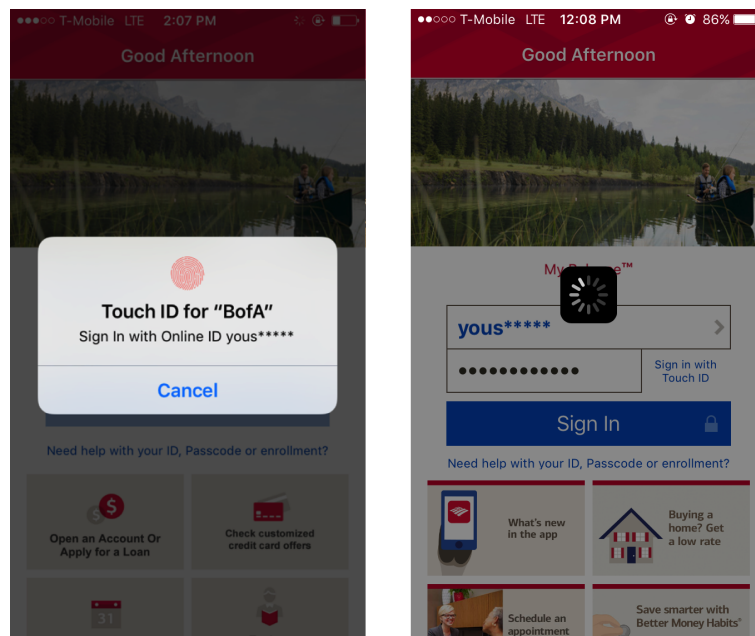
Touch ID-based sign-in - Once the user enables Touch ID for the application, all subsequent sign-ins to the application can be accomplished with either Touch ID or a password. If the user chooses to sign-in with Touch ID, the Touch ID popup appears on the application's sign-in activity (see Figure 4(b)), where the user taps a registered finger on the home button and is verified by the third-party application through the Local Authentication Framework [10] as the owner of the device. If the user is verified as the owner of the device, then the account username and password is securely retrieved from the keystore and is used to authenticate them. Figure 4(b) shows that the password field is autofilled with the user's account password once it is retrieved after verifying the user's provided fingerprint.

2.3 The Communication-Human Information Processing Model

The C-HIP model is a widely accepted theoretical framework for warning processing, that comes from psychology [47]. It describes a general sequencing of stages and the effects warning information might have as it is processed. It assumes two agents, the source and the receiver, and describes a set of sequential stages with feedback loops that the receiver should pass through, with flow of information or processing from one stage to the next, until a change of behavior attributable to a warning happens (see Figure 5). In the case of computer dialogs, the source is the software displaying the dialog (e.g., the operating system) and the developers and designers of the application. The receiver is the user of the warning. If the warning is success-



(a) Touch ID setup (Left: Touch ID terms and conditions dialog, Right: Touch ID setup popup)



(b) Touch ID-based sign-in (Left: Touch ID popup on sign-in activity, Right: User account password retrieval)

Figure 4: Touch ID-based user authentication in third-party applications

ful, the behavior change will protect the receiver from harm. Each stage represents a necessary condition for the stages that follow. The authors describe the different

stages of the model as follows:

1. Attention switch: The warning captures the receiver's attention. In this phase, a warning has to compete for the receiver's attention with other stimuli present in the environment, possibly including other warnings.
2. Attention maintenance: The receiver decides to pay extended attention to the warning. Warnings need a certain minimum time span of display to be decoded and internalized. If too short, the message may not be read in its entirety and may be misunderstood. One specific factor that may affect the attention maintenance stage is text length and saliency. If the text is too long, the receiver may decide that it is not worth reading; if the warning is not salient enough, the receiver may decide not to read with the belief that, if it were important, it would have been larger.
3. Comprehension, Memory: The receiver understands the warning content along with how to respond to it and commits the message to working memory.
4. Attitudes, Beliefs: The receiver judges that the warning is applicable.
5. Motivation: The receiver perceives that it is important to heed the warning.
6. Behavior: The receiver changes behavior to comply with the warning.

The C-HIP model has been used to design and evaluate the effectiveness of security indicators and warning messages. Felt et al. [26] based their inquiry on the C-HIP model to explore whether Android permissions are usable security indicators that

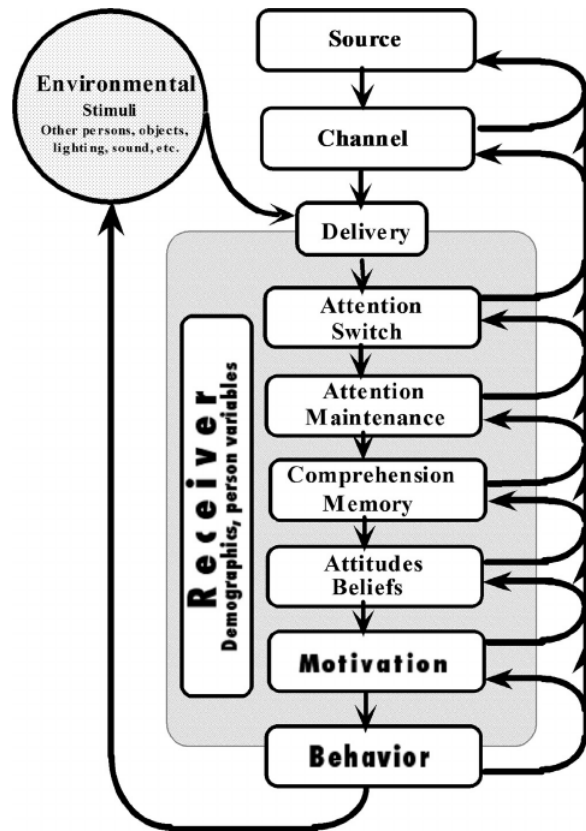


Figure 5: Communication-Human Information Processing Model

attract user attention and influence user comprehension and behavior. Egelman et al. [24] mapped the C-HIP model onto the anti-phishing problem, and explored design choices that are more or less congruent to it. They found that designs that were more congruent to C-HIP model led to better outcomes for users. Similarly, Fagan et al. [25] conducted a study to investigate user attitudes and perceptions regarding software update and warning messages and argued that human factors such as personal attitudes, beliefs, and specific software type may change the effectiveness of software update messages.

2.4 Human In The Loop Security Framework

Many secure systems rely on humans to perform security-critical functions such as responding to a permission authorization dialog or a terms and conditions dialog. In such scenarios, threats to system security include not only malicious attackers, but also non-malicious humans who don't understand when or how to perform security-related tasks, humans who are unmotivated to perform security-related tasks or comply with security policies, and humans who are not capable of making sound security decisions. The human-in-the-loop (HITL) security framework is designed to understand the behavior of humans whom we expect to perform security-critical functions [19]. This framework is based on the C-HIP model because security-related actions by non-experts are generally triggered by a security-related communication—for example an on-screen alert, software manual, or security tutorial.

Figure 6 shows the components and information processing stages in the HITL framework that impact security-related behaviors. The first component is the communications relevant to security tasks. These include warnings, notices, status indicators, training, and policies. The next component is communication impediments that include environmental stimuli and activities that may divert user's attention away from the security communication and may prevent the communication from being received as the sender intended. Once the user receives the security communication, they bring to the situation a set of personal variables, intentions, and capabilities that impact a set of information processing steps: communication delivery, communication processing, and application. Personal variables include user demographics and

personal characteristics such as age, gender, culture, education, occupation, and disabilities. Intentions include attitudes and beliefs, as well as motivation—factors that will influence whether a user decides that a communication is worth paying attention to and acting upon. Capabilities include specific knowledge, or cognitive or physical skills that may be necessary to complete an action.

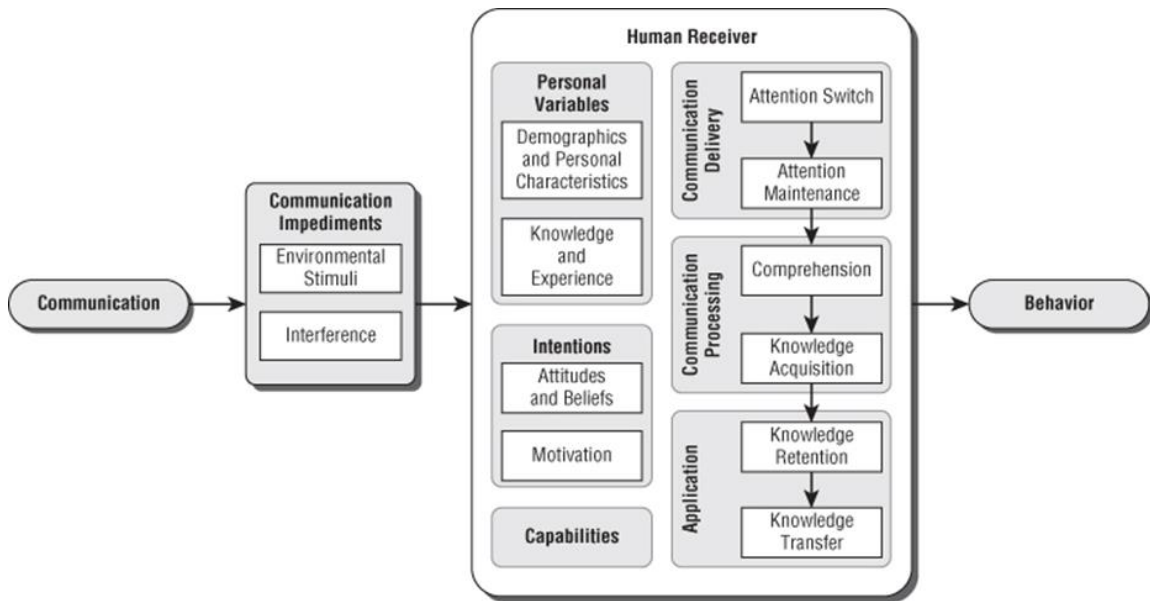


Figure 6: Human In The Loop Security Framework

2.4.1 Communication delivery

This is the first information-processing stage that includes attention switch and maintenance. Unless the user notices the communication and pays attention to it long enough to process it, the communication will not succeed. Research shows that many users do not notice security indicators in softwares they use regularly. For example, user studies indicate that some users have never noticed the presence of the SSL lock icon in their web browser [21, 22]. A study that used an eye tracker to observe participants’ behaviors when visiting SSL-enabled websites found that most

users do not even attempt to look for the lock icon [46]. Many factors influence attention switch and maintenance. Habituation or the reduced attentional response to repeated exposure to a stimulus [34], is a major factor that impacts this information processing stage.

When non-compliant behavior does not cause harm over time, people may develop an automated response, habituation, that does not take into account changes in security dialog context or messaging [33]. Habituation decreases dialog effectiveness when people become less alert to the information presented in dialogs. Computer dialogs, just like their physical counterparts, have iconic and informational elements. In a warning, iconic elements include size, color, icons, typography, and geometry. The informational elements are those that communicate a message to the receiver of the warning. The distinction is blurred, and some elements, such as the main warning word (e.g., “Danger!”), may incorporate both. Usually the icons in a computer security dialog are associated with salience, however, the dialog’s text is not. Habituation occurs when a person recognizes the iconic elements and prematurely stops processing the informational elements in the dialog. The problem is worsened by the fact that most systems have standardized the appearance of dialogs or have at most a limited number of different templates. Visual variability between different messages is accordingly limited, which may increase the likelihood of appearance of habituation or reinforce already existing habituation.

2.4.2 Communication processing

This is the next information-processing stage which includes comprehension and knowledge acquisition. The user should have the ability to understand the communication and know what to do in response to it. A user mental model is an integral part of what drives their behavior. Based on their limited understanding, users may not understand the message being communicated or the options available in the dialog. For example, many users do not understand the meaning of web browser security symbols and pop-up warnings [22, 20].

2.4.3 Application

The final information-processing stage is application, that consists of knowledge retention and knowledge transfer. The user should be able to remember the communication's meaning and be able to recognize situations where this communication is applicable and how to apply it. For example, remembering an anti-phishing training and applying it to future email messages.

CHAPTER 3: RELATED WORK

This chapter presents the literature most relevant to this research. First, a discussion of the problems with warnings and security dialogs is presented. Next, existing work on design guidelines for improving user attention and comprehension of security dialogs is presented along with a discussion of how we build upon this work.

3.1 Problems with Security Dialogs

There is a wealth of research that demonstrates that users ignore security dialogs. Habituation is a major human factor that causes users to pay less attention to these dialogs over time. Anderson et al. [12] used fMRI data to demonstrate a clear drop in visual processing after one repetition of a warning message. Felt et al. [26] found that only 17% participants paid attention to permissions during application installation. Moreover, lack of understanding and the dialog’s poor wording/technical jargon creates misconceptions about the message being communicated or the options available in the dialog. Vaniea et al. [41] showed that the difficulty of assessing whether an update is “worth it” and the confusion about why an update is necessary is one of the reasons why users ignore update messages and choose not to install the update. Other human factors such as personal attitudes, beliefs, and specific software type can also impact the effectiveness of software update messages [25].

3.2 Design Guidelines for Security Dialogs

Several design guidelines have been proposed to improve software warning effectiveness with regards to user attention and habituation. We apply these guidelines to third-party application dialogs and analyze their effectiveness. Moreover, we discuss existing work on improving the comprehension of third-party application authorization dialogs and how we contribute to it.

3.2.1 Improving Attention: Attractors and Warning Designs

Bravo-Lillo et al. [15, 14] proposed several attractors to draw users' attention to a text field within a dialog and to resist habituation. Among these, four were inhibitive attractors which prevent the user from proceeding until some time has passed (e.g., waiting for the text to gradually appear or become highlighted), or the user performs a required action (e.g., moving the mouse over a field or typing the text). One attractor was non-inhibitive and included an attention-grabbing stylistic change of text font and background. The authors studied the attractors' resiliency to habituation. The two inhibitive attractors that forced users to interact with the text field by moving the mouse over it or typing the text proved to be effective even after increasing the level of habituation. The applicability and effectiveness of these attractors to third-party application dialogs has not been investigated. We explore the use of active eye-tracking as a potential inhibitive attractor where the user has to look at the dialog's content to activate the decision button.

Anderson et al. [12] proposed the use of polymorphism in warning design by changing its appearance with each presentation. Functional magnetic resonance imaging

(fMRI) and mouse cursor tracking was used in the experiments to show that polymorphic warning was effective in combating habituation compared to conventional warnings. However, there are only a finite number of possible warning designs based on the authors' approach. Hence, there is a strong likelihood of users getting habituated to these designs after repeated exposures. Moreover, the applicability of these designs to third-party application dialogs has not been investigated.

Some design enhancements have been proposed to the existing permission authorization dialogs for Facebook applications to assist the end-users in making informed decisions. Wang et al. [44, 48] proposed two Fair Information Practice Principles (FIPPs)-based interface designs—monochrome and polychrome—to overcome the limitations of existing authorization dialogs. The monochrome design 1) showed what information was requested by the third-party and how it was used 2) gave the user more control to decide what information could be accessed 3) provided a warning signal (red exclamation point) if the users' current privacy settings were violated by the application's publishing permissions. The rows in their design represent the user and the user's friend information requested by the application. The columns represent how each piece of information will be used. For example, email permission can be used to send a message to the user.

The polychrome design is an enhanced version of the monochrome with a three-color scheme to reflect users' current privacy settings. Green indicates that the privacy setting is public and will not be violated by installing the application. Whereas, red and yellow indicate that the privacy settings are such that there will be full and partial violation, respectively, after the application is installed. Their study showed

that participants preferred the polychrome design. In [43], the authors have further studied the effectiveness of variations of their monochrome design. Although their design proved effective in the fine-grained access control compared to the default design, an eye-tracking based evidence of whether participants read the entire dialog before making decisions would be interesting. Moreover, this design lacks personal information examples, which could further enhance participants' permission comprehension. We compare our proposed designs to a simplified version of this design to understand their effectiveness.

3.2.2 Improving Comprehension: Dialog Readability and Risk Signal

Communication

Harbach et al. [29] explored the use of readability measures on the descriptive text of warning messages to estimate how understandable a warning is for the user. The linguistic properties of warning message texts also has an effect on its perceived difficulty [30]. Keeping headlines simple, using as few technical words as possible and creating short sentences without complicated grammatical constructions makes warning messages more pleasant for the user. We used these guidelines in our authorization dialog design and terms and conditions dialog designs.

Egelman et al. [23] proposed design changes to the Facebook Connect dialog by presenting the actual information requested by the public profile permission. They observed that the changes were noticed, but because users had such low expectations for privacy, the additional information did not dissuade them. Passive eye-tracking was used to analyze the readability of this dialog design compared to others by observ-

ing the frequency and duration of a user’s eye-gaze fixations over the dialog content [27]. The results showed that, although the participants who were shown information verbatim took longer to read the dialog, it did not affect their decision to authenticate using Facebook Connect. Since the list-based text presentation improved attention, we incorporate this design guideline on third-party application dialogs, and use eye-tracking in our experiments to assess the readability and effectiveness of our proposed designs.

Several researchers have made efforts to improve the risk communication for authorization dialogs. Harbach et al. [32] proposed a modified permission dialog for Android applications to improve security risk communication to the end-user. They display a personal information example along with each permission to help the user understand the risk associated with a permission’s authorization. Their study showed a significant difference in the behaviors of participants who were presented with the modified dialog design compared to the ones presented with the default design. The participants who were shown information examples for each permission spent more time on the dialog and appeared to be more aware of the security and privacy risks. However, the authors used sample data for their study and did not explore the use of actual user information. The use of eye-tracking could have further reinforced the evidence of their results. We incorporate information examples together with animation and eye-tracking on application authorization dialogs and terms and conditions dialogs.

Sarma et al. [39] proposed a mechanism for creating effective risk signals for Android applications that 1) are easy to understand by both the users and the devel-

opers, 2) are triggered by a small percentage of applications, and 3) are triggered by malicious applications. They use the permissions an application requests, the category of the application, and the permissions requested by other applications in the same category to better inform users whether the risks of installing an application are commensurate with its expected benefits.

Social navigation is defined as the use of social information to aid a user's decision. Besmer et al. [13] explored the use of social navigation cues (e.g., the percentage of users who have allowed/denied a particular permission) to help users make better permission authorization decisions when installing Facebook applications. They found that social cues have minimal effect on users' Facebook privacy settings. Hence, only a small subset of users who take the time to customize their settings may be influenced by strong negative social cues.

CHAPTER 4: INVESTIGATION OF ANIMATION ON APPLICATION AUTHORIZATION DIALOGS

Moving elements are a powerful tool to attract users' attention [37]. Visuals are processed significantly faster than text, and they quickly affect user's emotions, which in turn greatly affect their decision-making [11]. The use of computer animations is increasingly becoming popular for creating security awareness among the users and helping them understand information security. To the best of my knowledge, the use of animation to draw user attention towards permissions and to create awareness about them has not been explored in the context of application permission dialogs.

The incorporation of end-user's personal information examples on the application authorization dialogs has recently been shown to be effective in communicating the security risks associated with authorizing an Android application's requested permissions, e.g., displaying a stored photo along with the *read SD card* permission to communicate the user's personal data that the developer can access. Harbach et al. [32] state that users take longer to install applications when presented with personal information examples along with permissions. Similarly, Serge Egelman et al. [23] explored the usefulness of displaying user's actual information along with permissions on the Facebook Connect dialog.

The use of personal information examples has not been studied extensively in the context of third-party application authorization dialogs. Moreover, I have found no

existing eye-tracking-based research that investigates whether users read the authorization dialogs while installing third-party applications.

I propose an animated permission dialog design for Facebook applications. I leverage the real-life analogy of luggage screening at airport security checkpoints and incorporate the end-user’s personal information examples to draw user attention and to communicate the potential information disclosure associated with each permission. I chose Facebook because of its widespread use, growing number of applications, and API to access the information of its large user base.

In this chapter, I describe my animated dialog design. I discuss the results of a pilot study that evaluates my proposed dialog prototype through its comparison with the checkbox-based dialog proposed by Wang et al. [43] and the dialog currently deployed by Facebook. I show that the animated dialog design performs well on the first stage of the C-HIP model, i.e., attention switch and maintenance. There are significantly more and longer eye-gaze fixations on the permission descriptions and personal information examples in the proposed dialog compared to other dialogs. The personal information examples prove to be a good indicator in making participants more aware and concerned about their personal information. A fewer number of permissions are authorized using the animated dialog compared to the other dialogs. Moreover, the animated dialog is easy to use and learnable.

4.1 Animated Authorization Dialog Design

I use a playful design approach on the application permission dialog and leverage the airport security checkpoint analogy to draw user attention towards permissions.

The end-user plays the role of a security guard who monitors the scanned luggage on a computer screen. The permissions are presented to the user one by one in a manner analogous to how the luggage is screened. To maintain user attention long enough to read and evaluate the permissions, I explore the use of personal information examples with each permission to communicate the associated information disclosure.

4.1.1 Design Elements

I map various elements involved at an airport security checkpoint to my context through the use of avatars.

- Luggage— I refer to the user information requested by the application permissions as the luggage items to be scanned. Each permission—read or write access to a user’s information—is represented by a box-shaped avatar. A permission box has an icon to symbolize the requested resource. I use Facebook’s existing icons for the information items requested by a permission. For example, for “access photos” and “access checkins” permissions, I use the photo and location icons present above the post-sharing text box on the user’s timeline.
- Scan Summary Screen— The permissions are scanned one by one. Once a permission is scanned, I display the permission’s scan summary on a screen. The summary consists of the following pieces of information:
 - Permission description: The type of user information accessed.
 - Personal information example: An example of the actual user data requested by the permission. The user data is extracted through the Face-

book API and presented beneath the permission description to highlight the actual user information disclosed as a result of granting the permission. For example, for the user photos and friend-lists permissions, I display one of the user’s album titles and one of the user’s created friend-list names, respectively. The personal information example is presented using a red font (Figure 7(b)) to emphasize its importance.

- Permission type: Whether the permission is required or optional to authorize.

After the permission scanning is complete, the user is alerted when the background color turns yellow, and the permission details are displayed on the screen. The user makes an authorization decision based on the provided summary by clicking the respective *Allow* and *Deny* buttons under the scan summary screen.

- Decision Options— The allow and deny buttons appear beneath the scan summary screen to grant or deny authorization for the permission. If the permission is a required permission, the deny button disappears. Therefore, only the optional permissions can be denied. To keep the design consistent with Facebook’s existing design, and the other proposed designs, a cancel button is displayed next to the allow and deny buttons to give the user an option to leave the application at any time.
- Permission Decision Carts— There are two decision carts—allowed and denied. The allowed cart stores the permissions that have been authorized, similar to the luggage at security checkpoint that has been cleared. The denied cart stores

the permissions that have been denied.

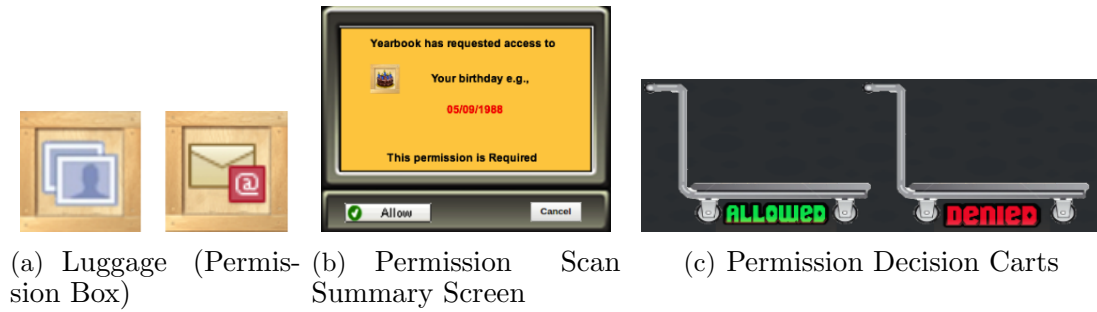


Figure 7: Animated Dialog Design Elements

4.1.2 Dialog Prototype

I implemented an HTML prototype of my model and conducted a pilot study on 16 participants recruited from my university. Figure 8 shows a screenshot of my proposed application permission dialog prototype.



Figure 8: Animated Dialog Design

4.2 Pilot Study

I conducted a pilot study¹ for a preliminary evaluation of my proposed dialog design. I compared my animated dialog design with 1) the design currently deployed by Facebook and 2) the design proposed by Wang et al. [43]. My study focuses on answering the following research questions:

- **Attention switch and maintenance-** Is the animated dialog design significantly different than the other designs in making the participants notice the permissions and pay attention towards them long enough to read them?
- **Comprehension-** Is the animated dialog’s permission layout effective in helping the users easily read and differentiate permissions, and making them aware and concerned about the associated information disclosure?
- **Behavior-** Does the animated dialog have an impact on the users’ installation decisions/allow-all permissions behavior?
- **Usability-** Is the animated dialog rated equal to the other dialog designs w.r.t ease of use and learnability?

4.2.1 Design

4.2.1.1 Conditions

- **Control**—This is the dialog currently deployed by Facebook (Figure 9(a)).
- **Treatment A (Checkbox)**—This is the checkbox-based dialog proposed by Wang et al. [43]. To enable direct comparison of this dialog and the animated dialog

¹Approved IRB Protocol #13-03-30

w.r.t the effectiveness of personal information examples, I developed a modified version of this dialog by incorporating information examples. I also removed the additional columns that represent how the information is being accessed, for two reasons i) this information is not yet incorporated in my proposed design ii) it was hard to classify this information for every permission. Figure 9(b) shows my modified version of this dialog design. From now on, I will refer to this dialog as the checkbox-based dialog design.

- Treatment B (Animated)—This is my proposed animated dialog design (Figure 8).

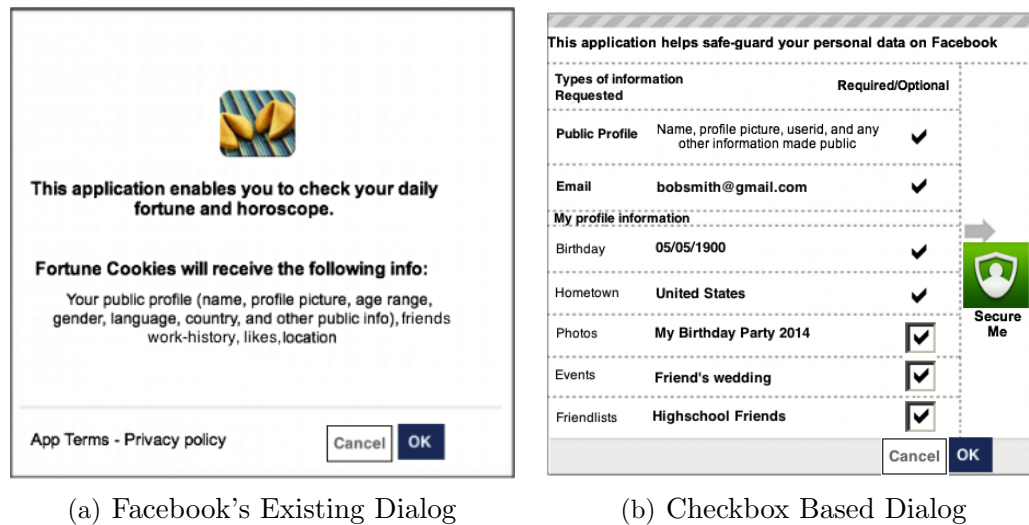


Figure 9: Control and Checkbox-based Dialog Designs

I developed 6 Facebook applications from categories including fortune telling, games, comics, and others, to incorporate each of the three conditions in my experiment. My applications were mockups of 6 popular Facebook applications using their logo and description. Each application requested the same number of permissions—4 required

and 3 optional.

4.2.1.2 Eye-Tracking Data

To collect evidence of whether the participants paid more attention to the animated dialog as compared to the other dialog designs, I logged eye-gaze data and analyzed the following information.

- **Eye-gaze fixation count**— An eye-gaze fixation refers to the maintenance of visual gaze at a single location. I used fixation counts to determine if the participants looked at the permission descriptions and information examples in the animated dialog more often compared to the other dialogs.
- **Eye-gaze fixation duration**— I used fixation duration to study whether the participants looked at the permission descriptions and information examples in the animated dialog for a duration longer than the other dialogs.
- **Saccades/Eye-movement pattern**— A saccade is a rapid eye movement (a jump) which is usually conjugate (i.e. both eyes move together in the same direction) and under voluntary control. I studied whether the participant eye-movements follow the expected pattern i.e., from permission description to information example, and then the decision area. Figure 10(b) shows an example of eye-gaze fixations and saccades of a participant over my animated dialog. The yellow circles represent the fixations and the lines represent the saccades.

I used **The Eye Tribe**² eye-tracker to record eye-gaze data in my experiment.

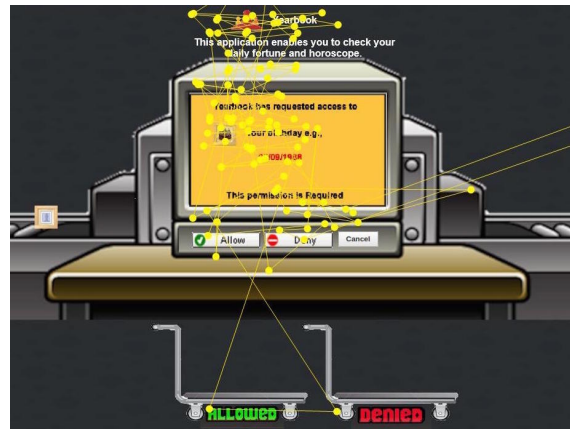
The participants completed a 9 point eye-calibration procedure at the beginning of

²<https://theeyetribe.com>

the study session. My study was designed as a slideshow experiment using the open source *The Open Gaze and Mouse Analyzer (OGAMA)* [42]. Each application installation task and survey was designed as a separate web slide. OGAMA supports The Tribe Eye-Tracker and records the eye-gaze data from the underlying slideshow based experiment. To log eye-gaze data over specific areas on each dialog design, I created areas of interests (AOIs) on the preview image of the application installation web slides. These AOIs include permission descriptions, personal information examples, decision buttons, decision summary carts, application logo, and description. Figure 10(a) shows my experimental setup. The eye-tracker was placed below the computer screen.



(a) Experimental Setup



(b) Eye-Gaze Fixations and Saccades of a Participant

Figure 10: Experimental Setup and Eye-Gaze Fixations/Saccades on the Animated Dialog

4.2.1.3 Surveys

- **Usability**— To evaluate the dialog designs w.r.t ease of use and learnability, I designed a questionnaire based on the System Usability Scale (SUS) [16].

- **Comprehension**— To study the effectiveness of permissions layout in each dialog design, I designed a Likert scale based survey focusing on the following:
 1. Ease of differentiating the required permissions from the optional permissions
 2. Ease of reading the permissions
 3. Extent to which personal information was informed
 4. Influence of personal information examples on authorization decision
 5. Increase of concern about personal information

4.2.1.4 Study Session

My study used a within-subject design. After signing the consent form, participants completed the demographic survey. The participants then logged into their Facebook account, and were given the following instructions:

“You will be using and evaluating 6 Facebook applications. You will complete a short survey after every two applications. At the end of the study, you will complete an exit survey”. At the beginning of the session, the participants underwent the eye-tracker calibration procedure. The participants were not informed about the purpose of eye-tracking in the study. The participants were given a brief tutorial on how to install an application using the three dialog designs. The order of the dialog designs and the applications shown to a participant was counterbalanced to prevent learning and practice effect.

4.2.2 Participants

I recruited my participants from the university through email announcements. An email describing the purpose of the study was sent to all students. In order to be

eligible, the participants were required to have a Facebook account and be users of Facebook applications. The eligible participants were invited to the lab to complete the tasks, and received a \$5 gift-card for participation.

A total of 16 participants successfully completed the study, 10 males and 6 females. My participants were active Facebook users who were members for more than 4 years. 70% were between the ages of 25 to 30. 90% had four or more years of college education. 50% of the participants frequently used Facebook applications.

4.3 Study Results

4.3.1 Attention Switch and Maintenance

I used eye-gaze fixation count and duration as metrics for measuring participant attention. I conducted a comparison of the repeated measures using Friedman’s test, showing a significant difference in the fixation counts on permission description of the three dialogs at the $p < .05$ level [$X^2(2) = 9.69$, $p = 0.004$]. Post-hoc analysis with Wilcoxon signed-rank test was conducted with a Bonferroni correction, resulting in a significant difference between the fixation counts on animated (mean=5.1, SD=2.7) and control (mean=3.1, SD=1.7) dialog with an effect size of 0.4, and between animated (mean=5.1, SD=2.7) and checkbox (mean=3.8, SD=2) based dialog with an effect size of 0.31 (See Figure 11(a)). Thus, the participants had significantly more eye-gaze fixations on permissions (descriptions and permission type) when using the animated dialog. Note that for the control dialog, I used fixations from both required and optional permission dialogs.

Similarly, I conducted a Friedman’s test for the effect of dialog design on eye-

gaze fixation duration over permission description. The experiment showed significant differences in the fixation durations of the three dialogs at the $p < .05$ level [$X^2(2) = 7.24$, $p = 0.04$] (See Figure 11(b)). Post-hoc analysis with Wilcoxon signed-rank test was conducted with a Bonferroni correction, resulting in a significant difference between the fixation durations on animated (mean=167 ms, SD=288 ms) and control (mean=128 ms, SD=111 ms) dialog with an effect size of 0.3. Thus, the participants had significantly longer eye-gaze durations on permissions (descriptions and permission type) when using the animated dialog. The higher number and longer

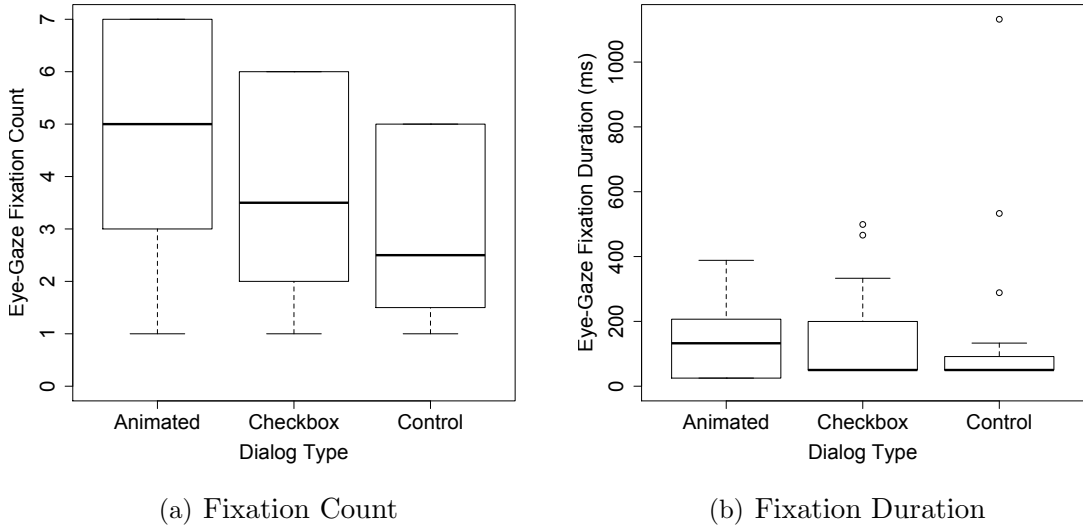


Figure 11: Eye-gaze Fixations On Permission Descriptions

eye-gaze fixations on permission descriptions in the animated dialog show that the animated dialog was able to switch and maintain the participants' attention towards the permissions. However, the higher fixations counts on the animated dialog can be attributed to the sequential display of permissions, and the fact that participants have to look at a single piece of information at a time.

The participants had more eye-gaze fixations and of longer duration over personal information examples while using the animated dialog as compared to the checkbox-based dialog. Wilcoxon signed-rank test showed significant differences between the eye-gaze fixation count on information examples of animated (mean=14.81, SD=14.73) and checkbox (mean=3.69, SD=5.21) dialog with $p=0.005$ and an effect size of 0.63. Similarly, the Wilcoxon signed-rank test for eye-gaze fixation duration on information examples showed significant difference between the animated (mean=287.39, SD=193.49) and checkbox (mean=181.66, SD=134.71) dialog with $p=0.002$ and an effect size of 0.49. Figure 12 shows the eye-gaze fixation counts and durations on animated and checkbox-based dialogs. Thus, the participants paid more attention to the personal information examples on the animated dialog as compared to the checkbox-based dialog. This may be attributed to the red font used to display the information in the animated dialog. The longer eye-gaze fixations on personal information examples in the animated dialog show that the animated dialog is able to maintain attention towards the permissions significantly more as compared to the checkbox-based dialog.

I also analyzed the participants' eye-movement (saccade) patterns in order to get a better understanding of the attention paid towards the permissions before making a decision. My hypothesis was that the participants will have more eye-movements from the permission description area to the decision (allow/deny/cancel button) area in the animated dialog compared to the other dialogs. I excluded the eye-movements towards and from the personal information examples areas. I performed a comparison of the repeated measures using Friedman's test on the effect of dialog design on

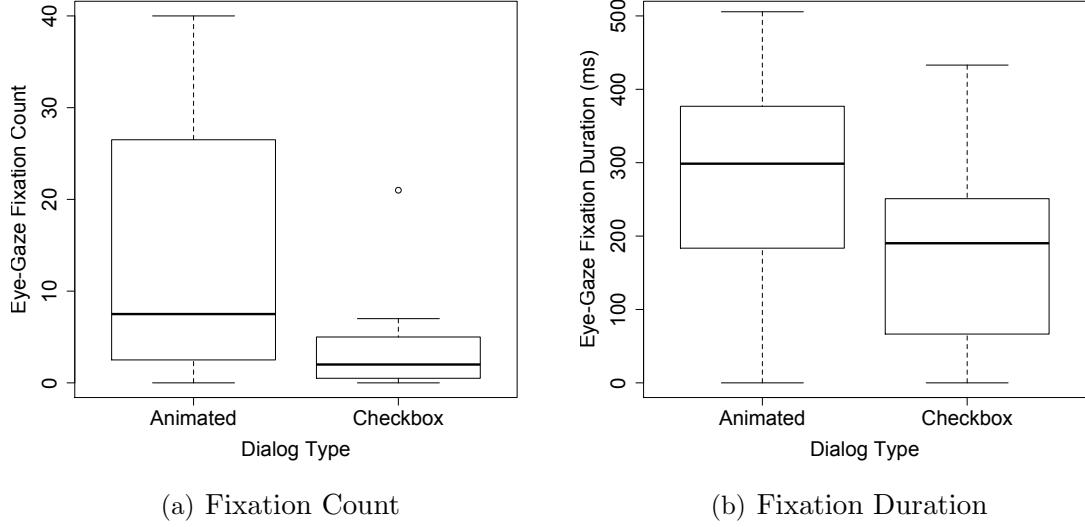


Figure 12: Eye-gaze Fixations On Information Examples

saccade counts from the permission description area to the decision area. However, the experiment showed no significant differences in the saccade counts of the three dialogs at the $p < .05$ level [$X^2(2) = 3.19$, $p = 0.18$] (see Figure 13(a)). Therefore, the participants seemed to have equal number of eye movements from the permission description to the decision area in each dialog. A possible reason for why this pattern was not observed more frequently in the checkbox-based and animated dialog is due to the presence of the personal information examples between the permission description and the decision area. Moreover, the animated dialog had many other elements which distracted the participant attention. For example, many participants also looked at the decision summary carts (containing their previous allowed and denied permissions), before making a decision on the current permission. Some participants also looked at the application logo and description to remind themselves about the application context. To verify this, I conducted another analysis on the checkbox-based

and animated dialog to study the eye movements from the permission description to information examples. Wilcoxon signed-rank test between the saccade counts from permission description to information example showed significant differences between the saccade count on animated (mean=3.69, SD=4.39) and checkbox (mean=1.06, SD=1.18) dialogs with $p=0.01$ and an effect size of 0.57. Figure 13(b) shows the saccade counts of the participants using the checkbox-based dialog and the animated dialog.

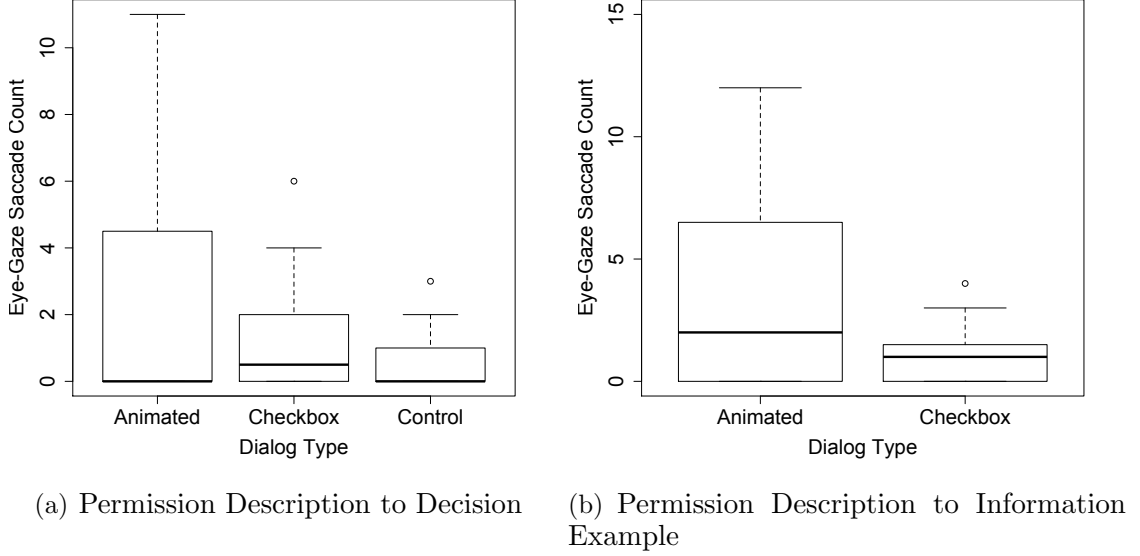


Figure 13: Participants Eye-gaze Saccades

A heat map is a visualization technique derived from the eye-gaze fixation maps [40]. A heat map separates different levels of observation intensity better than the fixation maps. Color mapping is usually selected so that the longer the observation, the warmer the color used to represent it. Figure 14 shows the heat map of the eye-gaze fixations on various elements (permission description, information examples, and decision areas) of the three dialog designs. The heat map for the control

dialog surprisingly covered the application logo, application description, permission descriptions, and the decision areas. However, the red region showing longer fixations did not cover any of these areas completely. The optional permissions dialog in the control design were not included in the calculation because a few participants chose not to install the application by clicking cancel on the first dialog, and therefore did not see the optional dialog. The heat map for the checkbox-based dialog had good coverage, with the participants paying more attention to the personal information examples, and the decision areas for the optional permissions. The permission descriptions were not looked at that much probably because the information examples seemed enough for making decisions. The heat map for animated dialog was quite unexpected and did not have the extent of dialog coverage as I had expected. The red region shows that participants paid most attention to the personal information examples and the permission descriptions in the animated dialog. This could have attracted the most attention because it showed the most important information to the participants. Moreover, this area was animated—the information appeared and disappeared, and the fonts and background color changed.

4.3.2 Permission Comprehension

Next, I evaluated the effectiveness of permission layout in my proposed dialog w.r.t helping the users easily read and differentiate permissions, and making them aware and concerned about the associated information disclosure.

I analyzed the (Likert scale-based) participant ratings of the permission layout and personal information examples for each dialog using their responses to the permission

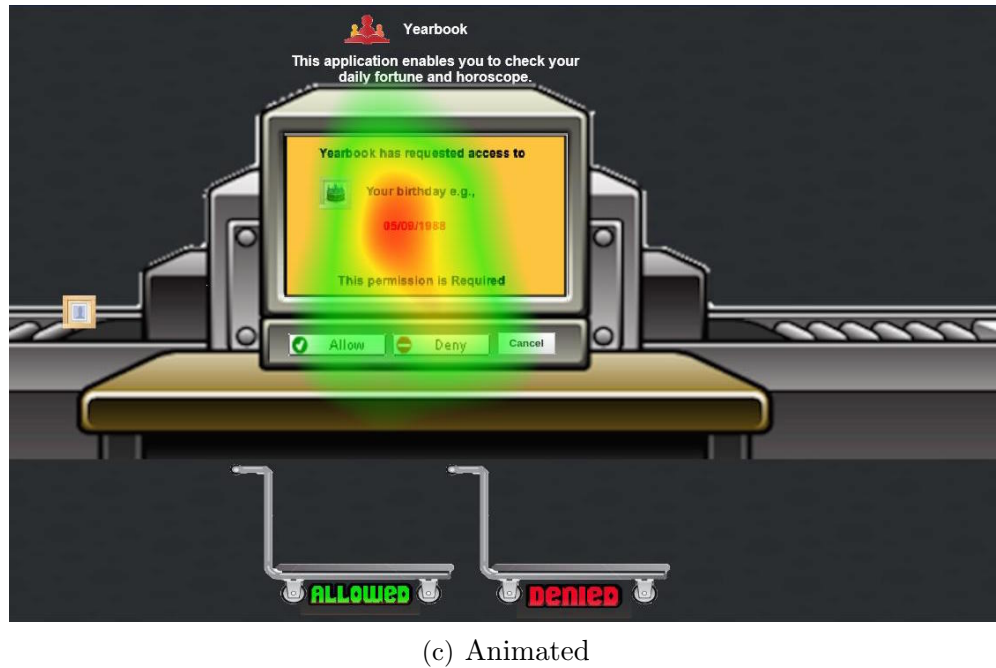
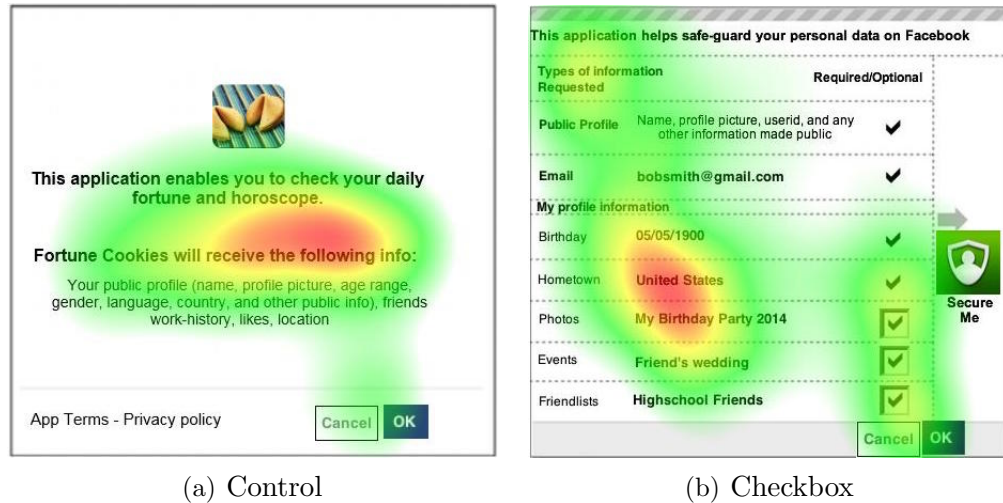


Figure 14: Heatmaps of eye-gaze fixations on the three dialog designs

comprehension survey presented to them at the end of the study.

Table 1 shows the average participant ratings for the permission layout and information examples presented on each dialog. In order for the participant to make a decision, it is important that they understand the permissions from which they can opt out. The ratings show that the participants found it easier to differentiate the

required permissions from the optional permissions on the animated dialog, primarily due to the explicit mention of permission type under each permission. The participants found it easier to read the permission descriptions on the control dialog design, possibly due to lesser amount of time required to read them.

The participant ratings for the personal information examples show that the inclusion of examples had an impact on their decision to allow or deny a permission. This rating is higher for the animated dialog than that of the checkbox-based dialog. Moreover, the participants indicated that if the personal information examples were included in the control dialog, it would have made an impact on their authorization decisions.

As compared to the checkbox based, and control dialog, the animated dialog had a higher average rating for how well it informed the participants of their personal information. Both the checkbox-based dialog and the animated dialog made the participants feel more concerned about their personal information as compared to the control dialog.

Table 1: Average participant ratings for the effectiveness of permission layout and information examples in each dialog

Dialog Type	Ease of differentiating required & optional permissions	Ease of reading the permissions	Personal information examples (would have) influenced the authorization decision	Informed about the personal information	Increased the concern about personal information
Control	3	5	5	3.66	3
Checkbox	3.33	3	4	4.33	4.33
Animated	4.33	4.33	4.66	4.66	4.33

4.3.3 Permission Authorization Behavior

To analyze the animated dialog’s influence on users’ installation decisions, and the deviation from *allow-all permissions* behavior, I measured the extent to which the participant’s openness to authorize permissions differed for the applications installed using the three dialogs.

The participant permission openness for an application was calculated as the number of permissions allowed out of the total number of permissions requested by the application. Therefore, the openness ranged from 0 to 1. I conducted a comparison of the repeated measures using Friedman’s test, showing a significant effect of dialog design on the permission openness at the $p < .05$ level for the three conditions [$\chi^2(2) = 8.481$, $p = 0.0012$]. Since the p value of 0.0012 is less than 0.05, I conclude that there is sufficient evidence to support the claim that the dialog used to install the application had a significant affect on the number of permissions authorized by the participants irrespective of the type of application showed. Post-hoc analysis with Wilcoxon signed-rank test was conducted with a Bonferroni correction, indicating that the mean permission openness for the animated dialog ($M = 0.35$, $SD = 0.47$) was significantly different from that of the checkbox-based dialog ($M=0.66$, $SD=0.41$) with an effect size of 0.10, and from the control dialog ($M=0.79$, $SD=0.49$) with an effect size of 0.41.

4.3.4 Ease of Use and Learnability

Based on the participant responses to the usability surveys, I calculated an aggregated System Usability Scale (SUS) score of the ease of use and learnability for each

dialog using the method described in [16]. My hypothesis was that the participants will rate the usability of animated dialog equal to that of the checkbox-based and control dialog designs. To test this hypothesis, a comparison of the repeated measures was performed using Friedman’s test. The test showed no significant differences in the SUS scores of the three dialogs at the $p < .05$ level, ($X^2(2) = 1.66$, $p = 0.45$) (see Figure 15).

A few participants complained that the animated dialog is slower than the other designs for application installation (see Table 2 for average visit duration per dialog). The likability of the animations was also subjective, with some participants indicating that it suits their style and some stating that they prefer the simpler text-based design. A few participants liked the control dialog design because of its simplicity. However, they preferred to see a single dialog instead of two. Some participants stated that the checkbox-based dialog had too much information and found it to be confusing. A few participants suggested to use colors to differentiate permissions.

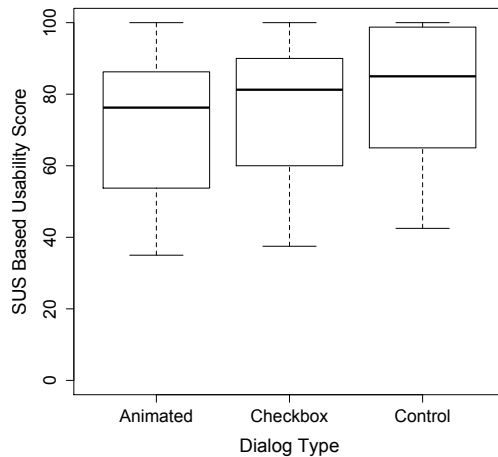


Figure 15: Usability scores of the three dialogs

Table 2: Average visit duration on each dialog

Dialog Type	Mean (ms)	Standard Deviation (ms)
Control	30.76	17.57
Checkbox	26.98	24.82
Animated	96.12	77.13

4.4 Discussion

My results show that the animated dialog is able to switch and maintain participant attention towards permissions. Unlike Bravo-Lillo et al. [15] I find that my non-inhibitive attractor—red font-based highlight on the information examples along with the background color beneath the text attracted the participants’ attention. However, I did not incorporate habituation in my study. The focus of my study was to investigate the viability of animation on permission dialogs as potential attention attractors, and how users perceive it. My future work involves conducting a habituation-based study on a larger sample (to represent the broader Internet population).

Similar to the eye-tracking results on Facebook connect dialog by Furman et al. [27], I find that participants had significantly more eye-gaze fixations on the permission descriptions and information examples in the animated dialog as compared to the control dialog. However, the authors found no difference in participants’ decision to authorize the dialogs in the three conditions. My results on the other hand, show a significant difference in the participants’ permission authorization decisions in the control and treatment conditions. My results also correlate with those of Harbach et al. [32] and show that the personal information examples are effective in making the users concerned about their information.

My results support the conclusions claimed by Wang et al. [43]. The checkbox-based dialog also had an impact on participants’ information disclosure as compared to the control dialog design. The personal information examples and decision areas

were found to be the primary attractors in the checkbox-based design. Therefore, I believe that the inclusion of personal information examples in the actual design proposed by Wang et al. [43] will further improve its effectiveness.

4.5 Conclusion

I explored the use of animation on application authorization dialogs as a possible attention attractor towards permissions. My preliminary study on the proposed animated dialog showed promising results. The participants had significantly more and longer eye-gaze fixations on permission descriptions in the animated dialog. The participants also looked longer at the personal information examples on the animated dialog as compared to the checkbox-based dialog. The personal information examples in particular, made the participants more concerned about their information and motivated them to read and evaluate the permissions. This was further observed in the participants' permission authorization decisions which were significantly more conservative compared to that on the other dialog designs. The participant ratings for the ease of use and learnability of the animated dialog were not significantly different than those of the other dialog designs.

CHAPTER 5: INVESTIGATION OF ACTIVE EYE-TRACKING ON APPLICATION AUTHORIZATION DIALOGS

Looking at permissions is the first step towards assessing the risks involved with application installation. I propose an eye-tracking based mechanism of enforcing user attention on application permissions. My approach is inspired by two existing systems. First is a mechanism on various websites to ensure that the user has read the privacy/consumer policies before clicking on the *I Agree* button. The decision buttons are initially deactivated, and once the user reads and scrolls down on the policy, they are activated. Second is an eye-tracking based mechanism to put the user into the habit of looking at the URL address bar to determine the website's legitimacy before entering sensitive information [35]. The input fields are initially deactivated, and once the user looks at the URL address (determined using the eye-gaze fixations on the URL address bar screen coordinates), they are activated. I deactivate the decision buttons on the dialog, and use feedback from the eye-tracker to ensure that the user has looked at the permissions. After determining user attention, the decision buttons on the dialog are activated. I implemented a Chrome browser extension for this purpose. The extension deactivates the decision buttons when it detects an application authorization dialog. It then uses a web-socket to receive eye-gaze data from the eye-tracking module. Based on the overlap of the received eye-gaze coordinates and the permission coordinates on the screen, the extension determines

when to enable the decision buttons on the dialog.

In this chapter, I propose an eye-tracking based mechanism of enforcing user attention on the application permissions. I implement a prototype of my proposed system and conduct two experiments to evaluate its effectiveness. I show my approach's preliminary evaluation through two experiments. My first experiment on 60 participants tested the participants' attention, where as, my second experiment on 45 participants focused on my approach's resistance to habituation. Using participants' eye-gaze fixations, permission identification, and authorization decision, I evaluate my participants' attention towards permissions.

5.1 Eye-Activated Permission Authorization

This section introduces a mechanism for enforcing end-user attention towards the application's requested permissions at install-time. Section 5.1.1 summarizes the overview and my assumption, that is, forcing the end-users to look at the permissions will be beneficial for them. Section 5.1.2 presents the design and implementation of my proposed scheme.

5.1.1 Overview

I speculate that forcing the user to look at the permissions is the first step towards combating habituation and installing safe applications. Once the user gets into the habit of looking at the permissions, this action will often be performed unconsciously. Even if the primary concern of the end-user is not security, the habit would work like a conditioned reflex action. The habit will also improve the chance of being aware of the security information.

In my pilot study in the previous chapter, I analyzed the eye-gaze data of 16 participants on a permission authorization dialog as they installed Facebook applications. Figure 16 shows a heatmap of eye-gaze fixations on various regions of the dialog. The red region shows the areas users looked at for a longer duration, while the green region shows the areas where the users looked at for a shorter duration. It can be observed from the figure that the majority of participants did not spend enough time on the dialog text to demonstrate that they had read the text.



Figure 16: Heatmap of eye-gaze fixations on Facebook application authorization dialog (as of early 2015)

I propose and develop a mechanism for enforcing user attention towards application permissions. Using eye-gaze data, I determine if the users look at a particular portion of the dialog on the screen. Failing to look at the permissions text area prevents the users from continuing the installation process.

5.1.2 Design and Implementation

My system has the following features:

- Dialog button control

My system has functions to detect and activate/deactivate the buttons on an installation dialog. The system deactivates the “Allow” and “Deny” buttons on the dialog at first. When it detects that the user has checked the permissions displayed on the dialog, these buttons are then activated.

- Eye-tracking

My system interacts with the eye-tracking device and identifies that the user has looked at a particular portion in the web browser with certainty.

- Permission localization

My system is able to locate the application’s permission text within the screen (assuming a maximized browser).

The architecture of my system is shown in Figure 17. It consists of an eye-tracking module, and a browser extension module. The browser extension module deactivates all decision buttons on the dialog at first. The task of the eye-tracking module is to interact with an eye-tracker and retrieve eye-gaze fixation coordinates. The eye-tracking module communicates with the eye-tracker server over a TCP socket connection, and retrieves the eye-gaze positions using the tracker API. The browser extension module receives these coordinates from the eye-tracking client module through a web socket, and determines whether the user looked within the permission text area. The buttons are activated when at least 30 consecutive eye-gaze fixations (measured at 10 eye-gaze fixations per second) are found in that area. This is equivalent to spending approximately 3 seconds scanning the permission text area. I used The Eye-Tribe

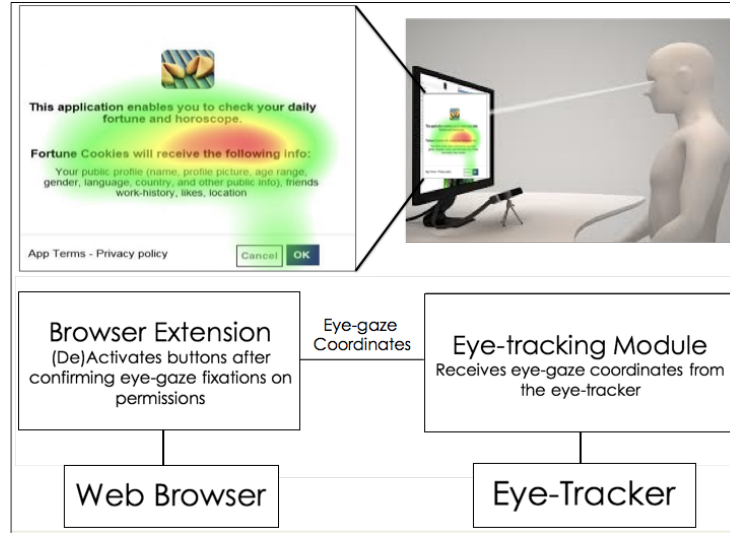


Figure 17: System Architecture

eye-tracker [1] as the eye-tracking device. Its software development kit (SDK) embeds the function of web server and provides the user’s eye-gaze position in JavaScript Object Notation (JSON) format messages.

The limitation of my prototype was the localization of permissions. I estimated the absolute position of the permission text on the screen, assuming the browser window is maximized.

5.2 Evaluation

I used two experiments to evaluate my approach’s effectiveness on Facebook’s existing application installation dialog (see Figure 18). The experiments were approved by UNC Charlotte’s IRB³. My first experiment intends to measure user attention towards the permissions displayed on the dialog. The second experiment focuses on measuring my system’s resistance to habituation. I gave each participant a \$5 Starbucks gift card at the end of the study.

³IRB Protocol #13-03-30

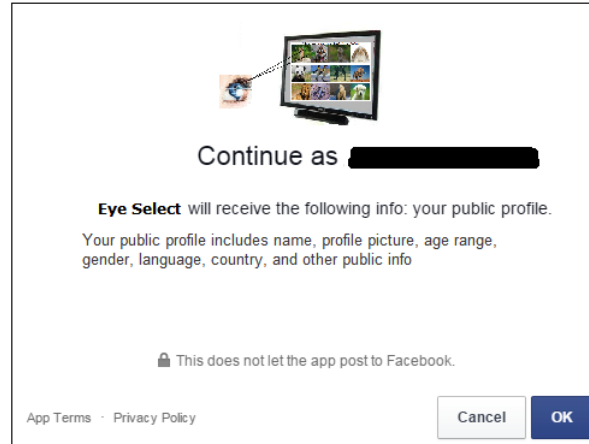


Figure 18: Eye-Select Facebook application dialog used in my experiment

5.2.1 Experiment 1: Attention

My first experiment focused on measuring participant attention towards permissions. I used a between-subjects design for this experiment. I placed participants either in the control or treatment group; exposure to both might have led the participants to suspect that I was studying the installation dialogs. In order to maintain ecological validity and more closely study participant behavior, some amount of deception was used. I did not tell the participants that they were participating in a security/privacy related study. The participants were asked to evaluate the feasibility of an eye-activated browser by performing a set of tasks that involved eye-tracking.

5.2.1.1 Methodology

I recruited my participants through Craigslist and word of mouth. I advertised my study on Craigslist and the eligible candidates were invited to campus for participation. I also asked the participants to spread the word about my study without revealing the actual goal of the study.

Conditions— I compared participants’ attention using my proposed approach to two other mechanisms. Therefore, my experiment had three conditions:

- Control - The participants in this group installed the applications using the default mechanism.
- Control with time constraint - The participants in this group spent 3 seconds (equivalent to 30 eye-gaze fixations) on the dialog before they made their decision. The decision buttons were activated after 3 seconds, instructing the participants to proceed. I added this condition to serve as a better indicator of whether spending more time on a dialog leads to better attention compared to my proposed system.
- Treatment - The participants in this group performed eye-gaze based button activation while installing an application. They were asked to look at the dialog’s permission text area to activate the decision buttons, and then proceed with the installation.

Tasks — The participants first logged into their Facebook account. I then briefed them about the tasks which involved eye-tracking. These tasks were implemented as Facebook applications which the participants installed and used. They also had the option of not installing an application. If the participants chose not to install an application, it did not harm my experiment since I was studying the dialog and not the application’s functionality. Therefore, in such scenarios, the participants were simply taken to the next application. I used the following three applications in my experiments:

- Eye-select application - This application asked participants to select an image by fixating their eyes on it. The participants selected a specific animal's image (for example, a lion) from the set of displayed animal images by finding and fixating on that animal's image until a popup confirming the selection appeared. The participants could continue to use the application if they wished. This application requested access to public profile information.
- Eye-draw application - This application asked participants to draw something on the screen using eye-gaze. The participants drew an object using their eye-gaze. This application requested access to public profile information.
- Eye-chase application - This is an eye-tracking based game in which the participant followed a set of random circles on the screen with his eye-gaze. The installation dialog for this application requested a Social Security Number (SSN) access permission, in addition to the public profile permission requested by the other two applications. Although SSN is never requested by any application, I chose it because the goal of my study was to see if participants would pay attention and identify strange text on the dialog.

The participants first installed and used the eye-select and eye-draw applications (order randomized), and finally installed and used the eye-chase application, and completed the post survey. All participants completed a 9 point eye-calibration process before using the applications.

Post Survey— Each participant completed a questionnaire at the end of the experiment. The first set of questions asked the participants about their eye-tracking

experience. To determine whether participants had noticed the permissions requested by the applications, they were asked questions related to the permissions. I asked the participants to write down the content displayed in each of the three dialogs. Next, the participants identified which of the displayed permissions were requested by the applications presented to them. In the end, the participants provided demographic information. After the participants completed the questionnaire, I informed them about the goal of my experiment.

Dependent Variables— I used the following metrics to measure participant attention on the authorization dialog’s permissions:

- Permission identification- The fraction of application permissions identified correctly. The requested permissions were public profile information and social security number.
- Eye-gaze fixation- The number of eye-gaze fixations on the permission text area of an application authorization dialog. An eye-gaze fixation refers to the maintenance of visual gaze at a single location.
- Authorization decision- The fraction of social security number permissions denied.

5.2.1.2 Participants

I ran my experiment between 1st Sept and 10th Oct 2016. A total of 60 participants completed the experiment—20 per group. Table 9 shows my study participant demographics.

Table 3: Participant demographics for the attention experiment

Age	n=60	% of n
18 to 20	9	15%
21 to 30	40	66.6%
31 to 40	11	18.3%
Gender		
Male	29	48.3%
Female	31	51.6%
Ethnicity		
Asian/Pacific Islander	36	60%
White/Caucasian	13	21.6%
Middle East	3	21.6%
Black/African-American	1	1.6%
Hispanic	1	1.6%
Decline to answer	2	3.3%
Education Level		
Bachelor's degree	28	38.3%
Master's degree	18	30%
Other	7	11.6%
Some college	7	11.6%
Associate's degree	5	8.3%

5.2.1.3 Eye-tracking Device

I used **The Eye Tribe**⁴ eye-tracker to retrieve eye-gaze information in my experiments. This eye-tracker can detect movement of the pupil with sub-millimeter precision. The average accuracy is around 0.5 degrees of visual angle. The system is capable of determining the on-screen gaze position roughly within the size of a fingertip (<10mm). All precision measurements in my experiments were done at a 60Hz sampling rate.

5.2.1.4 Results

To determine how each dependent variable (attention metric) differed for the independent variable (installation mechanism), I conducted the Kruskal-Wallis test for

⁴<https://theeyetribe.com>

each dependent variable below. I used Bonferroni correction to account for multiple tests being run. Therefore, I accepted statistical significance at $p < 0.016$.

- **Permission Identification**

I first analyzed whether there is a significant difference between the three participant groups with respect to the fraction of permissions identified correctly on the application installation dialogs. The post-survey questions asked the participants to select all the permissions requested by the three applications. I used this response to calculate the fraction of permissions correctly identified by the participants. Figure 19 shows the number of participants in each group who identified the public profile information, social security number, or both permissions. The participants who used the eye-activated dialog were able to identify both permissions better compared to the other two groups.

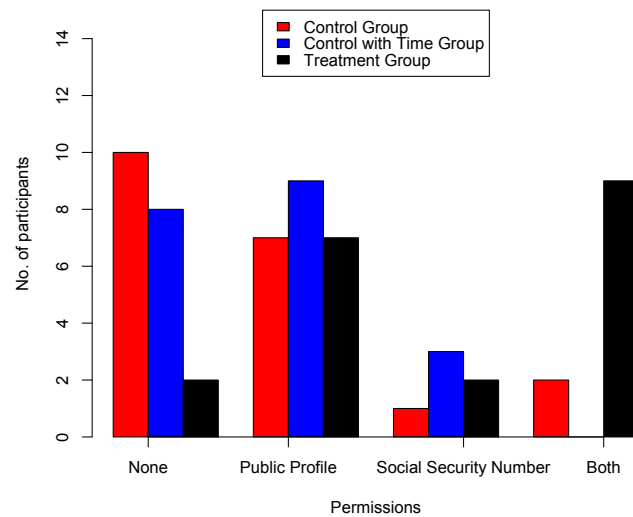


Figure 19: Number of participants who identified one or both permissions
(Attention)

The Kruskal-Wallis test showed a significant difference between the number of permissions correctly identified by the participants in the treatment group (mean=0.67, SD=0.37), the participants in the control group (mean=0.3, SD=0.34), and participants in the control with time constraint group (mean=0.27, SD=0.34) with $p=0.001862$.

Post-hoc comparisons using Nemenyi test, showed that there is a significant difference between the number of permissions correctly identified by the control and treatment group with $p=0.015$, and between the control with time constraint and treatment group with $p=0.0084$.

I also measured the precision and recall for the permissions identified by the participants. I calculated the precision and recall for each participant as follows.

$$\text{Precision} = \frac{\text{No. permissions correctly identified by participant}}{\text{No. permissions selected by participant}} \quad (1)$$

$$\text{Recall} = \frac{\text{No. permissions correctly identified by participant}}{\text{No. permissions requested by the applications}} \quad (2)$$

Figure 20 shows the permission identification precision and recall averaged over all the participants. The average precision and recall was higher for both the control with time constraint group, and treatment group, as compared to the control group.

- **Eye-Gaze Fixations**

I used eye-gaze fixation count as another metric for measuring participant attention towards application permissions. I logged the participants' eye-gaze coordinates while they were interacting with the installation dialogs. I defined

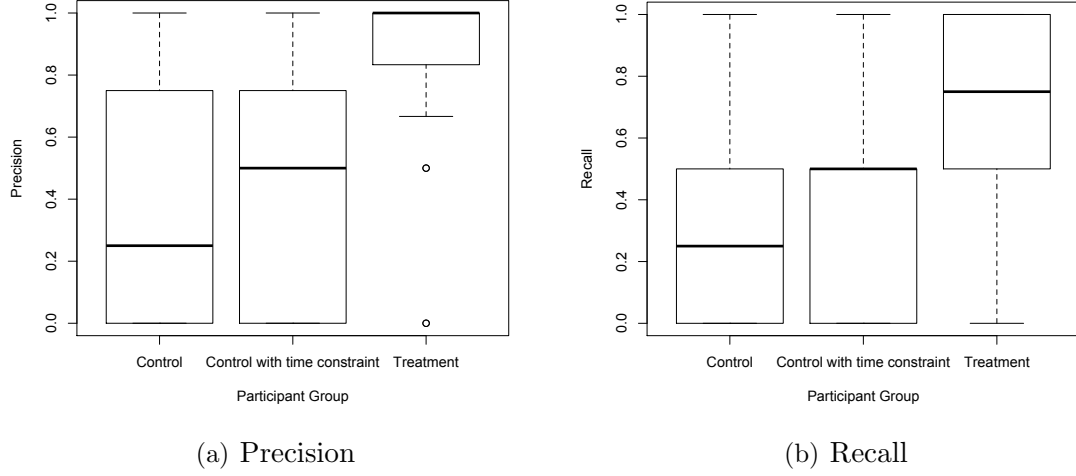


Figure 20: Participant permission identification precision and recall during the attention experiment

an area of interest around the permission text area and only counted the eye-gaze fixations within this area of interest.

Kruskal-Wallis test showed a significant difference between the number of eye-gaze fixations of the control group (mean= 14.16, SD= 19.12), control with time constraint group (mean=33.3, SD=30.08), and treatment group (mean= 38.2, SD= 6.7) averaged over the three application dialogs with $p=0.0003$. Pairwise comparisons using Nemenyi test showed that the treatment group had significantly more eye-gaze fixations than the control group with $p=0.00019$. However, the difference in the average number of eye-gaze fixations for the control with time constraint group and the treatment group was not significant. Figure 21 shows the eye-gaze fixation counts (averaged over the three application authorization dialogs) of participants in the three groups.

Figures 22 shows the total eye-gaze fixation coordinates of all participants in the

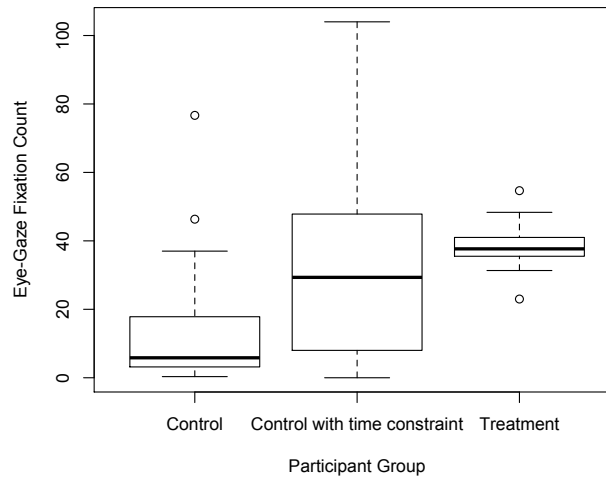


Figure 21: Average eye-gaze fixation counts on application permissions area of interest for the control, control with time constraint, and treatment group (Attention)

three groups, over the eye-select, eye-draw, and eye-chase application dialogs respectively.

- **Authorization Decision**

I also analyzed participants' authorization decisions on application installation dialogs which requested the social security number permission. Since there was only one application which requested the social security number permission, my dependent variable—fraction of social security number permissions denied by the participants, became a categorical variable. Therefore, I conducted a Chi-squared test on whether the social security number permission was denied or not. The test did not show a significant difference between the number of participants who denied the social security number permission in the control group (mean=0, SD=0), control with time constraint group (mean=0, SD=0),

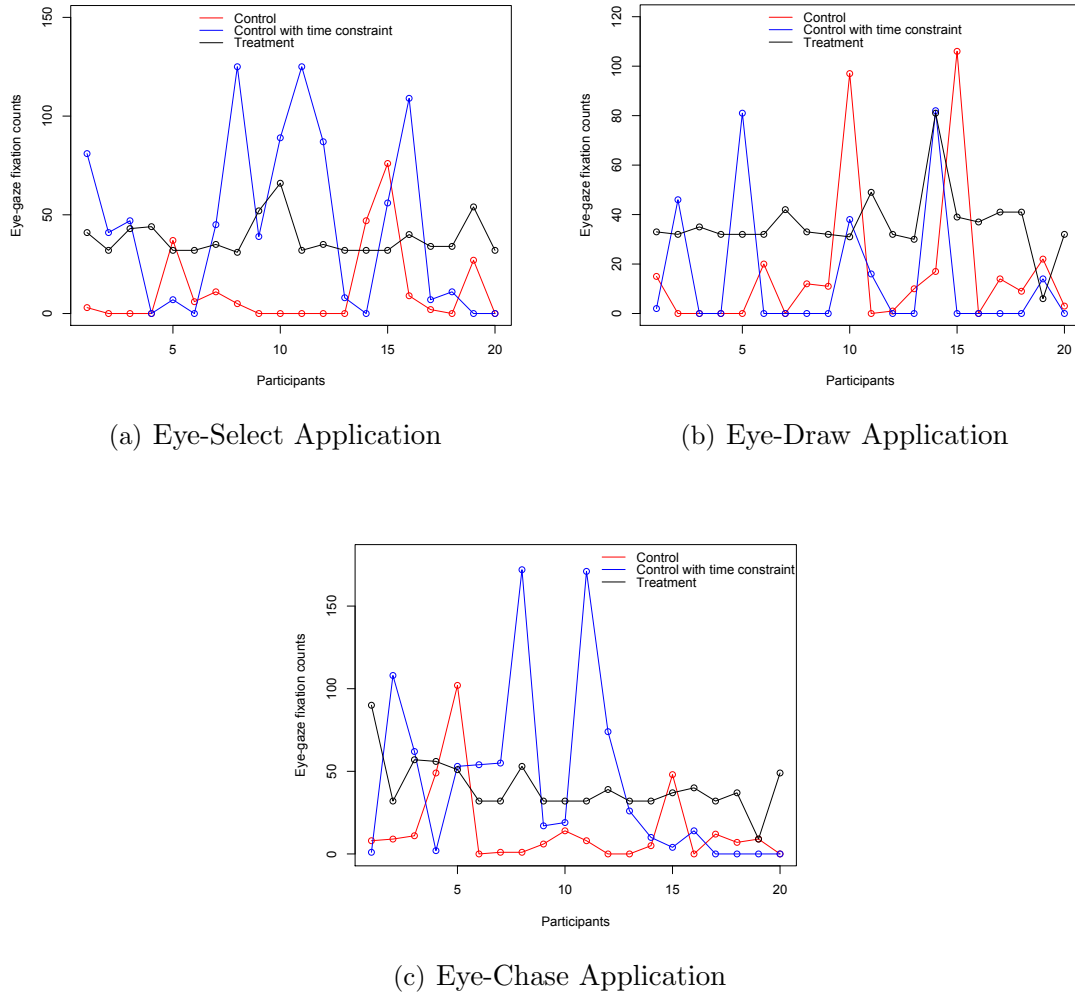


Figure 22: Eye-gaze fixations of participants on the application installation dialog permission area of interest (Attention)

and the treatment group (mean=0.15, SD=0.36) with $p=0.04$. 0 out of the 20 participants in the control group (0%) denied the social security number permission request as compared to 0 out of 20 participants in the control with time constraint group (0%), and 3 out of 20 participants in the treatment group (15%).

When debriefed about the goal of the experiment, a majority of the participants

reported that they had noticed the social security permission and thought it was strange that Facebook was requesting such information. However, they still authorized the permission because the experiment was being conducted in a lab environment. Although explicitly told about the option of not installing an application, some participants thought that they had to authorize all the permissions in order for the application to work.

5.2.2 Experiment 2: Habituation

My second experiment focused on finding my approach’s resistance against habituation. My design is inspired from Bravo-Lillo et al. work on attractors for security dialogs [15, 14]. They used attractors to highlight a field that was of no value during habituation, but contained critical information after the habituation period. I adapted their design by first habituating the participants to the dialogs (randomly from eye-select and eye-draw applications) with similar and safe permissions, and then dialogs from the eye-chase application containing additional SSN permission after the habituation period.

Similar to the attention experiment, I used a between-subjects design and the participants were presented with one of the three mechanisms of installing authorization dialogs.

5.2.2.1 Methodology

I recruited my participants through Craigslist and word of mouth. My study was advertised on Craigslist and the eligible candidates were invited to campus for participation. I also asked the participants to spread the word about my study without

revealing the actual goal of the study.

The participants logged into their Facebook account, and were told that they would be answering a set of 30 Facebook application dialogs inside the browser, and then complete a survey. The participants were repeatedly exposed to an installation dialog of eye-select and eye-draw applications during the habituation period. These applications showed the same public profile permission on their dialog. After the habituation period of 20 dialogs concluded, I presented the participants with the eye-chase application dialog (10 times) with a dangerous permission added to the permission list, to see if participants would notice it. My habituation experiment had the same three conditions as in the attention experiment. The participants in the time constraint group had to wait for 3 seconds on each dialog before they could make a decision, whereas the treatment group participants had to perform eye-gaze based button activation on each dialog by scanning the dialog's permission text with their eyes.

Task— I instructed the participants that they would spend approximately 2-3 minutes answering a set of 30 consecutive application installation dialogs. I informed them that I was studying how long it takes a user to answer such dialogs, in order to help us design better dialogs. The participants were also informed that eye-tracking would be performed as part of the study to check the eye-tracker's accuracy for future experiments. The participants had to go through the eye-tracker calibration procedure before beginning the task.

During the habituation period, the dialogs from eye-select and eye-draw applica-

tions were presented, which only requested access to public profile information. After the participant made a decision (install/cancel) on one dialog, the browser immediately presented the next dialog. To inform the participant of how many dialogs have been answered, a counter was displayed on top right corner of the dialog. The dialogs were mimicked as Facebook dialogs by adding the participant's name on it, and were shown centered on the screen. The habituation period of 20 dialogs was followed by a test period of 10 dialogs. However, the transition to the test period was not noticeable. Immediately after the first 20 dialogs, the participants were presented with 10 installation dialogs from eye-chase application, which had an additional dangerous permission of "social security number". These dialogs were also presented one by one. Participants who read the text in the test period ideally should have noticed the extra permission and clicked the "cancel" button.

Post Survey— After the test period concluded, I presented the participants with a questionnaire. I asked the participants to recall and type the contents of the last few presented dialogs. I used this response together with other follow-up questions to analyze my approach's resistance to habituation. After the participants completed the questionnaire, I informed them about the goal of my experiment.

Dependent Variables— I used the same dependent variables as in my attention experiment.

- Permission identification- The fraction of permissions identified correctly. The requested permissions were public profile information and social security number.

- Eye-gaze fixations- The number of eye-gaze fixations on the permission text area of an application authorization dialog. An eye-gaze fixation refers to the maintenance of visual gaze at a single location.
- Authorization decision- The fraction of social security number permissions denied by the participant.

5.2.2.2 Participants

I ran this experiment in parallel with the attention experiment between 1st Sept and 10th Oct 2016. A total of 45 participants completed the experiment, 15 per group. These participants were different from the participants in the other experiment. Table 4 shows my study participant demographics.

Table 4: Participants demographics for the habituation experiment

Age	n=45	% of n
18 to 20	10	22.2%
21 to 30	26	58.3%
31 to 40	8	19.4%
50 to 60	1	2.2%
Gender		
Male	27	60%
Female	18	40%
Ethnicity		
Asian/Pacific Islander	16	35.5%
White/Caucasian	21	46.6%
Black/African-American	6	13.3%
Other/Multi-Racial	2	4.4%
Education Level		
Some college	16	35.5%
Associate's degree	6	13.3%
Bachelor's degree	14	31.1%
Master's degree	9	20%

5.2.2.3 Results

Similar to the previous experiment, I studied my approach's resistance to habituation by conducting Kruskal Wallis test on each of the three dependent variables.

- **Permission Identification**

First, I analyzed the percentage of participants who correctly identified the public profile information, and social security number permissions at the end of the test period. The post-survey questions asked the participants to select the permissions requested by the last few applications. The Kruskal-Wallis test showed a significant difference between the number of permissions correctly identified by the control group (mean=0.6, SD=0.38), control with time constraint group (mean=0.53, SD=0.29), and the treatment group (mean=0.9, SD=0.2) with $p=0.0047$.

Post-hoc comparisons using Nemenyi test however only showed significant difference between the treatment and the control with time constraint group with $p = 0.013$.

Figure 23 shows the number of participants who correctly identified one or both permissions correctly. The average number of participants who identified both permissions correctly was higher for the treatment group as compared to the other two groups.

I also calculated the precision and recall for the permissions identified by the participants using the equations described in Section 5.2.1.4.

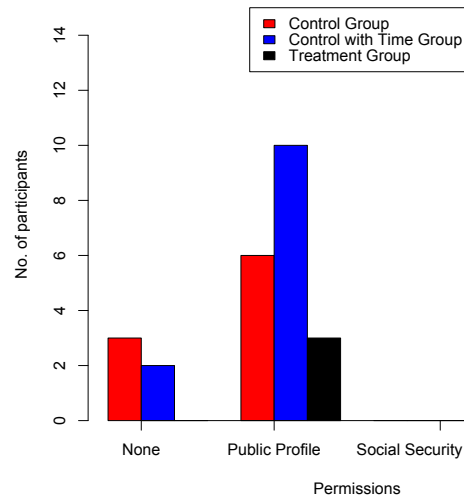


Figure 23: Number of participants who identified one or both permissions (Habituation)

Figure 24 shows the permission identification precision and recall. The precision and recall was higher for treatment group as compared to the control, and control with time constraint groups.

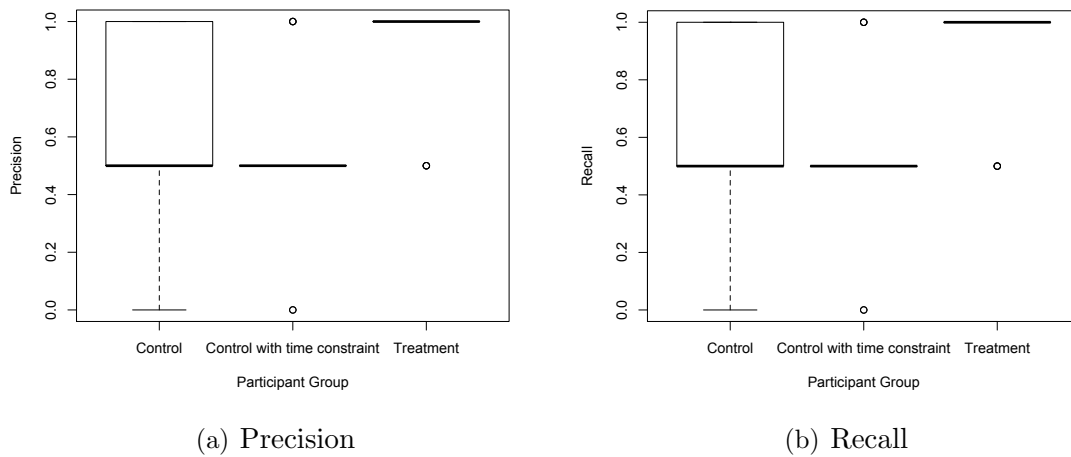


Figure 24: Participant permission identification precision and recall during habituation experiment

• Eye-Gaze Fixations

I used eye-gaze fixation count as another metric for measuring participants' resistance to habituation. I used the same area of interest defined in my attention experiment around the permission text area and only counted the eye-gaze fixations within this area of interest. Figures 25(a) and 25(b) show the average eye-gaze fixations of all 45 participants in the control, control with time constraint, and treatment groups on the dialogs shown during habituation and test period respectively.

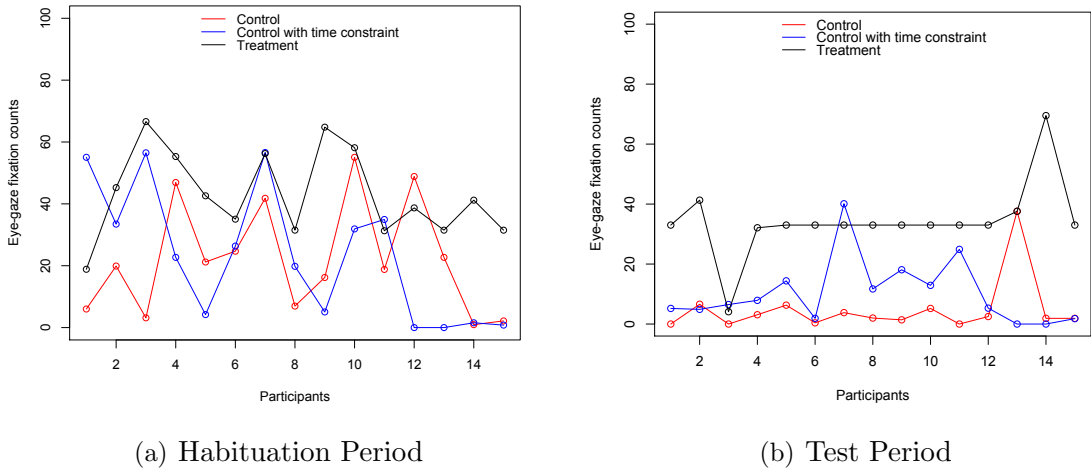


Figure 25: Eye-gaze fixations of participants on the application installation dialogs area of interest during habituation and test period

The Kruskal-Wallis test on the eye-gaze fixation counts during the test period showed a significant difference between the control group (mean =16.5, SD=12.74), control with time constraint group (mean=18.96, SD=16.02), and the treatment group (mean=40.26, SD= 9) with $p = 0.0001$. Post-hoc comparisons using Nemenyi test showed a significant difference between the number of

eye-gaze fixations of the control group and treatment group with $p=0.0003$, and between the treatment and control with time constraint group with $p=0.0013$.

Figure 26 shows the average eye-gaze fixation counts of the three groups during the habituation (first two applications' dialogs) and test period (last application's dialogs).

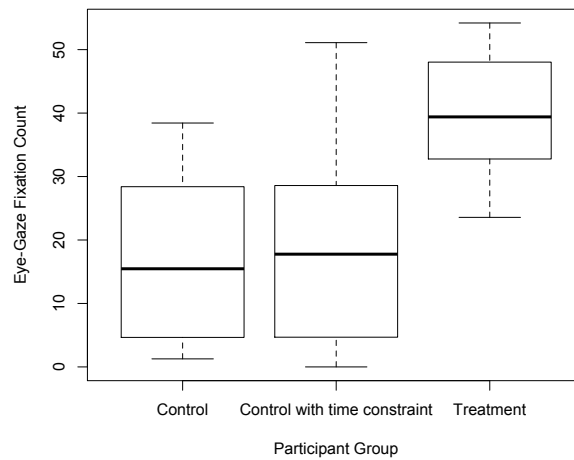


Figure 26: Average eye-gaze fixation counts on the application permissions for the control, control with time constraint, and treatment groups (Habituation)

- **Authorization Decision**

Lastly, I analyzed if participants' authorization decisions are affected by habituation. For this purpose, I calculated the number of social security number permissions denied by the participants (out of 10). Kruskal-Wallis test on the fraction of social security number permissions denied did not show a significant difference between the control group (mean=0.20, SD=0.378), control with time constraint group (mean=0.293, SD=0.447), and the treatment group (mean=0.32, SD=0.526) with $p=0.754$.

5.3 Discussion

Due to the requirement of staring at the dialog text, the number of eye-gaze fixations for the treatment group participants were naturally higher compared to that of the control group participants in both experiments. In order to verify that the participants actually read the permissions, I determined if they could identify which permissions were requested by the applications. The participants who used my proposed approach were able to identify both permissions (public profile, and the social security number permission) better than the other two participant groups, namely the control, control with time constraint group. Moreover, the permission recall and precision was higher for the treatment group participants.

I did not observe any difference in the authorization decisions of the three participant groups. Although the participants were explicitly told that they are free to choose not to install an application, most participants mentioned that they still installed the application despite being surprised by a Facebook application requesting “social security permission” because they trusted the experimenter.

I tried to evaluate participant attention in a realistic dialog scenario; however, the validity of my experiments is still limited. The sample size of 45-60 participants per experiment is small. In future, I intend to design a larger study to examine actual behaviors, and whether users would make different choices when forced to read the dialogs, by incorporating the following:

1. Give users the choice to install one of several different applications that vary based on the permissions requested, and see if the users would make different choices when

they are forced to read the dialogs.

2. Expose the users to my proposed approach for a longer duration to analyze resistance to habituation.

5.4 Conclusion

In this chapter, I investigated the hypothesis that forcing a user to look at the application permissions will increase the probability of the user paying attention to and reading the permissions. Therefore, I explored the viability of an eye-tracking based approach in enforcing user attention towards permissions, and therefore mitigating habituation. I implemented a prototype of my approach as a Chrome browser extension.

My experiment on 60 participants showed that the participants who were forced to look at the permissions by using my extension to install the applications demonstrated a slight improvement in attention. The treatment group participants were able to better identify the requested permissions as compared to the rest of the participants. The participants' logged eye-gaze coordinates supported my hypothesis and there was a significant difference between the eye-gaze fixations of the control, control with time constraint, and treatment group participants. However, the hypothesized increase in the rate at which participants denied a dangerous/unnecessary permission, from the control groups to the treatment group was not statistically significant. This could primarily be due to the study design and it being conducted in a lab environment.

My experiment on 45 participants showed similar results as from the first experiment, after the participants were repeatedly exposed to a set of application dialogs.

The participants who were forced to look at the permissions were able to better identify requested permissions correctly as compared to the control group participants, with higher precision and recall. The participants' logged eye-gaze coordinates on the dialogs presented during the test period showed that there was a significant difference between the eye-gaze fixations of the three participant groups. Once again, the hypothesized increase in the rate at which participants denied a dangerous/unnecessary permission, from the control group to the treatment group was not statistically significant. There was no difference in the fraction of social security number permissions denied by the three groups.

CHAPTER 6: IMPACT OF ADVERTISEMENTS ON USER ATTENTION AND DECISION ON AUTHORIZATION DIALOGS

Third-party application providers are relying heavily on advertising revenues. *Zynga*—a provider of popular games such as Farmville on Facebook, grew its advertising from \$74 million in 2011 to \$173 million in 2015.

Various types of advertisements are displayed in and around third-party applications. For example, *Zynga*, displays three types of advertisements in games it provides on Facebook (see Figure 29) [28]:

1. Banner advertisements –these are standard advertisements that show up above or below the game
2. Video advertisements –these are shown when the game is loading a new screen, or through incentive-based advertising, where the user gets either an in-game reward or Facebook credits (i.e., money) for watching the ad.
3. Product placement advertisements –in this type of advertisement, a brand or product is injected in the game in some way. For example, McDonald’s product can be placed in a farm inside the game FarmVille.

An eye-tracking study on users’ web page reading patterns showed that users often read web pages in an F-shaped pattern: two horizontal stripes followed by a vertical stripe [36]. Figure 28 shows heatmaps of user eye-gaze fixations on three websites

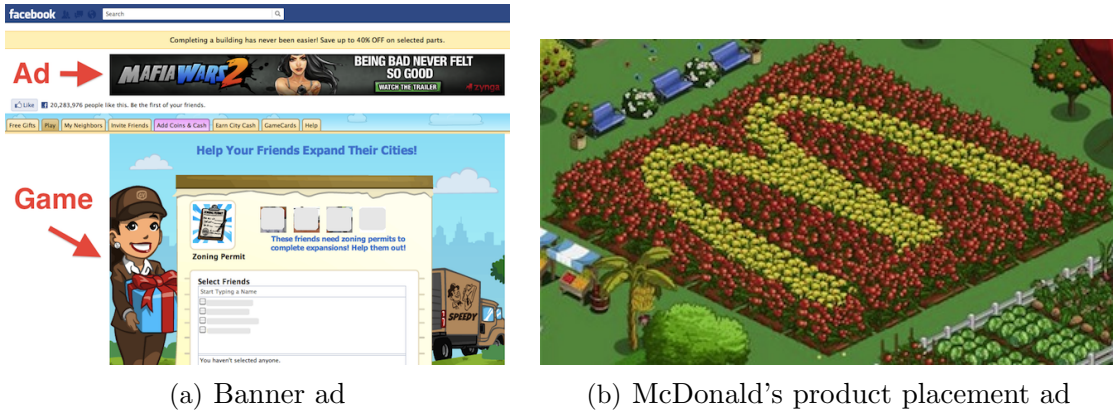


Figure 27: Banner and product placement advertisements in and around Zynga games on Facebook [28]

used in this study. It can be observed in the figure that users pay more attention to the top horizontal part of the web page. Hence, if advertisements are placed on top of the webpage, the users are more likely to pay attention to them.



Figure 28: Heatmaps from an eye-tracking study on three websites. The areas where users looked the most are colored red; the yellow areas indicate fewer views, followed by the least-viewed blue areas. Gray areas didn't attract any fixations.

The impact of such advertisements on user attention and decision while they are authorizing a third-party application has not been studied. In this chapter, I investigate whether the introduction of banner advertisements above an application's

authorization dialogs negatively impacts user attention towards permissions and their decision. I discuss the results of a user study on popular Facebook game applications.

6.1 User Study

I designed a user experiment focused on answering the following research questions:

- **Effect of advertisements' presence:** Does the introduction of advertisements above application authorization dialogs cause the users to pay less attention towards permissions and affect their decision to play the game?
- **Effect of advertisement content type:** Does the content type of an advertisement play a role in user's attention towards permissions and their decision to play the game?

I focused specifically on banner advertisements for my user study and employed a between-subjects design. Moreover, I only displayed the advertisements above authorization dialogs. I placed participants either in the control or treatment groups; exposure to all may have led the participants to suspect that I was studying the installation dialogs and/or advertisements. In order to maintain ecological validity and more closely study participant behavior, some amount of deception was used. I did not tell the participants that they were participating in a security/privacy related study and were asked to explore a few games on a popular gaming website *Zynga*. I developed a mockup of this website (see Figure 30). I told the participants that I am interested in analyzing how they interact with Facebook applications and for this purpose their eye-gaze will be tracked during the experiment. The experiment was

approved by UNC Charlotte's IRB⁵. I paid each participant a \$5 Starbucks gift card at the end of the study.

6.1.1 Methodology

6.1.1.1 Independent Variables

I compared participants' attention and decision on authorization dialogs in the absence of advertisements with that in the presence of two types of banner advertisements. Therefore, my experiment had three conditions:

1. Control - The participants in this group were not shown any advertisements above the application's authorization dialog
2. Static advertisements - The participants in this group were shown advertisements displaying a static image
3. Animated advertisements - The participants in this group were shown advertisements as images in Graphics Interchange Format (gif) which appeared to be short videos

Participants in each of the three conditions were exposed to four types of advertisement content:

1. Shopping—this content category displayed advertisements related to deals on shoes, clothes etc.
2. Food—this content category displayed advertisements related to deals on food items.

⁵IRB Protocol #13-03-30

3. Politics—this content category displayed advertisements related to politicians.
4. Sports—this content category displayed advertisements related to sports and players.

Figure 29 shows four examples of static advertisements, one for each content type.



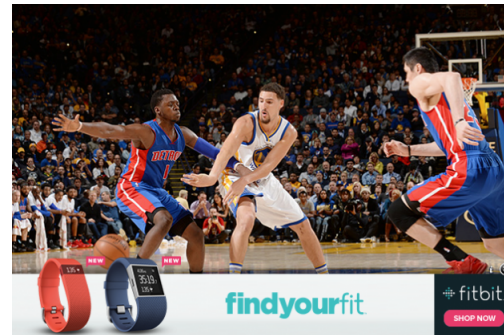
(a) Shopping



(b) Food



(c) Politics



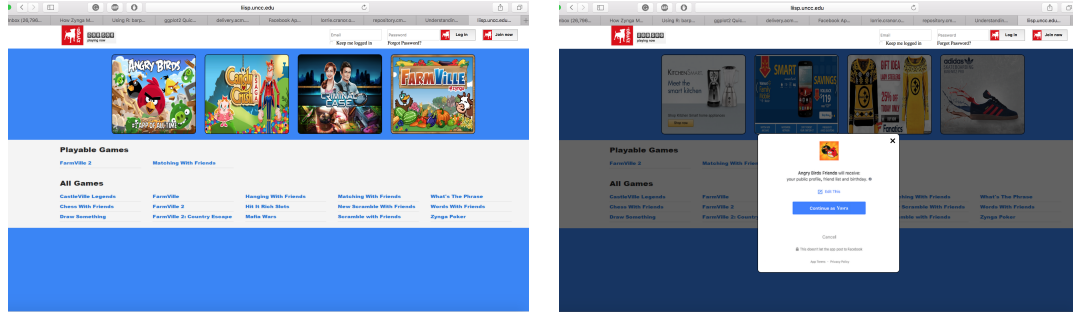
(d) Sports

Figure 29: Static advertisements with four types of content

6.1.1.2 Tasks

The participants first logged into their Facebook account. Each participant then completed a 12 point eye-tracking calibration procedure. I then presented the participants with a mockup of a popular gaming website. This website contained four popular Facebook applications namely, Candy Crush, Farm Ville, Angry Birds, and Criminal Case (See Figure 30(a)). I instructed the participants to explore this web-

site and play the games which they liked. Upon clicking a specific game’s icon, the Facebook authorization dialog was displayed along with advertisements of a specific content type above it (See Figure 30(b)). If the user chose to authorize the application’s requested permissions, they used the application for a few minutes.



(a) Website displaying applications used in our experiment (b) Advertisements displayed above the application authorization dialog upon clicking on an application

Figure 30: Mockup of the gaming website *Zynga* used in my experiment

6.1.1.3 Post Survey

Each participant completed a questionnaire at the end of the experiment. The first set of questions asked the participants about their gaming experience. To determine whether participants had noticed the permissions requested by applications, they were asked questions related to the permissions. I asked the participants whether they noticed any advertisements and if they were distracted by them. Next, the participants identified the content types of advertisements displayed to them. In the end, the participants provided their demographic information. After the participants completed the questionnaire, I informed them about the goal of my experiment.

6.1.1.4 Dependent Variables

I used the following metrics to measure user attention and decision on authorization dialogs in the presence of advertisements:

- Eye-gaze fixations- An eye-gaze fixation refers to the maintenance of visual gaze at a single location. I used the ratio of number of eye-gaze fixations on permission text area of an application authorization dialog and the number of eye-gaze fixations on the advertisements area. More specifically, I calculated the eye-gaze fixation count ratio as follows:

$$\text{Eye-gaze fixation count ratio} = \frac{\text{Eye-gaze fixation count on permissions area}}{(\text{Eye-gaze fixation count on permissions area} + \text{advertisements area})} \quad (3)$$

- Permission identification- The fraction of application permissions identified correctly. The permissions requested by applications were public profile information, friendlists, birthday, and email address.
- Authorization decision- The fraction of application authorization dialogs accepted.

6.1.2 Participants

I recruited my participants from the university through email announcements and word of mouth. An email describing the purpose of the study was sent to all students. In order to be eligible, the participants were required to have an active Facebook account. The eligible participants were invited to the lab to complete the tasks, and

received a \$5 gift-card for participation. I also asked the participants to spread the word about my study without revealing the actual goal of the study.

A total of 30 participants successfully completed the study, 18 males and 12 females. My participants were active Facebook users who were members for more than 4 years. 86% of the participants were between the ages of 25 to 30. 90% had four or more years of college education.

6.1.3 Study Results

6.1.3.1 Effect of advertisement's presence on user attention and decision

I used three metrics to measure user attention and decision in the presence of advertisements. To determine how each of the three dependent variables differed for the independent variable (advertisement type), I conducted individual Kruskal-Wallis tests (non-parametric version of a one-way ANOVA test).

1. Eye-gaze fixations — My first attention metric was the ratio of eye-gaze fixation counts on the permission text area and the sum of eye-gaze fixation counts on the advertisements and permission text area. I logged the participants' eye-gaze coordinates while they were interacting with the installation dialogs. I defined an area of interest around the permission text area and the advertisements and only counted the eye-gaze fixations within this area of interest.

Kruskal-Wallis test did not show a significant difference between the eye-gaze fixation count ratio of the control group (mean= 0.6, SD= 0.36), the group with static advertisements (mean=0.31, SD=0.41), and the group with animated advertisements (mean= 0.45, SD=0.40) averaged over four applications' dialogs with $p=0.06$. Fig-

Figure 31(a) shows the eye-gaze fixation count ratio (averaged over the four application authorization dialogs) of participants in each of the three groups. Although not significant, it can be observed that the mean of eye-gaze fixation count ratio for the participants who were not shown any advertisements is higher than that of those participants who were shown animated or static advertisements. In other words, the participants in the treatment groups were distracted by the advertisements and looked at the advertisements more compared to the permissions on authorization dialog. A larger sample size could have resulted in a significant difference.

2. Permission identification — My second attention metric was the fraction of requested permissions identified correctly. I analyzed whether there is a significant difference between the three participant groups with respect to permission identification. The post-survey questions asked the participants to select all the permissions requested by the four applications. I used participant response to these questions to calculate the fraction of permissions correctly identified by the participants.

Kruskal-Wallis test did not show a significant difference between the fraction of permissions correctly identified by the participants in the control group (mean=0.57, SD=0.37), the participants in the static advertisements group (mean=0.37, SD=0.31), and participants in the animated advertisements group (mean=0.32, SD=0.37) with $p=0.055$. Figure 31(b) shows that the participants who were presented with animated advertisements, on average recalled the least number of permissions correctly, whereas the control group participants had relatively high permission recall although this difference was also not significant. Once again increasing the sample size may result

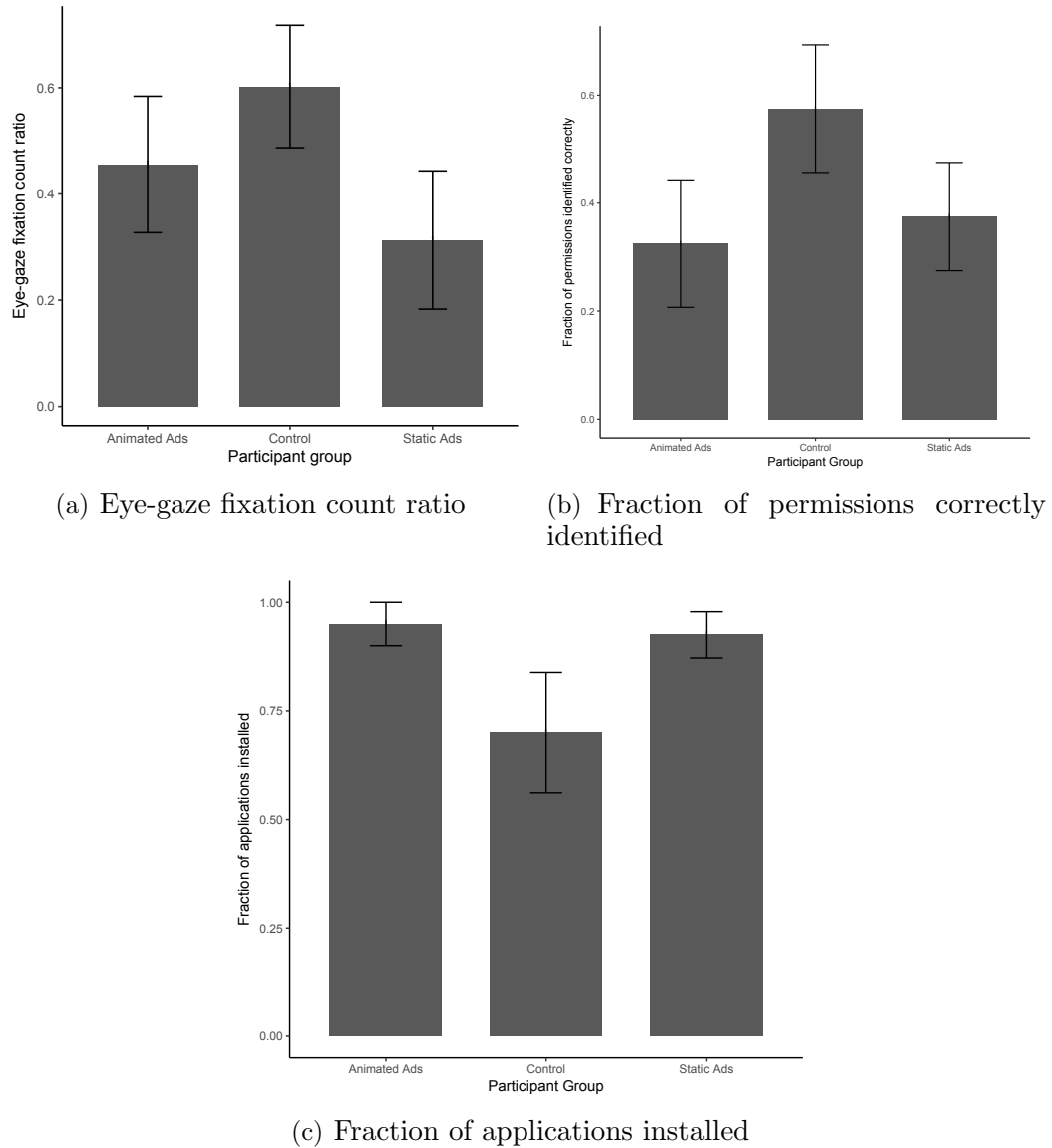


Figure 31: Effect of advertisement’s presence on user attention and decision on authorization dialog

in this trend becoming significant.

3. Authorization decision — I also analyzed whether the presence of advertisements affected participants’ decision to use an application. Since there were four game applications in my study, I calculated authorization decision as the fraction of applications installed/played.

I conducted a Kruskal-Wallis test on the fraction of applications installed by each of the three participant groups. The test showed a significant difference between the fraction of applications installed by the control group (mean=0.7, SD=0.43), the group with static advertisements (mean=0.92, SD=0.16), and the group with animated advertisements (mean=0.95, SD=0.15) with $p=0.04$. Figure 31(c) shows the fraction of applications installed by each participant group. Post-hoc comparisons using Nemenyi test showed that there is a significant difference between the number of applications installed by the control and animated advertisements group with $p = 0.045$.

Although the fraction of applications installed was significantly different for participants who were presented with advertisements and those who were not, one could argue that there could be many reasons for not using a particular application. For example, the participants in the animated and static distractions group could have genuinely liked most of the applications and therefore installed more applications than the control group. Therefore, the presence of advertisements might not have played a role in their decision.

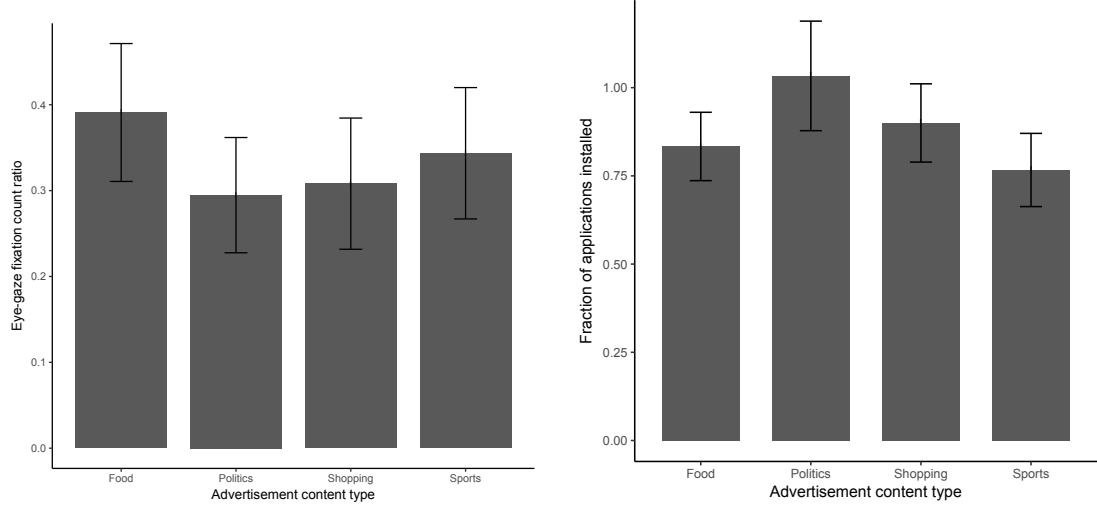
6.1.3.2 Effect of advertisement content type on user attention and decision

I displayed four advertisement content types to the users, namely, shopping, food, politics, and sports. Although I did not see a significant effect of advertisement's presence around authorization dialogs on user's attention and decision, I was interested in analyzing whether there is an impact of advertisement content type on user attention and decision. I used eye-gaze fixation count ratio and fraction of applica-

tions installed as my attention and decision metrics respectively. To determine how each dependent variable differed for the independent variable (advertisement content type), I conducted the Friedman test (non-parametric version of one-way repeated measures ANOVA test) for each dependent variable.

1. Eye-gaze fixations — I used participants' eye-gaze fixation count ratio (Equation (1)) as my attention metric. This time however, I only counted the eye-gaze fixations over a specific advertisement content type. I conducted a Friedman test on the eye-gaze fixation count ratio in the presence of each advertisement content type. The test did not show a significant difference between the eye-gaze fixation count ratio for shopping related advertisements (mean= 0.3, SD= 0.41), food related advertisements (mean=0.39, SD=0.43), politics related advertisements (mean= 0.29, SD= 0.36), and sports related advertisements (mean=0.34, SD= 0.41), with $p=0.7$. Figure 32(a) shows the eye-gaze fixation count ratio on application permissions area of interest in the presence of shopping, food, politics, and sports advertisements respectively. It appears that participants paid the least attention on the application authorization dialog in the presence of political advertisements since the eye-gaze fixation count ratio is the smallest for political advertisements. Moreover, food related advertisements distracted participants the least from paying attention to the authorization dialog. However, this difference was not found out to be significant.

3. Authorization decision — I used the fraction of applications installed/played in the presence of an advertisement content type to analyze whether the content type of advertisements affected participants' decision to use an application.



(a) Eye-gaze fixation count ratio on application permissions area in the presence of shopping, food, politics, and sports advertisements
 (b) Fraction of applications installed in the presence of shopping, food, politics, and sports advertisements

Figure 32: Effect of advertisement content type on user attention and decision

Friedman test did not show a significant difference between the number of applications installed in the presence of shopping advertisements (mean=0.9, SD=0.6), food advertisements (mean=0.83, SD=0.53), political advertisements (mean=1.0, SD=0.85), and sports advertisements (mean=0.76, SD=0.56) with $p=0.6$ (see Figure 32(b)). Complimenting the trend in Figure 32(a), it can be observed that the participants installed the most applications in the presence of political advertisements. Although this difference is not significant, a larger sample size could have supported this argument if the eye-gaze fixation count ratio in the presence of political advertisements also becomes significant.

6.2 Conclusion

In this chapter, I analyzed the effect of an advertisement's presence and its content type on user's attention and decision on application's authorization dialog. I focused

on a gaming website *Zynga* that earns a significant revenue from displaying advertisements in and around its games and is a contributor of the most popular third-party game applications on Facebook. Therefore, it is important to understand the role of advertisements on user attention and decisions on application authorization dialogs.

I conducted a between-subjects experiment on a mockup of Zynga's website and focused on banner advertisements. The control group was presented with no advertisements above the application authorization dialog. Whereas, the treatment groups were presented with static and animated (GIF based) advertisements. The average eye-gaze fixation count ratio and fraction of permissions recalled correctly were higher for the control group participants compared to the static and animated advertisements group. This difference was not found to be significant. However, the control group participants installed significantly less number of applications as compared to the animated advertisements group.

My advertisements contained four types of content i.e., food, shopping, politics, and sports. The average eye-gaze fixation count ratio was the lowest for the political advertisements and highest for the food advertisements. Although this difference was not significant, it is interesting to see that political advertisements distracted participants the most. Similarly, the participants installed more applications in the presence of political advertisements.

CHAPTER 7: IMPROVEMENT OF USER COMPREHENSION OF TOUCH ID USE WITH THIRD-PARTY APPLICATIONS

With the growing amount of personal data stored in smartphones today, and the fact that most users do not lock their phones with a PIN/passcode, smartphone vendors are now offering fingerprint authentication in their handsets to serve as a fast and secure alternative to PIN/passcode.

Apple's Touch ID technology is gaining popularity over other fingerprint sensors w.r.t its accuracy. Initially introduced for motivating users to lock their device by not having to enter a passcode, Touch ID is now also being used for purchasing applications from the Apple store to skip entering Apple ID password. Recently, Apple opened Touch ID to third-party applications, giving third-party developers the ability to utilize the secure Touch ID fingerprint sensor for user sign-in and authentication during sensitive tasks such as money transfer and purchase completion.

In this chapter, I first investigate user misconceptions regarding the use of Apple's Touch ID technology with third-party applications. I then discuss my efforts for resolving these misconceptions by improving the design of the Touch ID terms and conditions dialog, which is presented by iOS applications that involve sensitive tasks (such as Banking, and Rewards applications).

7.1 Potential User Misconceptions

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 applications, however, it introduces this mental model that the fingerprint and passcode are interchangeable methods of authentication. Herein lies the root of potential misconceptions regarding the 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, I 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, I formulated the following hypotheses in order to drive my investigation of whether Touch ID users lack comprehension and risk perception of Touch ID technology:

H1– Users are not aware of how the fingerprint is being used during the Touch ID-based authentication process for third-party applications

H2– Users are not aware of where their fingerprint is stored and how it is accessed during Touch ID-based authentication

H3– 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 my hypotheses, I first conducted an in-person study, and then an online study in order to corroborate my findings from the in-person study.

7.1.1 In-Person Study

7.1.1.1 Participant Tasks

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.

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, security consciousness, and familiarity with Touch ID. Participants were then asked to install the Amazon application (version 5.4.0 at the time of my study) which implements TouchID to allow users to authenticate into 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. I used the Amazon application to highlight the misconceptions surrounding Touch ID-based authentication in third-party applications. Once the prompt for Touch ID was displayed prior to making a payment on Amazon, as seen in Figure 33, participants were asked to complete another set of questions directly related to the purchase scenario, which evaluated their understanding of how 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 was for an intruder to circumvent Touch ID to unlock the device and make purchases.

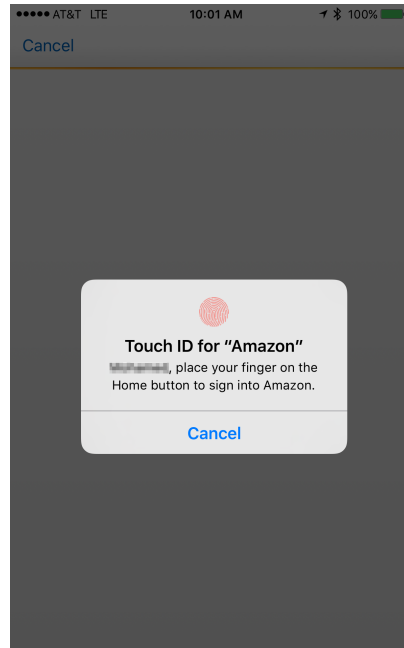


Figure 33: Touch ID prompt for authentication in Amazon Application

Task 3 - Fingerprint management: The third task was related to participant perceptions regarding fingerprint management. I told the participants that I was able to eavesdrop over their shoulder and figure out the passcode they created as part of Task 1. Therefore, I was able to unlock the iPad using their passcode and register a new fingerprint to allow me to use Touch ID. Based on this attack vector information, the participants were required to answer additional questions about whether they believed I would be able to unlock the device and assume their identity, and whether changing the PIN/password on the device would prevent the attack. Once they responded, I enrolled my 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. Lastly, the participants answered a final set of questions that inquired about what kind of controls they can take to stop this attack and manage their fingerprints.

Once these tasks were completed, I walked the participants through clearing their fingerprints stored on my device, signing them out of the Amazon application, and clearing the saved PIN/password. Participants received a \$5 Amazon gift card for participating in the study. The study took approximately 25 minutes to complete. I recruited my participants through mass distribution emails and flyers around campus. Respondents were screened for eligibility based on ownership of a Touch ID enabled Apple device.

7.1.2 Online Study

7.1.2.1 Participant Tasks

Perceptions about Touch ID based unlock/ authentication, fingerprint access/storage, and ease of circumvention: The online study participants only completed Task 2 of the in-person study. Each participant first answered a set of questions about demographics, security consciousness, and familiarity with Touch ID. 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 account (Amazon application version 5.4.0), and making a purchase using Touch ID. After viewing the video, the online participants were asked to answer a set of questions related to the demonstrated scenario. These questions 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 purchases.

To ensure recruitment of owners of a Touch ID-enabled Apple device, 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 device. Similar to Cherapau et al., the verification task required each participant to provide (1) a picture of their iPhone/iPad, taken using the front-facing camera in front of a mirror, and (2) a screenshot of their iPhone/iPad's lock screen with the masked PIN/password entered [17].

7.1.3 Results

7.1.3.1 Demographics

A total of 31 participants participated in the in-person study, and 155 participants participated in the online study. Out of the 155 participants in my online study, I selected the responses of 125 participants based on their answers to the attention check questions and device verification task. A breakdown of demographics from the two studies can be seen in Table 5. These covered gender, ethnicity, age, education, and duration of Touch ID use.

7.1.3.2 Hypothesis 1

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

Table 5: Descriptive statistics for the demography of the in-person and online study

Demographics		% of participants (in-person study)	% of participants (online study)
Gender	Female Male	22.58 77.41	53.6 46.4
Highest level of completed education	Bachelor degree Associate degree High school Graduate degree	41.9 16.1 25.8 16.1	43.2 16 20.8 20
Ethnicity	Black/African-American Asian/Pacific Islander Hispanic White/Caucasian	0 54.83 9.67 35.48	8.8 16.8 5.6 68.8
Age	18-35 35-50 ≥50	100 0 0	76 20.8 3.2
Duration of Touch ID use	6-12 months More than 1 year <6 months More than 2 years I don't know	19.3 29 48.3 3.2 0	31.2 34.4 20 11.2 3.2

The Touch ID authentication process only takes place on the device. This means that the locally stored fingerprint data is used to verify an authorized user, and in doing so, the user's associated PIN/password is provided to the device or application for authentication. Therefore, to the device or any application requiring authentication, it is technically as if a PIN/password was entered in the first place. However, I conjectured that many users likely hold a misconception regarding how the fingerprint is being used for Touch ID. With this particular hypothesis, I am specifically addressing participants' understanding of the role of fingerprint during authentication, i.e., that they believe that fingerprint authentication is equivalent to PIN/password

authentication, and that their fingerprint data is being accessed by applications to authenticate participant's identity, when in fact, neither of these are the case.

To evaluate this hypothesis, I analyzed responses to two questions from the post-survey of the in-person study: (1) Is being authenticated with your fingerprint the same as authenticating with 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". Table 6 shows the participant responses to these questions. Recomputing the variables in order to reduce responses to two levels, I combined the "No" and "I don't know" responses into one. Since each of these questions could be considered a single categorical variable with two groups, this required a single-sample non-parametric test. Consequently, I used a Chi-square goodness-of-fit test in order to determine whether the distribution of cases for each question follows a known or expected distribution. For this expected distribution, I hypothesized that an equal proportion of participants would believe that fingerprint authentication was equivalent to PIN/password authentication, and that Amazon did access their fingerprint data for authentication. Since no standard or known proportion of Touch ID users exists for these cases, I used the probability that at least half of the users would hold incorrect assumptions about Touch ID authentication as a reasonable assumption. I use the same expected distribution for other Chi-square goodness-of-fit tests conducted.

I hypothesized that approximately half of my participants would believe that fingerprint authentication was equivalent to PIN/password authentication, and also believe that Amazon did use their fingerprint to authenticate them.

Table 6: Responses to survey questions regarding Touch ID authentication process perception for the in-person and online study

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 data being accessed by Amazon to authenticate you in this transaction?	Yes No I don't know	60 26.66 13.33	77.6 14.4 8

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 I supplied ($\chi^2(1) = .290$, $p = .590$). 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 access to their fingerprint data in order to authenticate them during the purchase transaction. Therefore, these perceptions do not differ significantly from the hypothesized (50%,50%) values that I supplied ($\chi^2(1) = 1.581$, $p = .209$). However, more than 50% of the online study participants had this incorrect perception

$(\chi^2(1) = 45, p = 1.97 \times e^{-11})$.

7.1.3.3 Hypothesis 2

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

Going beyond users' understanding of what it means to be authenticated using Touch ID, I hypothesized that users are not clear on how the process works with regards to where their fingerprint data is stored and how it is accessed. Specifically, I hypothesized that at least half of Touch ID users likely believe that their fingerprint data is stored beyond the Apple device itself, and that it is accessed by parties beyond the device. In the case of my user study, the provided scenario involved using Touch ID to make a purchase in the Amazon application, and so the study 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? For these questions, the possible responses included iPhone/iPad, iCloud account, Apple server, and Amazon server; participants could select all that they believed applied. I recoded these responses into two groups: iPhone/iPad only, and Other (iPhone/iPad and/or other server(s)). This was done since I was mainly interested in determining what percentage of the participants realized that the data was stored on the iPhone/iPad only versus any other location(s).

The recoded number of responses can be found in Table 7. I evaluated each set of responses as a single categorical variable with two groups, which required the Chi-square goodness-of-fit test. I also evaluated these sets of responses as two related

groups (*before* and *after*) with the same dichotomous dependent variable (storage location). In other words, I sought to determine whether the proportion of participants who believed the fingerprint was stored on the iPhone/iPad 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. Additionally, regarding the matter of fingerprint access, I asked participants (3) Who has access to your fingerprint *during* the payment transaction? Recoding this third set of responses into two groups and treating it as a single categorical variable with two groups, I again conducted the Chi-square goodness-of-fit test.

Table 7: Participant perceptions of fingerprint storage before/after, and fingerprint access during the Touch ID-based Amazon in-app purchase transactions

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

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 ($\chi^2(1) = .806$, $p = .369$) 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 ($\chi^2(1) = .032$, $p = .857$) and online responses ($\chi^2(1) = 0.2$, $p = 0.6547$). This means that for both of these, I can not reject the null hypothesis, and confirm that

my 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 statistically insignificant.

Lastly, for the third question regarding fingerprint access *during* the transaction, the Chi-square goodness-of-fit test result was not statistically significant in the in-person ($\chi^2(1) = .032$, $p = .857$) or the online responses ($\chi^2(1) = 3.528$, $p = 0.06034$). Therefore, I again confirm that I was correct in assuming that the proportion of users who are not aware of how authentication with Touch ID works is approximately 50%; these are the users who perceive the fingerprint to be accessed by iPhone/iPad and/or other entities (Apple server, iCloud server, Amazon server).

7.1.3.4 Hypothesis 3

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

This hypothesis addresses users' lack of understanding of how someone besides themselves can take advantage of Touch ID to act as an authorized user and unlock the owner's device, or, in the case of my scenario, potentially make a purchase through device owner's Amazon account. Evaluating this hypothesis consisted of analyzing responses to four questions, each with a slightly different variation, as seen in Table 8. These questions deal with who the device owner is, who the Amazon account holder

is, and whose fingerprint is being used. For each, the participant was asked whether it would be possible to make a purchase. Each of these questions were evaluated using the Chi-squared goodness-of-fit test, and I found that for all of them, the p-value was less than 0.05. This means that there was a significant difference between my expected proportion of 50%/50% and the actual proportion regarding users who responded accurately regarding the possibility of each of these.

Table 8: Responses to survey questions regarding perceptions on the ease of getting into a Touch ID-enabled device and making a purchase

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

Chi-square goodness-of-fit test on perceptions of whether a stranger could use their own fingerprint to make a purchase on the owner's Touch ID-enabled device 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 I supplied (for in-person: $\chi^2(1) = 17.065$, $p < .0001$; for online: $\chi^2(1) = 84.872$, $p = 2.2 \times e^{-16}$).

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 device 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 I supplied in both studies (for in-person: $\chi^2(1) = 5.452$, $p = .020$; for online: $\chi^2(1) = 60.552$, $p = 7.166 \times e^{-15}$).

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 device 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 I supplied (for in-person: $\chi^2(1) = 17.065$, $p < .0001$; for online: $\chi^2(1) = 78.408$, $p = 2.2 \times e^{-16}$).

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 I supplied (for in-person: $\chi^2(1) =$

14.226, $p < .0001$; for online: $\chi^2(1) = 84.872$, $p = 2.2 \times e^{-16}$).

Lastly, as part of this hypothesis for the in-person study, I also demonstrated a scenario where I took advantage of Touch ID to act as an authorized user of the device. This was done to corroborate the results for the previous four questions about the feasibility of bypassing Touch ID. There were additional survey questions evaluated here, based on this scenario. Specifically, I asked them to respond whether they believed (1) I could unlock the device and potentially make a purchase without their PIN/password if my fingerprint was registered (for which the correct answer is Yes), 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 (for which the correct answer was No).

I conducted a Chi-squared goodness-of-fit test on two separate sets of responses. For the first question, regarding if I would be able to unlock the device and potentially make a purchase on participant's account with my fingerprint, I found that the result was significant ($\chi^2(1) = 7.258$, $p = .007$), meaning it differed from the hypothesized proportion. This is what I expected, however, as I anticipated most participants would realize this was possible, and so my 50%/50 % proportion would not hold here. For the second question, however, the result of the goodness-of-fit was not significant ($\chi^2(1) = 1.581$, $p = .209$), meaning my expected proportion of those who would incorrectly assume a PIN change would help was indeed about 50%. I also conducted a McNemar test between the two sets of responses to determine whether the proportion of participants who believed I could bypass Touch ID on their device with my fingerprint would decrease based on the change in PIN 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.

7.1.3.5 Limitations

While my results were significantly positive, my studies were not without 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 my results are overall. Along those lines, the participants in the online study who completed the HIT might not necessarily represent the general population of iPhone/iPad users. Additionally, I suspected that the other data I 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 my sample with respect to these variables was such that I was unable to make a proper evaluation of the impact that varying levels of these factors may have. Lastly, while my sample for the online study was sizable, I had anticipated an even greater number of participants. It is possible that the additional verification requirement of uploading two iPhone/iPad photos could have been a deterrent to additional participants.

7.1.4 Discussion

It is clear from my results 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 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.

7.2 Proposed Solution for Resolving These Misconceptions

Our investigation shows that Touch ID users have the following misconceptions regarding using Touch ID with third-party applications:

Application account access: First misconception is that nobody other than the device owner can access the application owner's account. In reality, however, any person whose fingerprint is registered on the Touch ID-enabled Apple device can ac-

cess the application account. This is because up to five fingerprints can be registered on the device and since there is no enhanced customization available to developers regarding who taps into Touch ID, any of the five registered fingerprints stored in the Touch ID-enabled device's secure enclave can be used to authorize access to an application. There are no fingerprint combination options, or the ability to add any more or unique prints. Therefore, any person whose fingerprint is registered on a Touch ID-enabled Apple device can access the application.

Fingerprint data access: Second misconception is that third-party developers can access the user's fingerprint data. In reality, third-party applications do not have access to the fingerprints, and only use the Local Authentication framework for requesting that the user authenticate using Touch ID [10].

Fingerprint use in Touch ID-based authentication: Third misconception is that using Touch ID for signing into the application is independent from using the user's username and password. In reality, however, Touch ID is only used to verify that the provided fingerprint is registered on the device. Once the provided fingerprint is verified, the username and password is retrieved from the secure enclave without the user having to enter it. Therefore, both fingerprint and password are being used in Touch ID-based authentication.

To address these three misconceptions, I take a first step towards improving user comprehension of Touch ID usage with smartphone applications. I focus on improving the design of the Touch ID terms and conditions dialog, which is presented by iOS applications that involve sensitive tasks (such as Banking, and Rewards applications). The Touch ID terms and conditions dialog is presented during the application's Touch

ID setup phase, to inform the users about the potential risks and benefits associated with using Touch ID in that application. This dialog focuses on three main areas:

1. Fingerprint use in Touch ID-based authentication: This information explains that using Touch ID removes the need for having the user to enter the account password.
2. Application account access: This information explains that anyone whose fingerprint is registered on the device can access the device owner's application account.
3. Fingerprint data access: This information explains that the application does not have access to the user's fingerprint data.

I propose four designs to better communicate information in the above three areas. I conduct an in-person study with 50 participants to analyze the effectiveness of my proposed designs. My findings show that my list with examples based dialog design was the most preferred by participants. It was the most effective in attracting participant attention towards Touch ID terms and conditions text. The participants who were presented the information as a list with examples, were better able to comprehend information related to fingerprint data access, and application account access by others. Our list with password-autofill animation based dialog was effective in understanding the role of fingerprint in Touch ID based sign-in.

7.2.1 Proposed Designs

The Touch ID terms and conditions dialog presents information in three areas (Figure 34(a)). I propose several dialog designs that simplify this information text, and present it in a bulleted format. I add visual examples and icons as cues to aid in the attention and comprehension of the presented information. I propose the following four designs:

1. List - This design simplifies the text and presents it as a bulleted list. Icons are presented with each piece of information to communicate whether the information represents a risk (red) or not (blue). Figure 34(b) shows the list-based dialog.

2. List with examples - The motivation behind this design was to further improve risk communication and information comprehension with the help of visual examples. Images are added along with the text to aid in understanding the presented information. I add an image showing username and password to inform the user that their username and password is also being used during Touch ID-based authentication. I also add images of potential users who can have access to the device owner's account. These are the people who have their fingerprint registered on the user's device. The user selects these people from five categories, namely, parent, sibling, friend, spouse, and coworker, during application account signup phase in my experiment (See Section 7.2.2). Lastly, I add an image of a fingerprint to inform the user that the corresponding information is regarding fingerprint data access. Figure 34(c) shows my list with examples dialog.

3. List with examples and trust ranking - This design communicates risk re-

lated to account access more effectively, by adding trust ranking to the user images displayed along with the account access text in the list with examples design. Once the user has selected the people who have registered their fingerprint on the user's device as part of the the application signup process, the user ranks the selected people based on how much he/she trusts them. These people are then presented on the dialog in ascending order of trust ranking (i.e., low trust first, and high trust last) to attract attention. Figure 34(d) shows my list with examples and trust ranking based dialog. Here the coworker is the least trusted and parent is the most trusted.

4. List with password autofill animation field - This design focuses on user comprehension of how fingerprint is used in Touch ID-based authentication. The idea is to inform the user that their username and password is being used during Touch ID-based authentication process. I communicate this by presenting the login activity with username and password field autofilled for a few milliseconds, after the user has tapped their finger on the home button to authenticate using Touch ID. Figure 34(e) shows my list with autofill password field based dialog.

7.2.2 Evaluation

I conducted a user study to evaluate the effectiveness of my proposed Touch ID terms and conditions dialog designs. The study was approved by my institution's IRB⁶ and intended to test the following hypotheses:

H1: Our proposed designs are effective in increasing participant attention towards
Touch ID terms and conditions dialog

⁶IRB Protocol #16-01-36

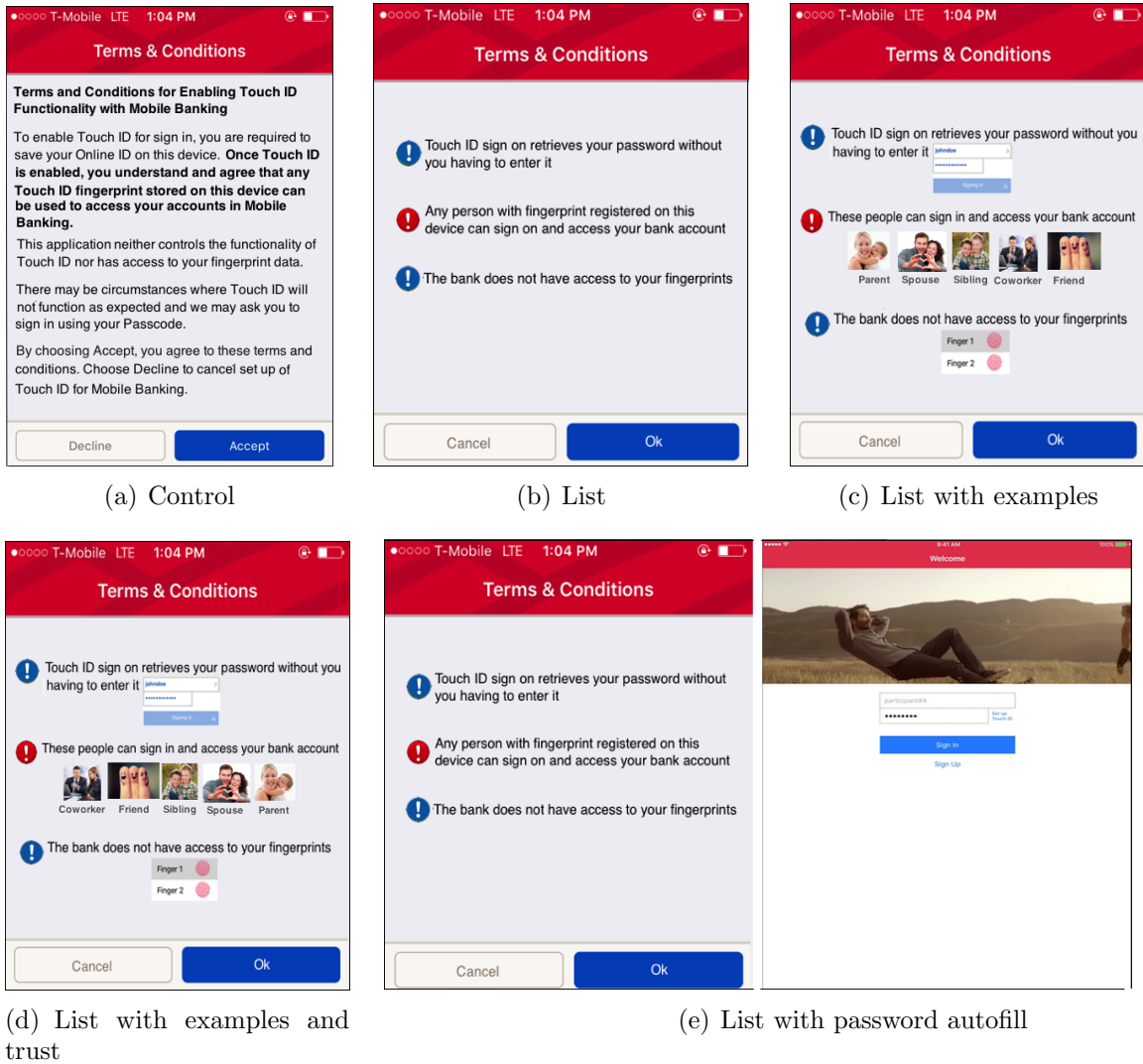


Figure 34: Touch ID terms and conditions dialogs inside Banking applications

- H2: Our proposed designs are effective in increasing participant comprehension of using Touch ID with third-party applications specifically w.r.t the role of fingerprint in Touch ID-based application authentication; fingerprint data access; and account access by others
- H3: Participants prefer my proposed dialog designs over the existing Touch ID terms and conditions dialog

I used a between-subjects design for my study. Each participant was either exposed to the control dialog design or one of the four proposed dialog designs. In order to maintain ecological validity, and more closely study participants' real behavior, I advertised the study as an evaluation of two Touch ID-enabled iOS applications.

7.2.2.1 Methodology

I recruited my participants through advertisements on Craigslist, flyers posted on campus, and through my university's mailing list. The eligible candidates were invited to campus for participation.

Conditions — I compared participants' behavior on my proposed dialog designs to their behavior on control dialog design. Therefore, my experiment consisted of five conditions:

- C1: Control - The participants in this group were presented with the existing Touch ID terms and conditions dialog.
- C2: List - The participants in this group were presented with the list-based Touch ID terms and conditions dialog.
- C3: List with examples - The participants in this group were presented with a Touch ID terms and conditions dialog showing information as a list along with visual examples to aid in attention and comprehension.
- C4: List with examples and trust - Similar to the "list with examples" group, the participants in this group were presented with a terms and conditions dialog which showed information as a list along with visual examples to aid in at-

tention and comprehension. However, the visual examples related to account access information were displayed based on participants' trust ranking of people categories.

C5: List with autofill password - The participants in this group were presented with list-based Touch ID terms and conditions dialog, which was followed by the login activity having the password field autofilled as soon as the participant tapped the home button with his/her registered finger.

Tasks — In order to test my proposed dialog designs, I developed two mockup iOS applications inspired by popular banking and rewards applications. I chose these applications since they involve sensitive tasks such as reloading the account, viewing a bank account statement, and reloading a card or making money deposits and transfers. The Touch ID terms and conditions dialog is only presented during Touch ID setup phase of an application. However, I displayed the terms and conditions dialog before every sensitive task. In other words, I display this dialog each time the Touch ID popup would appear, i.e., during Touch ID set-up, application sign-in, viewing transactions, and reloading account or making money deposit/transfer. Figures 35(a) and 35(b) show the Touch ID popup as it appears during sign-in and card reload tasks inside my banking and rewards applications respectively.

1. Pre Survey — The interested participants first completed an eligibility survey which checked if they owned a Touch ID-enabled Apple device. The eligible participants were asked to bring their Touch ID-enabled device along with them to the study session. Each participant answered a pre-test questionnaire related to finger-

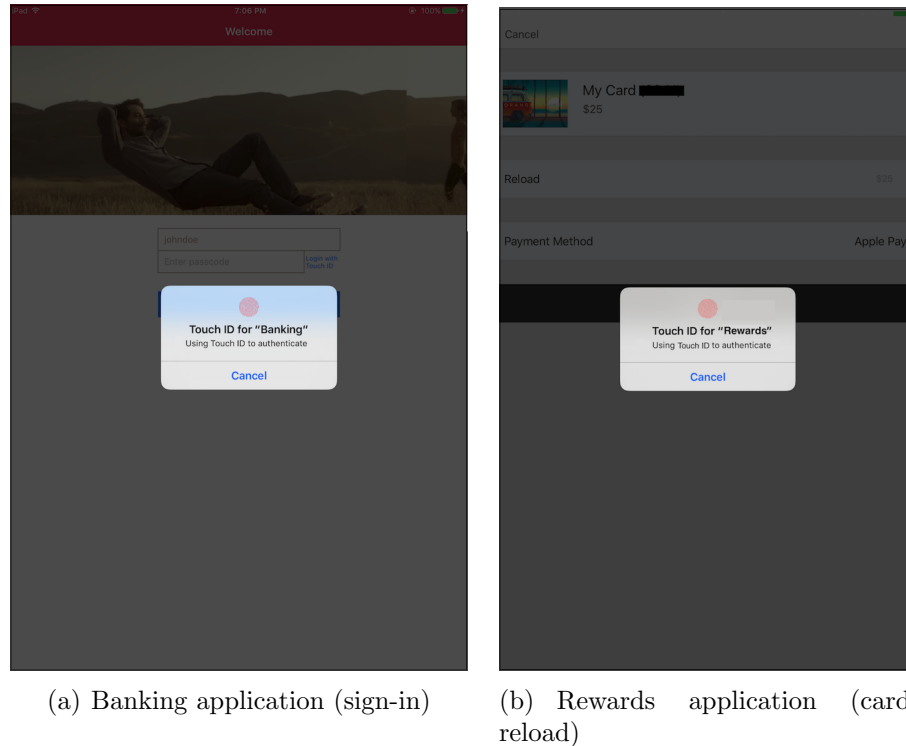


Figure 35: Screenshot of Touch ID popup appearing during sensitive tasks inside my user study applications

print data access by applications, fingerprint role in Touch ID-based authentication for application, and application account access.

2. Application Tasks — The participants used my applications on a Touch ID-enabled device that had their fingerprints already registered. Each participant then completed five tasks inside each application. I randomized the order in which the two applications were presented to the participants to avoid a carry-over effect. Below is a description of the tasks inside each application.

- Task 1: Account signup

The participants first created an account inside each application. This consisted of entering basic information like first name, last name, username and password.

To keep the data anonymous, the participants were asked not to enter their real information. I assigned each participant an anonymous username that they used for the applications and questionnaires. As part of the sign-up process, the participants selected the list of people (from the categories mentioned in Section 7.2.1) who have registered their fingerprints on the participant's Touch ID-enabled device. If the participants selected people from at least two categories, they ranked the chosen categories based on how much trust they placed on the people in each category.

- Task 2: Touch ID setup

The participants then registered their fingerprint on the user study iPad and completed the Touch ID setup process for the current application. For the rest of the tasks, participants had the option of either using Touch ID, or entering their account username and password.

- Task 3: Authentication for account access

In this task, the participants signed into the application using Touch ID or username and password.

- Task 4: Re-authentication for account transactions view

For this task, the participants viewed their bank account transactions and purchase history in the banking and rewards application respectively. The banking application had two fake bank accounts, namely, checking and savings account with a certain amount of money in them. Each account had some deposit and transfer transactions. Similarly, the rewards application had a few hard-

coded purchase transactions. By default, the Touch ID popup appeared to re-authenticate the participants. However, the participants could either use Touch ID, or, enter their account username and password to re-authenticate for this task.

- Task 5: Re-authentication for money transfer/deposit

For this task, the participants transferred money from one of their bank accounts to an imaginary friend's bank account, and reloaded money on the card, in the banking and rewards applications respectively. Similar to the previous task, the participants could either use Touch ID, or, enter their account username and password to re-authenticate for this task.

3. Post Survey — Each participant completed a post-test questionnaire at the end of the experiment. The participants first answered the same set of questions presented to them in the pre-test questionnaire. Next, the participants rated the presented dialog design based on a Likert scale w.r.t attention, and the extent to which its information layout communicated risk related to application account access; and helped understand the application's fingerprint data access, and the role of fingerprint in Touch ID-based authentication. The participants also stated their preference among the five dialog designs. After the participants completed the questionnaire, I informed them about the goal of my experiment.

Dependent Variables — I used the following metrics to measure participant attention and comprehension of the Touch ID terms and conditions dialog:

- Time on the dialog - This metric served as an indicator of whether the partici-

participant is paying attention and reading the Touch ID terms and conditions dialog content. I calculated the average time (ms) from the moment the dialog appears to the moment the participant made a decision on the dialog.

- Dialog comprehension - This metric measured the improvement in participant's comprehension of information in each of the three areas. I used the responses to pre-test and post-questionnaires.
- Decision on the dialog - This metric calculated the fraction of tasks inside an application for which the participant decided to authenticate using Touch ID despite its risks. Since there were four tasks in which the participant could use Touch ID-based authentication, I calculated this fraction out of 4.
- Dialog rating - This metric evaluated the dialog design based on participant's Likert scale ratings.

Participants — I ran my experiment between 1st Dec 2016, and 30th Jan 2017. A total of 50 participants completed the experiment—10 per group. Table 9 shows my study participant demographics.

7.2.2.2 Results

Hypothesis 1: *Proposed dialog designs are more effective in increasing participant attention towards Touch ID terms and conditions dialog.*

To measure participant attention, I calculated the average time spent on the dialog. Since I had two applications with different sensitivity levels, I was interested in analyzing whether the application type (banking, rewards) had an effect on par-

Table 9: Participant demographics

Age	n=50	% of n
18 to 20	9	18%
21 to 30	27	54%
31 to 40	5	10%
41 to 60	9	18%
Gender		
Male	25	50%
Female	25	50%
Ethnicity		
White/Caucasian	22	44%
Asian/Pacific Islander	19	38%
Middle East	6	12%
Hispanic	3	6%
Education Level		
Bachelor's degree	25	50%
Master's degree or higher	12	24%
High school	10	20%
Associate's degree	3	6%

participant attention towards the terms and conditions dialog. Therefore, to determine how the dependent variable (time spent on dialog) differed for the independent variables (dialog design, and application type), I conducted a factorial ANOVA test. Note that dialog design here is a between-subjects factor and application type is a within-subjects factor. Before conducting the factorial ANOVA test, I checked for the following assumptions:

- All samples are drawn from normally distributed populations

To check this assumption, I plotted the histogram and normal probability plot of the residuals. Figure 36 shows that my dependent variable approximately follows a normal distribution.

- All samples have an equal variance

To check this assumption, I conducted the Levene's test for homogeneity of

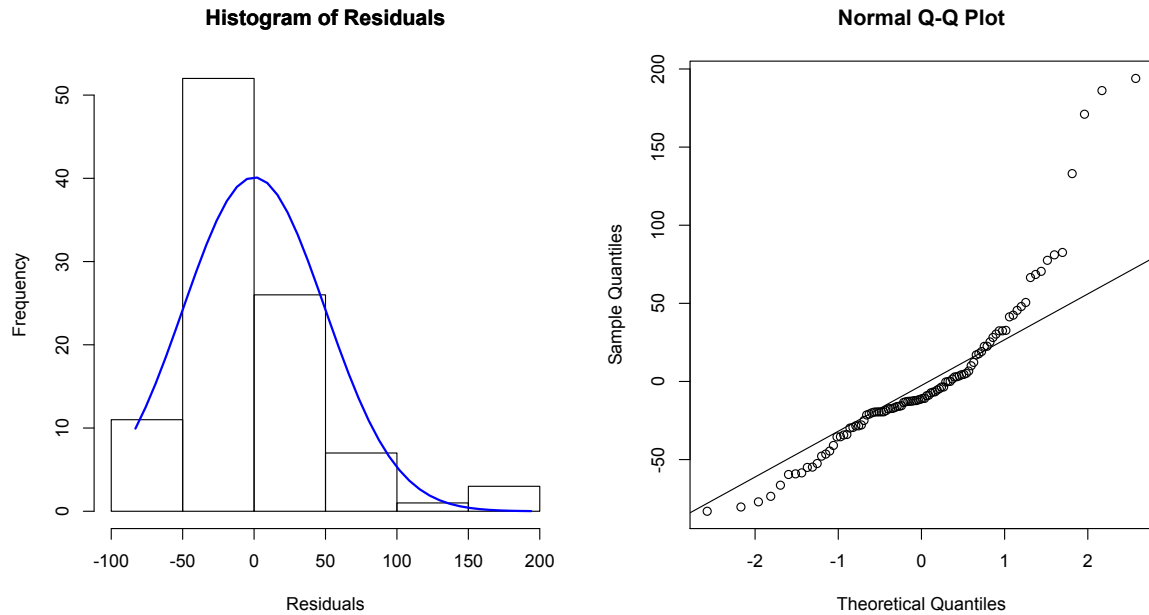


Figure 36: Normality assumption for factorial ANOVA in Hypothesis# 1

variance for the between-subjects and within-subjects factor. This test was not found out to be significant for both the dialog design ($p=0.17$) and application type ($p=0.14$). This shows that my null hypothesis that the samples have equal variance is true.

- Subjects are independent and randomly selected from the population

This is true since all participants were randomly selected from the university and through Craigslist.

Since the assumptions were met, I conducted the factorial ANOVA test. The interaction effect of dialog design and application type, on the time spent on the dialog was not found out to be significant at the $p < .05$ level [$F(4,15785) = 2.102$, $p = 0.0962$]. Since this p value of 0.09 is greater than 0.05, I cannot reject H_o for interaction effect of dialog design and application type, and conclude that there is

not sufficient evidence to support the claim that there is a combined effect of dialog design and application type on the time spent on dialogs.

There was a significant main effect of application type on the time spent on dialog at the $p < .05$ level for the two conditions [$F(1, 8526) = 4.542$, $p = 0.0386$]. Since the p value of 0.0386 is less than 0.05, I reject H_o for the main effect of application type, and conclude that there is sufficient evidence to support the claim that the sensitivity level of the application affects the time spent on the dialog. The average time spent on banking application ($M = 84.32$ ms, $SD = 62.89$ ms) was significantly more than the average time spent on rewards application ($M = 65.85$ ms, $SD = 42.45$ ms). It can be observed in Figure 37 that the average time spent on banking application is longer as compared to the average time spent on the rewards application. There was no

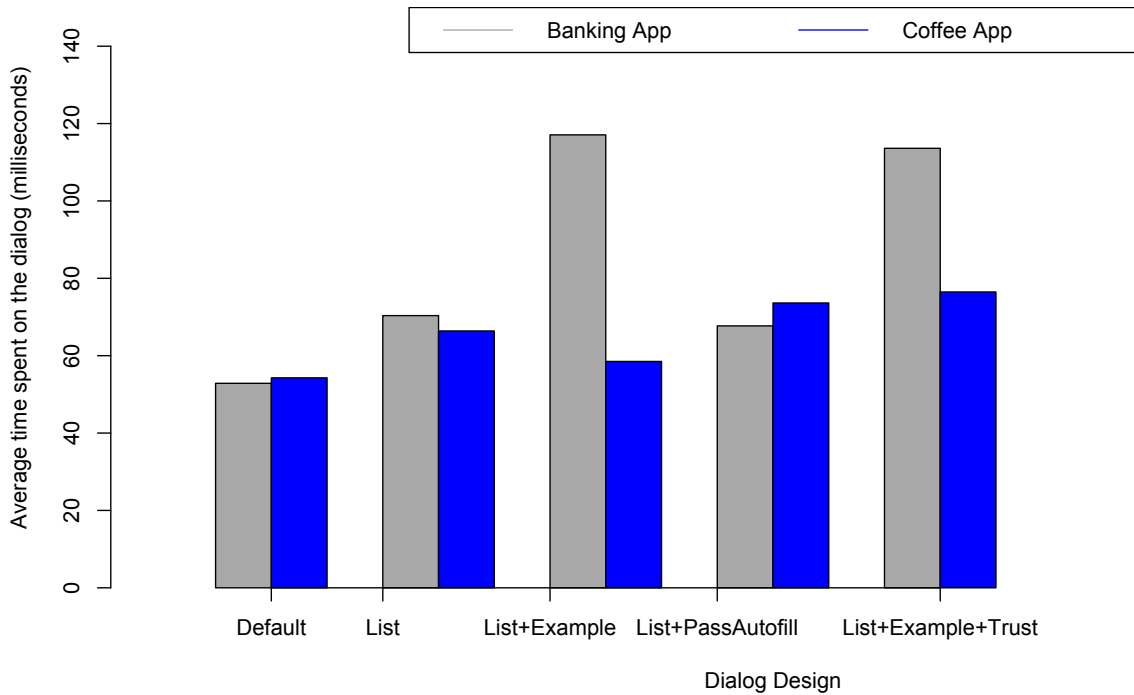


Figure 37: Average time (ms) spent on each dialog design

significant main effect of dialog design on the time spent on dialog at the $p < .05$ level for the five conditions [$F(4, 21746) = 1.528$, $p = 0.21$]. Since the p value of 0.21 is greater than 0.05, I cannot reject H_o for the main effect of dialog design, and conclude that there is not sufficient evidence to support the claim that the proposed dialog designs increased user attention towards the dialog text as compared to the default dialog design. In other words, there was no significant difference in the average time spent on default dialog design ($M=53.57$ ms, $SD= 17.08$ ms), list-based dialog ($M=68.38$ ms, $SD= 38.36$ ms), list with examples design ($M=87.80$ ms, $SD= 35.33$ ms), list with password autofill animation design ($M=70.66$ ms, $SD= 51.30$ ms), and list with examples and trust ranking design ($M=95.04$ ms, $SD= 33.93$ ms). However, Figure 37 shows that the average time spent on the default dialog design for both banking and rewards applications is shorter as compared to the rest of the dialog designs.

Hypothesis 2: *Proposed dialogs are more effective in increasing participant comprehension and risk perception of using Touch ID with third-party applications.*

I measured participant comprehension of Touch ID terms and conditions through their responses to pre-test and post-test questionnaires. For this purpose, I analyzed the responses for questions in each of the three studied information categories separately. Table 10 shows the percentage of participants in each group who answered a specific question correctly.

The first two questions are related to the role of fingerprint in Touch ID-based

Table 10: Percentage of participants in each group who answered a pre-test and post-test question correctly

Question	Control		List		List with examples		List with examples + trust		List with password autofill	
	Pre-test	Post-test	Pre-test	Post-test	Pre-test	Post-test	Pre-test	Post-test	Pre-test	Post-test
What is being used when you sign-in to a mobile application using Touch ID?	30%	30%	30%	30%	30%	40%	20%	30%	30 %	60%
What is being used when you authenticate with Touch ID during a sensitive task inside a mobile application?	20%	20%	30%	50%	20%	40%	30%	50%	30%	80%
Do mobile apps installed on your Touch ID enabled iPhone/iPad, have access to your fingerprint data?	0%	20%	10%	30%	10%	60%	0%	30%	0%	20%
Can someone else use HIS/HER fingerprint to log into YOUR mobile application account on YOUR Touch ID enabled iPhone/iPad if their fingerprints are registered?	10%	20%	30%	40%	30%	60%	20%	65%	20%	40%

authentication. Once the provided fingerprint is verified as registered on the device, the user's account password is retrieved from the keystore. Therefore, the correct answers for the first two questions was that both fingerprint and password are being used to sign into the application and to authenticate for a sensitive task using Touch ID. I analyzed what percentage of participants selected both fingerprint and password as the answer. Participants in group 5 were presented with a password autofill animation as an additional information to answer these questions correctly.

I ran separate McNemar tests between the pre-test and post-test responses of each group for question 1. I found a significant difference between the correct pre-test response (30%) and correct post-test response (60%) of group having password-autofill animation with $p = 0.03$. I also ran separate McNemar tests on the pre-test and post-test responses of each group for question 2, and found a significant difference between the correct pre-test response (30%) and correct post-test response (80%) for group having password-autofill animation with $p = 0.04$.

The third question was related to fingerprint data access by a Touch ID-enabled third-party application. Since, the applications only use the local authentication framework to know whether the provided fingerprint matches any of the stored fingerprints on the device, the applications do not have access to user's actual fingerprint data. All groups received information about fingerprint data access in the third bullet point. However, groups 3 and 4 also received visual examples to further understand this information. I ran separate McNemar tests on the pre-test and post-test responses of each group for question 3. I found a significant difference between the correct responses of pre-test (10%) and post-test (60%) for group 3, which was presented the list with examples based dialog design, with $p = 0.0004$.

The fourth question was related to application account access by people other than the owner of the account. Anyone who has registered their fingerprint on the device can unlock the device and sign into the application and perform sensitive tasks on behalf of the account owner. Groups 3 and 4 received additional information related to who can access their account, in the form of visual examples and trust ranking. Once again, I ran separate McNemar tests on the pre-test and post-test responses of each

group for question 4. I found a significant difference between the correct responses of pre-test (20%) and post-test (65%) for group having list with visual examples and trust ranking, with $p = 0.02$.

I was also interested in analyzing participants' risk perception specifically w.r.t account access by other people, i.e., whether the proposed dialog designs had an affect on participant behavior. For this purpose, I looked at the participant decision on the dialog, i.e., the fraction of accepted terms and conditions dialogs. I was also interested in analyzing whether the application type had an effect on participant decision to use Touch ID after being presented with the terms and conditions dialog. Therefore, to determine how the dependent variable (fraction of accepted Touch ID dialogs) differed for the independent variables (dialog design and application type), I conducted another factorial ANOVA test.

Once again, I first checked for the following assumptions before conducting factorial ANOVA test:

- All samples are drawn from normally distributed populations: To check this assumption, I plotted histogram and normal probability plot of the residuals. Figure 38 shows that my dependent variable, fraction of accepted Touch ID dialogs, follows an approximately normal distribution.
- All samples have an equal variance: To check this assumption, I conducted the Levene's test for homogeneity of variance for the between-subjects (dialog design) and within-subjects factor (application type). The test was not found out to be significant for both dialog design ($p=0.29$) and application type ($p=0.77$).

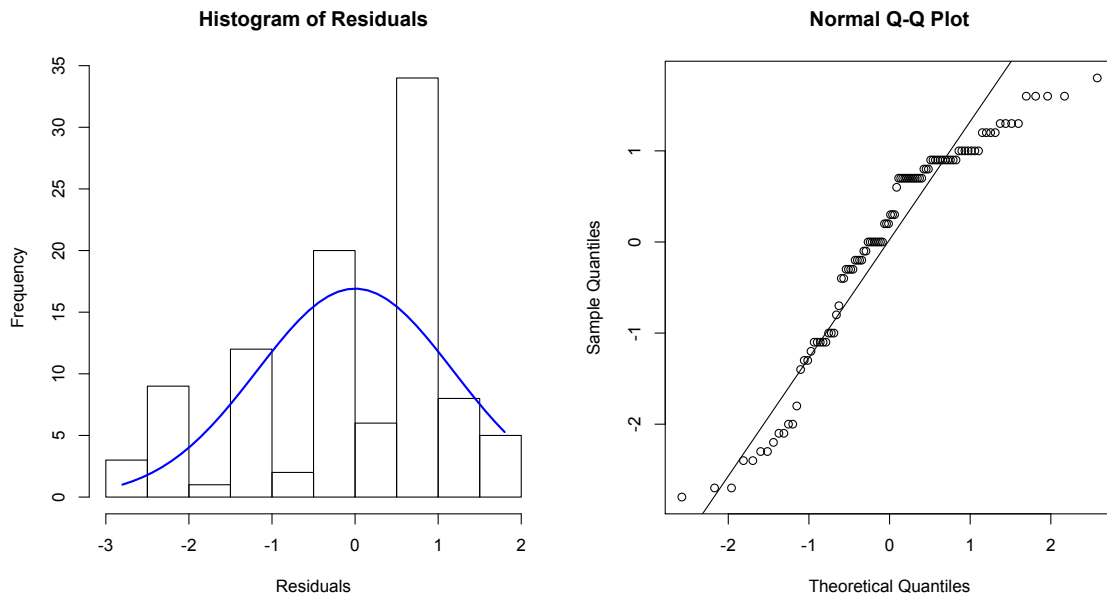


Figure 38: Normality assumption for factorial ANOVA in Hypothesis# 2 (decision on dialog)

This shows that the null hypothesis (samples have equal variance) is true.

- Subjects are independent and randomly selected from the population: This is true since all participants were randomly selected from the university and Craigslist.

Since the assumptions were met, I conducted a factorial ANOVA test. The interaction effect of dialog design and application type on the dialog decision was not found out to be significant at the $p < .05$ level [$F(4,4) = 2.222$, $p = 0.0816$]. Since this p value of 0.0816 is greater than 0.05, I cannot reject H_0 for interaction effect of dialog design and application type, and conclude that there is not sufficient evidence to support the claim that there is a combined effect of dialog design and application type on participants' decision to use Touch ID for authentication.

There was a significant main effect of application type on user decision at the $p < .05$

level for the two conditions [$F(1, 2.25) = 5, p = 0.0304$]. Since the p value of 0.0304 is less than 0.05, I reject H_0 for the main effect of application type, and conclude that there is sufficient evidence to support the claim that the type of application affects the user decision to use Touch ID for authentication. The fractions of Touch ID dialogs accepted for banking application ($M = 0.760, SD = 0.30$) was significantly more as compared to the fraction of Touch ID dialogs accepted for rewards application ($M = 0.685, SD = 0.30$). This is possible because banking applications have more sensitive tasks as compared to the rewards applications.

There was no significant main effect of dialog design on user decision at the $p < .05$ level for the five conditions [$F(4, 1.7) = 0.352, p = 0.841$]. Since the p value of 0.841 is greater than 0.05, I cannot reject H_0 for the main effect of dialog design, and conclude that there is not sufficient evidence to support the claim that the proposed dialog designs increased user comprehension of the Touch ID terms and conditions text as compared to the default dialog design. In other words, there was no significant difference in the participant decision for the control dialog design ($M = 0.78, SD = 0.24$), list based dialog ($M = 0.76, SD = 0.30$), list with examples design ($M = 0.66, SD = 0.30$), list with password autofill animation design ($M = 0.76, SD = 0.25$), and list with examples and trust ranking design ($M = 0.63, SD = 0.33$).

Hypothesis 3: *Participants prefer the proposed Touch ID terms and conditions dialogs over the existing one*

At the end of the session, the participants in each group rated the dialog presented to them on a Likert scale (1=Strong Disagree, 5=Strong Agree) w.r.t how much

attention it attracted towards the text, and to what extent it helped the participants understand the information in the three areas which my designs focused to improve.

First, the participants rated the dialog in their group w.r.t whether it helped them understand whether the applications have access to participants' fingerprint data if they use Touch ID with the applications. Figure 39(a) shows that the average rating for control dialog design (3.2) is lower than that of my proposed designs. However, a Kruskal Wallis test showed that this difference is not significant with $p = 0.3649$.

Second, the participants rated the dialog in their group w.r.t whether it helped them understand who can access their banking/rewards application account if they use Touch ID-based authentication for the applications. Figure 39(b) shows that the average rating for control dialog design (3.2) is lower than that of my proposed designs. However, a Kruskal Wallis test showed that this difference is not significant with $p = 0.2357$.

Third, the participants rated the dialog in their group w.r.t whether it helped them understand the role of fingerprint in retrieving participants' username/password during authentication. Figure 39(c) shows that the average rating for control dialog design (3.3) is lower than that of my proposed designs. However, a Kruskal Wallis test showed that this difference is not significant with $p = 0.6836$.

Lastly, the participants rated the dialog in their group w.r.t whether it attracted their attention towards the dialog text. Figure 39(d) shows that the average rating for control dialog design (3.1) is lower than that of my proposed designs. However, a Kruskal Wallis test showed that this difference is not significant with $p = 0.5058$.

Participants were then shown all five dialog designs and asked to state which one

they preferred the most. 20% of the participants selected the list-based design with the reasoning that it is simpler and has less information. 80% of the participants selected the list with examples/trust ranking based design since the images attracted their attention and helped them understand what information was presented on the dialog.

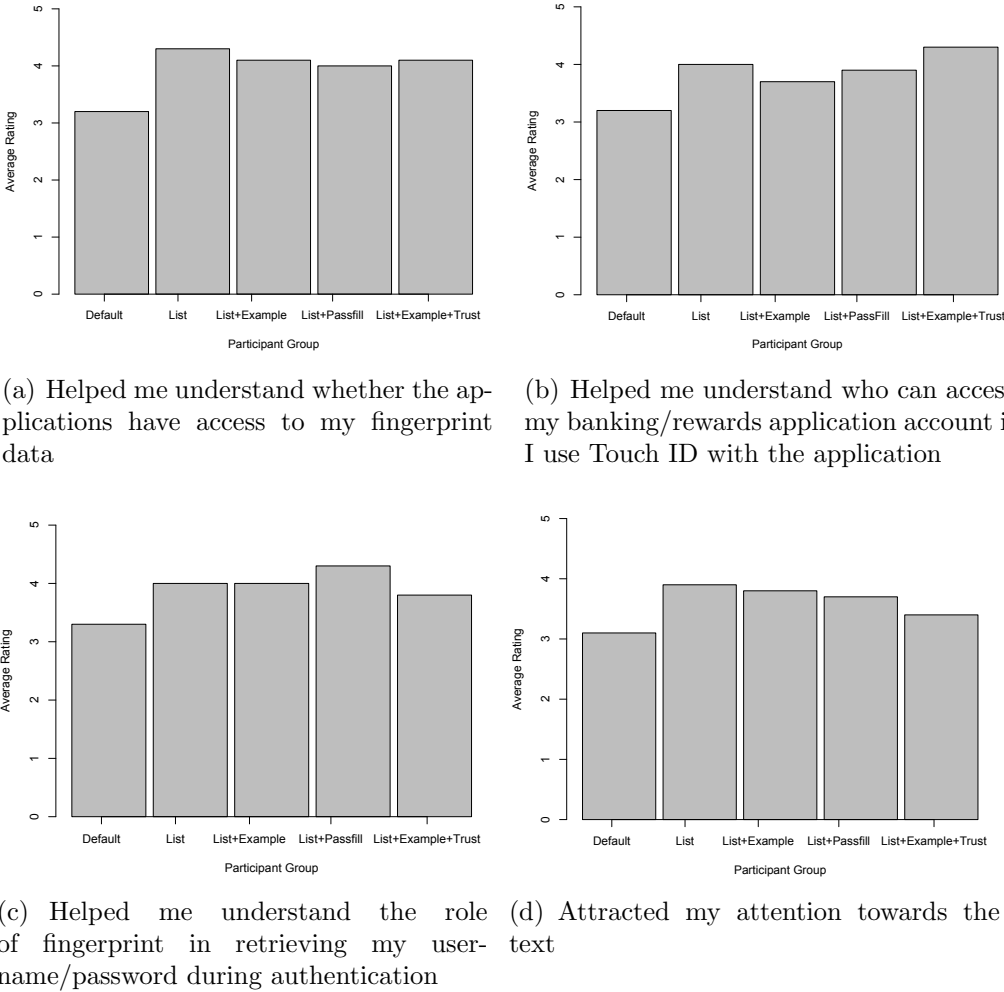


Figure 39: Participants dialog rating on Likert Scale

7.2.2.3 Discussion

In this section, I discuss my user study results along with limitations.

User attention on proposed Touch ID terms and conditions dialogs —

The average time spent on my proposed dialog designs was higher as compared to that on the control design. In particular, the designs with visual examples and trust ranking had the highest time spent. This is in line with the participants' overall dialog preference. 80% of study participants stated that they preferred the list with examples design. This shows that using images on the dialog can help in attracting participant attention towards the important information. However, since the sample size of 10 participants per group is small, I did not see a significant difference between the time spent on the dialog for the five groups. A study with a larger sample size could result in a significant difference. My list, and list with password autofill animation based designs were also rated high for drawing attention.

I also noticed that the sensitivity level of the application played a role on participant attention towards the dialog. Since banking applications involve more sensitive tasks/information as compared to rewards applications, participants paid more attention to the dialog while completing the tasks inside the banking application. The average time spent on the dialogs inside the banking application was significantly higher as compared to the average time spent on the dialogs inside the rewards application.

User comprehension of Touch ID terms and conditions — I discuss user comprehension of information in the three areas.

1. The role of fingerprint in Touch ID-based authentication in applications

The participant group who was shown the password autofill animation answered the

questions in this category better compared to the other groups. Moreover, the participants who were exposed to my proposed dialog designs rated the dialog high in terms of helping them understand the role of fingerprint in retrieving username and password during authentication.

2. Fingerprint data access by applications

All designs were rated high w.r.t understanding fingerprint data access by applications. However, designs with visual examples did better in answering the question related to whether an application has access to participant's fingerprint data.

3. Application account access by other people

List with examples and trust ranking did better on the question asking whether a stranger can access the device owner's application account using their own fingerprint.

Only 17 out of the 50 participants selected at least one person who had registered their fingerprint on the participant's device. Since a majority of the participants were the only users of their Touch ID-enabled devices, this could be a possible reason for their decision to use Touch ID-based authentication during the study despite its associated risk of account access by other people. Moreover, the fraction of Touch ID dialogs accepted for the banking application was significantly more as compared to the rewards application. This is possibly due to the fact that banking applications have more sensitive tasks as compared to the rewards applications.

7.3 Conclusion

In this chapter, I discussed several misconceptions that users have about the use of Touch ID authentication with third-party applications. I proved that users 1) are not

aware of how the fingerprint is being used during the Touch ID-based authentication process for third-party applications, 2) are not aware of where their fingerprint is stored and how it is accessed during Touch ID-based authentication and 3) 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.

I proposed a solution to increase user comprehension of Touch ID-based authentication in applications. My solution focused on improving the design of Touch ID's terms and conditions dialog which is presented during the Touch ID setup phase of sensitive task-based applications. I proposed four designs and evaluated them on 50 participants. My results showed that the list with examples based dialog design was the most effective in drawing participant attention towards Touch ID terms and conditions text, with average time spent on this dialog being more than the other dialogs. The participants who were presented with the list with examples were better able to comprehend information related to fingerprint data access, and application account access by others. Our list with password-autofill based dialog was affective in understanding the role of fingerprint in Touch ID based sign-in. However, my proposed dialog designs did not affect participants' decision to use Touch ID for sensitive tasks. This is because 66% of the participants had not registered other persons' fingerprint on their device, and therefore, considered it safe to use Touch ID-based sign-in instead of username and password.

CHAPTER 8: CONCLUSION

In this dissertation, I argued that third-party application dialog effectiveness with respect to attention switch, attention maintenance, and comprehension can be improved by 1) incorporation of design heuristics such as animation, eye-tracking, risk signals/examples, and simplified text and 2) by investigation of potential misconception avenues and environmental stimuli that impede user attention. To this end, I first explored the use of animation on application authorization dialogs as a possible attention attractor towards permissions. My preliminary results demonstrated the usefulness of animation on authorization dialogs. The eye-tracking data showed evidence of attention switch and maintenance towards the application permissions in animated dialog design. This work reconfirmed the effectiveness of personal information examples in communicating risk to the user. The participants in my study looked longer at the personal information examples as compared to the other elements of the dialog. The personal information examples made the participants more concerned about their information, and motivated them to consider and evaluate the permissions. This was further observed in the participants' permission authorization decisions which were significantly more conservative compared to that of the other dialog designs. There is room for improvement in the usability of my proposed animated dialog design. The sequential display of permissions slows the permission authorization process. Therefore, my approach can be more effective if the animation

can be made faster.

Due to the usability challenges associated with the use of animation on authorization dialogs, I then investigated the viability of active eye-tracking to combat habituation and enforce attention. I implemented a prototype of my approach as a Chrome browser extension. My experiment on 60 participants showed that participants who were forced to look at the permissions to activate the decision button and install the applications demonstrated a slight improvement in attention and permission recall compared to the control group participants. However, the hypothesized increase in the rate at which participants denied a dangerous/unnecessary permission, from the control groups to the treatment group was not statistically significant. This could primarily be due to the study design and it being conducted in a lab environment. My second experiment on 45 participants showed my approach's resistance to habituation. The participants who were forced to look at the permissions were still able to identify requested permissions. Due to the fact that eye-tracking technology is becoming affordable, this approach can be incorporated in mobile applications. Since the eye-tracking is only limited to permissions text area, the argument of privacy concerns does not hold.

Further, I investigated external factors that can potentially impede user attention towards permission authorization dialog. Specifically, I looked at advertisements, given the wide use of advertising in third-party gaming applications for generating revenue. I analyzed the effect of an advertisement's presence and its content type on user's attention and decision on application's authorization dialog. Due to my pilot study's small sample size, I did not have any conclusive results. However, I

had some interesting observations that could result in significance if a larger participant pool were studied. The average eye-gaze fixation count ratio and the fraction of permissions recalled correctly were higher for the control group participants compared to advertisements group participants. My advertisements contained four types of content i.e., food, shopping, politics, and sports. The average eye-gaze fixation count ratio was the lowest for the political advertisements and highest for the food advertisements. Although this difference was not significant, it is interesting to see that political advertisements distracted participants the most.

Finally, to test my hypothesis that the investigation of potential misconception avenues can aid in improving dialog content comprehension, I first explored the misconceptions that users have about the use of Touch ID authentication with third-party applications. I proved that users 1) are not aware of how the fingerprint is being used during Touch ID-based authentication process for third-party applications, 2) are not aware of where their fingerprint is stored and how it is accessed during Touch ID-based authentication and 3) 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. I proposed a solution to increase user comprehension of Touch ID-based authentication in applications. My solution focused on improving the design of Touch ID terms and conditions dialog which is presented during the Touch ID set-up phase of sensitive task-based applications. I proposed four designs and evaluated them on 50 participants. My results showed that my list with examples-based dialog design was the most effective in attracting participant attention towards Touch ID terms and conditions text, with average time spent on this dialog being more than the other

dialogs. The participants who were presented list with examples were better able to comprehend information related to fingerprint data access, and application account access by others. My list with password-autofill animation based dialog was affective in understanding the role of fingerprint in Touch ID-based sign-in. This simple design change can be implemented inside Touch ID-enabled third-party applications to help user understand the authentication process. This work further reconfirmed the usefulness of design heuristics including simple list-based text, animation, and visual examples. However, my proposed dialog designs did not affect participant decision to use Touch ID for sensitive tasks. This is because, 66% of the participants had not registered other person's fingerprint on their device, and therefore, found it ok to use Touch ID-based sign-in instead of username and password.

Future Work: In the continuation of this work, I plan on extending my proposed solutions for third-party application dialogs to further support my hypothesis that addressing human factors of habituation and misconceptions through techniques that motivate the end-users to pay attention and improve comprehension, will help the end-users make informed decisions.

My proposed authorization dialog designs for enforcing user attention towards permissions were primarily tested on web applications using a stand-alone eye-tracking device. Future work could involve testing the applicability of my animated and eye-activated authorization dialogs on mobile applications. My work on the investigation of advertisements as a potential communication impediment factor is a work-in-progress. Many variables were not taken into consideration while designing the

study. For example, the advertisement's location was fixed above the authorization dialog. However, the presence of advertisement below, to the left, or to the right of the authorization dialog could also have an impact on user attention. Once again, this work was conducted on web applications. The next step could be to replicate this study for mobile applications.

My work on improving user comprehension of Touch ID terms and conditions dialogs have several future directions. First, eye-tracking could be used to further understand how users interact with the dialog and to correlate it with their time spent on the dialog. Second, the design heuristics proposed in this work could be applied on other content-heavy dialogs presented by mobile applications.

REFERENCES

- [1] The eye tribe tracker. <http://theeyetribe.com>.
- [2] Facebook application development documentation. <https://developers.facebook.com/docs/facebook-login/permissions/>.
- [3] How many apps do smartphone owners use? <https://www.emarketer.com/Article/How-Many-Apps-Do-Smartphone-Owners-Use/1013309>.
- [4] The 'most used words' facebook quiz app accused of data stealing. <http://www.forbes.com/sites/amitchowdhry/2015/11/29/the-most-used-words-facebook-quiz-app/#73c615c14bb6>.
- [5] Number of apps available in leading app stores as of march 2017. <https://www.statista.com/statistics/263795/number-of-available-apps-in-the-apple-app-store/>.
- [6] People ignore software security warnings up to 90 percent of the time. <https://phys.org/news/2016-08-people-software-percent.html>.
- [7] The problem with your computer's security warnings. <http://www.ideas42.org/blog/problem-computers-security-warnings/>.
- [8] Third-party apps becomes significant source of malware attacks on android smartphones. <https://goo.gl/3l7b0f>.
- [9] Facebook login flow. <https://developers.facebook.com/docs/facebook-login/login-flow-for-web/v2.2>, 2014.
- [10] Local authentication framework. <https://developer.apple.com/reference/localauthentication>, 2014.
- [11] Power of visual communication. <http://blog.wyzowl.com/power-visual-communication-infographic>, 2014.
- [12] B. B. Anderson, C. B. Kirwan, J. L. Jenkins, D. Eargle, S. Howard, and A. Vance. How polymorphic warnings reduce habituation in the brain: Insights from an fmri study. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, pages 2883–2892, New York, NY, USA, 2015. ACM.
- [13] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy configuration. In *SOUPS*, 2010.
- [14] C. Bravo-Lillo, L. Cranor, S. Komanduri, S. Schechter, and M. Sleeper. Harder to ignore? revisiting pop-up fatigue and approaches to prevent it. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 105–111, Menlo Park, CA, July 2014. USENIX Association.

- [15] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: Designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 6:1–6:12, New York, NY, USA, 2013. ACM.
- [16] J. Brooke. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.
- [17] 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.
- [18] P. H. Chia, Y. Yamamoto, and N. Asokan. Is this app safe?: a large scale study on application permissions and risk signals. In *Proceedings of the 21st international conference on World Wide Web*, pages 311–320. ACM, 2012.
- [19] L. F. Cranor. A framework for reasoning about the human in the loop. *UPSEC*, 8(2008):1–15, 2008.
- [20] L. F. Cranor and S. Garfinkel. *Security and usability: designing secure systems that people can use.* ” O'Reilly Media, Inc.”, 2005.
- [21] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, pages 581–590, New York, NY, USA, 2006. ACM.
- [22] J. S. Downs, M. B. Holbrook, and L. F. Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, pages 79–90, New York, NY, USA, 2006. ACM.
- [23] S. Egelman. My profile is my password, verify me!: the privacy/convenience tradeoff of facebook connect. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2369–2378. ACM, 2013.
- [24] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1065–1074, New York, NY, USA, 2008. ACM.
- [25] M. Fagan, M. M. H. Khan, and R. Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519, 2015.
- [26] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 3:1–3:14, New York, NY, USA, 2012. ACM.

- [27] S. Furman and M. Theofanos. Preserving privacy—more than reading a message. In *Universal Access in Human-Computer Interaction. Design for All and Accessibility Practice*, pages 14–25. Springer, 2014.
- [28] P.-E. Gobry. How zynga makes money. <http://www.businessinsider.com/zynga-revenue-analysis-2011-9>, 2011.
- [29] M. Harbach, S. Fahl, T. Muders, and M. Smith. Towards measuring warning readability. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS '12*, pages 989–991, New York, NY, USA, 2012. ACM.
- [30] M. Harbach, S. Fahl, P. Yakovleva, and M. Smith. Sorry, i don't get it: An analysis of warning message texts. In *International Conference on Financial Cryptography and Data Security*, pages 94–111. Springer, 2013.
- [31] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, CHI '14*, pages 2647–2656, New York, NY, USA, 2014. ACM.
- [32] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, CHI '14*, pages 2647–2656, New York, NY, USA, 2014. ACM.
- [33] M. J. Kalsher and K. J. Williams. Behavioral compliance: Theory, methodology, and results. *Handbook of warnings*, pages 313–331, 2006.
- [34] S. Kim and M. S. Wogalter. Habituation, dishabituation, and recovery effects in visual warnings. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 53, pages 1612–1616. Sage Publications, 2009.
- [35] D. Miyamoto, T. Iimura, G. Blanc, H. Tazaki, and Y. Kadobayashi. Eyebit: Eye-tracking approach for enforcing phishing prevention habits. In *2014 Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS)*, pages 56–65. IEEE, 2014.
- [36] K. Pernice, K. Whitenon, and J. Nielsen. *How People Read on the Web: The Eyetracking Evidence*. 2014.
- [37] J. Pratt, P. V. Radulescu, R. M. Guo, and R. A. Abrams. It's alive! animate motion captures visual attention. *Psychological Science*, 21(11):1724–1730, 2010.
- [38] M. S. Rahman, T.-K. Huang, H. V. Madhyastha, and M. Faloutsos. Frappe: detecting malicious facebook applications. In *Proceedings of the 8th international conference on Emerging networking experiments and technologies*, pages 313–324. ACM, 2012.

- [39] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy. Android permissions: A perspective combining risks and benefits. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies, SACMAT '12*, pages 13–22, New York, NY, USA, 2012. ACM.
- [40] O. Špakov and D. Miniotas. Visualization of eye gaze data using heat maps. 2007.
- [41] K. E. Vaniea, E. Rader, and R. Wash. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*, pages 2671–2674. ACM, 2014.
- [42] A. VOßKÜHLER, V. Nordmeier, L. Kuchinke, and A. M. Jacobs. Ogama (open gaze and mouse analyzer): open-source software designed to analyze eye and mouse movements in slideshow study designs. *Behavior research methods*, 40(4):1150–1162, 2008.
- [43] N. Wang, J. Grossklags, and H. Xu. An online experiment of privacy authorization dialogues for social applications. In *Proceedings of the 2013 conference on Computer supported cooperative work*, pages 261–272. ACM, 2013.
- [44] N. Wang, H. Xu, and J. Grossklags. Third-party apps on facebook: Privacy and the illusion of control. In *Proceedings of the 5th ACM Symposium on Computer Human Interaction for Management of Information Technology, CHIMIT '11*, pages 4:1–4:10, New York, NY, USA, 2011. ACM.
- [45] R. Wash, E. Rader, K. Vaniea, and M. Rizor. Out of the loop: How automated software updates cause unintended security consequences. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 89–104, 2014.
- [46] T. Whalen and K. M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Proceedings of Graphics Interface 2005, GI '05*, pages 137–144, School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, 2005. Canadian Human-Computer Communications Society.
- [47] M. S. Wogalter. Communication-human information processing (c-hip) model. *Handbook of warnings*, pages 51–61, 2006.
- [48] H. Xu, N. Wang, and J. Grossklags. Privacy by redesign: Alleviating privacy concerns for third-party apps. 2012.

APPENDIX A: ANIMATED DIALOG USER STUDY DEMOGRAPHICS SURVEY

Demographic Survey

7/26/17, 2:03 PM

Demographic Survey

* Required

1. Full Name *

2. MTurk Worker ID *

3. Age *

Mark only one oval.

- ☐ 18-20
☐ 20-30
☐ 30-40
☐ 40- 50
☐ 50 or older

4. Gender *

Mark only one oval.

- ☐ Male
☐ Female

5. Education *

Mark only one oval.

- ☐ High school
☐ 2 years of college
☐ 4 years of college
☐ More than 4 years of college

6. Facebook membership *

Mark only one oval.

- ☐ Less than 1 year
- ☐ 2 years
- ☐ 4 years
- ☐ More than 4 years

7. Do you use Facebook applications *

Mark only one oval.

- ☐ Yes
- ☐ No

8. Are you concerned about online security and privacy when you install a Facebook application *

Mark only one oval.

- ☐ Yes
- ☐ No

9. How many Facebook applications have you installed *

Mark only one oval.

- ☐ More than 10
- ☐ 1 – 10
- ☐ 0

APPENDIX B: ANIMATED DIALOG USER STUDY PERMISSION COMPRE- HENSION SURVEY

Comprehension Survey

Please rate the effectiveness of permission layout and personal information examples in each of the three Facebook application permission models you just used

Question	Answer choice (Likert Scale) 1(Strongly disagree) 7(Strongly agree)
It was easy to differentiate the required and optional permissions in this interface	1 2 3 4 5 6 7
It was easy to read the permissions in this interface	1 2 3 4 5 6 7
If the personal information examples are added to this interface, they would have influenced my decision to allow or deny a permission	1 2 3 4 5 6 7
This interface informed me about my personal information well	1 2 3 4 5 6 7
This interface made me think before granting access to my personal information	1 2 3 4 5 6 7

APPENDIX C: ANIMATED DIALOG USER STUDY USABILITY SURVEY

Usability Survey

7/26/17, 2:06 PM

Usability Survey

* Required

1. Name *

2. MTurk Worker ID *

3. Is the interface easy to use *

1(Strongly disagree) 7(Strongly agree)
Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

4. Did you enjoy using the interface *

1(Strongly disagree) 7(Strongly agree)
Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. Were you able to differentiate between basic and extended permissions *

1(Strongly disagree) 7(Strongly agree)
Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. Were you able to differentiate between safe and unsafe permissions *

1(Strongly disagree) 7(Strongly agree)

Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. Were you able to understand the purpose of the asked permissions *

1(Strongly disagree) 7(Strongly agree)

Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. Do you think the interface is flexible in editing the permissions *

1(Strongly disagree) 7(Strongly agree)

Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. Users have lost all control over how personal information is collected and used by companies. *

1(Strongly disagree) 7(Strongly agree)

Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

10. Most businesses handle the personal information they collect about users in a proper and confidential way. *

1(Strongly disagree) 7(Strongly agree)

Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

11. Existing laws and organizational practices provide a reasonable level of protection for user privacy today. *

1(Strongly disagree) 7(Strongly agree)

Mark only one oval.

1	2	3	4	5	6	7
<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Powered by



APPENDIX D: EYE-ACTIVATED DIALOG USER STUDY EXIT SURVEY (ATTENTION EXPERIMENT)

Exit Survey

1/13/16, 2:10 PM

Exit Survey

Please answer the following questions about your eye-tracking experience

*** Required**

1. Rate your over-all experience with eye-tracking *

Mark only one oval.

	1	2	3	4	5	
Poor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Excellent

2. Rate the accuracy of eye-tracking during application installation tasks *

Mark only one oval.

	1	2	3	4	5	
Poor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Excellent

3. Rate the accuracy of eye-tracking during the eye-draw task *

Mark only one oval.

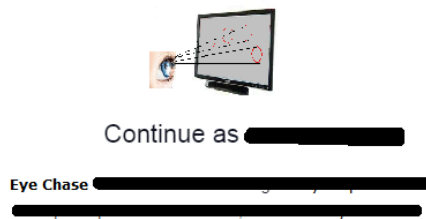
	1	2	3	4	5	
Poor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Excellent


4. Rate the accuracy of eye-tracking during the image selection task *

Mark only one oval.

	1	2	3	4	5	
Poor	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Excellent

You were presented with three installation windows during this study



 This does not let the app post to Facebook.

[App Terms](#) · [Privacy Policy](#)

Cancel

OK

5. Please type in the contents of the third window (shown above), to the best of your memory.
If you have no memory, please type "none": *

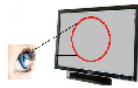
.....

.....

.....

.....

.....



Continue as [redacted]

Eye Draw [redacted]

[redacted]

This does not let the app post to Facebook.

[App Terms](#) · [Privacy Policy](#)

Cancel

OK

6. Please type in the contents of the second window (shown above), to the best of your memory. If you have no memory, please type "none": *

.....

.....

.....

.....

.....



Continue as [REDACTED]

Eye Select [REDACTED]

[REDACTED]

 This does not let the app post to Facebook.

[App Terms](#) · [Privacy Policy](#)

Cancel

OK

7. Please type in the contents of the first window (shown above), to the best of your memory.
If you have no memory, please type "none": *

.....

.....

.....

.....

.....

8. During this study, did you see any installation windows that requested permissions to your information? *

Mark only one oval.

- ☐ Yes
- ☐ No

9. If you answered yes to the previous question, which permission(s) did these installation windows request. Select all that apply *

Check all that apply.

- ☐ Public profile information
- ☐ Phone number
- ☐ Social Security Number
- ☐ Photos
- ☐ Mother's maiden name
- ☐ Other:

10. If yes, which installation windows requested such permissions

Check all that apply.

- ☐ Installation window 1
- ☐ Installation window 2
- ☐ Installation window 3
- ☐ All of the above

11. Please select the option that most accurately completes the following sentence: *

"When an installation window appeared on my screen, I believed it was..."

Mark only one oval.

- ☐ "displayed by Facebook"
- ☐ "displayed by my browser"
- ☐ "displayed by Microsoft Windows"
- ☐ "displayed by a virus or malware"
- ☐ Other
- ☐ I'm not sure

12. Did you think that the installation windows were part of the study? *

Mark only one oval.

- ☐ Yes
- ☐ No
- ☐ I'm not sure

13. **At the time you saw the installation window, did you suspect that the window was actually faked by the website?**

Mark only one oval.

- ☐ I never suspected
- ☐ Something felt funny or suspicious, but I had no idea what it was
- ☐ I suspected that the warning was faked by the website
- ☐ I was completely sure that the warning was faked by the website

14. **On most of the installation windows you saw, did you intentionally read the text in the installation window? ***

Mark only one oval.

- ☐ I ignored it
- ☐ I tried to read a little
- ☐ I read every word

15. **On the last installation window you saw, did you intentionally read the text in the installation window? ***

Mark only one oval.

- ☐ I ignored it
- ☐ I tried to read a little
- ☐ I read every word

Demographic questions

Lastly, please answer the following demographic questions

16. **What is your gender? ***

Mark only one oval.

- ☐ Female
- ☐ Male
- ☐ Decline to answer

17. What is the highest level of education you have completed? **Mark only one oval.*

- ☐ Some high school
- ☐ High school/GED
- ☐ Some college
- ☐ Associate's degree
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctorate degree
- ☐ Law degree
- ☐ Medical degree
- ☐ Trade or other technical school degree
- ☐ Decline to answer

18. What is your age? **Mark only one oval.*

- ☐ 20-30
- ☐ 30-40
- ☐ 40-50
- ☐ 50-60
- ☐ 60 and above

19. What is your current occupation? **Mark only one oval.*

- ☐ Administrative Support (eg., secretary, assistant)
- ☐ Art, Writing and Journalism (eg., author, reporter, sculptor)
- ☐ Business, Management and Financial (eg., manager, accountant)
- ☐ Education (eg., teacher, professor)
- ☐ Legal (eg., lawyer, law clerk)
- ☐ Medical (eg., doctor, nurse, dentist)
- ☐ Science, Engineering and IT professional (eg., researcher)
- ☐ Service (eg., retail clerks, server)
- ☐ Skilled Labor (eg., electrician, plumber, carpenter)
- ☐ Student
- ☐ Other Professional
- ☐ Not Currently Working/Currently Unemployed
- ☐ Retired
- ☐ Other
- ☐ Decline to answer

20. What is your race/ethnicity? **Mark only one oval.*

- ☐ Asian/Pacific Islander
- ☐ Black/African-American
- ☐ White/Caucasian
- ☐ Hispanic
- ☐ Native American/Alaska Native
- ☐ Other/Multi-Racial
- ☐ Decline to answer

APPENDIX E: EYE-ACTIVATED DIALOG USER STUDY EXIT SURVEY (HABITUATION EXPERIMENT)

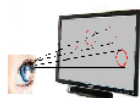
Post-task Survey

1/13/16, 2:11 PM

Post-task Survey

The image below corresponds to one of the dialogs you saw during this study:

* Required



Continue as [redacted]

Eye Chase [redacted]
[redacted]

This does not let the app post to Facebook.

[App Terms](#) · [Privacy Policy](#)

Cancel

OK

1. Please type in the contents of the most-recently shown dialog, to the best of your memory.
If you have no memory, please type "none" *

.....

.....

.....

.....

.....

2. What did the last dialog you saw communicate **Mark only one oval.*

- ☐ The quality of my performance in the study
- ☐ The application requires access to public profile information and social security number
- ☐ The amount of money I will be paid for the study
- ☐ The application requires access to public profile information and photos
- ☐ I'm not sure

3. How many times did you see this message **Mark only one oval.*

- ☐ Just once
- ☐ Between 2 and 4
- ☐ Between 5 and 8
- ☐ 9 or more
- ☐ I don't have any recollection

4. Overall, how annoying was this task **Mark only one oval.*

	1	2	3	4	5	
Not annoying at all	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	Very annoying

5. Did you suspect that the study may require you to answer questions about the content of the dialog? **Mark only one oval.*

- ☐ Definitely
- ☐ Somewhat
- ☐ Maybe a little
- ☐ Definitely not

6. During most of the dialogs you saw, did you intentionally read the text inside them? **Mark only one oval.*

- ☐ I ignored it
- ☐ I tried to read a little
- ☐ I read every word

7. During the last dialog you saw, did you intentionally read the text inside it? **Mark only one oval.*

- ☐ I ignored it
- ☐ I tried to read a little
- ☐ I read every word

8. Please let us know what, if anything, was not working with the dialogs that popped up on your browser *

.....

.....

.....

.....

.....

Demographic questions

Lastly, please answer the following demographic questions

9. What is your gender? **Mark only one oval.*

- ☐ Male
- ☐ Female
- ☐ Decline to answer

10. What is the highest level of education you have completed? **Mark only one oval.*

- ☐ Some high school
- ☐ High school/GED
- ☐ Some college
- ☐ Associate's degree
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctorate degree
- ☐ Law degree
- ☐ Medical degree
- ☐ Trade or other technical school degree
- ☐ Decline to answer

11. What is your age? **Mark only one oval.*

- ☐ 20-30
☐ 30-40
☐ 40-50
☐ 50-60
☐ 60 and above

12. What is your current occupation? **Mark only one oval.*

- ☐ Administrative Support (eg., secretary, assistant)
☐ Art, Writing and Journalism (eg., author, reporter, sculptor)
☐ Business, Management and Financial (eg., manager, accountant)
☐ Education (eg., teacher, professor)
☐ Legal (eg., lawyer, law clerk)
☐ Medical (eg., doctor, nurse, dentist)
☐ Science, Engineering and IT professional (eg., researcher)
☐ Service (eg., retail clerks, server)
☐ Skilled Labor (eg., electrician, plumber, carpenter)
☐ Student
☐ Other Professional
☐ Not Currently Working/Currently Unemployed
☐ Retired
☐ Other
☐ Decline to answer

13. What is your race/ethnicity? **Mark only one oval.*

- ☐ Asian/Pacific Islander
☐ Black/African-American
☐ White/Caucasian
☐ Hispanic
☐ Native American/Alaska Native
☐ Other/Multi-Racial
☐ Decline to answer

APPENDIX F: ADVERTISEMENTS USER STUDY POST-TEST AND DEMOGRAPHICS SURVEY

Exit Survey

3/12/17, 3:50 PM

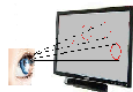
Exit Survey

Please complete the questions in this survey

* Required

You were presented with three applications during this study

Eye Chase Application



Continue as [REDACTED]

Eye Chase [REDACTED]
[REDACTED]

 This does not let the app post to Facebook.

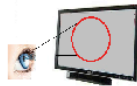
[App Terms](#) · [Privacy Policy](#)

Cancel

OK

1. Please type in the contents of the above window (marked black), to the best of your memory. If you have no memory, please type "none": *


Eye Draw Application



Continue as [REDACTED]

Eye Draw [REDACTED]

[REDACTED]

 This does not let the app post to Facebook.

[App Terms](#) · [Privacy Policy](#)

Cancel

OK

2. Please type in the contents of the above window (marked black), to the best of your memory. If you have no memory, please type "none": *

Eye Select Application



Continue as [REDACTED]

Eye Select [REDACTED]

[REDACTED]

 This does not let the app post to Facebook.

[App Terms](#) · [Privacy Policy](#)

Cancel

OK

3. Please type in the contents of the above window (marked black), to the best of your memory. If you have no memory, please type "none": *

4. Did any of the above application installation windows request permissions to your information? *

Mark only one oval.

☐ Yes

☐ No

5. If you answered yes to the previous question, which permission(s) did these application installation windows request. Select all that apply *

If you answer no to the previous question, select other
Check all that apply.

- ☐ Public profile information
- ☐ Phone number
- ☐ Social Security Number
- ☐ Photos
- ☐ Mother's maiden name
- ☐ Other: _____

6. If you selected permissions in the previous question, which installation windows requested such permissions *

If you selected other in the previous question, click none
Check all that apply.

- ☐ Application installation window 1
- ☐ Application installation window 2
- ☐ Application installation window 3
- ☐ All of the above
- ☐ None of the above

7. Did you suspect that these installation windows were part of the study? *

Mark only one oval.

- ☐ Yes
- ☐ No
- ☐ I'm not sure

8. On most of the installation windows you saw, did you intentionally read the text in the installation window? *

Mark only one oval.

- ☐ I ignored it
- ☐ I tried to read a little
- ☐ I read every word

9. **On the last installation window you saw, did you intentionally read the text in the installation window? ***

Mark only one oval.

- ☐ I ignored it
- ☐ I tried to read a little
- ☐ I read every word

10. **Did you notice the advertisements around these application windows? ***

Mark only one oval.

- ☐ Yes
- ☐ No
- ☐ I don't remember

11. **If yes, were you distracted by these advertisements? ***

Mark only one oval.

- ☐ Yes
- ☐ No

Demographic questions

Lastly, please answer the following demographic questions

12. **What is your gender? ***

Mark only one oval.

- ☐ Female
- ☐ Male

13. What is the highest level of education you have completed? **Mark only one oval.*

- ☐ Some high school
- ☐ High school/GED
- ☐ Some college
- ☐ Associate's degree
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctorate degree
- ☐ Law degree
- ☐ Medical degree
- ☐ Trade or other technical school degree
- ☐ Decline to answer

14. What is your age? **Mark only one oval.*

- ☐ 18-20
- ☐ 20-30
- ☐ 30-40
- ☐ 40-50
- ☐ 50-60
- ☐ 60 and above

15. What is your current occupation? **Mark only one oval.*

- ☐ Administrative Support (eg., secretary, assistant)
- ☐ Art, Writing and Journalism (eg., author, reporter, sculptor)
- ☐ Business, Management and Financial (eg., manager, accountant)
- ☐ Education (eg., teacher, professor)
- ☐ Legal (eg., lawyer, law clerk)
- ☐ Medical (eg., doctor, nurse, dentist)
- ☐ Science, Engineering and IT professional (eg., researcher)
- ☐ Service (eg., retail clerks, server)
- ☐ Skilled Labor (eg., electrician, plumber, carpenter)
- ☐ Student
- ☐ Other Professional
- ☐ Not Currently Working/Currently Unemployed
- ☐ Retired
- ☐ Other
- ☐ Decline to answer

16. What is your race/ethnicity? **Mark only one oval.*

- ☐ Asian/Pacific Islander
- ☐ Black/African-American
- ☐ White/Caucasian
- ☐ Hispanic
- ☐ Native American/Alaska Native
- ☐ Other/Multi-Racial
- ☐ Middle East
- ☐ Decline to answer

17. ID *

APPENDIX G: TOUCH ID MISCONCEPTIONS IN-PERSON USER STUDY DEMOGRAPHICS AND POST-TEST SURVEY

1/10/2017

Demographics Survey - Google Forms

Pre-Task Survey

Form Description

Participant ID*

What is your age*

What is your gender*

- ☐ Female
☐ Male
☐ Prefer not to answer

What is your highest level of completed education*

- ☐ High school
☐ Associate degree
☐ Bachelor degree
☐ Master's, PhD, or other graduate degree

What is your ethnicity*

- ☐ White/Caucasian
☐ Black/African-American
☐ Asian/Pacific Islander
☐ Hispanic
☐ Native-American
☐ Middle Eastern

Are you right-handed or left-handed?*

- ☐ Right-handed
☐ Left-handed
☐ Ambidextrous (Both)

What is the model of your iPhone*

- ☐ 3G, 3GS, 4, 4S, 5, or 5c
☐ 5S, 6, 6 Plus, 6S, 6S Plus
☐ I don't know/ other

- ☐ iPad Air 2, Pro, Mini 3, or Mini 4
- ☐ I don't own an iPhone/iPad

What is the model number of your iPhone?*

You can find the model number in the About section of your iPhone. Go to Settings > General > About

How long have you been using an iPhone/iPad during the last 5 years?*

- ☐ Less than a year
- ☐ 1 to 2 years
- ☐ 2 to 3 years
- ☐ Over 3 years

What is your proficiency as an iOS developer?*

- ☐ Never developed
- ☐ Novice
- ☐ Beginner
- ☐ Advanced
- ☐ Expert

Does your iPhone store any sensitive or confidential information?*

- ☐ Yes
- ☐ No
- ☐ I don't know

How often do you change your PIN or password?*

- ☐ Weekly
- ☐ Monthly
- ☐ Every six months
- ☐ Once a year
- ☐ Never
- ☐ I don't know

Do you use the same PIN or password anywhere else (for websites, credit cards, or other online service?)*

- ☐ Yes
- ☐ No

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

What is your iPhone auto lock time (the amount of time the screen stays on if the device is not being used)?*

- ☐ Never auto locks
- ☐ 1 min
- ☐ 2 min
- ☐ 3 min
- ☐ 4 min
- ☐ 5 min
- ☐ I don't know

In your opinion, what unlocking method is more secure?*

- ☐ Alphanumeric password
- ☐ 4-digit PIN
- ☐ 6-digit PIN
- ☐ Fingerprint (TouchID)
- ☐ Eye recognition
- ☐ Face recognition
- ☐ None of them
- ☐ I have no idea

After page 1

Add item ▼

Continue to next page

Page 2 of 2

Touch ID questions

How long have you been using Touch ID for?*

- ☐ <6 months
- ☐ 6-12 months
- ☐ More than 1 year
- ☐ More than 2 years
- ☐ I don't know

What apps do you use Touch ID for? List them. (Open-ended)*

What fingerprint(s) do you register to use with Touch ID? Mark all that apply.*

- ☐ Left thumb
- ☐ Right thumb
- ☐ Left index finger
- ☐ Right index finger
- ☐ Left middle finger
- ☐ Right middle finger
- ☐ Left ring finger
- ☐ Right ring finger
- ☐ Left pinky finger
- ☐ Right pinky finger

Why do you use Touch ID? (Mark all that apply)*

- ☐ Convenience
- ☐ Reliability
- ☐ Novelty
- ☐ Privacy
- ☐ Security
- ☐ Cool to use
- ☐ Time
- ☐ Fun to use
- ☐ Ease of use
- ☐ Other

How easy or difficult do you think it is to bypass Touch ID?*

- ☐ Very difficult
- ☐ Difficult
- ☐ Decent
- ☐ Easy
- ☐ Very easy

Does use of Touch ID affect your privacy?*

- ☐ Yes
- ☐ No
- ☐ I don't know

How much do you agree: My iPhone is more secure if I use Touch ID over PIN/password?*

- ☐ Strongly disagree
- ☐ Disagree
- ☐ Neutral

1/10/2017

Demographics Survey - Google Forms

- ☐ Agree
- ☐ Strong Agree

Can someone use their fingerprint to get into your device using Touch ID?*

- ☐ Yes
- ☐ No
- ☐ I don't know

What is your major security or privacy concern about Touch ID, if any?*

Add item ▼

Post-Task Survey

Form Description

Participant ID*

What was being used to authenticate you during this Touch ID based transaction on Amazon?*

- ☐ Fingerprint
☐ My password/PIN
☐ Both (a) and (b)

Is being authenticated by your fingerprint the same as by your username/password?*

- ☐ Yes
☐ No
☐ I don't know

Is your fingerprint being used by Amazon to authenticate you during this transaction?*

- ☐ Yes
☐ No
☐ I don't know

Where is your fingerprint being stored BEFORE this transaction? (Mark all that apply)*

- ☐ In my iPhone
☐ In my iCloud account
☐ On an Apple server
☐ On an Amazon server
☐ On a third-party server

Where is your fingerprint being stored AFTER this transaction? (Mark all that apply)*

- ☐ In my iPhone
☐ In my iCloud account
☐ On an Apple server
☐ On an Amazon server
☐ On a third-party server

Who has access to your fingerprint DURING this transaction? (Mark all that apply)*

- ☐ My iPhone

- ☐ Apple
- ☐ Amazon
- ☐ An independent third-party

Can someone else use YOUR fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone?*

- ☐ Yes
- ☐ No
- ☐ I don't know

Can someone else use YOUR fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?*

- ☐ Yes
- ☐ No
- ☐ I don't know

Can someone else use HIS/HER fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone?*

- ☐ Yes
- ☐ No
- ☐ I don't know

Can someone else use HIS/HER fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?*

- ☐ Yes
- ☐ No
- ☐ I don't know

After page 1

Add item ▼

Continue to next page

Page 2 of 3

Would I (the interviewer) have been able to unlock/make a payment on YOUR device without your password/PIN if my fingerprint is registered?*

- ☐ Yes
- ☐ No
- ☐ I don't know

Can changing your password/PIN protect against a stranger unlocking/making a payment on YOUR device?*

1/10/2017

Post-Task Survey - Google Forms

- ☐ Yes
- ☐ No
- ☐ I don't know

Add item ▼

After page 2

Continue to next page

Page 3 of 3

What can you do to prevent this from happening? (Choose all that apply)*

- ☐ Reset password/PIN to something more secure
- ☐ Reset stored fingerprints
- ☐ Disable Touch ID
- ☐ Reset device
- ☐ Contact Apple
- ☐ I don't know

Can you control how many fingerprints are registered using Touch ID?*

- ☐ Yes
- ☐ No
- ☐ I don't know

What security changes would you make to Touch ID to protect against malicious fingerprint enrollment?*

Add item ▼

APPENDIX H: TOUCH ID MISCONCEPTIONS MTURK USER STUDY DEMO- GRAPHICS AND POST-TEST SURVEY

1/10/2017

Research Survey - Google Forms

age 1 of 8

Research Survey

Form Description

Amazon Turk ID*

What is your age*

What is your gender*

- ☐ Female
☐ Male
☐ Prefer not to answer

What is your highest level of completed education*

- ☐ High school
☐ Associate degree
☐ Bachelor degree
☐ Master's, PhD, or other graduate degree

What is your ethnicity*

- ☐ White/Caucasian
☐ Black/African-American
☐ Asian/Pacific Islander
☐ Hispanic
☐ Native-American
☐ Middle Eastern

Are you right-handed or left-handed?*

- ☐ Right-handed
☐ Left-handed
☐ Ambidextrous (Both)

What is the model of your iPhone*

- ☐ 3G, 3GS, 4, 4S, 5, or 5C
☐ 5S, 6, 6 Plus, 6S, 6S Plus

- ☐ I don't know/ other
- ☐ iPad Air 2, Pro, Mini 3, or Mini 4
- ☐ I don't own an iPhone/iPad

What is the model number of your iPhone?*

You can find the model number in the About section of your iPhone. Go to Settings > General > About

How long have you been using an iPhone/iPad during the last 5 years?*

- ☐ Less than a year
- ☐ 1 to 2 years
- ☐ 2 to 3 years
- ☐ Over 3 years

What is your proficiency as an iOS developer*

- ☐ Never developed
- ☐ Novice
- ☐ Beginner
- ☐ Advanced
- ☐ Expert

After page 1

Add item

Continue to next page

Page 2 of 8

You do not qualify for the study. Please return the HIT

Page 3 of 8

After page 2

Add item

study. Please accept the HIT and click "Continue" to begin the study

You are qualified to participate in the

Page 4 of 8

Add item

First, please answer the following questions**Does your iPhone store any sensitive or confidential information?***

- ☐ Yes
- ☐ No
- ☐ I don't know

How often do you change your PIN or password?*

- ☐ Weekly
- ☐ Monthly
- ☐ Every six months
- ☐ Once a year
- ☐ Never
- ☐ I don't know

Do you use the same PIN or password anywhere else (for websites, credit cards, or other online service)?*

- ☐ Yes
- ☐ No

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

What is your iPhone auto lock time (the amount of time the screen stays on if the device is not being used)?*

- ☐ Never auto locks
- ☐ 1 min
- ☐ 2 min
- ☐ 3 min
- ☐ 4 min
- ☐ 5 min
- ☐ I don't know

In your opinion, what unlocking method is more secure?*

- ☐ Alphanumeric password
- ☐ 4-digit PIN
- ☐ 6-digit PIN
- ☐ Fingerprint (TouchID)
- ☐ Eye recognition
- ☐ Face recognition
- ☐ None of them
- ☐ I have no idea

For this question, please click the option "Eyes"*

- ☐ Face
- ☐ Eyes

☐ Fingers

Page 5 of 8

[Add item](#)

Touch ID questions

Please answer the following questions about your familiarity with TouchID

How long have you been using Touch ID for?*

- ☐ <6 months
- ☐ 6-12 months
- ☐ More than 1 year
- ☐ More than 2 years
- ☐ I don't know

What apps do you use Touch ID for? List them. (Open-ended)*

What fingerprint(s) do you register to use with Touch ID? (Mark all that apply)*

- ☐ Left thumb
- ☐ Right thumb
- ☐ Left index finger
- ☐ Right index finger
- ☐ Left middle finger
- ☐ Right middle finger
- ☐ Left ring finger
- ☐ Right ring finger
- ☐ Left pinky finger
- ☐ Right pinky finger

Why do you use Touch ID? (Mark all that apply)*

- ☐ Convenience
- ☐ Reliability
- ☐ Novelty
- ☐ Privacy
- ☐ Security
- ☐ Cool to use
- ☐ Time
- ☐ Fun to use
- ☐ Ease of use

☐ Other**How easy or difficult do you think it is to circumvent Touch ID?***

- ☐ Very difficult
☐ Difficult
☐ Decent
☐ Easy
☐ Very easy

Does use of Touch ID affect your privacy?*

- ☐ Yes
☐ No
☐ I don't know

How much do you agree: My iPhone is more secure if I use Touch ID over PIN/password?*

- ☐ Strongly disagree
☐ Disagree
☐ Neutral
☐ Agree
☐ Strong Agree

Can someone use their fingerprint to get into your device using Touch ID?*

- ☐ Yes
☐ No
☐ I don't know

What is your major security or privacy concern about Touch ID, if any?*

Page 6 of 8 After page 5

[Add item](#)

Informed Consent

Project Purpose

The purpose of this research project is to study the user awareness and comprehension of Apple's Touch ID technology, which allows users to unlock their iPhone devices and make purchases with their fingerprint by tapping the home button. The study is being conducted by PhD students Emmanuel Bello-Ogunu and Yousra Javed, under the direction of Dr. Mohamed Shehab, and has been approved by the University Institutional Review Board at UNC Charlotte.

Investigator(s)

Emmanuel Bello-Ogunu – Software and Information Systems
Yousra Javed – Software and Information Systems

Dr. Mohamed Shehab – Software and Information Systems**Eligibility**

Any adult 18 years of age or older who owns an iPhone/iPad with Touch ID

Overall Description of Participation

Participants in the study will complete a short survey, and then will be required to watch a video and complete a set of questions directly related to scenario presented in the video.

Length of Participation

The estimated completion time of the tasks is approximately 15 minutes. Each participant will be rewarded with a \$0.5 upon the completion of user study tasks.

Risks and Benefits of Participation

The study involves no more than minimal risk (i.e., the level of risk encountered in daily life).

Volunteer Statement

The decision to participate in this study is completely voluntary. If you decide to be in the study, you may stop at any time. You will not be treated any differently if you decide not to participate in the study or if you stop once you have started.

Confidentiality Statement

Any information about your participation, including your identity, is completely confidential. The following steps will be taken to ensure this confidentiality: Your data will be anonymized and you will be assigned a participant number, which will be used to refer to your data set. In analysis of results, all data will be pooled and published in aggregate form only. All files will be stored on an external hard drive in a locked cabinet.

Statement of Fair Treatment and Respect

UNC Charlotte wants to make sure that you are treated in a fair and respectful manner. If you have further questions or concerns about your rights as a participant in this study, contact the Compliance Office at 704-687-1871. If you have questions concerning the study, contact Emmanuel (ebelloog@uncc.edu), Yousra (yjaved@uncc.edu), or Dr. Shehab (mshehab@uncc.edu).

I have read the information in this consent form. I have had the chance to ask questions about this study, and those questions have been answered to my satisfaction. I am at least 18 years of age, and I agree to participate in this research project.

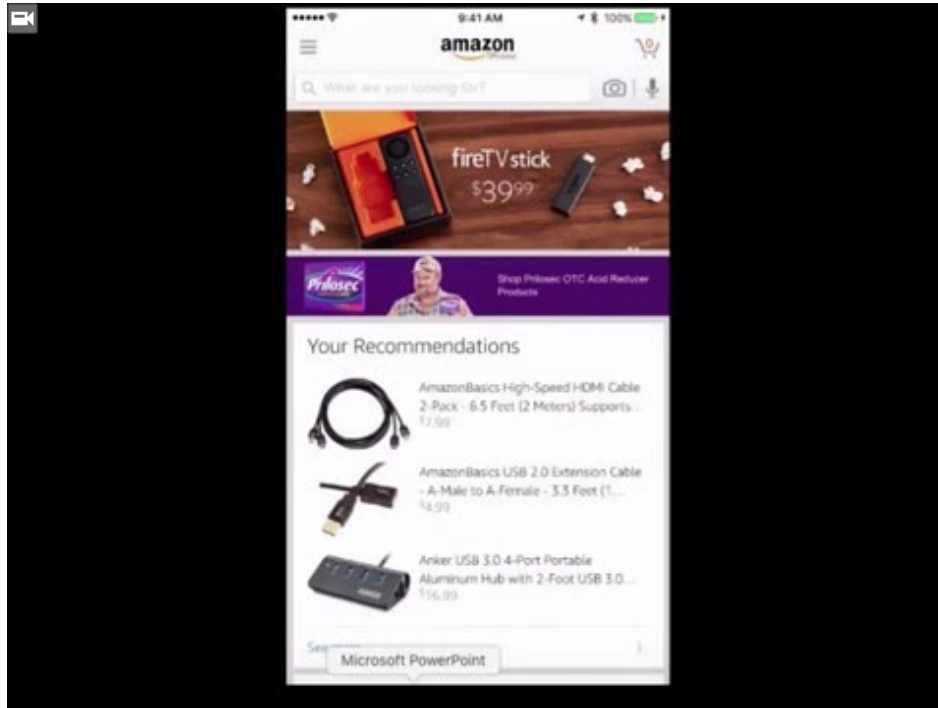
*

☐ I Agree☐ I Do Not Agree

Page 7 of 8

[Add item](#)[Add page](#)[Go to page 4 \(First, please answer the following questions\)](#)

This video shows you a scenario of Amazon purchase using TouchID on iPhone. Please watch the video below



After page 7

Add item ▼

Continue to next page

Page 8 of 8

Post-Task Questions

Please answer the following questions based on the scenario presented to you in the video

What was being used to authenticate you during this Touch ID transaction?*

- ☐ Fingerprint
- ☐ My password/PIN
- ☐ Both (a) and (b)

Is being authenticated by your fingerprint the same as by your username/password?*

- ☐ Yes
- ☐ No
- ☐ I don't know

Is your fingerprint being used by Amazon to authenticate you during this transaction?*

- ☐ Yes
☐ No
☐ I don't know

Where is your fingerprint being stored BEFORE this transaction? (Mark all that apply)*

- ☐ In my iPhone
☐ In my iCloud account
☐ On an Apple server
☐ On an Amazon server
☐ On a third-party server

Where is your fingerprint being stored AFTER this transaction? (Mark all that apply)*

- ☐ In my iPhone
☐ In my iCloud account
☐ On an Apple server
☐ On an Amazon server
☐ On a third-party server

Who has access to your fingerprint DURING this transaction? (Mark all that apply)*

- ☐ My iPhone
☐ Apple
☐ Amazon
☐ An independent third-party

Can someone else use YOUR fingerprint to make a purchase with YOUR Amazon account on YOUR iPhone?

- ☐ Yes
☐ No
☐ I don't know

For this question, please click the option "I'm not sure"*

- ☐ No
☐ Yes
☐ I'm not sure

Can someone else use YOUR fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?*

- ☐ Yes
☐ No

1/10/2017

Research Survey - Google Forms

☐ I don't know

Can someone else use HIS/HER fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?*

☐ Yes

☐ No

☐ I don't know

Can someone else use HIS/HER fingerprint to make a purchase with YOUR Amazon account on HIS/HER iPhone?*

☐ Yes

☐ No

☐ I don't know

Add item ▼

APPENDIX I: TOUCH ID TERMS AND CONDITIONS DIALOG DESIGNS USER STUDY: DEMOGRAPHICS, TOUCH ID COMPREHENSION, PRE-TEST AND POST-TEST SURVEY

Pre-Task Survey

9/26/16, 1:47 PM

[Request edit access](#)

Pre-Task Survey

Demographic questions

*** Required**

Participant ID *

What is your age *

What is your gender *

- ☐ Female
- ☐ Male
- ☐ Prefer not to answer

What is your highest level of completed education *

- ☐ High school
- ☐ Associate degree
- ☐ Bachelor degree
- ☐ Master's, PhD, or other graduate degree

What is your ethnicity *

- ☐ White/Caucasian
- ☐ Black/African-American
- ☐ Asian/Pacific Islander
- ☐ Hispanic
- ☐ Native-American
- ☐ Middle Eastern

Are you right-handed or left-handed? *

- ☐ Right-handed
- ☐ Left-handed
- ☐ Ambidextrous (Both)

What is the model of your iPhone *

- ☐ 3G, 3GS, 4, 4S, 5, or 5c
- ☐ 5S, 6, 6 Plus, 6S, 6S Plus
- ☐ I don't know/ other
- ☐ iPad Air 2, Pro, Mini 3, or Mini 4
- ☐ I don't own an iPhone/iPad

What is the model number of your iPhone? *

You can find the model number in the About section of your iPhone. Go to Settings > General > About

How long have you been using an iPhone/iPad during the last 5 years? *

- ☐ Less than a year
- ☐ 1 to 2 years
- ☐ 2 to 3 years
- ☐ Over 3 years

What is your proficiency as an iOS developer *

- ☐ Never developed
- ☐ Novice
- ☐ Beginner
- ☐ Advanced
- ☐ Expert

Does your iPhone store any sensitive or confidential information? *

- ☐ Yes
- ☐ No
- ☐ I don't know

How often do you change your PIN or password? *

- ☐ Weekly
- ☐ Monthly
- ☐ Every six months
- ☐ Once a year
- ☐ Never
- ☐ I don't know

Do you use the same PIN or password anywhere else (for websites, credit cards, or other online

service?)* *

- ☐ Yes
☐ No

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

What is your iPhone auto lock time (the amount of time the screen stays on if the device is not being used)? *

- ☐ Never auto locks
☐ 1 min
☐ 2 min
☐ 3 min
☐ 4 min
☐ 5 min
☐ I don't know

In your opinion, what unlocking method is more secure? *

- ☐ Alphanumeric password
☐ 4-digit PIN
☐ 6-digit PIN
☐ Fingerprint (TouchID)
☐ Eye recognition
☐ Face recognition
☐ None of them
☐ I have no idea

Continue »

Powered by

This form was created inside of UNC Charlotte.

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

Pre-Task Survey

* Required

Touch ID questions

How long have you been using Touch ID for? *

- ☐ <6 months
- ☐ 6-12 months
- ☐ More than 1 year
- ☐ More than 2 years
- ☐ I don't know

What apps do you use Touch ID for? List them. (Open-ended) *

What fingerprint(s) do you register to use with Touch ID? Mark all that apply. *

- ☐ Left thumb
- ☐ Right thumb
- ☐ Left index finger
- ☐ Right index finger
- ☐ Left middle finger
- ☐ Right middle finger
- ☐ Left ring finger
- ☐ Right ring finger
- ☐ Left pinky finger
- ☐ Right pinky finger

Why do you use Touch ID? (Mark all that apply) *

- ☐ Convenience
- ☐ Reliability
- ☐ Novelty
- ☐ Privacy
- ☐ Security
- ☐ Cool to use
- ☐ Time
- ☐ Fun to use
- ☐ Ease of use
- ☐ Other

« Back

Submit

Never submit passwords through Google Forms.

Powered by

This form was created inside of UNC Charlotte.

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

[Request edit access](#)

Pre-test Questionnaire

* Required

Participant ID *

What is being used when you sign into a mobile application using Touch ID? *

- ☐ Fingerprint
- ☐ Account password
- ☐ Both (a) and (b)
- ☐ I don't know

What is being used when you are authenticated with Touch ID during a sensitive task inside the mobile application? *

- ☐ Fingerprint
- ☐ Account password
- ☐ Both (a) and (b)
- ☐ I don't know

Where is your fingerprint being stored BEFORE you sign in/authenticate with Touch ID from within the mobile application? (Mark all that apply) *

- ☐ In my iPhone
- ☐ In my iCloud account
- ☐ On an Apple server
- ☐ On a third-party server
- ☐ I don't know

Where is your fingerprint being stored AFTER you sign in/authenticate using Touch ID from within the mobile application? (Mark all that apply) *

- ☐ In my iPhone
- ☐ In my iCloud account
- ☐ On an Apple server
- ☐ On a third-party server
- ☐ I don't know

Where is your fingerprint being stored DURING your signing in/authentication using Touch ID from within the mobile application? (Mark all that apply) *

- ☐ In my iPhone
- ☐ In my iCloud account
- ☐ On an Apple server
- ☐ On a third-party server
- ☐ I don't know

Can someone else use HIS/HER fingerprint to access YOUR mobile application account on YOUR iPhone? *

- ☐ Yes
- ☐ No
- ☐ I don't know

Submit

Never submit passwords through Google Forms.

Powered by

This form was created inside of UNC Charlotte.

[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

[Request edit access](#)

Post-test Questionnaire

* Required

Participant ID *

Please write down the contents of the dialog presented to you while you used Touch ID *

If you have no memory, please type "none"

What is being used when you sign into a mobile application using Touch ID? *

- ☐ Fingerprint
- ☐ Account password
- ☐ Both (a) and (b)
- ☐ I don't know

What is being used when you are authenticated with Touch ID during a sensitive task inside the mobile application? *

- ☐ Fingerprint
- ☐ Account password
- ☐ Both (a) and (b)
- ☐ I don't know

Where is your fingerprint being stored BEFORE you sign in/authenticate with Touch ID from within the mobile application? (Mark all that apply) *

- ☐ In my iPhone
- ☐ In my iCloud account
- ☐ On an Apple server
- ☐ On a third-party server

☐ I don't know

Where is your fingerprint being stored AFTER you sign in/authenticate using Touch ID from within the mobile application? (Mark all that apply) *

- ☐ In my iPhone
- ☐ In my iCloud account
- ☐ On an Apple server
- ☐ On a third-party server
- ☐ I don't know

Where is your fingerprint being stored DURING your signing in/authentication using Touch ID from within the mobile application? (Mark all that apply) *

- ☐ In my iPhone
- ☐ In my iCloud account
- ☐ On an Apple server
- ☐ On a third-party server
- ☐ I don't know

Can someone else use HIS/HER fingerprint to access YOUR mobile application account on YOUR iPhone? *

- ☐ Yes
- ☐ No
- ☐ I don't know

[Continue »](#)

Powered by

This form was created inside of UNC Charlotte.
[Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

Post-test Questionnaire

* Required

State how much you agree or disagree with the following statements

The proposed terms and conditions dialog design helped me better understand fingerprint storage, access, and Touch ID authentication process *

1 2 3 4 5

Strongly disagree ☐ ☐ ☐ ☐ ☐ Strongly agree

The icons on the proposed terms and conditions dialog helped me better differentiate between the sensitivity of information provided *

1 2 3 4 5

Strongly disagree ☐ ☐ ☐ ☐ ☐ Strongly agree

The icon colors on the proposed terms and conditions dialog attracted my attention towards the text *

1 2 3 4 5

Strongly disagree ☐ ☐ ☐ ☐ ☐ Strongly agree

The proposed terms and conditions dialog was easy to read *

1 2 3 4 5

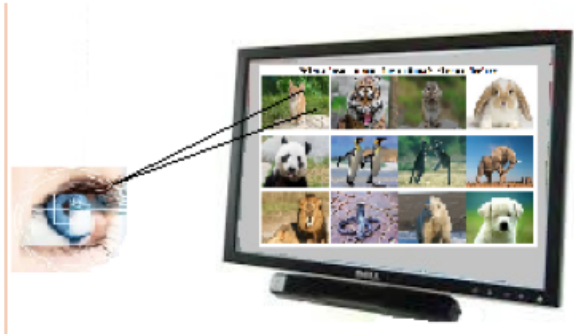
Strongly disagree ☐ ☐ ☐ ☐ ☐ Strongly agree

« Back

Submit

Never submit passwords through Google Forms.

Participants Needed For A Research Study



A graduate student in the Software and Information Systems department is conducting a research study to learn about the viability of an eye-activated browser that uses eye-gaze to perform various tasks inside the browser.

Who can participate?

Anyone who

- Is 18 years or older
- Owns an active Facebook account

What you will do?

Each participant will perform a set of tasks that involve eye-tracking and complete a survey about their experience. The duration of an individual session will be 10-20 minutes.

Want more information?

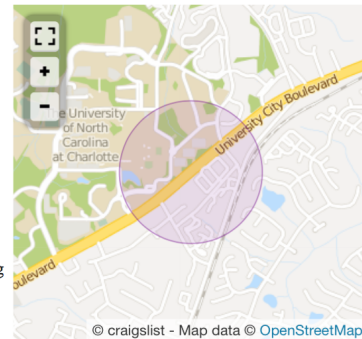
If you are interested in participating, please contact us
yjaved@uncc.edu

**Get a \$5
Starbucks card
for your time**

APPENDIX K: EYE-ACTIVATED DIALOG USER STUDY CRAIGSLIST RE- CRUITMENT FLYER

[reply](#) ☐ [prohibited](#) ^[?] Posted 8 minutes ago [print](#)

★ Participants Needed For A Research Study At UNCC- Get \$5 Giftcard ^[?]



Would you like to use an Eye-Activated Web Browser?

A graduate student in the Software and Information Systems department at UNC Charlotte is conducting a research study to learn about the viability of an eye-activated browser that uses eye-gaze to perform various tasks inside the browser.

Who can participate?

- Anyone who
- Does not have eye-sight problem
 - Owns an active Facebook account

What will you do?

Each participant will perform a set of tasks that involve eye-tracking and will be complete a survey to discuss their experience. The duration of an individual session will be 20-30 minutes. Each participant will receive a \$5 Starbucks giftcard for their time.

Where and when?

Woodward Hall, Aug 30th- Sept 10th, 2016

Want more information?

If you are interested in participating and have questions, please contact us by responding to this ad

- do NOT contact me with unsolicited services or offers

post id: 5746323825

posted: 8 minutes ago

[email to friend](#)

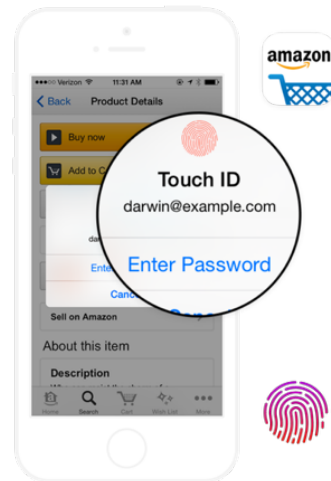
♥ [best of](#) ^[?]

APPENDIX L: TOUCH ID PERCEPTIONS USER STUDY ON-CAMPUS RE- CRUITMENT FLYER

iPhone Touch ID User Study

- **Help** us learn about using Apple's Touch ID technology for making mobile payments
- **Receive** \$5 Amazon credit to use for an Amazon purchase using Touch ID - no cost to participate
- **Complete** a set of survey questions related to the Touch ID transaction
- **Earn** an additional \$5 Amazon credit at the end for participating in the user study

Eligible participants will be ones who own a Touch ID-enabled Apple device (ex. iPhone 5s and up) and are familiar with using this feature. If interested, please email ebelloog@uncc.edu or yjaved@uncc.edu.



This research is being conducted by PhD candidates Emmanuel Bello-Ogunu and Yousra Javed, under the direction of Dr. Mohamed Shehab from the College of Computing & Informatics. It has been approved by UNC Charlotte—Protocol #, Approval Date: .

For more information, contact Emmanuel: ebelloog@uncc.edu or Yousra: yjaved@uncc.edu

APPENDIX M: TOUCH ID TERMS AND CONDITIONS USER STUDY RE- CRUITMENT FLYER

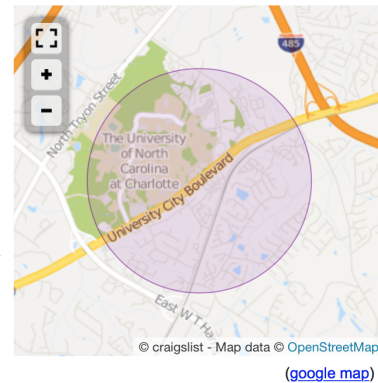
★ \$5 Gift Card - Participants required for research study at UNCC

I am a PhD candidate in the Software & Information Systems department. I am looking for people who own a Touch ID enabled iPhone/iPad to participate in a research study.

The purpose of this research study (approved by UNC Charlotte's IRB, Protocol#16-01-36) is to learn about user experience and perceptions about Touch ID technology. Participants should own a Touch ID enabled iPhone/iPad. Each participant will perform a set of tasks inside two iOS applications. Participants will then complete a questionnaire regarding their experience. The estimated time required is approximately 20-25 minutes. Each participant will receive a \$5 Starbucks gift card at the end of the study.

The study will take place in Woodward from Dec13 onwards. If anyone is interested in participating, please book a time-slot for the study here <https://touchid-research-study.youcanbook.me/>

- do NOT contact me with unsolicited services or offers



post id: 5916857111 posted: 29 days ago email to friend ♥ best of [7]