# TOUCH INTERACTION FOR USER AUTHENTICATION

by
Shahshuja Shahzada

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF APPLIED SCIENCE

Human-Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2014

## Abstract

Touchscreens that permit multi-touch and gestures interaction are now commonplace. This thesis explores whether these new capabilities might support novel password schemes that could be a viable alternative to traditional text passwords. We conducted a preliminary study with a multi-touch graphically oriented password scheme that we designed called Passgrid and a main study with a multi-touch password scheme called GesturePass, which we designed to focus more on gestures.

Our study compared Passgrid to a text password scheme in terms of login time, effect of screen size, and the overall user experience. Our findings showed that users made little use of the multi-touch capability and so Passgrid had longer login times. We also found that users preferred using smaller touchscreen devices, and users responded favourably to the use of gestures.

We then designed GesturePass specifically to focus on gestures and smaller touchscreen devices. Our study compared the usability of GesturePass to a PIN password scheme. GesturePass required more initial practices, and had somewhat longer login times, but required a similar number of login attempts. We determined that the longer login times stemmed from certain complex gestures that could potentially be simplified, and that GesturePass could potentially be a viable authentication approach.

## Acknowledgements

I would like to thank my supervisors, Robert Biddle and Sonia Chiasson. This thesis would not have been possible without their guidance, enthusiasm, and expertise. Thank you for being patient, and sharing your wisdom.

I would like to thank the members of my committee, Ali Arya, Andrew Patrick, and Chris Joslin for their time and feedback.

Finally, I would also like to thank my parents for their love, support, and encouragement.

# Table of Contents

## List of Tables

## List of Figures

# Chapter 1

# Introduction

## 1.1 Motivation

Authentication is crucial when accessing accounts containing valuable information. The role of authentication is for the system to determine whether the user has the right to access the information they are requesting. The main form of authentication online involves password schemes, where the user must enter a secret that has been previously agreed on. There are other forms of authentication, but passwords are inexpensive and easy to deploy on multiple platforms [5]. The traditional approach involves a password entered on a keyboard with letters, numbers and special symbols. Recently, however, touchscreen devices have become widespread and these allow other forms of passwords. Screens on mobile devices are generally getting larger and are replacing physical keyboards. On tablets, the primary source of interaction is touch. Even modern laptops and large screen displays now have multi-touch capabilities. Text passwords are still most commonly used on these devices even though studies show that users generally perform better with text input using a physical keyboard than a virtual keyboard [50]. New mobile devices promote more visual and graphically orientated interactions and therefore we wish to explore these possibilities, especially those involving multi-touch interaction.

## 1.2 Research Question

For many years, computers have featured graphical displays and pointing devices such as a mouse and trackpad. Recently, touchscreens also allow recognition of multiple touches and gestures. For example, smart phones and tablets have become extremely commonplace and users now routinely use multi-touch interaction and gestures. Multi-touch interaction allows for faster input by simultaneous pointing with

multiple fingers. It also allows gestures, an expressive form of interaction that allows fast input of a range of complex concepts. This thesis will investigate the question: Can we design a multi-touch or gesture password scheme for touchscreen devices that is a viable alternative to a traditional text password scheme?

## 1.3 Contributions

The main contributions of this thesis involve the design, implementation, and empirical evaluation of two novel password schemes.

The first scheme is a new multi-touch graphical password scheme called Passgrid. Passgrid was compared to a traditional text password scheme in terms of login time, effect of screen size, level of user acceptance and overall user experience. Our main focus was the general user experience, and whether people would use multiple simultaneous dragging. Our findings, however, showed that the users responded more favourably to the use of gestures.

The second scheme involved passwords consisting entirely of set gestures, such as tapping, dragging, and pinching. This scheme, named GesturePass, was compared to a PIN password scheme on a Nexus 4 phone and a Nexus 7 tablet. The factors which were analyzed in this study included number of password practices, login attempts, gesture times and usability questionnaire responses.

Our design and evaluation work shows that multi-touch gesture passwords may well form a viable authentication approach on touchscreen devices.

## 1.4 Thesis Outline

This thesis is organized as follows:

**Chapter 2** : We discuss background material on authentication and different types of passwords, including graphical passwords.

**Chapter 3** : We describe Passgrid, our preliminary multi-touch pointing graphical password scheme, and our study to assess its usability.

**Chapter 4** : We describe GesturePass, our gesture based password scheme, and our study to assess its usability.

**Chapter 5** : We provide an overall interpretation of our two password schemes and the results of our studies, address our research question, and discuss possibilities for future work.

# Chapter 2

# Background

## 2.1 Authentication

Authentication is the act of proving that someone is who they claim to be [33]. The three main categories of authentication that can be used to identify users are knowledge, ownership and biometric [33]. Table 2.1 defines and provides examples of each category. Authentication by something known is the most popular authentication category and is dominated by text passwords. Some systems require multi-factor authentication that involves using several different categories. For example, automated banking machines require users to provide a bank card (something owned) and their PIN (something known). Authentication can take place in many forms in order to protect valuable information. In the following sections we focus on knowledge based authentication systems.

### Password Spaces

The strength of a knowledge based authentication system is usually measured by the size of its theoretical password space. The theoretical password space is the total number of possible password combinations that a password scheme can produce.

| Category | Definition | Examples |
|---|---|---|
| Knowledge | Something the user knows | Text, graphical and gesture passwords, PINs, pass-phrases |
| Ownership | Something the user owns (also known as token-based authentication) | ID cards, smartcards, mobile phones, one-time password generators, hardware tokens or soft tokens |
| Biometric | Something that user is (biological or behavioral feature) | Fingerprints, retinal scans, voice, DNA, typing patterns |

Table 2.1: Authentication Types

For example, the theoretical password space of a text password is calculated as $95^n$, where 95 is the number of typeable characters on a US English keyboard, and $n$ is the variable length of the password. Therefore a 6-character password has the theoretical password space of $95^6 = 735,091,890,625$. Theoretical password spaces are expressed as exponents of base-2 and are traditionally referred to as being measured in bits. Therefore the theoretical password space in this example can be expressed as $95^6 = 2^{39}$ or approximately 39 bits. Table 2.2 shows a few password configurations and their approximate theoretical password space in bits. Large theoretical password spaces give an indication of a strong password system. The strength of a password system is important because it indicates the amount of effort (time and computational resources) for an attacker to guess a password.

The effective password space is another password space concept which approximates the number of passwords typically chosen by users. In our example, the user can theoretically choose any of the 95 typeable keyboard characters in their password. However in practice, users often limit their choices to smaller subsets of the character combinations such as only using alphabet letters or digits for particular accounts. This can make the effective password space much smaller than theoretical password space and difficult to calculate since users have different subset preferences. In 2009, a gaming website called RockYou that provided applications for numerous social networking sites such as Facebook, MySpace and Friendster had a security breach that publicly leaked 32 million passwords [7]. Studies on these passwords revealed that the average text password length was 7.9 characters, and although a majority of passwords contained digits, it was found that roughly less than ten percent of passwords contained special characters [7, 58].

Ideally, the effective passwords space should equal the theoretical password space of a password system. If these passwords spaces are not the same because of user subset preferences, the theoretical password space becomes an over-estimate because users do not select all of the possible password combinations. One solution to this issue is randomly assigned passwords which can equalize the theoretical and effective password spaces, but randomly assigned passwords are often difficult to remember [61].

| Condition | Input Options | Length (n) | Size | Theoretical Password Space |
|---|---|---|---|---|
| All typeable characters | 95 | 6 | 735,091,890,625 | 39 bits |
| Upper and lower case letters, with digits | 62 | 6 | 56,800,235,584 | 36 bits |
| Upper and lower case letters | 52 | 6 | 19,770,609,664 | 34 bits |
| Digits | 10 | 6 | 1,000,000 | 20 bits |
| Digits | 10 | 4 | 10,000 | 13 bits |

Table 2.2: Theoretical Password Space Examples

**Threat Models**

Password systems are vulnerable to guessing and capture attacks [5]. Guessing attacks occur when an attacker attempts to break into an account by repeatedly guessing the password. Capture attacks consist of using illicit techniques to obtain direct captures of a password.

There are various forms of guessing attacks, including brute force and dictionary attacks. A brute force guessing attack occurs when an attacker systematically guesses all possible password combinations. This type of attack is most successful against password systems that have small theoretical password spaces. A dictionary attack takes place when attackers guess passwords based on a list (dictionary) consisting of probable passwords selected by the user, such as common words and names. For text passwords, dictionary attacks also take into account predictable patterns such as leading capitalization, trailing punctuation and digit additions. When users are given the choice to select their own passwords, they typically choose passwords which are easily guessed by dictionary attacks [19]. Secure passwords, on the other hand, can be hard to remember and difficult to enter [61].

Capture attacks include shoulder-surfing, phishing and certain types of malware. Shoulder-surfing occurs when an attacker obtains a password by watching the user enter it. Phishing is a type of social engineering where the attacker tricks the user into sharing their login credentials through a fraudulent website while recording their

input. Malware such as keyloggers use unauthorized software which is installed on the user's computer to capture keyboard entries containing password information.

## 2.2 Text/PIN Passwords

Authentication is dominated by text passwords. They are easy and inexpensive to implement on multiple platforms, are familiar to essentially all users, they do not require users to carry additional hardware such as physical tokens [5], and can theoretically have a reasonably sized password space [20]. Text passwords also contain numerous drawbacks including: users often choose insecure passwords [1, 19], secure passwords are hard to remember [61], and users reuse passwords for multiple accounts [2]. Using a standard physical keyboard to enter a text password provides a comfortable experience. However, there has been a dynamic shift towards an increased number of touchscreen devices with virtual onscreen keyboards [3, 25, 44]. Studies show that users generally perform better in text input using a physical keyboard than a virtual keyboard [22, 47, 50, 62]. PIN passwords are a subset of text passwords and therefore have smaller password spaces. PINs are also susceptible to all weaknesses of text passwords [36].

## 2.3 Graphical Passwords

A graphical password is a secret that is entered or displayed in the form of drawings, icons or graphics [5]. Graphical passwords are proposed alternatives to text passwords that have good security and usability properties. These passwords provide various advantages. They are more memorable than text passwords, harder to write down or share, and resistant to password reuse [10]. Touchscreen and mobile devices are also graphically orientated and therefore are more suitable for graphical input rather than text input. Attacks on graphical passwords must be scheme specific because of variation between graphical password schemes.

Graphical passwords claim to leverage the picture superiority effect [42]. The picture superiority effect proposes that people have better memory for images than words. However, numerous tests have challenged this concept. Nelson, Reed and

| Category | Authentication Procedure | Examples |
|---|---|---|
| Recall | Users are asked to reproduce a drawing on a grid | Draw-A-Secret [26], Pass-GO [54] |
| Recognition | Users are asked to identify & recognize a set of objects | Passfaces [43], Deja Vu [14] |
| Cued-recall | Users are asked to select a sequences of points on a image | Passpoints [59] |

Table 2.3: Types of Graphical Password Schemes

Walling found that the effect is diminished when schematically similar pictures are shown [17]. Nelson, Reed and McEvoy showed that the effect can be eliminated by a rapid image presentation rate [16]. Another explanation for the picture superiority effect is that images have implicit properties that make them more memorable. The sensory-semantic model proposed by Nelson, Reed and McEvoy showed that images are accompanied by more distinct sensory codes which allows them to be more easily accessed [16].

### 2.3.1 Types of Graphical Passwords

Graphical password schemes can be classified into three categories based on the password's required memory retrieval technique [13]. Surveys of graphical password schemes structure these categories as recall, recognition, and cued-recall [5, 46]. Recall-based passwords have to be recalled by the user without any cues or hints. Recognition-based passwords involve recognizing the correct password from a set of distractors. Cued-recall-based passwords also require recall memory but provide users with cues and hints of the password. Table 2.3 outlines each category with its authentication procedure and a few distinguished examples.

#### Recall-Based Graphical Passwords

Generally, authentication in recall-based password schemes is executed by users drawing a secret image on a grid [5]. Draw-A-Secret (DAS) is one of the earliest recall-based graphical password schemes [26]. In DAS, the user draws a secret picture on a blank grid (figure 2.1). The grid squares in DAS are identified by a unique set

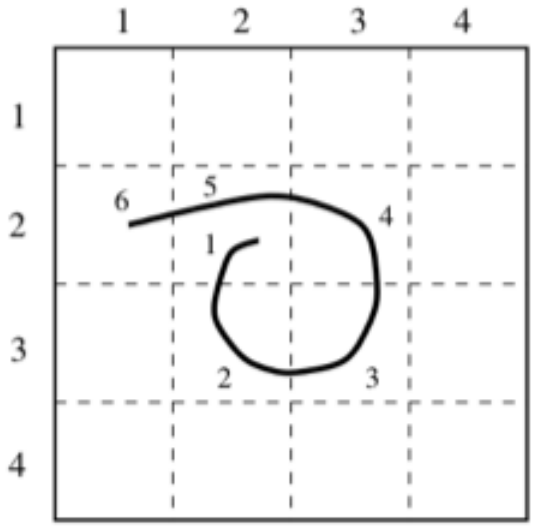



Figure 2.1: Draw-A-Secret Password Example [26]

of coordinates. To successfully login, the user is asked to reproduce the drawing on the grid by going through the same grid squares in exactly same order. In addition, the user has to make sure that the strokes must begin and end in the correct grid squares. One of the drawbacks of DAS is that users tend to draw their passwords in predictable patterns [41]. Pass-Go is another example of a recall-based graphical scheme that was proposed by Tao and Adams in 2008 [54]. Pass-Go is similar to DAS since the user draws a figure on a grid. Pass-Go's differentiation is that the user draws their password by connecting the intersections of the grid lines. Figure 2.2 shows Pass-Go's interface with an example password. The Android operating system developed by Google Inc. uses a graphical password to unlock touchscreen devices (figure 2.3). This Android pattern unlock scheme contains nine points arranged in a 3 by 3 grid. To set a password, the user must choose at least four points, choose no points, use only straight line paths, and not jump over previously selected points [56].

**Recognition-Based Graphical Passwords**

Usually, recognition based graphical passwords require users to choose secret images from a set of distractor images. Passfaces is an example of a commercial recognition-based scheme [43]. In Passfaces, the user selects, or has assigned, face

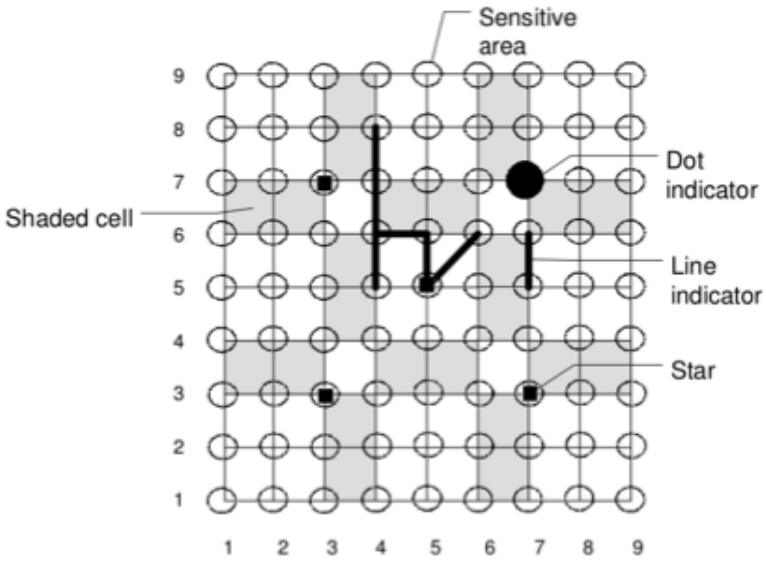



Figure 2.2: Pass-Go Password Example [54]

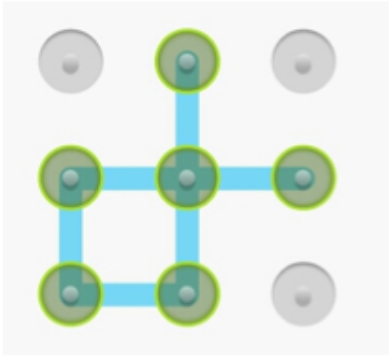


Figure 2.3: Android Pattern Unlock Interface [56]

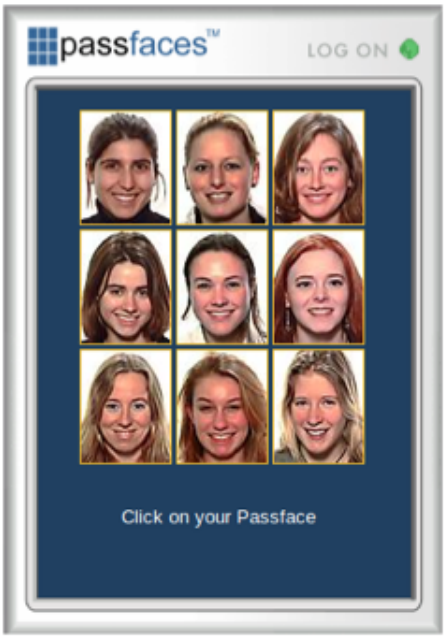



Figure 2.4: Passfaces Interface [43]

images that make up their password. In order to successfully login, they are asked to choose previously selected face images from a grid of distractor faces. For each login, the placement of the faces are shuffled but the distractor faces always remain the same. Deja Vu is another recognition based graphical password scheme that uses a set of random art images to authenticate users [14]. To successfully login, users must select five pre-defined images from a panel of 25 random art patterns (figure 2.5).

### Cued-Recall Based Graphical Passwords

PassPoints is an example of a cued-recall based graphical password [59]. In PassPoints, users select five points from any single image as their password. The scheme also has acceptable tolerance areas for these selected points since users may be unable to re-select the exact pixel point during login. Figure 2.6 shows an example of a PassPoints password with rectangles representing tolerance areas. One major issue that PassPoints encounters is the hot-spot problem [15, 55]. A hot-spot is an area or selection of areas on a image which users select more frequently as their password.

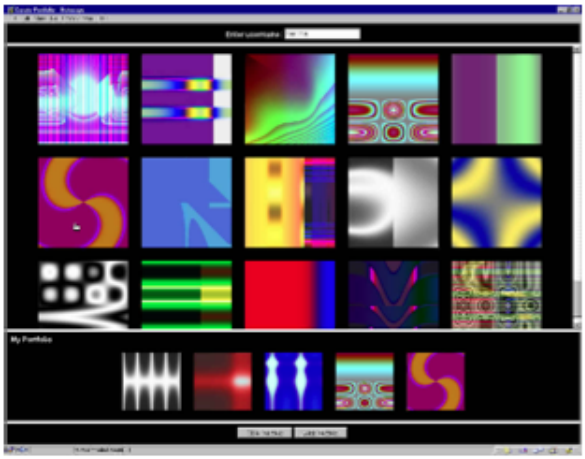


Figure 2.5: Deja Vu Interface [14]

Studies conducted by Thorpe and van Oorschot showed that hot-spots occur on images used cued-recall schemes [55]. Figure 2.7 shows an example these hot-spots on an image of cars used in PassPoints. Hot-spots can increase the vulnerability of a system because they can be used to create dictionaries for dictionary attacks [55].

Cued Click Points (CCP) was proposed by Chiasson et al. in 2007 [11] in order to reduce dictionary attacks. CCP provides more security compared to PassPoints by utilizing a series of images rather than just one image for a password. During the CCP password creation mode, the coordinates of the click events determine the next displayed image. If an incorrect point was selected when reentering the password, an image different from the original password was displayed. Figure 2.8 illustrates an example of CPP's unique image selection process.

Another scheme called Persuasive Cued Click-Points (PCCP) [9], was later proposed to eliminate the hot-spots problem on each image. PCCP removed the hot-spot problem by encouraging users to randomly select their passwords points. PCCP was able to achieve this by using a viewport. As seen in figure 2.9, a viewport is a randomly selected and highlighted area on each image during the password creation mode. Users can only select password points within these highlighted areas. This reduces the chances of hot-spots. If users are unable to find a suitable password point within the viewport, the scheme can shuffle the viewport to another randomly

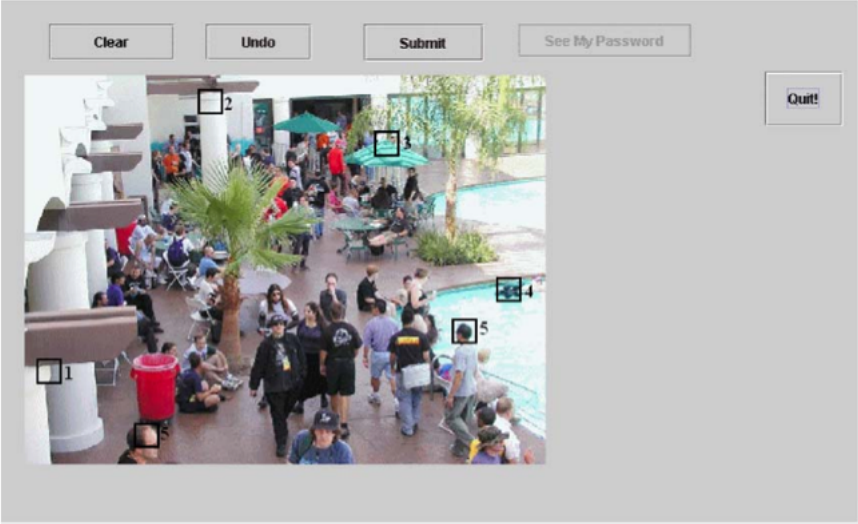



Figure 2.6: PassPoints Interface [59]

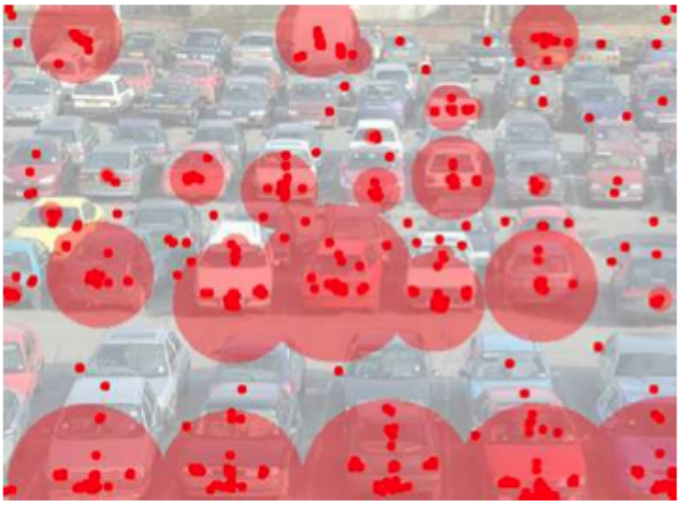


Figure 2.7: Hot-spots of an image used in PassPoints [55]

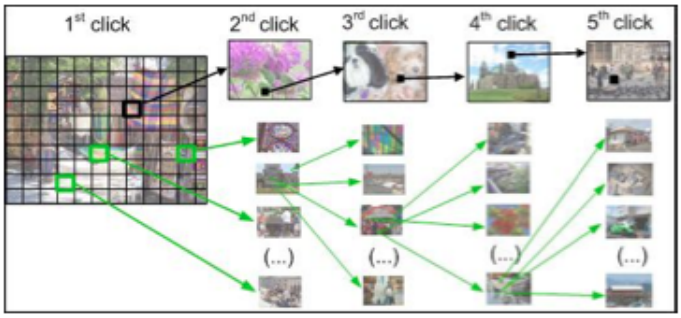



Figure 2.8: Cued Click Points Image Selection Example [11]


Figure 2.9: PCCP Viewport Example [9]

selected area on the image. All of these factors result in more PCCP passwords than CCP passwords falling outside of the predicted hot-spots [9].

## 2.4 Multi-Touch Gesture Authentication

The origins of multi-touch interaction can be traced back to the early 80s, to Mehta's flexible machine interface [49], and Nakatani and Rorlich's soft machines [38]. Since then, multi-touch interaction has evolved significantly, mostly in terms of the hardware supporting multi-touch devices.

The growing popularity of touchscreen devices have also introduced the possibility and importance of multi-touch gesture authentication interactions [23, 28, 32]. Multi-touch interactions allow the user to directly manipulate the interface simultaneously with multiple fingers, which often leads to an intuitive, expressive and dynamic user experience [23, 32]. Generally, when people communicate and express themselves, they can use multiple hands and fingers to help convey their thoughts and ideas. If a similar concept is applied to communicating and interacting with touchscreen devices, then multi-touch should help facilitate an improved overall user experience. Buxton states that multi-touch greatly expands the types of gestures that we can use [6]. He also states that the current interaction with computers is like eating Chinese food with only one chopstick or trying to hug someone with only one fingertip [6]. Basically, multi-touch has presented an opportunity to enhance the overall user interaction experience.

Multi-touch can also be faster than mouse interactions. A study was conducted that compared the interactions of multi-touch to physical and mouse interactions [40]. The tasks involved sorting or organizing coloured circular chips into groups. The results showed that multi-touch interaction was faster than the mouse but slower than the physical interaction [40]. Another study compared differences in performing select and drag tasks for unimanual and bimanual tasks [21]. The unimanual task comparison was done using a single touch and a single mouse whereas the bimanual task comparison was done using two mice and two fingers. The results shows that users may be better off using a mouse for unimanual input and their fingers for bimanual input when working on a large horizontal display.

Most graphical passwords on touch screen devices require some form of simple gestures such as tapping or dragging. One of the most popular gesture authentication schemes is the Windows 8 Picture Password. Picture Password is a permutation of the DAS (see section 2.3.1) login scheme [29]. To setup, Picture Password requires users to choose a picture and a set of three single touch gestures (circles, straight lines or taps) to trace on the picture [34]. To confirm a password and to login, users have to reenter the same the size, position, direction and order of each gesture on the selected picture. Although a very simple and straight forward scheme, one major

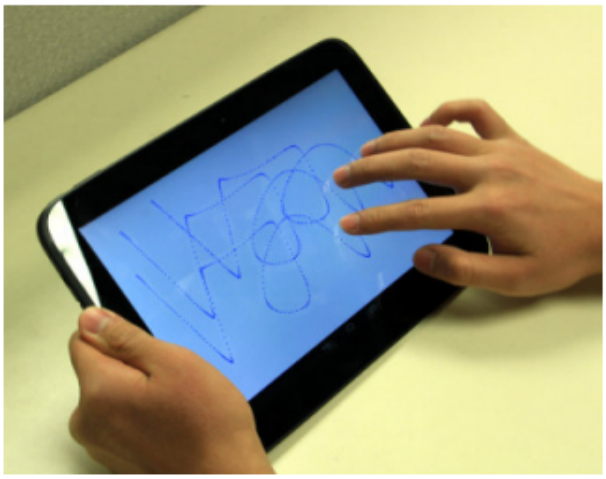


Figure 2.10: Free-Form MultiTouch Gesture Authentication Scheme [51]

drawback is that users may choose simple background pictures that might contain focal points (or hotspots) that naturally suggest certain gestures [18, 29].

Recently, a study of 63 participants on free-form multi-touch gestures for touch-screen devices showed that roughly half of the participants decided to generate one finger gestures and the other half generated multi-finger gestures [51]. The free-form multi-touch gestures allowed all fingers to draw a trajectory on a black screen with no grid or other template (figure 2.10). Their results also suggested that brief gestures can have high security, complex gestures are more difficult to reproduce precisely, and no visual cues could help reduce shoulder-surfing attacks [51]. Another study on the gesture authentication suggested that adding tap gestures could also reduce shoulder-surfing attacks and prevent attackers from emulating gestures [39]. Another study that analyzed the use of five-finger gestures suggested that the user ratings of a desirable gesture characteristic (ease, pleasure, excitement) correlated with gestural security, in contrast to typical text based passwords [48].

Touchscreen devices and multi-touch interaction do facilitate use of some graphical password schemes. We are not aware however, of any password schemes that have been specifically created to leverage multiple simultaneous pointing to move objects to enter a password in a predefined order.

## 2.5 Summary

In this chapter we discussed authentication, password spaces, threat models, text passwords, various types of graphical passwords and multi-touch interactions. We found that graphical passwords are more suitable than text passwords for touchscreen devices for various reasons. Graphical passwords are more memorable than text passwords, typing text on touchscreens is difficult, graphical passwords are hard to write down or share and are more resistant to password reuse. In addition, touchscreen devices are graphically orientated and usually do not contain a keyboard with physical keys. Multi-touch may also be a faster and more expressive form of input. Therefore, we decided to create a multi-touch graphical password scheme and conduct a preliminary study to outline its potential usability features. In the next chapter, we discuss our preliminary experiment and findings.

# Chapter 3

# Preliminary Study: Passgrid

## 3.1 Objective

This study analyzes the potential usability of a new multi-touch graphical password scheme called Passgrid. Passgrid was compared to a traditional text password scheme in order to examine the overall user experience and to determine the capability of the graphical password scheme. Other factors that were comparatively analyzed included login time, an exploratory analysis of the effect of screen size and the level of user acceptance. The study attempts to answer whether a multi-touch graphical password scheme can be utilized as a viable alternative password system to a traditional text password scheme on touchscreen devices.

## 3.2 Passgrid Authentication Scheme

### 3.2.1 Rationale

Passgrid was created with multi-touch capabilities which allows for multiple simultaneous points of interaction. These multiple points of interaction should provide quicker and more efficient login experiences. Generally, when using a standard keyboard only one character can be entered at a time. Passgrid simultaneously recognizes multiple fingers through touch and records the movements of these touches. These touches can also originate from fingers on both hands which should further quicken login time and improve the overall user experience.

### 3.2.2 Design

We designed a cued recall scheme where users organize image tiles according to a pre-assigned order. The design took several aspects into consideration. Firstly, we wanted to incorporate images to gain the benefits from graphical passwords. These

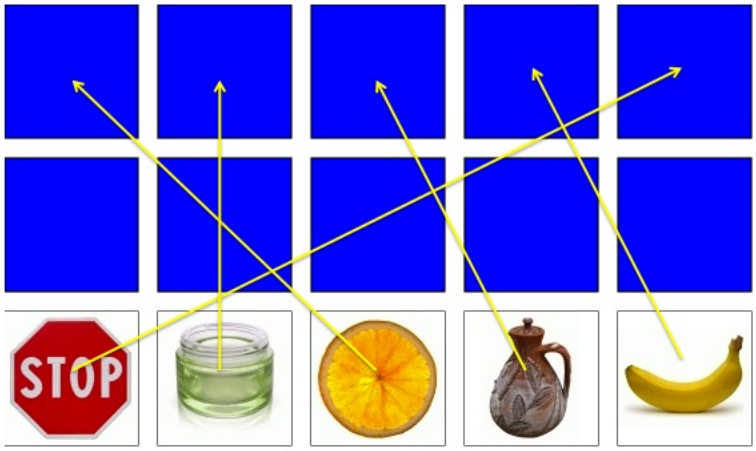



Figure 3.1: Passgrid Scheme (The user must drag the images from the bottom to the top in a predefined arrangement as shown by the arrows. The arrows are for illustrative purposes only and do not appear in the real system.)

images could be moved simultaneously using simple dragging gestures from multiple fingers. It was also important to create relatively large objects to make them easier to target with fingers. Secondly, we wanted to take advantage of multi-touch capabilities by allowing user to choose single or multi-touch as preferred. We also wanted to completely eliminate the need for typing. Lastly, we wanted the system to assign passwords in order to reduce the risk of guessing attacks.

Passgrid interface consisted of a 3 x 5 grid, in which images appear on the bottom row in a shuffled order. To login, users must move the images to the top row, placing them in the correct order as memorized when the password was assigned. Images are moved by dragging them with a finger. Multiple images can be dragged at once if multiple fingers are used. Figure 3.1 illustrates how the scheme works.

## 3.3 Study

### 3.3.1 Participants

This experiment was approved by the Carleton University Research Ethics Board and its ethics clearance form can be found in Appendix G. This preliminary study was carried out in a 45-minute session in a lab environment for each participant. The study consisted of 17 participants who were recruited from the Carleton University community by posters and word of mouth. There were 8 female and 9 male participants with an average age of 23 years. 8 participants were studying at the undergraduate level, 6 were studying at a Masters level and 3 participants choose not to respond. All participants either owned or were familiar with touchscreen display devices and text passwords.

### 3.3.2 Apparatus

The apparatus used in the study included a 7-inch Nexus 7 Tablet and 46 inch SONY large screen display with PQ Labs multi-touch capability [45]. The large screen display was driven using a PQ Labs iStick A200 also running the Android system. We choose these devices because we wanted to analyze if users would prefer interacting with Passgrid on a larger or smaller touchscreen device. These represent the two major classes of touchscreen devices, mobile and collaborative surfaces. Each participant tested the text and Passgrid passwords on both devices. The method of input for the text scheme was a touchscreen Android keyboard (figure 3.2). The method of input for Passgrid involved single or multi-touch dragging motions. All questionnaires in the study were administered online using LimeSurvey software [31] on the Linux server in our lab.

### 3.3.3 Text Password Scheme

A text based password scheme was created to mimic a simple and traditional text password scheme to serve as a comparative control variable in our experiment. We decided to use a text password scheme because we wanted to compare Passgrid's interaction to something that participants already use or would at least find familiar.

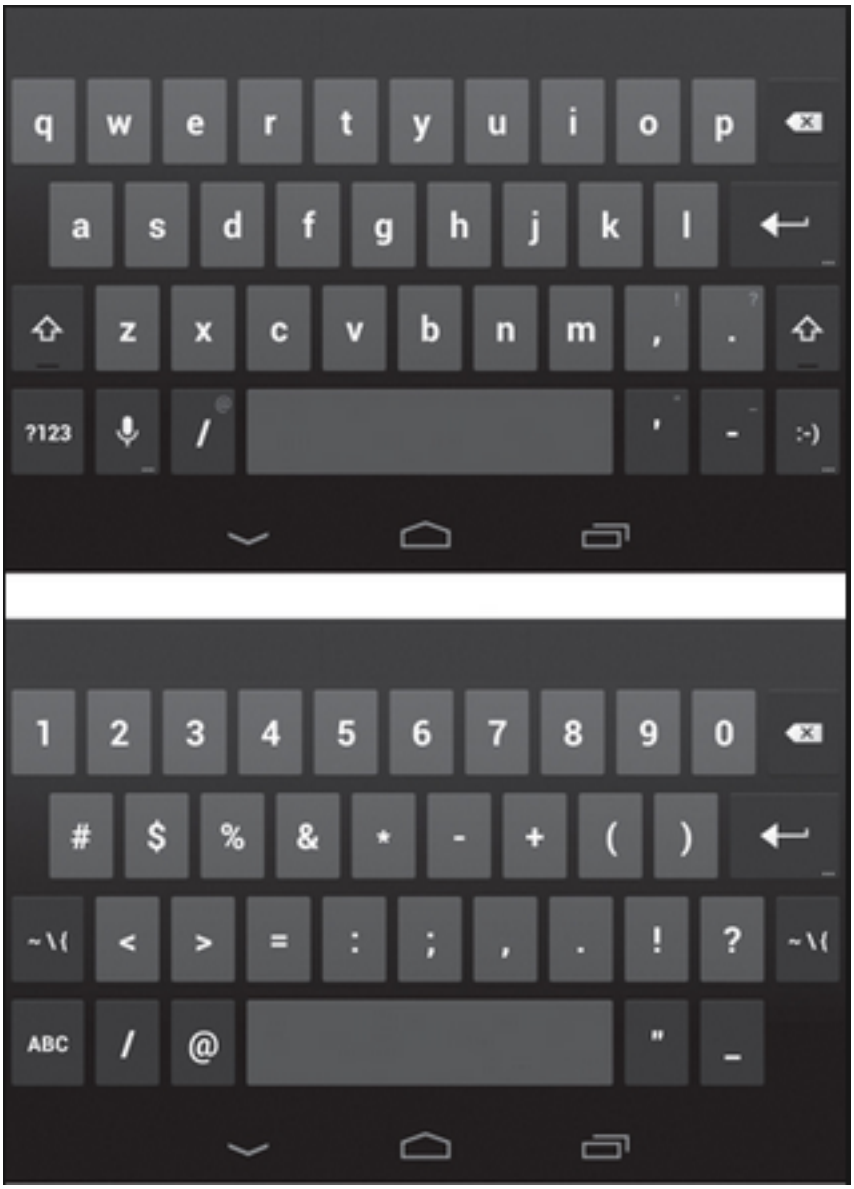



Figure 3.2: Android Keyboard used for the Text Password Scheme


Figure 3.3: MVP Password Trainer

This text password scheme was deployed as a part of the existing MVP framework [8].

The MVP framework is a web based custom system specifically designed for conducting research studies of authentication schemes [8]. The MVP framework uses server side PHP scripting and Javascript and serves as a platform for running user studies of different password systems on the same websites [8]. MVP also logs data about each user study for further detailed analysis. MVP features a training component where users can learn to use new password systems by creating new passwords and practicing password entry [8]. The MVP trainer (figure 3.3) utilized for this experiment had three main control buttons to create, re-enter, and check passwords.

The text passwords in this study had the following parameters. Each password consisted of 6 lowercase alphabetic characters which were randomly generated and assigned. This created a theoretical password space of $26^6 = 308{,}915{,}776$ or approximately 28 bits.

**Text Create Mode** The create button generated a window (figure 3.4) that contained a randomly assigned password, a box to practice and test the password and an accept password button. There was no limit to the number of times a participant could practice their password.

**Text Re-enter & Check Mode** The re-enter button generated a window (figure

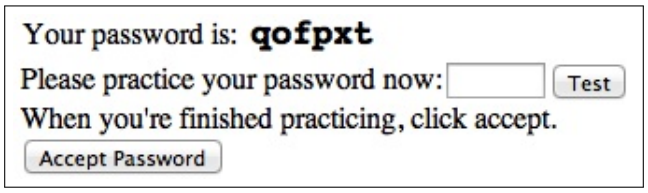



Figure 3.4: MVP Trainer Text Password Create Window

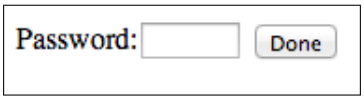



Figure 3.5: MVP Trainer Text Password Re-enter Window

3.5) that allowed participants to re-enter their password. In order to successfully login, participants had to correctly enter the predefined 6 character text password. Lastly, participants could check if they entered their passwords correctly by selecting the check button. Figure 3.6 shows the outcome of the check button after a successful login.

### 3.3.4 Passgrid

Passgrid was written in JavaScript using the Raphael library [4]. Coding in JavaScript and using the Raphael library allowed the program to run in all major browsers and gave the program the ability to recognize multiple fingers. As seen in figure 3.8, Passgrid's user interface consisted of a grid of squares including 5 columns and 3 rows with images in the last row. The images used for Passgrid came from an MVP folder

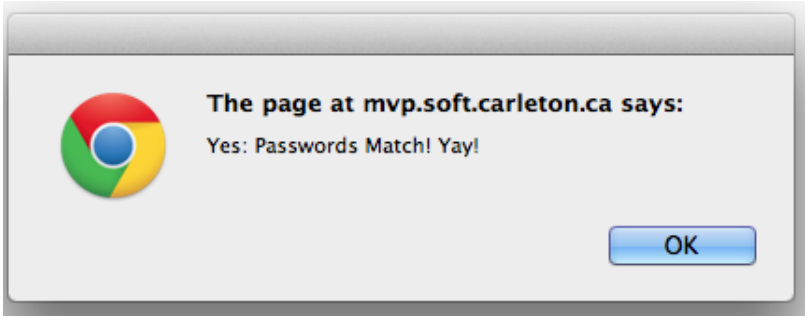



Figure 3.6: MVP Trainer Successful Match

containing random images of objects obtained from a repository used in an earlier study [24]. The original images were chosen from the stock.xchange website [53] for their distinctiveness and were used in accordance with the published terms and conditions. Each time a password was created or assigned, a new set of five images were randomly selected and displayed in a randomly generated order. To login, users had reorganize shuffled images into this assigned order. User could perform this action by using multi-touch gestures. The Passgrid scheme was deployed as one of the MVP plugins, and was written as a PHP generated Javascript web application, adapted from the PassTiles scheme developed by Stobert and Biddle [52]. The code is about 100 lines of PHP, and about 200 lines of Javascript. The PHP code runs on the server, and generates Javascript code that runs in the web browser. While participants were learning how to use Passgrid, they were explained that the middle row of squares was for illustrative purposes only. The middle row can also be used as a reference of how much space there is between the top and bottom rows. Alternatively, the space could have been replaced with a rectangle or could have been left blank. All participants clearly understood this layout.

Passgrid's theoretical password space was $5! = 120$ or 7 bits. Ideally we would want to keep the same theoretical password space for both schemes. However, since this was a preliminary study, we chose to compare it with a traditional text password. Our main focus was to investigate how users reacted to the multi-touch properties of Passgrid.

**Passgrid Create Mode** During Passgrid's create mode, the squares on the top and bottom rows of the grid contained identical images that were arranged in a different order (figure 3.7). The placement of the images on the top row represented the randomly assigned generated password. In order to accept a password, participants had to move and match the images from the bottom row to the top row.

**Passgrid Re-enter & Check Mode** In order to successfully log in during the re-enter mode, participants had to rearrange shuffled images on the bottom row by dragging them to the top in the predefined order set during the creation mode


Figure 3.7: MVP Trainer Passgrid Create Mode

(figure 3.8). During this phase, the top row was empty. Users had to remember the order on their own.

### 3.3.5 Materials

The materials used in the study included a consent form (Appendix A) and a questionnaire (Appendix B). The consent form contained: a brief explanation of the study, contact information, a summary of the task requirements, information about data anonymization and an explanation of the withdrawal policy. The questionnaire contained two major parts. Part 1 of the questionnaire contained questions regarding participant demographics and a series of questions regarding the text password scheme. Part 2 of the questionnaire contained questions regarding Passgrid and other usability questions. These two sections were completed at different times depending on a participant's testing order (see section 3.3.7). After a participant completed using a scheme on both devices, they would complete the corresponding questionnaire section for that scheme. Some of the questionnaire questions were repeated for each

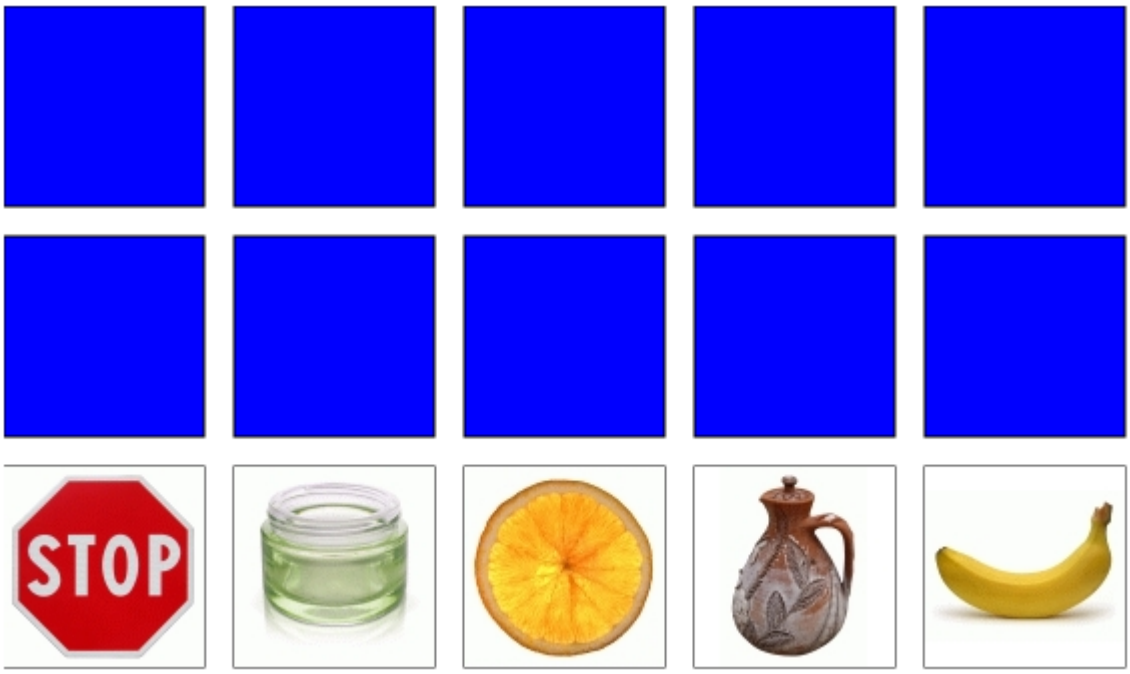



Figure 3.8: Passgrid Re-enter Mode

scheme in order to compare the two password schemes. While participants interacted with Passgrid, we also recorded which fingers were used, what type of selection method (single touch or multi-touch) and what type of movements (single drag or multi-drag) they were utilizing. Appendix C shows the form used by the experimenter to input this data for each participant.

### 3.3.6 Acceptance Model (TAM)

In order to compare Passgrid and the text password scheme, we created questions based on the Technology Acceptance Model (TAM) [12]. TAM attempts to examine and predict the determinants of user acceptance towards a new system. The model proposes that the success and actual use of a system depends on four components including: perceived usefulness (PU), perceived ease of use (PEOU), attitude towards using (A) and behavioral intention to use (BI) [35]. Figure 3.9 illustrates the TAM with its structural components. Perceived usefulness (PU) is an individual's perception that using a system will enhance job or task performance. Perceived ease of use

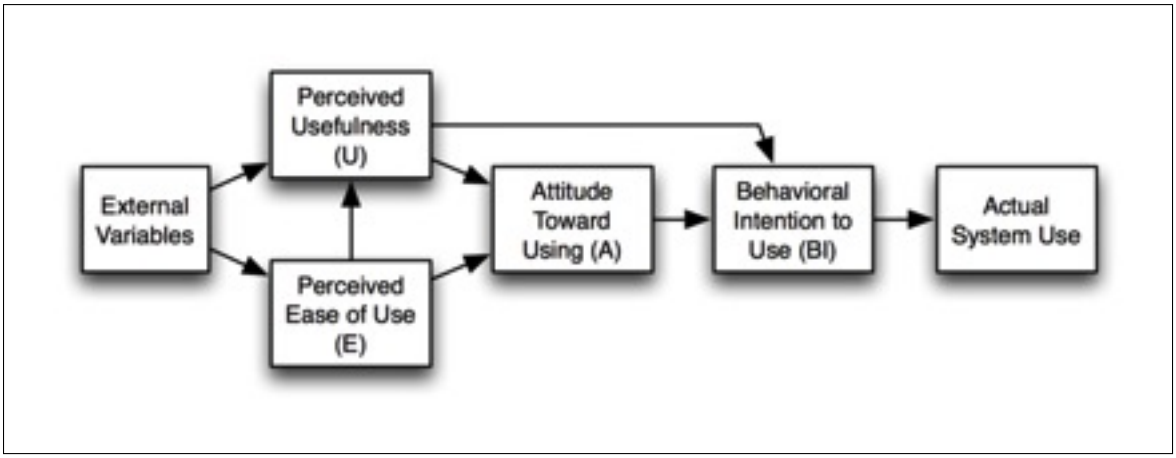



Figure 3.9: Technology Acceptance Model (TAM [12])

(PEOU) is an individual's perception that using a technology will be free of effort. Attitude toward usage (A) is a combination of previous two factors and is an individual's evaluative judgment of the system. Lastly, behavioral intention to use (BI) is an individual's motivation or willingness to exert effort to use the system. In order to analyze user acceptance, participants completed twenty Likert scale questions based on the TAM for each password scheme. These questions included five questions for each of the four components of the TAM and are included in Part 1 TAM and Part 2 TAM sections of Appendix B.

### 3.3.7 Procedure

In order to randomize the order of the password schemes and touchscreen devices for each participant, we constructed and used a partial latin square (table 3.1). A traditional latin square is an n-by-n array in which each of n symbols appear exactly once in each row and column and is used to reduce ordering effects in an experiment [30]. The first participant was assigned testing order 1 and each subsequent participant was assigned the next testing order according to table 3.1. This process was iterated as necessary. Each row shuffled presentation order of the password schemes and the order of the devices for the experiment.

The remainder of the experiment was conducted using the following steps:

| Testing Order | Device & Scheme | | | |
|---|---|---|---|---|
| 1 | T-Text | LS-Text | T-Passgrid | LS-Passgrid |
| 2 | LS-Text | T-Text | LS-Passgrid | T-Passgrid |
| 3 | T-Passgrid | LS-Passgrid | T-Text | LS-Text |
| 4 | LS-Passgrid | T-Passgrid | LS-Text | T-Text |

Table 3.1: Latin Square (T=Tablet, LS=Large Screen)

**Step 1** Introduce scheme. Participants were given a brief introduction to the study and were asked to sign an informed consent form.

**Step 2** Learn scheme. Depending on a participant's assigned testing order, they were given verbal instructions on how to use a specific password scheme. Participants had the opportunity to familiarize themselves with the scheme by practicing it using the MVP Password Trainer (figure 3.3). During the training phase of the experiment, participants were given a practice username and could create, re-enter and check as many passwords as they wanted. Once the participant felt comfortable and understood the scheme's interaction capabilities, they continued to the next stage of the experiment with a dedicated username.

**Step 3** Password Creation & Login. During the password creation phase, participants were assigned randomly generated passwords. Participants confirmed these passwords by entering them into the system. A new password was given for each device and scheme. If they were unable to confirm a password, they were assigned another randomly generated password. Once a participant had successfully logged in on both devices using a password scheme, they were asked to complete the related section of the questionnaire.

**Step 4** The participants were asked to complete steps 2 and 3 for the other password scheme according to their testing order and completed the corresponding sections of the questionnaire.

**Step 5** Lastly, each participant was thanked and compensated $10 for their time.

### 3.4 Hypotheses

We had a $2 \times 2$ study design which included two password systems (Text and Passgrid) and two screen sizes (tablet and large screen display). Our dependent measures were login time and the four measures based on the TAM (Perceived Usefulness, Perceived Ease of Use, Attitude Towards Using, Behavioral Intention to use). Our H1 hypotheses related to login time and H2 hypotheses focused on the TAM.

**H1(a)** Login time for Passgrid on the tablet will be faster than the login time for text passwords on the tablet.

**H1(b)** Login time for Passgrid on the large screen will be faster than the login time for text passwords on the large screen.

**H2(a)** Perceived usefulness (PU) will be higher for Passgrid than for the text passwords.

**H2(b)** Perceived ease of Use (PEOU) will be higher for Passgrid than for the text passwords.

**H2(c)** Attitude towards Using (A) will be higher for Passgrid than for the text passwords.

**H2(d)** Behavioral intention to use (BI) will be higher for Passgrid than for the text passwords.

**H3(a)** Users will use two hands and multiple fingers to enter their passwords.

### 3.5 Analysis Plan

We used statistical analysis to determine significant differences between conditions. To test H1(a) and H1(b), we conducted Wilcoxon signed rank tests because it is a non-parametric statistical test used when comparing two related samples to assess whether their population mean ranks differ when the population cannot be assumed to be normally distributed. See table refskew1, for statistics of skewness and kurtosis of the data distributions. To test H2(a), H2(b), H2(c) and H2(d), we conducted

```
(grd108/limesurvey: warning/N/A) activity, survey, 32726
(grd108/pwdtrainer: passgrid/LargeScreen) enter, SUCCESS, 01234==01234
(grd108/pwdtrainer: passgrid/LargeScreen) enter, moveto, 3=4;0#2013-08-15T16:26:25.983Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, finished, 2013-08-15T16:26:24.075Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, movefrom, 3=2;2#2013-08-15T16:26:22.875Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, moveto, 2=3;0#2013-08-15T16:26:22.360Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, movefrom, 2=1;2#2013-08-15T16:26:21.052Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, moveto, 4=2;0#2013-08-15T16:26:18.519Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, moveto, 1=1;0#2013-08-15T16:26:16.581Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, movefrom, 4=3;2#2013-08-15T16:26:17.319Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, movefrom, 1=0;2#2013-08-15T16:26:15.328Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, moveto, 5=0;0#2013-08-15T16:26:14.250Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, movefrom, 5=4;2#2013-08-15T16:26:12.278Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, passgrid, start
(grd108/pwdtrainer: passgrid/LargeScreen) enter, enter, 2013-08-15T16:26:05.881Z
(grd108/pwdtrainer: passgrid/LargeScreen) enter, ,
(grd108/pwdtrainer: passgrid/LargeScreen) enter, start, Mozilla/5.0 (iPad; CPU OS 5_1 like Mac OS X)
```

Figure 3.10: Gesture Log File Example

paired t-tests. The paired t-test compares two means that are assumed to come from the normal distribution with equal variances where the two samples are assumed to be paired. The paired t-test is a suitable measure to identify significant differences between Passgrid and text password scheme because each participant tried the two password schemes on both devices and then answered the TAM related questions. We choose these statistical tests because we determined the nature and distribution of the data from pilot studies of this experiment. To test H3(a), we will observe how user interact with Passgrid and record results using Appendix C.

All of the raw login time data was collected from the MVP trainer log files and analyzed using RStudio [57]. Each participant's log file contained four sections for each of the conditions in the experiment (each of the components of the testing order). Figure 3.10 is an example of a participant's log file for Passgrid on the large screen display. In this example, the log file shows a record of the participant's username, activity (password trainer or survey), password scheme, device, movement of images (move to or move from) and the time for each movement. Pre-processing of the logs and all of the statistical tests were also conducted in RStudio [57].

| Condition | $V$ | $p$ |
|---|---|---|
| Tablet Text Scheme vs Tablet Passgrid | 7 | 0.0016 |
| Large Screen Text Scheme vs Large Screen Passgrid | 23 | 0.0376 |

Table 3.2: Wilcoxon Signed Rank Test for Login time

| Device | Password Scheme | Mean | SD | Median |
|---|---|---|---|---|
| Tablet | Text | 6.71 | 1.83 | 6.00 |
| Tablet | Passgrid | 9.82 | 4.02 | 9.00 |
| Large Screen | Text | 10.71 | 3.39 | 10.00 |
| Large Screen | Passgrid | 13.76 | 5.64 | 14.00 |

Table 3.3: Descriptive Statistics for Password Login Time (s)

## 3.6 Results and Interpretation

### 3.6.1 Hypothesis 1: Login Time

To investigate H1(a) and H1(b), that login time for Passgrid will be faster than the login time for the text password scheme for both devices, Wilcoxon signed rank tests were conducted. As seen in table 3.2 and figure 3.11, there was a significant difference in the login time between tablet text and tablet Passgrid conditions ($V = 7$, $p < 0.01$). There was also a significant difference in login time between large screen text and large screen Passgrid conditions ($V = 23$, $p = 0.04$).

Table 3.3 shows the average time it took for participants to login. The login time was recorded from the first touch event of their password to the last touch event of their password. The results showed that on average, login took longer on Passgrid than the text password scheme. In addition, the larger the screen size, the longer it took to login. Figure 3.11 contains login time histograms for all four conditions and clearly illustrates these findings.

### 3.6.2 Hypothesis 2: TAM

To investigate H2(a), H2(b), H2(c), H2(d), we examined whether all four components of the TAM were higher for Passgrid. Each participant completed a set of TAM related questions for each password scheme. These question sets included five Likert

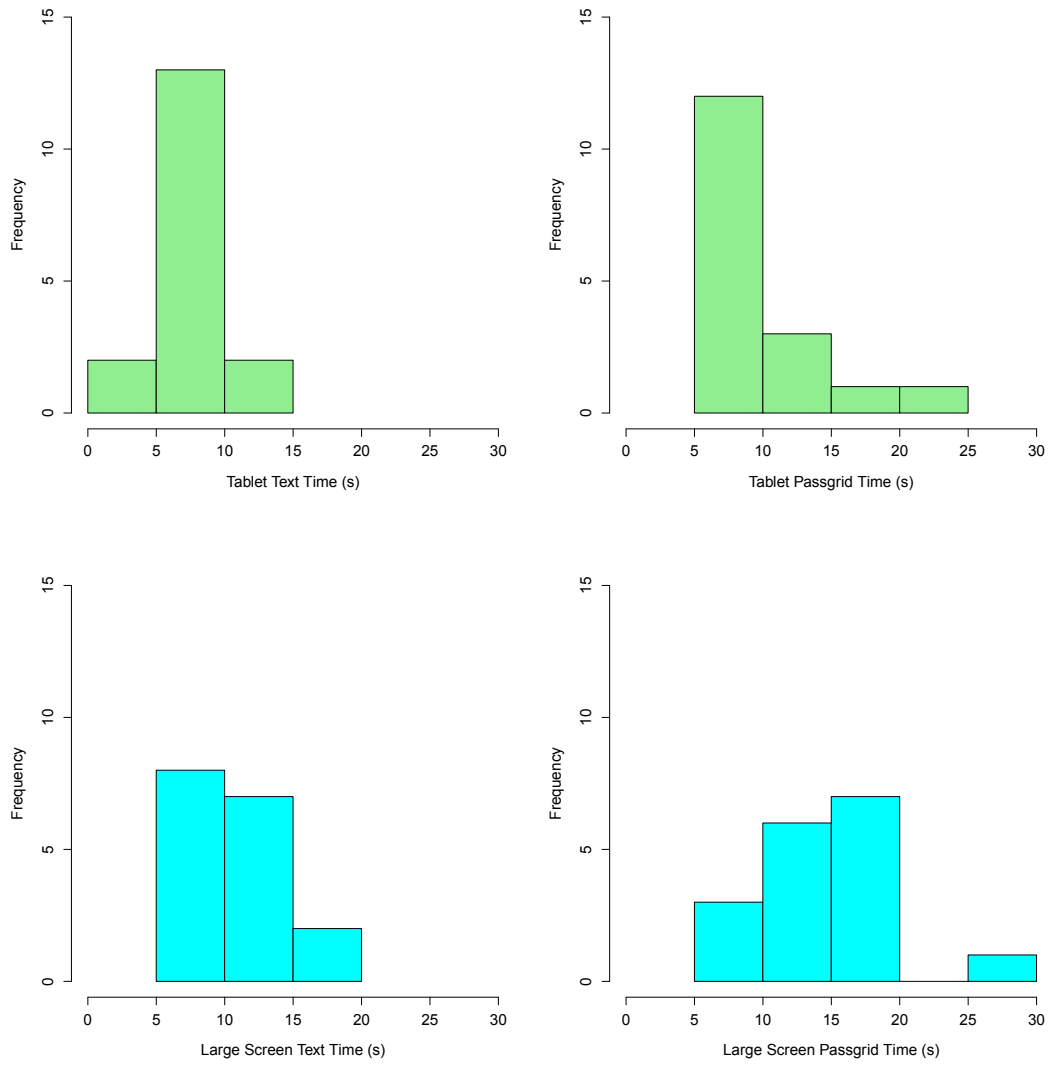



Figure 3.11: Login Time Histograms

| Condition | Skewness | Kurtosis |
|---|---|---|
| Tablet Text | 0.1466 | 0.4924 |
| Tablet Passgrid | 1.7301 | 2.9128 |
| Large Screen Text | 0.8558 | 0.6079 |
| Large Screen Passgrid | 1.0497 | 1.999 |

Table 3.4: Skewness & Kurtosis Results for Hypothesis 1

questions for each of the four component (PU, PEOU, A, BI) of the TAM. In order to test for statistical significance between responses from the two password schemes, we conducted paired t-tests and created histograms to illustrate the data. As seen in table 3.5, the paired t-tests showed that there was a statistical difference between the responses from Attitude Towards Using (A) ($t(16) = -2.133$, $p < 0.05$). We noted that both distributions for the A data were positively skewed so we applied a log transformation to address the skewness and repeated the test; again the result was significant($p = 0.047$). The other three TAM components did not show any statistical significance.

Analysis of TAM results commonly use parametric methods. The questionnaires, however, do use Likert scales for which non-parametric ordinal methods are more appropriate. We therefore, also used Wilcoxon tests to compare each dimension, and the results are shown in table 3.6. As can be seen, the results closely resemble the results of the parametric tests.

Figure 3.12 shows histograms of the Likert scale responses for the TAM related questions. Overall the graphs for the text and Passgrid schemes look very similar but Attitude Towards Using (A), seems to have higher values for the Passgrid. This shows that participants had a favourable attitude towards using Passgrid and a positive outlook towards the new password scheme. Attitude toward using (A) is a very strong factor because it is a combination of perceived usefulness (PU), perceived ease of use (PEOU) and is an individual's evaluative judgment of the system. In relation to Attitude towards Using (A), participants also commented that they found Passgrid to be more enjoyable and entertaining, and they liked the overall idea of using this scheme. Participants also noted that they would be willing to use Passgrid on multiple touchscreen devices.

Other TAM factors including perceived usefulness (PU), perceived ease of use (PEOU), and behavioural intention to use (BI) did not show statistical significance. This can be a result of multiple factors. Some possible reasons for lack of significance from the other findings is that both the password schemes are useful since they accomplish their specific task, are fast and easy to execute. These factors can have a domino effect on the resulting relatively low rated behavioural intention to use (BI)

| TAM Component | $t$ | $df$ | $p$ |
|---|---|---|---|
| Perceived Usefulness (PU) | -0.1932 | 16 | 0.8492 |
| Perceived Ease of Use (PEOU) | -1.2572 | 16 | 0.2267 |
| Attitude Towards Using (A) | -2.1325 | 16 | 0.0488 |
| Behavioral Intention to Use (BI) | 0.8638 | 16 | 0.4004 |

Table 3.5: T-Test for TAM

| TAM Component | $V$ | $p$ |
|---|---|---|
| Perceived Usefulness (PU) | 73.5 | 0.9057 |
| Perceived Ease of Use (PEOU) | 41.5 | 0.3060 |
| Attitude Towards Using (A) | 38 | 0.0720 |
| Behavioral Intention to Use (BI) | 93 | 0.4487 |

Table 3.6: Wilcoxon Signed Rank Test for TAM

and therefore could be a reason why there was also no significant differences in this category.

### 3.6.3 Hypothesis 3: Use of two hands and multiple fingers

Our results showed that participants mainly used one or both their index fingers to interact with Passgrid. We were very surprised because we had speculated that the ability of multiple fingers would have been attractive to users. However, in all of our 17 participants using each of our two devices, we saw this at most twice. Participants may have not used multiple fingers because when arranging the shuffled images, the random path of the images may have caused their fingers to collide. This could have resulted in participants moving one image at a time.

### 3.6.4 Exploratory Analysis: Questionnaire Responses

The questionnaire of this experiment contained several usability questions in order to identify patterns and understand how individuals interact with passwords. We first explore where users typically enter passwords. Figure 3.13 shows the type of devices that participants have a password on. The results showed that participants utilize passwords on multiple devices. We see that most users are used to entering passwords on laptops and mobile phones, but only a few report using them on tablets

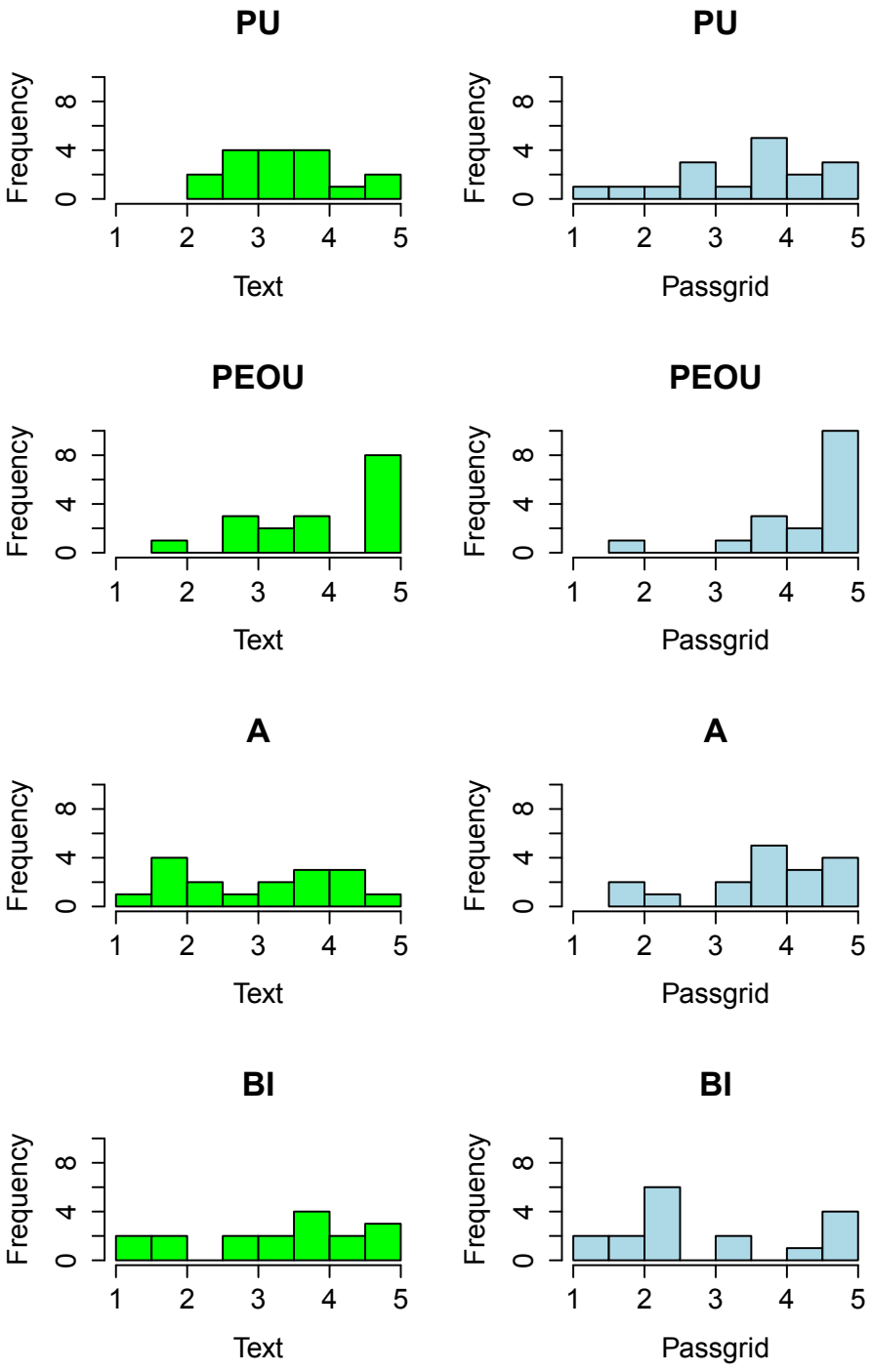



Figure 3.12: Histograms for TAM Responses (1=Most Negative, 5= Most Positive)

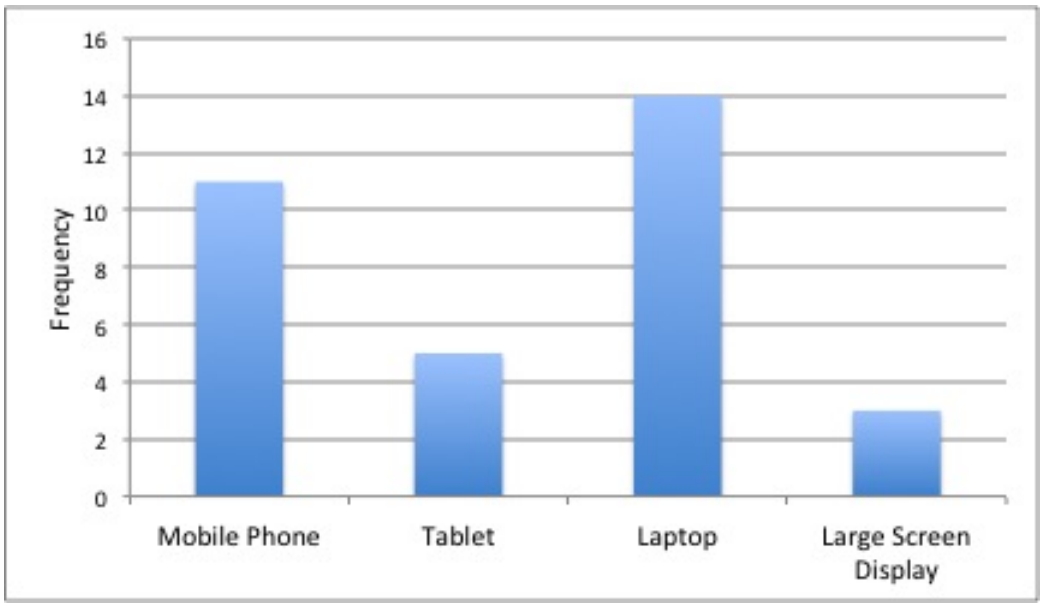



Figure 3.13: User Responses to *Do you currently use a password on a. . . ?*

or large screens. Another question (figure 3.14) showed that all participants use text passwords. Some participants had experience with graphical passwords and biometrics. Experience with graphical passwords likely comes from mobile phone screen unlock mechanisms. No one mentioned use of tokens or voice authentication.

Figure 3.15 shows user responses to *How often do you enter a password on a touchscreen device?* 9 participants said that they enter a password on a touchscreen more than 12 times day. 2 participants said that they performed this interaction between 10-12 times per day and another 2 participants said that they performed this interaction between 1-3 times per day. 4 participants said that they never performed this action. These participants stated that they do not interact with touchscreen devices on a daily basis.

Another questionnaire response showed that the participants thought the three most important aspects of a password scheme were login speed, memorability, and ease of entry. It is not surprising that login speed was the most important factor because of the number of times an individual has to enter a password. Memorability and ease of entry are understandable factors because generally an individual cannot keep the same password for everything and therefore has to remember multiple text

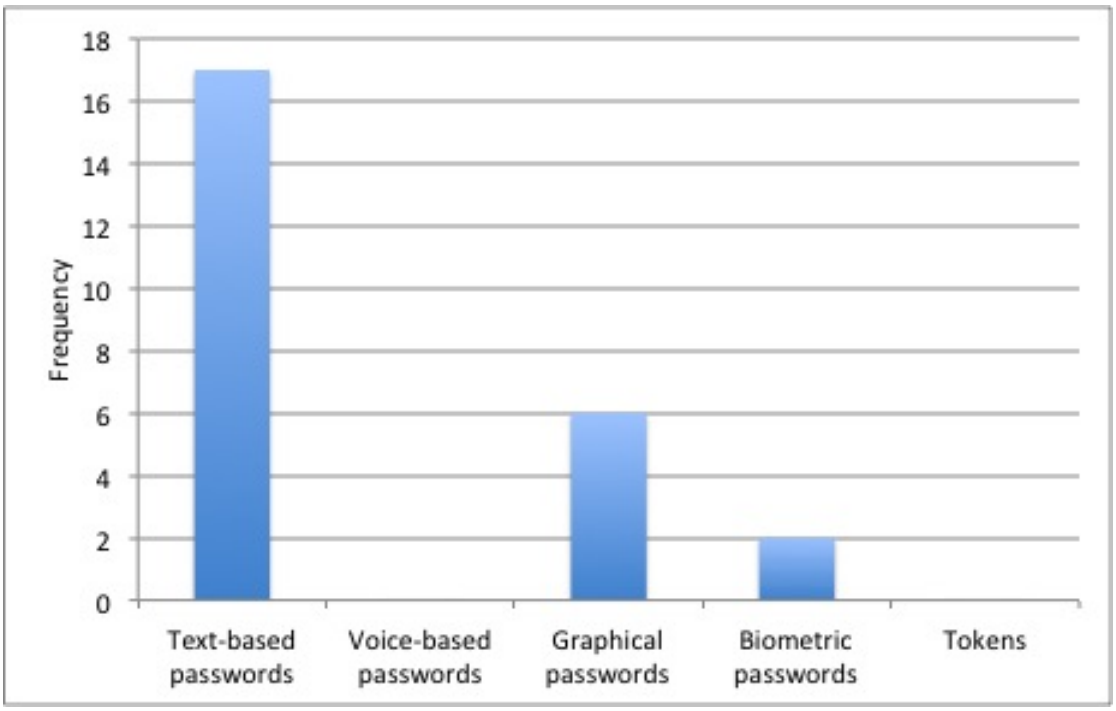



Figure 3.14: User Responses to *What type of passwords do you normally use?*

passwords which can be difficult to remember and enter. The majority of participants also commented that they were unsatisfied with their current password interaction because of issues such as tedious repetition, lack of graphics and creativity.

Figure 3.16 shows user responses to *On which of the following devices would you most likely use a graphical multi-touch password?* This data shows that participants would generally like to use a graphical password scheme on smaller devices such as mobile phones and tablets. Figure 3.17 shows that, overall, participants thought that using a graphical password a tablet would enhance the strength of their passwords. In comparison, a lot of participants indicated that using a graphical password on laptop or large screen display would not enhance password strength. Participants may have prefer tablets to large screen displays because tablets provide more privacy for password entry. There was also a lot of uncertainty whether using a graphical password on a mobile phone would enhance password strength.

Participants were also asked to rank motion gestures including single and multi-touch clicking and dragging in order of preference. The responses showed that single

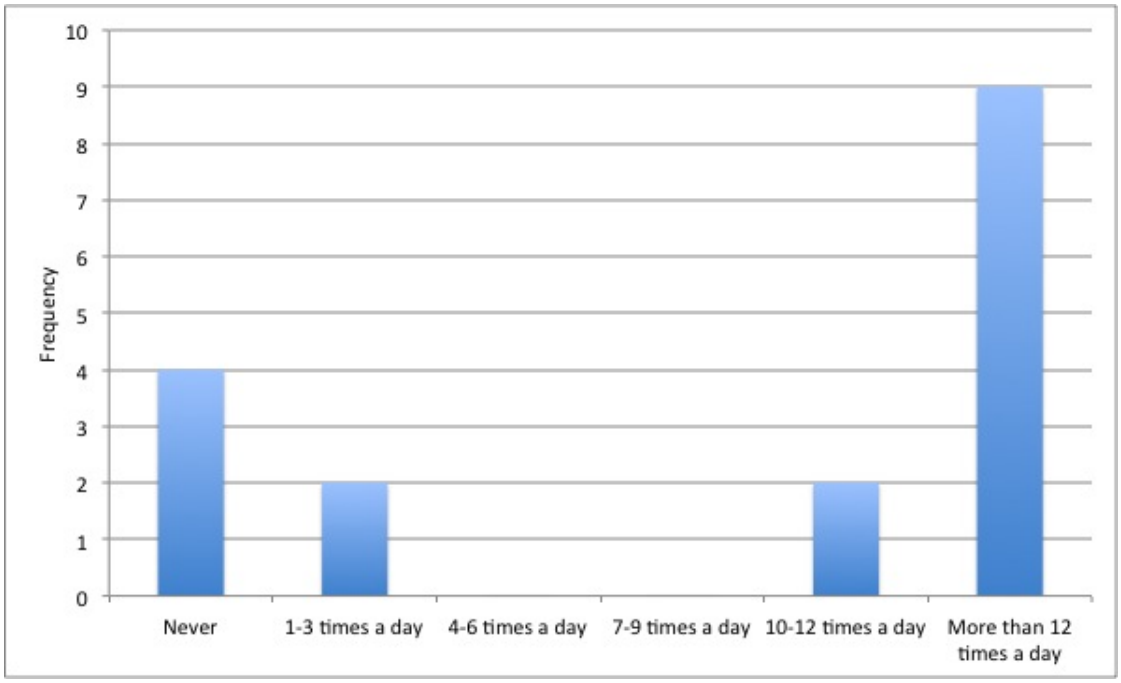



Figure 3.15: User Responses to *How often do you enter a password on a touchscreen device?*

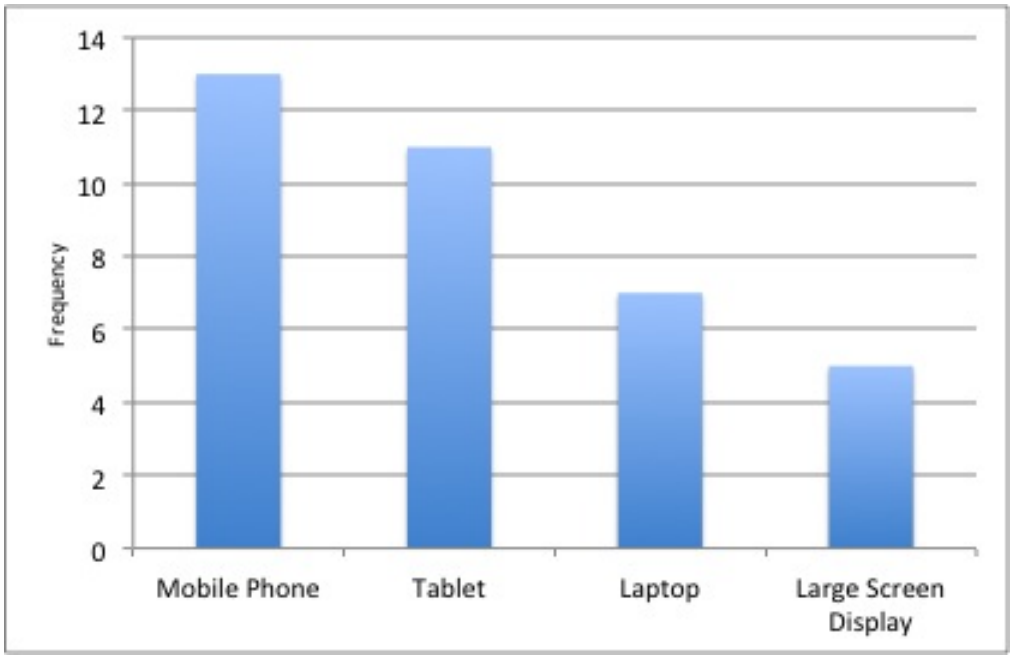



Figure 3.16: User Responses to *On which of the following devices would you most likely use a graphical multi-touch password?*

touch clicking and dragging were preferred over multi-touch clicking and dragging. A majority of participants also noted in the questionnaire that even though Passgrid's images were not engaging, they enjoyed moving the images and finger interaction. All of these exploratory usability findings show that substantial improvements can be made in the password interaction experiences.

## 3.7 Discussion

Addressing our hypotheses, our experiment showed that login took longer on Passgrid than the text password. This is in spite of the Passgrid condition having much lower strength. In addition, login on the large screen took longer than login on the tablet. Participants may have had faster login times for the text passwords because they were familiar with the Android keyboard input method. This familiarity could result in faster key selection for their text passwords. Participants found Passgrid more enjoyable and did not have any major issues with input that took slightly longer. Using multiple fingers allows for more space and more points of interaction. The increased points of interaction should have reduced the average login time. However, participants were reluctant to use multiple fingers and took longer to login. This may have been a result of Passgrid's novelty and with more interaction practice, shorter login times may be achieved. For the tablet, participants generally used one finger (index or middle finger). For the large screen display, participant generally either used one or both index fingers.

The Attitude Towards Using (A) component of TAM showed statistical differences favouring Passgrid. In addition, participants also commented that they would like to use Passgrid for multiple touchscreen devices and described Passgrid as being more intuitive, enjoyable and entertaining. Other exploratory usability questions showed high password usage, frustration with traditional text-based passwords and a positive response to alternative password schemes. Participants also indicated that they would prefer graphical password schemes on tablets rather than large screen displays. This could be because tablets provide a more personal form of interaction than large screen displays and therefore more suitable for graphical passwords. In terms of multi-touch, participants preferred to use fewer fingers on Passgrid. They also felt that using a

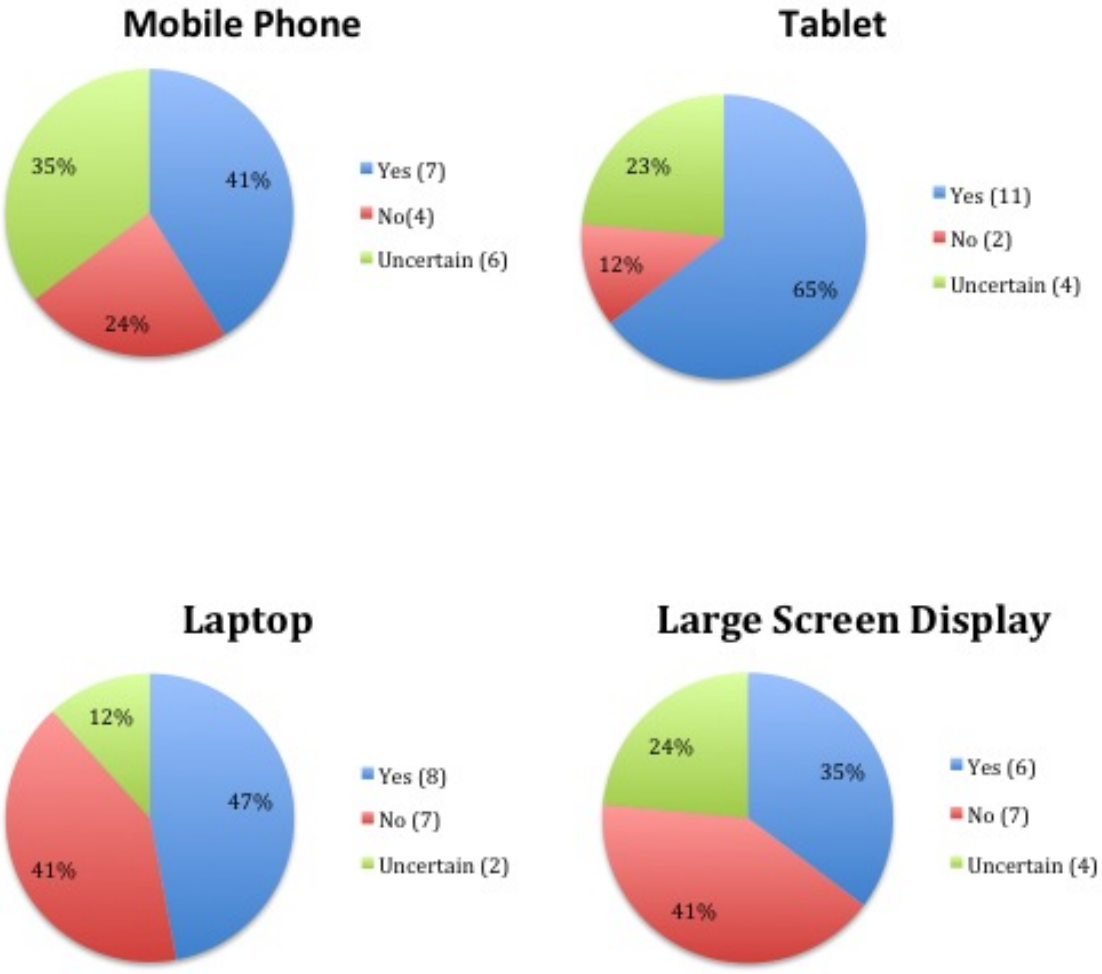



Figure 3.17: User Responses to *Do you think that using a graphical password will enhance the strength of your password on a . . . ?*

graphical password on a tablet might enhance the strength of their passwords.

One major observation we made was that while individuals interacted with Passgrid, the main enjoyment of the scheme did not originate from the graphics of the scheme but from the gesture motions of the graphical password. The graphics of the scheme were fairly plain and included five simple random images on a grid of squares. These images were randomly selected, arranged and set as a password by the system, not by the user. Individuals liked Passgrid because they could move these images. Therefore we decided to focus further research on investigating motion or gesture passwords. To a certain extent, gesture passwords can be considered a subcategory of graphical passwords because any graphical password which requires a motion interaction includes a gesture. These gestures may be simple touch tap selections, touch drag motions or pinching gestures but can provide a completely different interaction experience.

### 3.8 Conclusions Drawn from the Preliminary Study

The objective of this experiment was to analyze Passgrid's user experience compared to a traditional text password, and to analyze if a multi-touch graphical passwords could be utilized as a viable alternative to a traditional text password. Passgrid was designed as a graphical password scheme that allowed multi-touch interactions which might improve the login experience. Our hypotheses were that Passgrid would have faster login times and would score higher in all four TAM components. Our results showed that Passgrid did not have faster login times and only showed statistical significance on one out of the four TAM components. Even though Passgrid had longer login times, participants still commented that Passgrid provided an enjoyable and entertaining experience. This was also further supported by the statistical significance found in the the Attitude Towards Using (A) component of TAM. In terms of multi-touch, participants were hesitant to utilize more than one finger. This directed our attention to the observation we made about participants liking the gesture motion of the graphical password more than the graphical password itself. Therefore we decided to design a gesture based password scheme for our main study.

There were also a few limitations that should be considered for this study. For

example, even though we used a latin square to reduce the ordering effects of the study, participants may still have rated the schemes based on comparisons between the schemes and devices rather than each condition individually. Furthermore, since the experiment was conducted in a controlled lab environment, it did not take into account external factors such as dim-lighting, noise, privacy concerns that may be present while individuals actually enter their password. Another limitation was the difference in theoretical password space of the two password schemes. Since this was a preliminary study investigating Passgrid's interaction, we did not focus on Passgrid's theoretical passwords space. However, in order to create a viable alternative password scheme for our main study we made sure the theoretical password spaces were comparable. All of our findings from our preliminary study were considered while designing the main user study as we describe in the following chapter.

# Chapter 4

# Main Study: Gesture Password

## 4.1 Objective

The objective of this study was to investigate the usability of a new gesture based password scheme on mobile devices. We compared a new gesture scheme called GesturePass to a traditional PIN on a Nexus 4 phone and a Nexus 7 tablet. The main focus was investigating GesturePass and the different devices were chosen for exploratory comparison. We analyzed the number of password practices, login attempts, login times, gesture times, and a range of usability questionnaire responses for each device. As a main study we took extra care in the comparability of conditions and the ecological validity of the study. For example, the password strength in both conditions was exactly the same, users used the password schemes to log in to real websites, and we tested over multiple sessions.

## 4.2 GesturePass

### 4.2.1 Rationale

Our preliminary study showed that participants liked the gesture motions of Passgrid more than the graphical password scheme itself. Therefore for our main study, we decided to design a gesture based password scheme, GesturePass. When designing GesturePass, we wanted to utilize simple one-handed gestures that are most commonly used, such as tapping, dragging and pinching. The familiarity of these gestures would minimize gesture learning time. We also decided to assign passwords to prevent users from choosing relatively easy and repetitive passwords. In addition, we wanted to create a gesture password scheme that had comparable theoretical password space to a traditional 4 digit PIN password. In GesturePass, the user enters a sequence of gestures in order as determined when the password is created (figure 4.1).

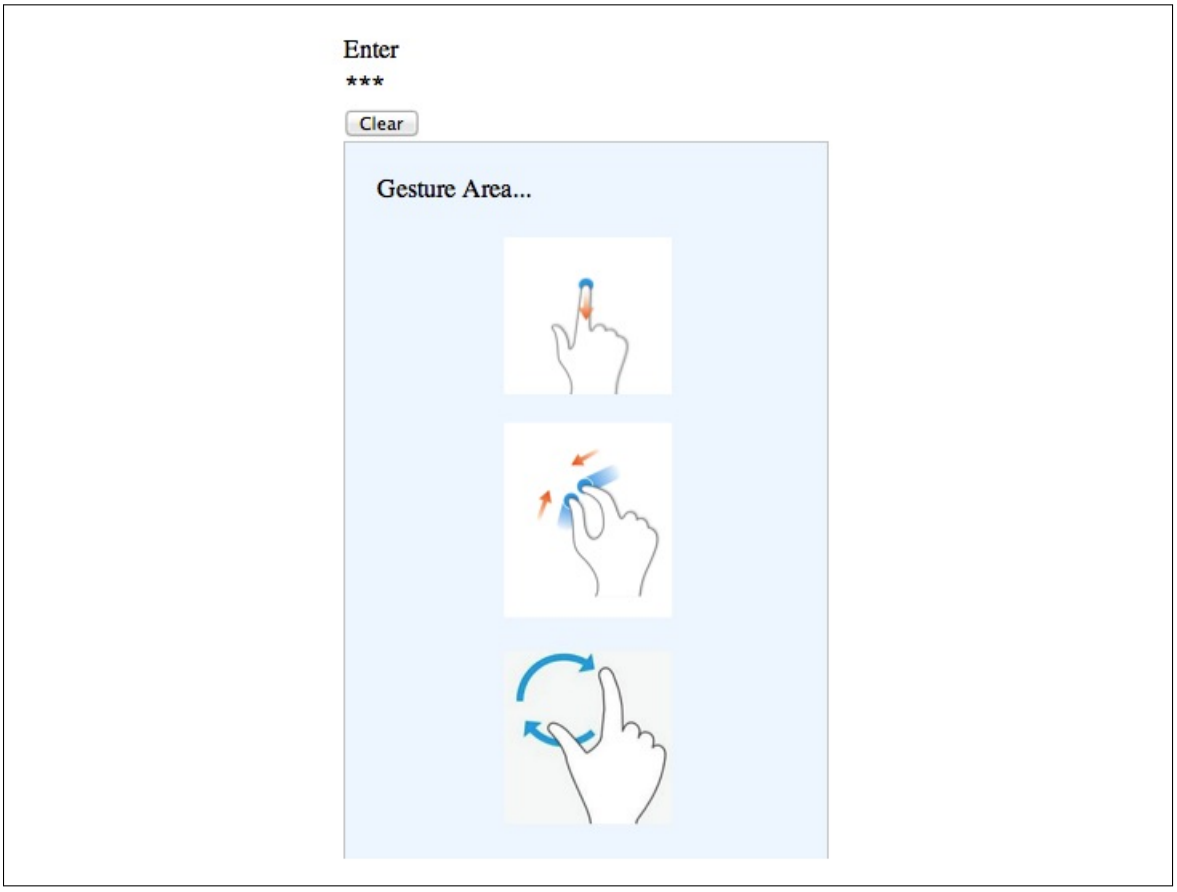



Figure 4.1: GesturePass Scheme (The user must enter gestures which have been previously assigned. The asterisks at the top of the screen show how many gestures have already been entered and clear button allows users to start again. The pictures inside of the Gesture Area are for illustrative purposes only and do not appear in the real system.)

### 4.2.2 Design

GesturePass is a recalled based scheme that randomly assigns a set of four simple gestures as a password. The ten gestures included are: drag up, drag down, drag left, drag right, tap, hold, pinch in, pinch out, rotate clockwise (described as turn right) and rotate anticlockwise (noted as turn left). Figures 4.2, 4.3, & 4.4 illustrate these gestures. We choose these gestures because they are commonly used gestures in applications that recognize gestures, such as Google Maps. Tap, hold and drag are single touch gestures, whereas the turns and pinches are multi-touch gestures. Single touch gestures require one finger (one point of interaction). Multi-touch gestures require the use of multiple fingers (multiple points of interaction) but do not specify exactly which fingers should form the gesture. Any two fingers that allowed the motion of the gesture could be utilized to perform a pinch or turn. For example, a pinch could be done with a index finger and a thumb, an index finger and a middle finger, or both index fingers (figures 4.5, 4.6). GesturePass contains about 100 lines of PHP, and about 200 lines of JavaScript. The PHP code runs on the server, and generates JavaScript code that runs in the web browser. The code was adapted from the Hammer JavaScript event logger sample program [27].

During the interface design phase of GesturePass, special consideration was made to the space needed to enter gestures on mobile devices. As seen in figure 4.7, a large gesture input area is provided with no visual cue. This enables entering your password without looking at the screen and reduces the possibility of shoulder surfing because the device can be held in any position. This gesture password scheme has theoretical password space of $10^4 = 10{,}000$ or approximately 13 bits. This is the same as a 4 digit PIN.

## 4.3 PIN Password Scheme

Our control condition used a system-assigned PIN password scheme that was implemented using JavaScript. Our system used an on-screen keypad input rather than the standard built-in Android keyboard. As seen in figure 4.8, this keypad covered the entire screen during any input mode. The number keys are big and colourful to

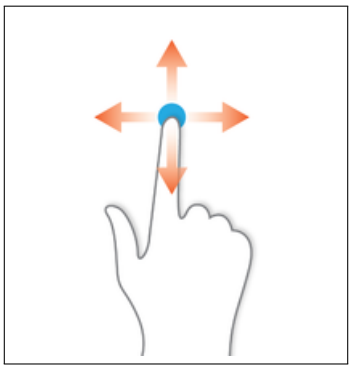


Figure 4.2: Example of Drag Gestures (Up, Down Left, Right) [60]

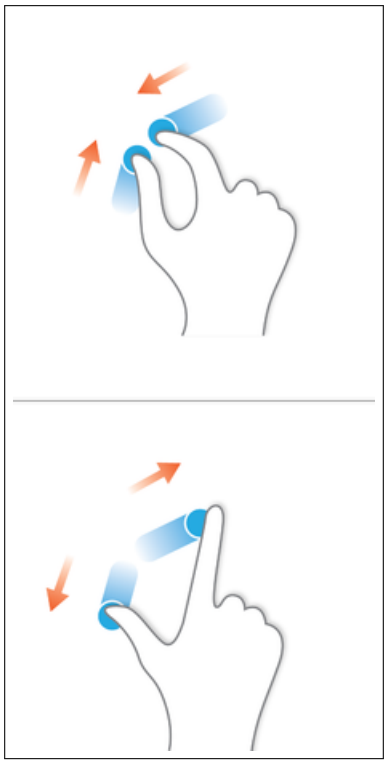


Figure 4.3: Example of Pinch In & Pinch Out Gestures [60]

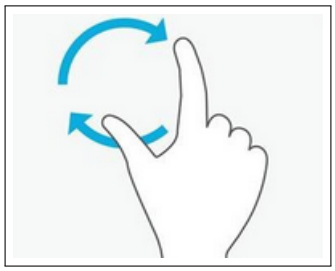


Figure 4.4: Example of the Rotate Gesture [37]

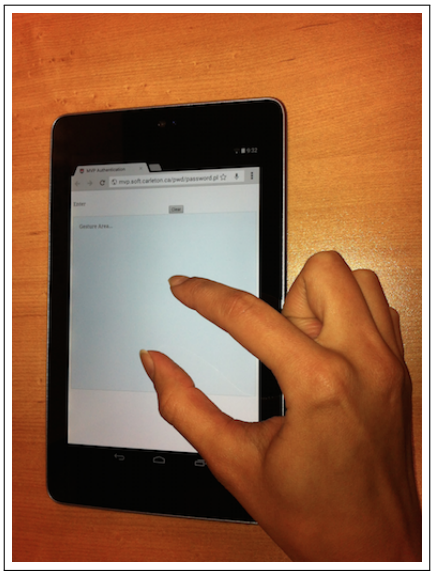


Figure 4.5: Example of Pinch In Gesture on GesturePass (with thumb and index finger)

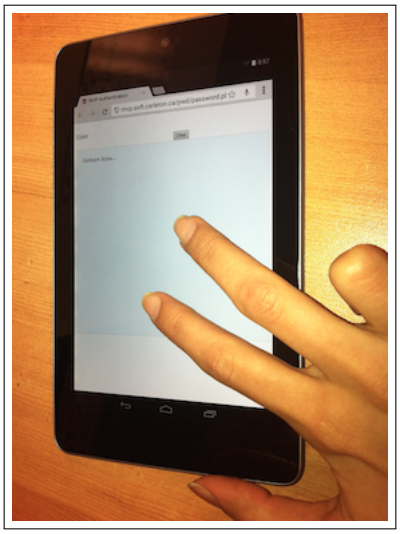


Figure 4.6: Example of Alternative Pinch In Gesture on GesturePass (with Index and middle fingers)

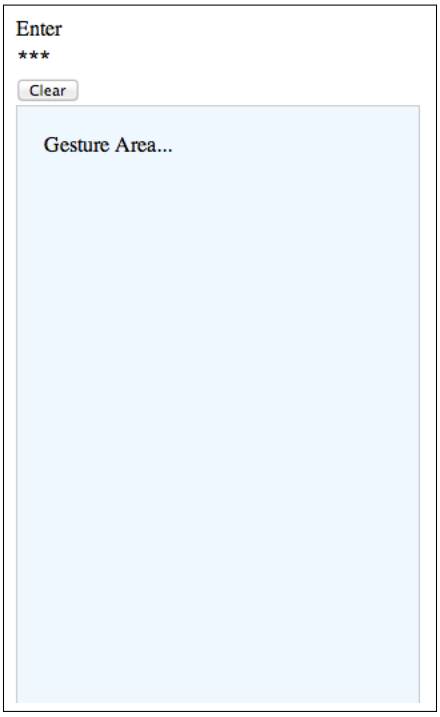



Figure 4.7: GesturePass Login Interface

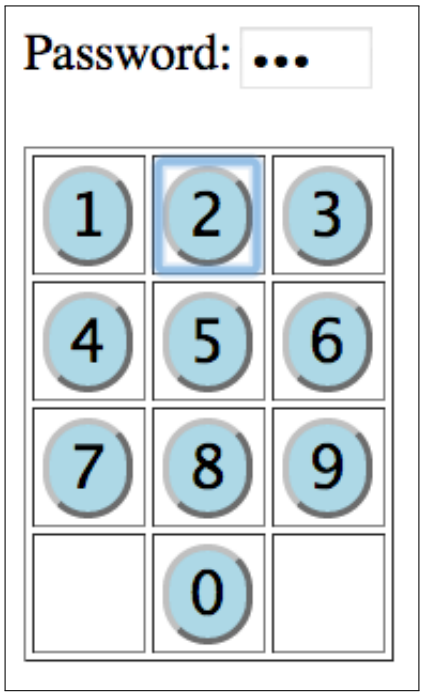



Figure 4.8: PIN Login Interface

mimic a typical standard keypad on a mobile device. We did not include the "*" or "#" key options since they would not be used in our PIN passwords. To log in successfully using this scheme, participants had to remember a randomly generated four digit PIN password. This PIN scheme has a theoretical password space of $10^4 =$ 10,000 or approximately 13 bits. All PIN passwords require selecting separate unique areas in order to enter numbers from the keypad. Usually this means that in order to enter a PIN, you have to look that the screen or keypad. The gesture password was specifically designed with a large input area so the user did not need to always look at the screen.

## 4.4 Study

### 4.4.1 Participants

This experiment was approved by the Carleton University Research Ethics Board and its ethics clearance form can be found in Appendix H. Participants were recruited from Carleton University and the wider community. To recruit from the university

community, we advertised the study by putting up posters in high foot traffic areas around campus. To reach the wider community, we recruited participants using additional posters, mailing lists and word of mouth. Our participants had to be accustomed to entering passwords to access websites. They were also required to be at least 18 years old.

There were 30 participants in this study. Each participant completed three sessions, each totalling 90 individual testing sessions. 15 participants were assigned the phone condition and 15 participants were assigned the tablet condition. Participants ranged in age from 18 to 33, with an average age of 24. 15 participants were female, 13 were male and two participants choose not answer the question. All of the participants were students. 12 participants were studying at the undergraduate level, 15 participants were pursuing a masters and 3 were in a Ph.D program. None of the participants were studying any topic relating to password systems. A few participants that completed the preliminary study also participated in the main study.

### 4.4.2 Apparatus

All sessions of the experiment were conducted in a lab environment. The apparatus used in the study included a Nexus 4 phone and a Nexus 7 tablet. These devices were chosen because our preliminary study indicated that users would most likely use a graphical password on a mobile device and a phone and tablet are the most common devices. The websites used in the study were hosted online (see section 4.4.3, and were accessed in the lab session using the Google Chrome web browser (version 32). All questionnaires were administered online, using LimeSurvey software [31] on a Linux server in our lab.

### 4.4.3 Materials

The materials used in the study included a consent form (Appendix D) and a questionnaire (Appendix E). The consent form contained a brief explanation of the study, contact information, a summary of the task requirements, information about data

anonymization, and an explanation of the withdrawal policy. The questionnaire contained a section for each of the three sessions of the study. For session one, the questionnaire included a usability questionnaire containing 10 point Likert scale questions for the PIN and gesture password schemes, demographic questions, and other questions regarding password usage. For sessions two and three, the questionnaire contained contained several usability and open ended questions about the two different password schemes. The two websites used in the study were hosted and maintained by our lab. The websites contained a series of generalized, non-offensive and non-controversial posts about world vacation destinations and student life. Visitors had to register and confirm a password through a specific password scheme which gave them the permission to login and post comments. Appendix F shows screen-shots of the two websites.

### 4.4.4 Procedure

This experiment consisted of three separate sessions, to test memorability and usability over time, totalling about an hour in a lab environment for each participant. The three sessions were separated by at least 24 hours. Participants were informed that they were going to be logging in and commenting on a couple of test websites using a PIN and gesture based password scheme. In session one, each participant was assigned a testing order based on a partial latin square in an effort to minimize the ordering effects of the study (figure 4.1). The partial latin square's testing order determined a participant's testing device (phone of tablet) for the entire study and in which order they were going to interact with the password schemes. This meant that participants were assigned either a Nexus 4 phone or a Nexus 7 tablet and started the experiment using a PIN or GesturePass. The first participant was assigned testing order 1 and each subsequent participant was assigned the next testing order, iterating as necessary.

**Session 1** At the start of the experiment, participants were asked to sign an informed consent form. Then participants were assigned to either the phone or tablet condition based on their testing order. For the training part of the experiment, participants were shown the features of the password scheme and could practice

| Testing Order | Device & Scheme | |
|---|---|---|
| 1 | Phone-PIN | Phone-Gesture |
| 2 | Tablet-PIN | Tablet-Gesture |
| 3 | Phone-Gesture | Phone-PIN |
| 4 | Tablet-Gesture | Tablet-PIN |

Table 4.1: Partial Latin Square (used to determine presentation order for the GesturePass Study)

the two different password schemes using the MVP trainer. They were allowed to create and test as many passwords as they wanted on both schemes. Once they were comfortable with the password schemes, they were given an overview of the two test websites used in the study.

Participants were asked to register and log in to two websites using their email address and an assigned username. The participants did not need to memorize their usernames as they were provided in each session. While registering, each participant was assigned one randomly generated PIN password and one randomly generated GesturePass password that they had to remember for all three sessions. Each password gave them access to a specific website. There were two websites and and each website used a different password type. The practice interfaces displayed the assigned password so users could learn it. The participants could practice these passwords as many times as they wanted before confirming them by clicking the accept button on each password interface (figures 4.9 & 4.10). After a successful login, participants were asked to comment on any post and log out. Finally, they were asked to complete the session one questionnaire (Appendix E). If at any point the participant could not remember their password after several attempts, we reminded them and let them continue. We followed this procedure for all following sessions.

**Session 2** Session two was scheduled at least 24 hours after session one for each participant. Participants had to log in, leave a comment on each website and complete the sessions two questionnaire (Appendix E).

**Session 3** Session three was scheduled at least 24 hours after session two for each

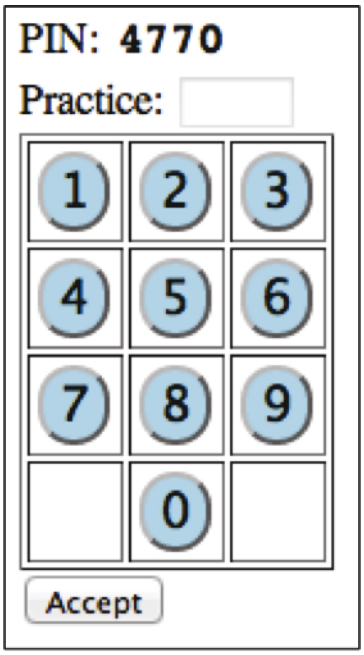



Figure 4.9: PIN Confirmation

participant. Once again, participants had to login, add a comment to each website and complete the session three questionnaire (Appendix E). Each participant was thanked and compensated ($10 honorarium) at the end of session three.

## 4.5 Hypotheses

We had a $2 \times 2$ study design which included two password systems (PIN and GesturePass) and two touchscreen sizes (phone and tablet). Our dependent measures were number of practices, number of login attempts, and login time. We made the following hypotheses:

**H1(a)** There will be significantly more password practices for GesturePass than PIN for both the phone and tablet devices.

**H2(a)** There will be no significant differences in the number of password login attempts between the PIN and GesturePass for both the phone and tablet devices.

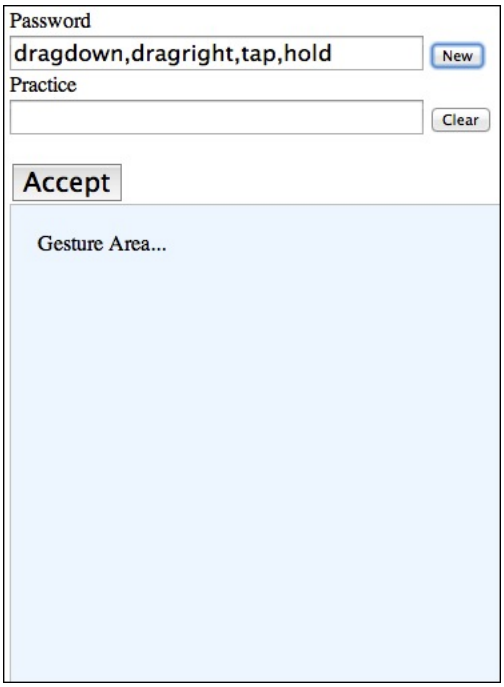



Figure 4.10: Gesture Confirmation

**H3(a)** Login time will be significantly less for GesturePass than PIN for both the phone and tablet devices.

## 4.6 Analysis Plan

For statistical comparisons we used non-parametric tests e.g. Wilcoxon test (also known as Mann-Whitney U tests) as the distributions suggested parametric tests would be inappropriate. See tables 4.5, 4.9, 4.12, for statistics of skewness and kurtosis of the data distributions.To test H1(a), we record the number of times each participant practiced their password before accepting it during session 1 for all devices (phone and tablet) and schemes (PIN and gesture password schemes). We examined if the number of practices would be significantly different for the two schemes. To analyze this data, we test within subjects for any effect of scheme (tablet PIN vs tablet gestures and phone PIN vs phone gesture) and test between subjects for any effect of device (phone PIN vs tablet PIN and phone gesture vs tablet gesture).

To test within subjects, we conduct paired Wilcoxon signed-rank tests which are

a non-parametric statistical test used when comparing two related samples to assess whether their population mean ranks differ when the population cannot be assumed to be normally distributed. To test between subjects, we conduct non paired Wilcoxon signed-rank tests because the data originates from different participants. To confirm the assumption that the data is not normally distributed, histograms were analyzed for skewness for all conditions.

To test H2(a), we record the number of password login attempts at session 3 for all conditions. Again, conduct paired Wilcoxon signed-rank tests were used to examine data within subjects and Wilcoxon signed-rank tests to analyze data between subjects. In addition, we created histograms for all conditions. We record the number of login attempts at sessions 3 because it gave participants a chance to interact and login with each scheme multiple times and get used to the password schemes before we perform our comparisons.

To test H3(a), we record the time it took to log in at session 3 for all devices and conditions. We represent this data using histograms and box-and-whisker plots, and compare it using Wilcoxon signed-rank tests. We decided not to use the TAM questionnaire for this study because our preliminary study showed that the login process is so quick and easy that the TAM has difficultly differentiating between password schemes.

## 4.7 Results and Interpretation

### 4.7.1 Hypothesis 1: Practices

Figure 4.11 shows that the number of practices for each condition. Generally, the graphs show that the PIN conditions are more positively skewed and the gesture conditions seem to be more negatively skewed. On average participants took fewer practices on the tablet than the phone (table 4.2). In addition within each device, on average participants took more practices with the gesture password scheme than the PIN password scheme (table 4.2). This may be a result of the novelty of the password scheme and that participants felt that they needed more practices to get comfortable with the scheme.

| Condition | Mean | SD | Median |
|---|---|---|---|
| Tablet PIN | 2.40 | 1.30 | 2.00 |
| Tablet Gesture | 3.60 | 1.55 | 4.00 |
| Phone PIN | 4.07 | 2.28 | 3.00 |
| Phone Gesture | 4.87 | 3.16 | 4.00 |

Table 4.2: Descriptive Statistics for Number of Practices at Session 1

| Condition | $V$ | $p$ |
|---|---|---|
| Tablet PIN vs Tablet Gesture | 6 | 0.0170 |
| Phone PIN vs Phone Gesture | 35 | 0.8934 |

Table 4.3: Paired Wilcoxon Signed-Rank Tests for Number of Practices (testing effect of scheme)

Table 4.3 shows that there were significant differences between tablet PIN and tablet gesture conditions. It also shows that there were no significant differences between the phone PIN and phone gesture conditions. Table 4.4 shows significant differences between phone PIN vs tablet PIN conditions. It also shows that there were no significant differences between the phone gesture and tablet gesture conditions.

### 4.7.2 Hypothesis 2: Login Attempts

Table 4.7 and Table 4.8 show that there were no significant differences in the number of login attempts at session 3 between any compared conditions. It appears that participants had learned how to use and had no more difficulty logging in with either scheme. As we conducted the experiments, we had noted that the participants had gained confidence with using the system. After the first session, they seemed more assured how it worked and clearly understood the scheme. As a result we decided that

| Condition | $W$ | $p$ |
|---|---|---|
| Phone PIN vs Tablet PIN | 62.0 | 0.0333 |
| Phone Gesture vs Tablet Gesture | 104.5 | 0.7524 |

Table 4.4: Wilcoxon Signed-Rank Tests for Number of Practices (testing effect of device)

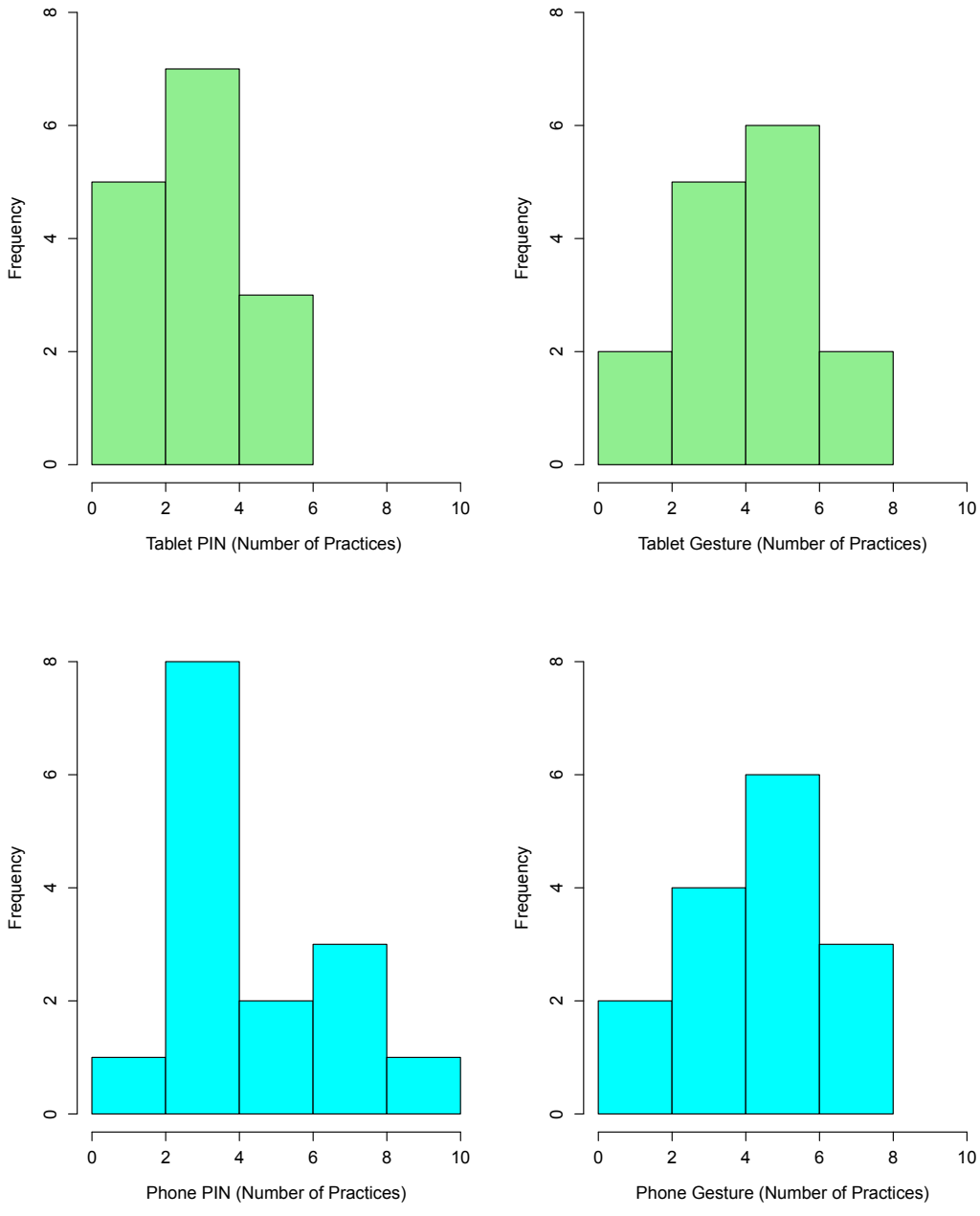



Figure 4.11: Number of Practices at Session 1

| Condition | Skewness | Kurtosis |
|---|---|---|
| Phone PIN | 0.4790 | -0.7293 |
| Phone Gesture | -0.1490 | -0.4762 |
| Tablet PIN | 0.7074 | -0.4053 |
| Tablet Gesture | -0.0319 | -1.1172 |

Table 4.5: Skewness & Kurtosis Results for Hypothesis 1: Number of Practices

| Condition | Mean | SD | Median |
|---|---|---|---|
| Tablet PIN | 1.13 | 0.35 | 1.00 |
| Tablet Gesture | 1.53 | 0.99 | 1.00 |
| Phone PIN | 1.20 | 0.77 | 1.00 |
| Phone Gesture | 1.47 | 0.74 | 1.00 |

Table 4.6: Descriptive Statistics for Number of Login Attempts at Session 3

comparing the session 3 login attempts would be the most reliable way of assessing their ability. Figure 4.12 illustrates that the number of login attempts were very similar for the tablet PIN, phone PIN and phone gesture conditions. By session 3, most participants required between 1 to 2 attempts per condition (tablet 4.6).

### 4.7.3 Hypothesis 3: Login Time

Table 4.10 shows that there were significant differences in login time between the tablet PIN and tablet gesture conditions. It also shows that there were significant differences between the phone PIN and phone gesture conditions. Table 4.11 shows that there was no significant differences in login time for the two password schemes between devices.

Figure 4.13 and figure 4.14 show that participants took longer to login using the gesture scheme than the PIN scheme for both devices. Figure 4.14 illustrates

| Condition | $V$ | $p$ |
|---|---|---|
| Tablet PIN vs Tablet Gesture | 4.0 | 0.2021 |
| Phone PIN vs Phone Gesture | 2.5 | 0.1048 |

Table 4.7: Paired Wilcoxon Signed-Rank Tests for Number of Attempts (testing effect of scheme)

| Condition | $W$ | $p$ |
|---|---|---|
| Phone PIN vs Tablet PIN | 120.0 | 0.5756 |
| Phone Gesture vs Tablet Gesture | 109.5 | 0.8979 |

Table 4.8: Wilcoxon Signed-Rank Tests for Number of Attempts (testing effect of device)

| Condition | Skewness | Kurtosis |
|---|---|---|
| Phone PIN | 2.4048 | 4.3491 |
| Phone Gesture | 1.6755 | 1.6224 |
| Tablet PIN | 3.8730 | 15 |
| Tablet Gesture | 1.3348 | 0.4706 |

Table 4.9: Skewness & Kurtosis Results for Hypothesis 2: Number of Attempts

| Condition | $V$ | $p$ |
|---|---|---|
| Tablet PIN vs Tablet Gesture | 105 | 0.0011 |
| Phone PIN vs Phone Gesture | 102.5 | 0.0019 |

Table 4.10: Paired Wilcoxon Tests for Login Time (testing effect of scheme)

| Condition | $W$ | $p$ |
|---|---|---|
| Phone PIN vs Tablet PIN | 118.5 | 0.5684 |
| Phone Gesture vs Tablet Gesture | 92.5 | 0.5993 |

Table 4.11: Wilcoxon Tests for Login Time (testing effect of device)

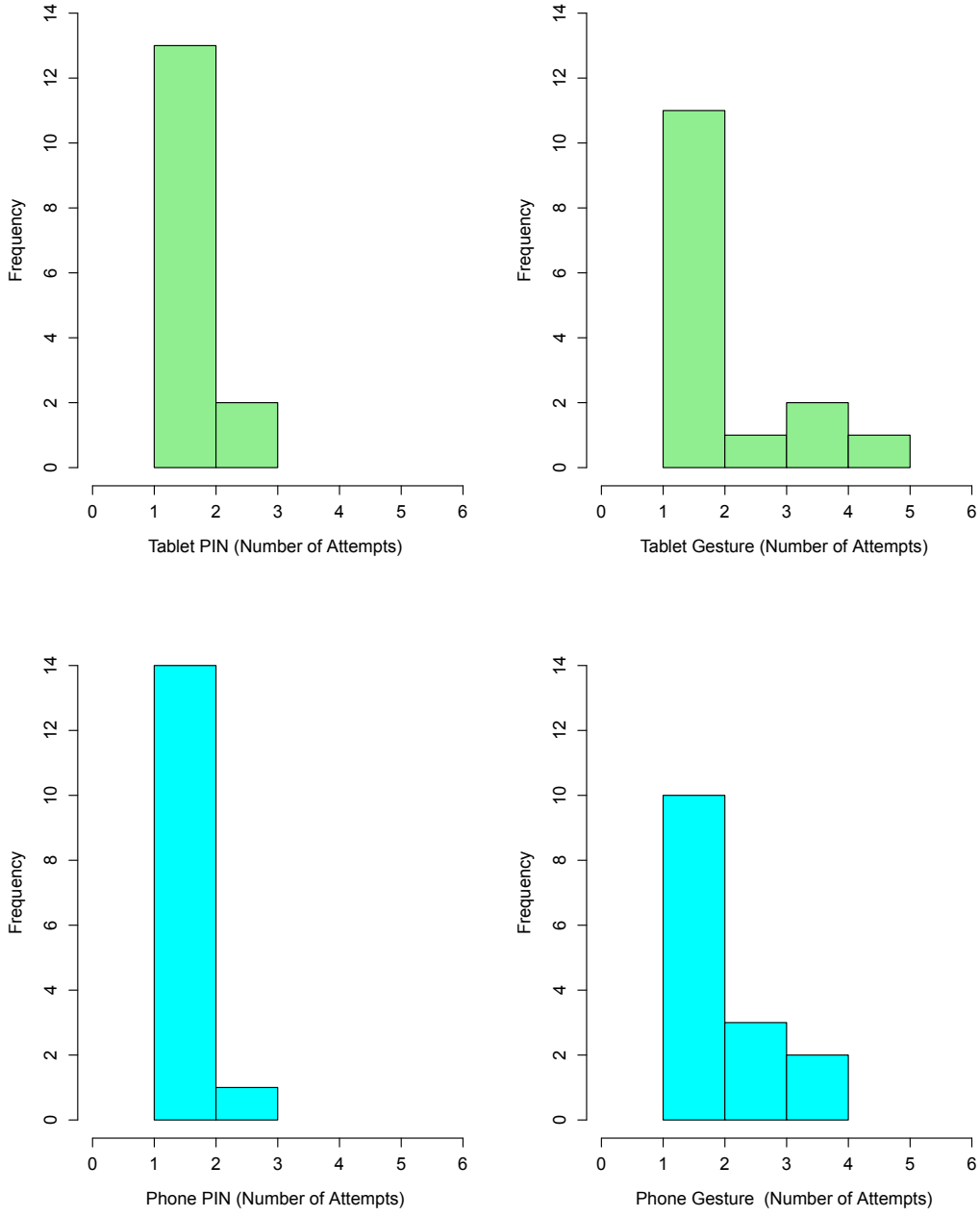



Figure 4.12: Number of Login Attempts at Session 3

| Condition | Skewness | Kurtosis |
|---|---|---|
| Phone PIN | 1.0997 | 0.5214 |
| Phone Gesture | 0.4366 | -0.3726 |
| Tablet PIN | 3.0891 | 10.6599 |
| Tablet Gesture | 3.0316 | 10.1222 |

Table 4.12: Skewness & Kurtosis Results for Hypothesis 3: Login Time

each login time distribution as a box plot. In a box plot the center quartiles are represented by the box with median shown as a dark horizontal line. The whiskers show the outer two quartiles. Circles on the graph show outliers. We see that PINs were faster on both devices. We further see that the distributions were wider for the gesture passwords and that some users were much quicker than other at entering their gestures.

For login time we also looked into specific gesture times for both the tablet and phone conditions. As seen by comparing figure 4.15 and figure 4.16, gesture times for both devices were very similar. As expected, tap was the quickest gesture and hold was the slowest gesture. By design the hold gesture require 500 milliseconds. The drag gestures, including dragup, dragdown, dragleft and dragright, were faster than the turn (turnright, turnleft) and pinch (pinchin, pinchout) gestures. The turn and pinch gestures also have very similar times for both devices.

### 4.7.4 Exploratory Analysis of Questionnaire Results

In our questionnaire, participants completed 14 usability questions on a 10 point Likert scale for each password scheme. These questions were divided into three general usability categories including ease of use, accessibility and security. Table 4.13 shows the usability questions, their category, and the code used to represent them in the following box-and-whisker plots. Some questions were presented in a negative direction on the questionnaire to avoid bias. For presentation of the results, the questions about size, daily, banking and multiple have been inverted so that a score of 10 is the most favourable result in each situation in the following graphs. We inspect the results, looking for general trends but did not conduct specific statistical tests.

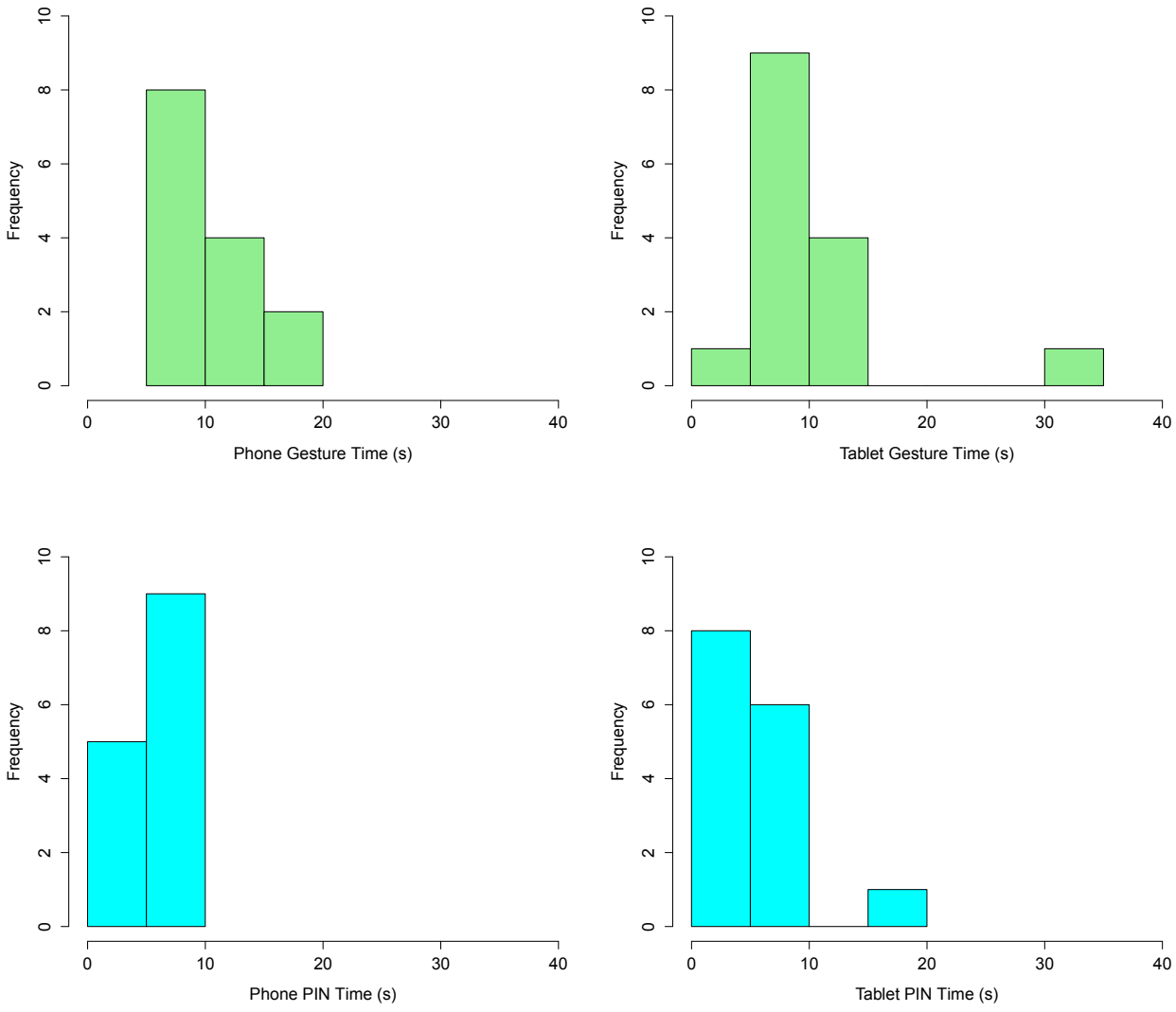



Figure 4.13: Password Login Time Histograms

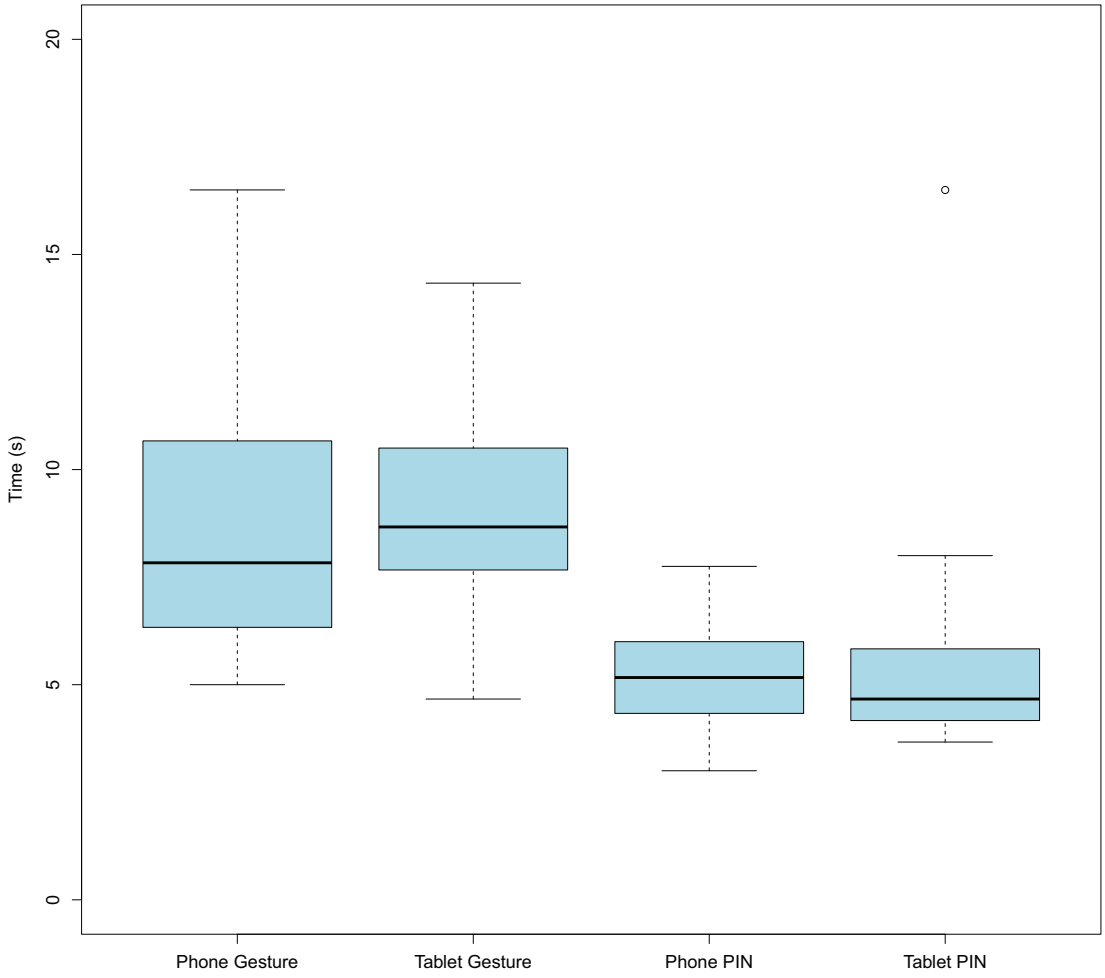



Figure 4.14: Password Login Time

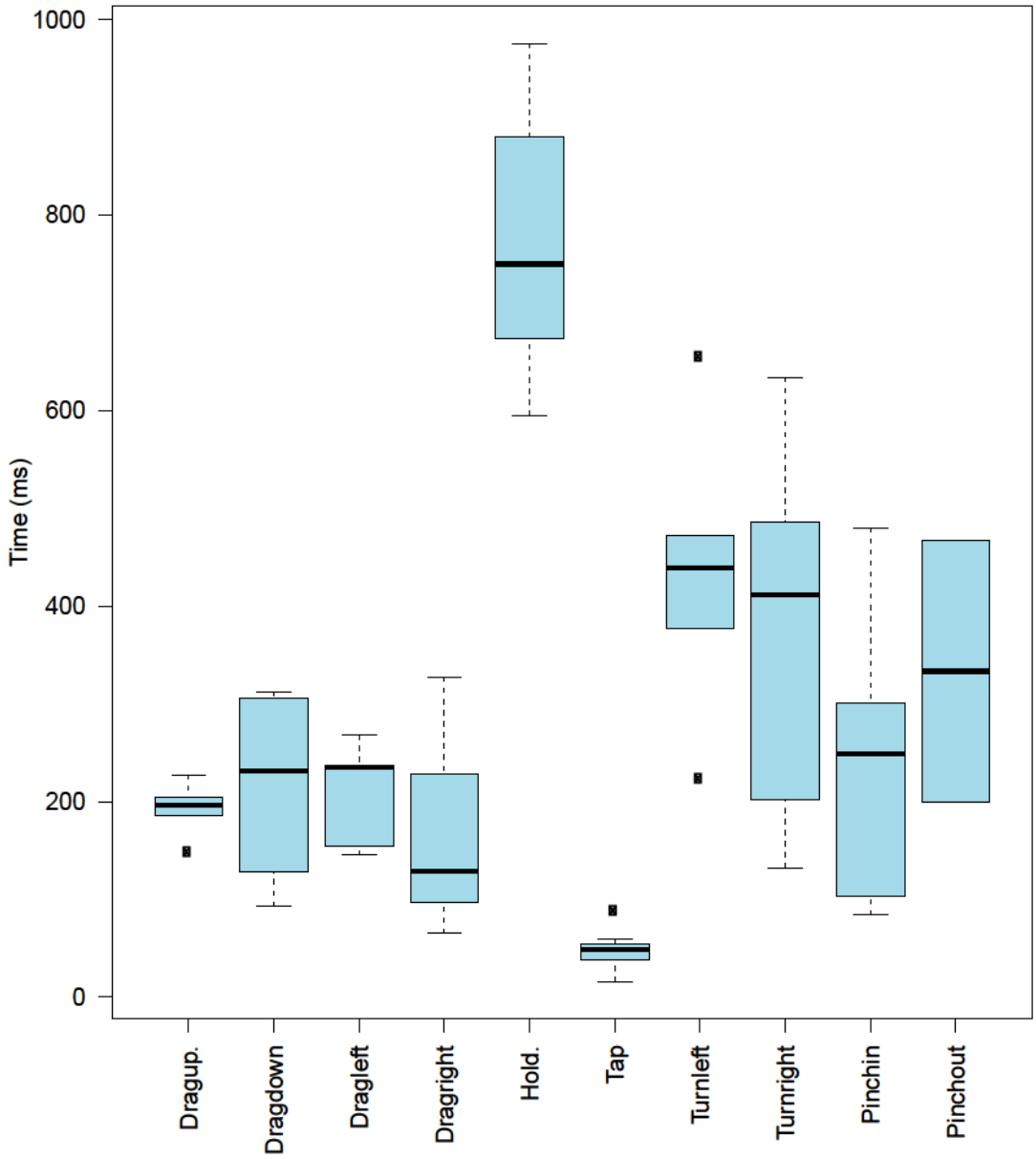



Figure 4.15: Phone Gesture Times

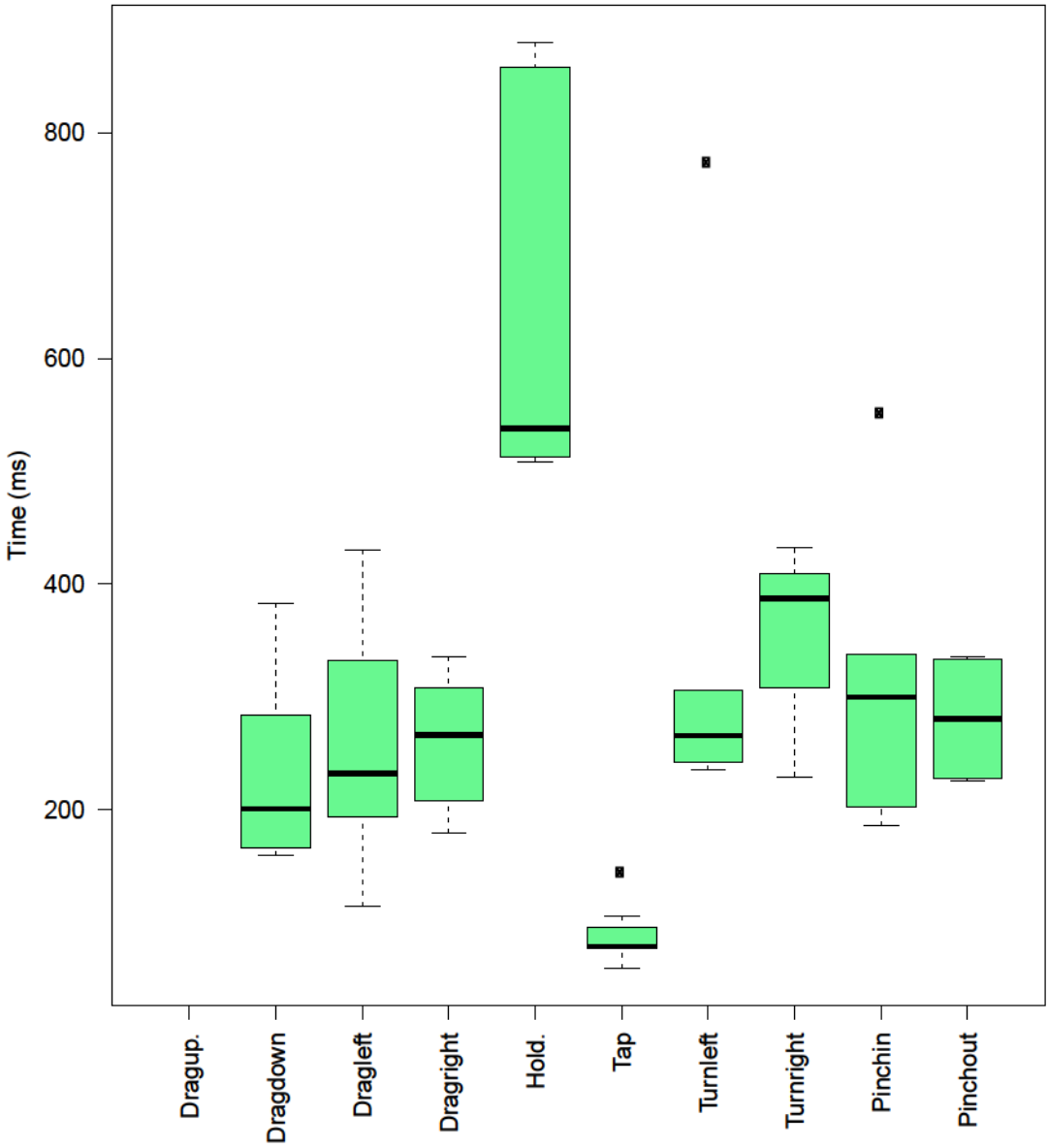



Figure 4.16: Tablet Gesture Times

| Question | Category | Code |
|---|---|---|
| ∗It would be challenging to remember multiple passwords on this scheme | Ease of Use | Many |
| I would be able to enter my password without looking | | Without |
| ∗It would be tedious to use this scheme on a daily basis | | Daily |
| ∗The size of the screen makes the scheme difficult to use | | Size |
| I found it easy to remember my password | | Remember |
| Entering my password was easy to do | | Enter |
| I found this password scheme easy to understand | | Understand |
| I would use this scheme for my email | Accessibility | Email |
| I would use this scheme on multiple devices | | Multiple |
| I found using this scheme to be enjoyable | | Enjoy |
| I found this password scheme useful | | Useful |
| ∗I would not use this scheme for important accounts (online banking) | Security | Banking |
| It would be difficult for someone to see my password | | See |
| It would be hard for someone to guess my password | | Guess |

Table 4.13: Likert Scale Questions (Those denoted with a ∗ have had their response scales inverted.)

Figure 4.17 shows participant responses for ease of use questions. Overall, the responses look very similar but our analysis did outline subtle differences. For example, question codes many and daily have higher medians for tablet PIN than phone PIN. This suggests that participants believed that it would be less challenging to remember multiple PIN passwords and less tedious to use the PIN on a daily basis on the tablet. Overall the PIN conditions seem to have lower medians (more negative) than the gesture conditions. Between the phone gesture and tablet gesture conditions, the tablet gesture responses seem to have slightly smaller ranges. This suggests that in terms of ease of use, the tablet gesture was the most preferred condition.

Figure 4.18 shows participant responses to the accessibility questions. These accessibility components contained aspects such as: usefulness, enjoyment, multiple device usage and email usage. Between the phone PIN and tablet PIN conditions, the tablet PIN had higher medians, representing more favourable opinions. Again, the gesture conditions had higher medians than the PIN conditions, suggesting that user preferred gestures for accessibility. The graphs also show that the tablet gesture seemed to be the most favourable condition in terms of accessibility.

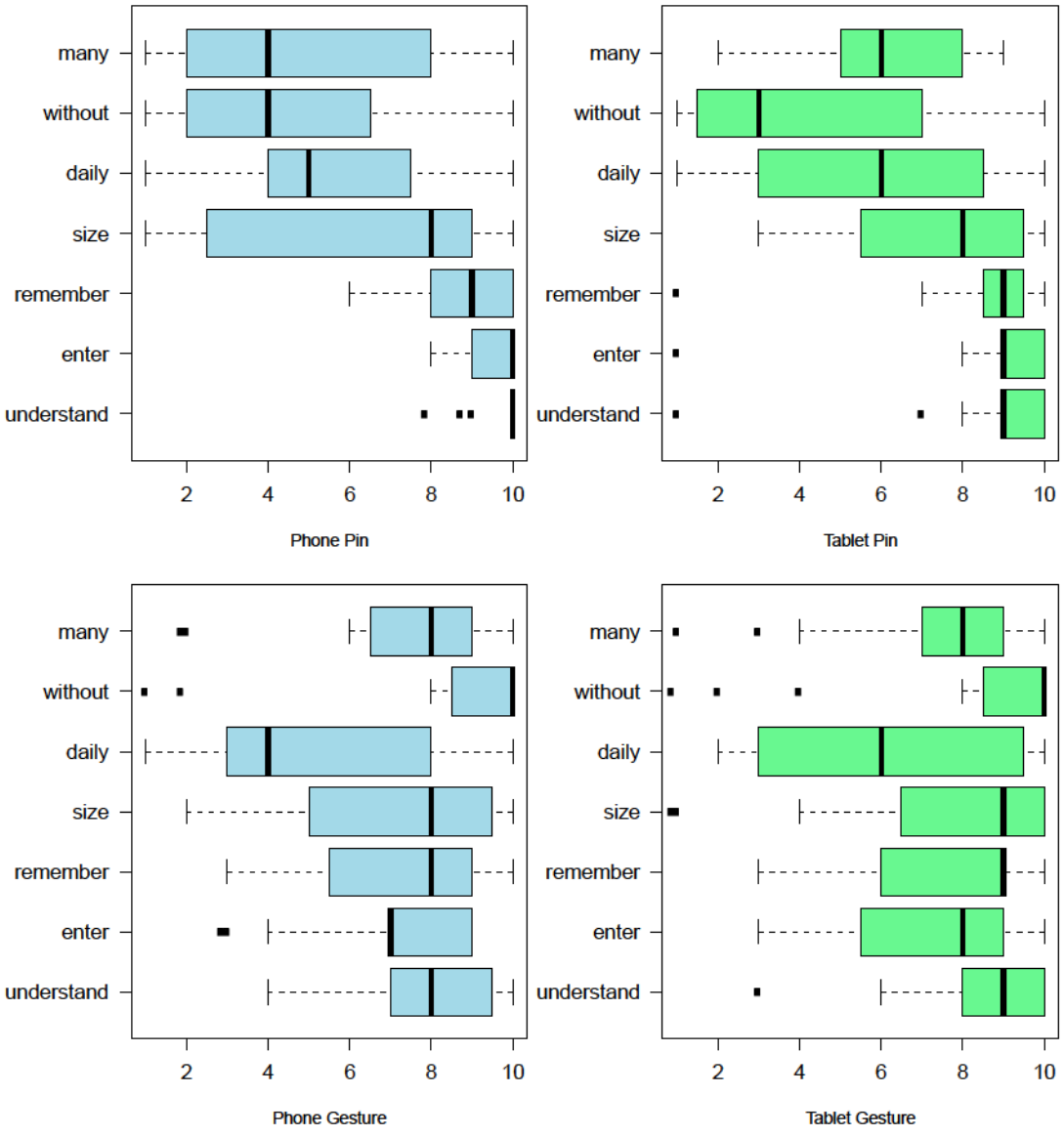



Figure 4.17: Ease of Use Questions - Likert Scale Responses

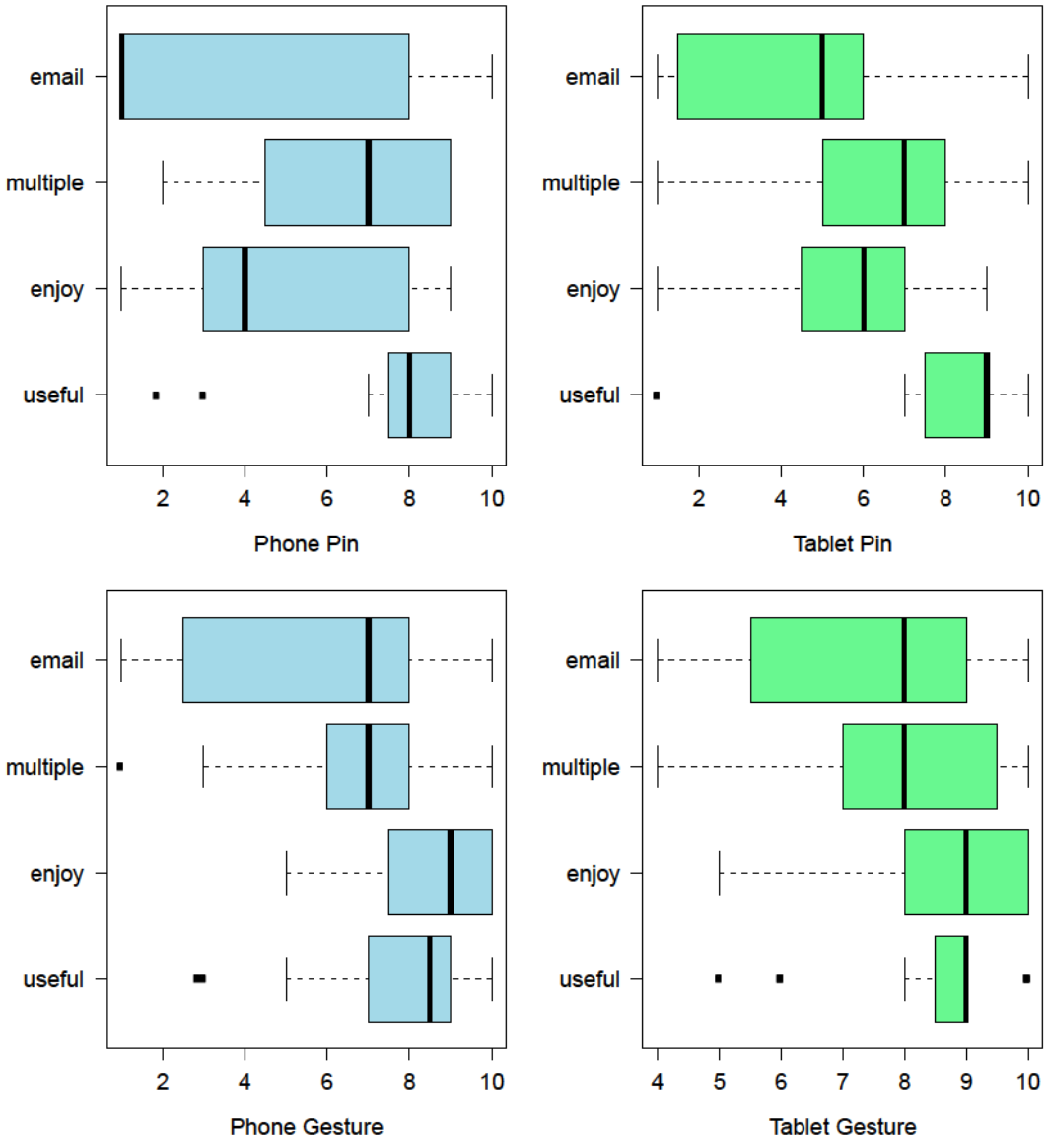



Figure 4.18: Accessibility Questions - Likert Scale Responses

Figure 4.19 shows participant responses to the security questions. These questions covered aspects such as difficulty of others seeing and guessing a password and using a scheme for important online banking accounts. The phone PIN condition seemed to have a higher median for banking but lower medians for other being able to see and guess a password than the tablet PIN condition. This suggests that participants still preferred using PINs on their phones when banking. Overall the gesture conditions seemed to have higher medians that the PIN conditions. This suggests that the gesture condition was considered to be more secure than the PIN condition. Within the gesture condition, the tablet received more positive responses than the phone. This indicated the most favourable condition for security was the tablet gesture.

### 4.7.5 Password Difficulty

Participants were assigned randomly generated passwords. However, some passwords may have been more easy to remember that others. For example, some PIN passwords contained two or three repetitive digits. This was a much easier password to remember than a PIN that contained four different digits. In addition, some PIN passwords contained digits with personal significance for participants which made it easier for them to remember the password. For the gesture passwords, some participants also had easier repetitive gestures to remember. Another observation was that participants had trouble with multi-touch gestures such as turn right, turn left, pinch in and pinch out. This could be because multi-touch gestures are less commonly used than simple single touch gestures such as tap, hold and drag.

## 4.8 Results Summary

Our initial objective was to investigate the usability of a gesture password scheme on mobile devices in comparison to a PIN password. Our hypotheses were that there would be significantly more password practices for GesturePass, there would be no significant differences in the number of password login attempts between the schemes and login time would be significantly less for GesturePass than the PIN password for both devices. Our results showed that participants did take more practices with

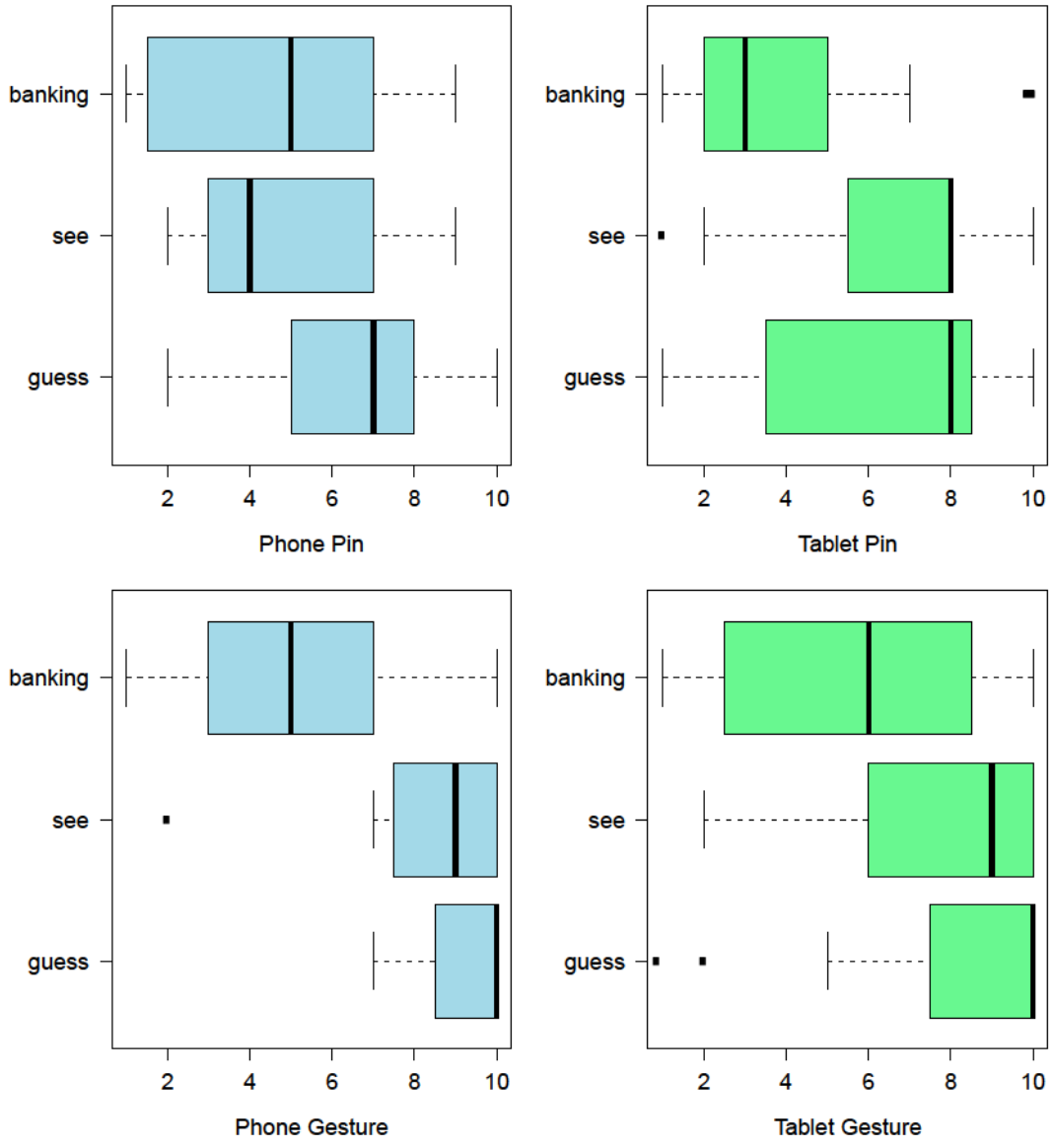



Figure 4.19: Security Questions - Likert Scale Responses

GesturePass than the PIN password in session 1, there were no significant differences in the number of password login attempts between the schemes in session 3, and participants took longer to login using GesturePass than the PIN password for both devices at session 3. Questionnaire responses suggest that in terms of the ease of use, accessibility and security components, GesturePass was preferred over PINs. In addition, the tablet gesture condition generally scored higher medians than the phone gesture condition. Our exploratory analysis suggest that most users preferred the tablet gesture condition. We speculate this is because users could more easily enter gestures (especially multi-finger gestures) on the tablet than the mobile phone. Participants also commented that they liked GesturePass because it was easy and fun to use, entertaining and more interactive. ("...Novel and pretty easy to use...", "...entertaining ...", "...fun new experience ..." ,"The gestures make it more interactive.")

Although this study's design was more ecologically valid, some limitations remain. For example, studies were conducted in a controlled lab environment. Alternative tests could be done in different mobile situations such as in public areas while walking. Another limitation is that although the memorability of the passwords was tested, participants were not required to follow traditional procedures to reset their passwords nor were the password restricting access to resources of value. In addition, even though we used a latin square to reduce the ordering effects the the study, participants may still have rated conditions based on comparisons between the schemes and devices rather than each condition individually. Using a larger single and multi-touch gesture character set may also provide more insights to which gestures users prefer and which gestures are more problematic. Another study could be conducted on analyzing potential shoulder-surfing attacks on GesturePass and the possibility of users being able to able to enter their password without looking at the device.

# Chapter 5

# Conclusions

## 5.1 Summary

The purpose of this thesis was to design a multi-touch or gesture password scheme that could be a viable alternative to a tradition text password. To investigate we conducted a preliminary study with a more graphically oriented password scheme and main study with a password scheme which focused more on gestures.

The objective of our preliminary study was to analyze a new multi-touch graphical password scheme called Passgrid. Passgrid was compared to a traditional text password scheme in terms of login time, effect of screen size, level of user acceptance, and overall user experience. For login time, we hypothesized that Passgrid's multi-touch capabilities would allow faster interaction resulting in quicker login times. To analyze the effect of screen size we conducted experiments with a tablet and large screen display. The level of user acceptance and overall user experience was examined by questions based on the four components of the Technology Acceptance Model (TAM) and other general usability questions.

Our results showed that Passgrid did not have faster login times than the text password scheme for either device. This is despite Passgrid having a lower password strength. Between the two devices, participants indicated that they would prefer Passgrid on a tablet rather than on a large screen display. The TAM questionnaire responses showed statistical significance on only one of the four TAM components. However, participant feedback also indicated that Passgrid provided an enjoyable and more entertaining experience. In regards to multi-touch, participants were hesitant to utilize more than one finger when interacting with Passgrid. We also observed that participants liked Passgrid's interactive gesture motions of selecting and dragging more than they liked the graphical elements of the scheme. Therefore we created a gesture based password scheme based on our initial preliminary findings.

The objective of our main study was to investigate the usability of a new gesture based password scheme called GesturePass. We compared GesturePass to a traditional PIN on a mobile phone and tablet. We analyzed the number of practices, the number of login attempts, login times, gesture times and other usability questionnaire responses. We hypothesized that GesturePass would require significantly more practices than the PIN password scheme, no significant differences would be present in the number of password login attempts between the schemes, and login time would be significantly less for GesturePass than the PIN password for both devices.

Our results showed that participants required more practices while using GesturePass than the PIN password scheme, no significant differences were present in the number of password login attempts between the schemes, and login took longer on GesturePass than the PIN password scheme for both devices. Usability questionnaire responses also suggested that in regards to ease of use, accessibility, and security aspects, GesturePass was preferred over PINs. In addition, most users preferred the tablet gesture conditions.

## 5.2 Discussion

In the summary above we described our research agenda, the studies we conducted, and the results we obtained. In this section, we discuss possibilities for *why* the results came about.

Login time for both Passgrid and GesturePass took longer than login time for the text and PIN password schemes. This could be a result of the novel aspects of Passgrid and GesturePass. In addition, participants may have had faster login times for the text and PIN passwords because they were familiar with traditional input structures which could have facilitated faster key selection. Another factor to consider is that even though all of our password schemes assigned randomly generated passwords, participants may have been assigned text and PIN passwords containing personal significance by chance. This could have made it easier and faster for participants to remember and enter text and PIN passwords.

Multi-touch capabilities were supposed to benefit both Passgrid and GesturePass.

For Passgrid, multi-touch was intended to help speed up login time by allowing participants to utilize multiple fingers to move multiple images. However, participants preferred to interact with fewer fingers or just one finger. For GesturePass, multi-touch enhanced the system by allowing participants to interact with a larger password character set by including more complex gestures. However, participants found it difficult to input multi-touch gestures, such as the pinch and rotate gestures. Our findings show that participants had trouble with the multi-touch components of Passgrid and GesturePass. This could be because single touch gestures are more commonly used than multiple touch gestures. Alternatively users may have had difficulty since there was no feedback or context for the gestures. Perhaps multi-touch gestures will thrive with the evolution of more complex applications that require more points of interaction. However, it is possible that the password login experience for these password schemes is such a simple and short interaction that single touch gestures may be more suitable than multi-touch gestures.

In study 1, the questionnaire responses to only one (Attitude Towards Using (A)) out of the four components of TAM showed statistical differences favouring Passgrid. Even though all of the TAM components did not show statistical differences, this one component which favours Passgrid illustrates a positive outlook towards the graphical password scheme. In addition, participants commented that Passgrid was more enjoyable and entertaining. Participants enjoyed the gesture motions of the password scheme more than the graphical components of the interaction. Gestures greatly enhance the typical interaction of the graphical password scheme, which is one of the reasons why we decided to investigate a gesture based password for our main study.

For our main study, participants took significantly more practices during session one with GesturePass than with the comparable PIN password scheme. However by session three, there were no significant differences in the number of password login attempts between the password schemes. This suggest that even though GesturePass initially requires more practice, after three login experiences the number of login attempts become comparable to a traditional PIN password scheme. Another positive factor is that in our exploratory analysis, our usability questionnaire responses suggest

that in terms of ease of use, accessibility, and security, GesturePass on the tablet was generally most preferred. ("... more fun than PINs and easier. You don't have to look to see the numbers ...", "The gestures makes it more interactive.") This suggests that participants preferred GesturePass over the PIN password scheme and that the optimal device for GesturePass is the tablet, possibility because they gesture were easier to perform on the larger surface.

## 5.3 Research Question

Our research question was: *Can we design a multi-touch or gesture password scheme for touchscreen devices that is a viable alternative to a traditional test password scheme?* Our results suggest that a gesture based password scheme can be a viable alternative to a traditional text password. GesturePass had a comparative theoretical and effective password space, statistically had no differences in the number of login attempts as a PIN passwords after three sessions, and GesturePass was favoured over PIN passwords in our usability analysis. However, our studies also show that participants did not favour using even simple multi-touch gestures. In addition, our usability analysis show that GesturePass was preferred over PINs especially for tablets.

## 5.4 Future Work

Future work could focus on investigating the use of more single and multi-touch gestures as password characters. Our studies showed that participants had difficulties with multi-touch passwords and therefore more studies could be created to examine why this occurs. Future work could also entail exploring how participants enter gesture passwords in different environments such as while walking or while being stationary in a public area. Another interesting factor to test is if and how participants would be able to remember multiple gesture passwords in comparison to multiple PIN passwords. It would also be intriguing to see how a visual cue could effect shoulder-surfing attacks and improve GesturePass's overall interaction experience.

## Bibliography


[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[2] Anne Adams, Martina Angela Sasse, and Peter Lunt. Making passwords secure and usable. In *Proceedings of HCI on People and Computers XII*, HCI 97, pages 1–19, London, UK, UK, 1997. Springer-Verlag.

[3] Lisa Anthony, Quincy Brown, Jaye Nias, and Berthel Tate. Examining the need for visual feedback during gesture interaction on mobile touchscreen devices for kids. In *Proceedings of the 12th International Conference on Interaction Design and Children*, IDC '13, pages 157–164, New York, NY, USA, 2013. ACM.

[4] Baranovskiy, D. Raphael JavaScript Library, 2014. `http://raphaeljs.com`.

[5] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Comput. Surv.*, 44(4):19:1–19:41, September 2012.

[6] Bill Buxton. Multi-touch systems that I have known and loved., 2009. `http://www.billbuxton.com/multitouchOverview.html`.

[7] Joseph Bonneau. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, SP '12, pages 538–552, Washington, DC, USA, 2012. IEEE Computer Society.

[8] Sonia Chiasson, Chris Deschamps, Elizabeth Stobert, Max Hlywa, Bruna Freitas Machado, Alain Forget, Nicholas Wright, Gerry Chan, and Robert Biddle. The mvp web-based authentication framework. In *Financial Cryptography and Data Security*, pages 16–24. Springer, 2012.

[9] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. Influencing users towards better passwords: Persuasive cued click-points. In *Proceedings of the 22Nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction - Volume 1*, BCS-HCI '08, pages 121–130, Swinton, UK, UK, 2008. British Computer Society.

[10] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. User interface design affects security: Patterns in click-based graphical passwords. *Int. J. Inf. Secur.*, 8(6):387–398, October 2009.

[11] Sonia Chiasson, P. C. Van Oorschot, and Robert Biddle. Graphical password authentication using cued click points. In *Proceedings of the 12th European Conference on Research in Computer Security*, ESORICS'07, pages 359–374, Berlin, Heidelberg, 2007. Springer-Verlag.

[12] Fred D. Davis. User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *Int. J. Man-Mach. Stud.*, 38(3):475–487, March 1993.

[13] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *Int. J. Hum.-Comput. Stud.*, 63(1-2):128–152, July 2005.

[14] Rachna Dhamija and Adrian Perrig. Déja; vu: A user study using images for authentication. In *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9*, SSYM'00, pages 4–4, Berkeley, CA, USA, 2000. USENIX Association.

[15] Ahmet Emir Dirik, Nasir Memon, and Jean-Camille Birget. Modeling user choice in the passpoints graphical password scheme. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 20–28, New York, NY, USA, 2007. ACM.

[16] C.L. McEvoy D.L. Nelson, V.S. Reed. Learning to order pictures and words: A model of sensory and semantic encoding. *Journal of Experimental Psychology: Human Learning and Memory*, 3 (5):485–497, 1977.

[17] J.R. Walling D.L. Nelson, V.S. Reed. Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory*, 2 (5):523–528, 1976.

[18] Paul Dunphy and Jeff Yan. Do background images improve "draw a secret" graphical passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, CCS '07, pages 36–47, New York, NY, USA, 2007. ACM.

[19] Dinei Florencio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, pages 657–666, New York, NY, USA, 2007. ACM.

[20] Dinei Florêncio, Cormac Herley, and Baris Coskun. Do strong web passwords accomplish anything? In *Proceedings of the 2Nd USENIX Workshop on Hot Topics in Security*, HOTSEC'07, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Association.

[21] Clifton Forlines, Daniel Wigdor, Chia Shen, and Ravin Balakrishnan. Direct-touch vs. mouse input for tabletop displays. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pages 647–656, New York, NY, USA, 2007. ACM.

[22] John D. Gould, Sharon L. Greene, Stephen J. Boies, Antonia Meluson, and Marwan Rasamny. Using a touchscreen for simple tasks. *Interact. Comput.*, 2(1):59–74, April 1990.

[23] Uta Hinrichs and Sheelagh Carpendale. Gestures in the wild: Studying multi-touch gesture sequences on interactive tabletop exhibits. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '11, pages 3023–3032, New York, NY, USA, 2011. ACM.

[24] Max Hlywa, Robert Biddle, and Andrew S. Patrick. Facing the facts about image type in recognition-based graphical passwords. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC '11, pages 149–158, New York, NY, USA, 2011. ACM.

[25] Eve Hoggan, Stephen A. Brewster, and Jody Johnston. Investigating the effectiveness of tactile feedback for mobile touchscreens. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1573–1582, New York, NY, USA, 2008. ACM.

[26] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, pages 1–1, Berkeley, CA, USA, 1999. USENIX Association.

[27] Jorik Tangelder. Hammer JavaScript Library: A JavaScript library for multi-touch gestures, 2014. `http://eightmedia.github.io/hammer.js/`.

[28] Dietrich Kammer, Jan Wojdziak, Mandy Keck, Rainer Groh, and Severin Taranko. Towards a formalization of multi-touch gestures. In *ACM International Conference on Interactive Tabletops and Surfaces*, ITS '10, pages 49–58, New York, NY, USA, 2010. ACM.

[29] Eben I. Kaplan. Tackling the password problem: Image- and gesture-based alternatives to alphanumeric passwords. *Information Security Journal: A Global Perspective*, 22(4):180–186, 2013.

[30] K. Kim and V. K. Prasanna-Kumar. Perfect latin squares and parallel array access. *SIGARCH Comput. Archit. News*, 17(3):372–379, April 1989.

[31] LimeSurvey. LimeSurvey: The Open Source Survey Application, 2014. `http://www.limesurvey.org/en/`.

[32] Hao Lü and Yang Li. Gesture studio: Authoring multi-touch interactions through demonstration and declaration. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '13, pages 257–266, New York, NY, USA, 2013. ACM.

[33] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

[34] Microsoft Corporation. Personalize your PC: Signing in with a picture password, 2014. `http://windows.microsoft.com/en-ca/windows-8/personalize-pc-tutorial`.

[35] Michael G. Morris and Andrew Dillon. How user perceptions influence software use. *IEEE Softw.*, 14(4):58–65, July 1997.

[36] Robert Morris and Ken Thompson. Password security: A case history. *Commun. ACM*, 22(11):594–597, November 1979.

[37] MSDN Blogs. Building Windows 8, 2014. `http://blogs.msdn.com/b/b8/`.

[38] Lloyd H. Nakatani and John A. Rohrlich. Soft machines: A philosophy of user-computer interface design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '83, pages 19–23, New York, NY, USA, 1983. ACM.

[39] Yuan Niu and Hao Chen. Gesture authentication with touch input for mobile devices. In Ramjee Prasad, Kroly Farkas, AndreasU. Schmidt, Antonio Lioy, Giovanni Russello, and FlaminiaL. Luccio, editors, *Security and Privacy in Mobile Information and Communication Systems*, volume 94 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 13–24. Springer Berlin Heidelberg, 2012.

[40] Chris North, Tim Dwyer, Bongshin Lee, Danyel Fisher, Petra Isenberg, George Robertson, and Kori Inkpen. Understanding multi-touch manipulation for surface computing. In *Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part II*, INTERACT '09, pages 236–249, Berlin, Heidelberg, 2009. Springer-Verlag.

[41] P. C. van Oorschot and Julie Thorpe. On predictive models and user-drawn graphical passwords. *ACM Trans. Inf. Syst. Secur.*, 10(4):5:1–5:33, January 2008.

[42] Smythe P. C. Paivo A., Rogers T. Why are pictures easier to recall than words? *Psychonomic Science*, 11 (4):137–138, 1968.

[43] PassFaces Corporation. The science behind passfaces, 2014. `http://www.passfaces.com/enterprise/contact_us/contact_us.html`.

[44] Keith B. Perry and Juan Pablo Hourcade. Evaluating one handed thumb tapping on mobile touchscreen devices. In *Proceedings of Graphics Interface 2008*, GI '08, pages 57–64, Toronto, Ont., Canada, Canada, 2008. Canadian Information Processing Society.

[45] PQ Labs. PQ Labs: Innovation Beyond PC, 2014. `http://multitouch.com/contact.html`.

[46] Jeroen GW Raaijmakers and Richard M Shiffrin. Models for recall and recognition. *Annual review of psychology*, 43:205–234, 1992.

[47] Jochen Rick. Performance optimizations of virtual keyboards for stroke-based text entry on a touch-based tabletop. In *Proceedings of the 23Nd Annual ACM Symposium on User Interface Software and Technology*, UIST '10, pages 77–86, New York, NY, USA, 2010. ACM.

[48] Napa Sae-Bae, Kowsar Ahmed, Katherine Isbister, and Nasir Memon. Biometric-rich gestures: A novel approach to authentication on multi-touch devices. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 977–986, New York, NY, USA, 2012. ACM.

[49] D. Saffer. *Designing Gestural Interfaces: Touchscreens and Interactive Devices*. O'Reilly Media, 2008.

[50] Andrew Sears, Doreen Revis, Janet Swatski, Rob Crittenden, and Ben Shneiderman. Investigating touchscreen typing: the effect of keyboard size on typing speed. *Behaviour & Information Technology*, 12(1):17–22, 1993.

[51] Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. User-generated free-form gestures for authentication: Security and memorability. *CoRR*, abs/1401.0561, 2014.

[52] Elizabeth Stobert and Robert Biddle. Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, pages 15:1–15:14, New York, NY, USA, 2013. ACM.

[53] Stock.xchnage(SXC). Stock.xchang: The leading free stock photography website, 2014. `http://sxc.hu`.

[54] Hai Tao and Carlisle Adams. Pass-go: A proposal to improve the usability of graphical passwords. *I. J. Network Security*, 7(2):273–292, 2008.

[55] Julie Thorpe and P. C. van Oorschot. Human-seeded attacks and exploiting hot-spots in graphical passwords. In *Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, SS'07, pages 8:1–8:16, Berkeley, CA, USA, 2007. USENIX Association.

[56] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz. Quantifying the security of graphical passwords: The case of android unlock patterns. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 161–172, New York, NY, USA, 2013. ACM.

[57] John Verzani. *Getting Started with RStudio*. O'Reilly Media, Inc., 2011.

[58] Matt Weir, Sudhir Aggarwal, Michael Collins, and Henry Stern. Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, pages 162–175, New York, NY, USA, 2010. ACM.

[59] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.*, 63(1-2):102–127, July 2005.

[60] Wikipedia. Multi-touch, 2014. `http://http://en.wikipedia.org/`.

[61] Jeff Yan, Alan Blackwell, Ross Anderson, and Alasdair Grant. Password memorability and security: Empirical results. *IEEE Security and Privacy*, 2(5):25–31, September 2004.

[62] Shumin Zhai, Michael Hunter, and Barton A. Smith. The metropolis keyboard - an exploration of quantitative techniques for virtual keyboard design. In *Proceedings of the 13th Annual ACM Symposium on User Interface Software and Technology*, UIST '00, pages 119–128, New York, NY, USA, 2000. ACM.

# Appendix A

## Preliminary Study: Informed Consent Form

Carleton UNIVERSITY
Canada's Capital University

**Informed Consent Form**

*The purpose of an informed consent is to ensure that you understand the purpose of the study and the nature of your involvement. The informed consent has to provide sufficient information such that you have the opportunity to determine whether you wish to participate in the study.*

*Study Title:* An Evaluation of Multi-Touch Passwords


| | | |
|---|---|---|
| *Research Personnel:* | Investigator: | Shahshuja Shahzada, shahshuja.shahzada@carleton.ca |
| | Faculty Advisors: | Dr. Robert Biddle, robert_biddle@carleton.ca |
| | | Dr. Sonia Chiasson, chiasson@scs.carleton.ca |


*Purpose:* To investigate how individuals create passwords using multi-touch on multiple mobile devices.

*Task Requirements:* The experiment will consist of a series of password creation tasks on a tablet and large screen display. Participants will be analysed on their creation and login times, how many and which fingers they utilize for each device and the strength of their passwords. Then they will complete a survey.

*Potential Risk/Discomfort:* There is no known risk/discomfort greater than those encountered by participants in similar aspects of their everyday life.

*Anonymity/Confidentiality:* The data will be kept anonymous and confidential. Only the research personnel directly involved with this experiment will have access to the data.

*Right to Withdraw:* You are allowed not to answer any question(s) that you choose to omit. You have the right to withdraw from this experiment at any time without penalty.

*Ethical Concerns:*
If you have any ethical concerns about this study, you may contact:
Professor Andy Adler, Chair of Research Ethics Board Carleton University Research Office Carleton University 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6 Telephone: (613) 520-2517 or E-mail: ethics@carleton.ca

---

*I have read the above description of the experiment and understand the conditions of my participation. My signature indicates that I agree to participate in this experiment and this in no way constitutes a waiver of my rights.*

| Name of Participant | Signature of Participant | Date |
|---|---|---|

| Name of Researcher | Signature of Researcher | Date |
|---|---|---|

# Appendix B

## Preliminary Study: Questionnaire

This survey asks questions about your experience with graphical passwords.

Welcome to the password grid questionnaire!

There are 26 questions in this survey

# Part 1 Background

### 1 [x]Please enter your username (Grd...)

Please write your answer here:

### 2 [1]Please select your gender

Please choose **only one** of the following:

- ○ Female
- ○ Male

### 3 [2]How old are you?

Please write your answer here:

## 4 [3]What is your occupation?

Please write your answer here:

## 5 [4]If you are a student, at what level are you studying?

Please choose **only one** of the following:

- ○ High School
- ○ Undergraduate
- ○ Masters
- ○ Ph.D.
- ○ N/A
- ○ Other

# Part 1 TAM

Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)

**6 [1]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Using this password scheme would enhance the effectiveness of my security systems. | ○ | ○ | ○ | ○ | ○ |
| Using this password scheme would improve the strength of my security systems. | ○ | ○ | ○ | ○ | ○ |
| This scheme would be useful on multiple types of devices | ○ | ○ | ○ | ○ | ○ |
| Using this password would enable me to accomplish tasks more quickly. | ○ | ○ | ○ | ○ | ○ |
| I found this password scheme very useful. | ○ | ○ | ○ | ○ | ○ |

**7 [2]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Overall I found this password scheme easy to use. | ○ | ○ | ○ | ○ | ○ |
| Learning to use this password scheme was easy. | ○ | ○ | ○ | ○ | ○ |
| My interaction with this password scheme was clear and logical. | ○ | ○ | ○ | ○ | ○ |
| It was easy to understand how this graphical password scheme works. | ○ | ○ | ○ | ○ | ○ |
| I found this password scheme to be intuitive and flexible to interact with. | ○ | ○ | ○ | ○ | ○ |

**8 [3]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| I have a generally favorable attitude toward using this password scheme. | ○ | ○ | ○ | ○ | ○ |
| I would use this password scheme for multiple touch screen devices. | ○ | ○ | ○ | ○ | ○ |
| I like the idea of using this password scheme. | ○ | ○ | ○ | ○ | ○ |
| Using this password scheme provided me with a lot of enjoyment. | ○ | ○ | ○ | ○ | ○ |
| Overall this password scheme provided me with a lot of entertainment. | ○ | ○ | ○ | ○ | ○ |

**9 [4]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| If available, I would use this password scheme on a daily basis. | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for my office | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for a safe | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for my car | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for my house | ○ | ○ | ○ | ○ | ○ |

## Part 1 Continued

**10 [1]**

**Do you currently use a password on a:**

Please choose **all** that apply:

- [ ] Mobile phone
- [ ] Tablet
- [ ] Laptop
- [ ] Large screen display
- [ ] Other:

**11 [2]**

**What type of passwords do you normally use?**

Please choose **all** that apply:

- [ ] Text-based passwords
- [ ] Voice-based passwords
- [ ] Graphical passwords
- [ ] Biometric passwords
- [ ] Tokens
- [ ] Other:

**12 [3]**

**How often do you enter a password on a touch screen device?**

Please choose **only one** of the following:

- ○ Never
- ○ 1-3 times a day
- ○ 4-6 times a day
- ○ 7-9 times a day
- ○ 10-12 times a day
- ○ More than 12 times a day

**13 [4]**

**On average how many fingers do you use when operating a:**

**(in total out of 10 fingers)**

Please write your answer(s) here:

| | |
|---|---|
| Mobile Phone | |
| Tablet | |
| Laptop | |
| Large screen display | |

**14 [5]**

**When using a password scheme, what is most important to you?**

Please number each box in order of preference from 1 to 6

- ☐ Login speed
- ☐ Password strength
- ☐ Ease of entry
- ☐ Visual Appeal
- ☐ Memorability
- ☐ Ability to enter without easedropping

# Part 2 TAM

**15 [1]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Using this password scheme would enhance the effectiveness of my security systems. | ○ | ○ | ○ | ○ | ○ |
| Using this password scheme would improve the strength of my security systems. | ○ | ○ | ○ | ○ | ○ |
| This scheme would be useful on multiple types of devices. | ○ | ○ | ○ | ○ | ○ |
| Using this password would enable me to accomplish tasks more quickly. | ○ | ○ | ○ | ○ | ○ |
| I found this password scheme very useful. | ○ | ○ | ○ | ○ | ○ |

**16 [2]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Overall I found this password scheme easy to use. | ○ | ○ | ○ | ○ | ○ |
| Learning to use this password scheme was easy. | ○ | ○ | ○ | ○ | ○ |
| My interaction with this password scheme was clear and logical. | ○ | ○ | ○ | ○ | ○ |
| It was easy to understand how this graphical password scheme works. | ○ | ○ | ○ | ○ | ○ |
| I found this password scheme to be intuitive and flexible to interact with. | ○ | ○ | ○ | ○ | ○ |

**17 [3]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| I have a generally favorable attitude toward using this password scheme. | ○ | ○ | ○ | ○ | ○ |
| I would use this password scheme for multiple touch screen devices. | ○ | ○ | ○ | ○ | ○ |
| I like the idea of using this password scheme. | ○ | ○ | ○ | ○ | ○ |
| Using this password scheme provided me with a lot of enjoyment. | ○ | ○ | ○ | ○ | ○ |
| Overall this password scheme provided me with a lot of entertainment. | ○ | ○ | ○ | ○ | ○ |

**18 [4]**

**Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, 2=Disagree, 3=Neither agree nor disagree, 4=Agree, 5=Strongly Agree)**

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| If available, I would use this password scheme on a daily basis | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for my office | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for a safe | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for my car | ○ | ○ | ○ | ○ | ○ |
| If available, I would use this password scheme as a lock for my house | ○ | ○ | ○ | ○ | ○ |

## Part 2 Continued

**19 [1]**

**Have you used a graphical password before?**

Please choose **only one** of the following:

- ○ Yes
- ○ No

**20 [2]If yes, please describe the password scheme**

Please write your answer here:

**21 [5]**

**On which of the following devices would you most likely use a graphical multi-touch password?**

Please choose **all** that apply:

- ☐ Mobile phone
- ☐ Tablet
- ☐ Laptop
- ☐ Large screen display
- ☐ Other:

**22 [6]**

**Do you think that using this graphical multi-touch password scheme will enhance the strength of your password on a:**

*

Please choose the appropriate response for each item:

| | Yes | Uncertain | No |
|---|---|---|---|
| Mobile phone | ○ | ○ | ○ |
| Tablet | ○ | ○ | ○ |
| Laptop | ○ | ○ | ○ |
| Large screen display | ○ | ○ | ○ |

**23 [7]Please number the following gestures in order of preference ***

Please number each box in order of preference from 1 to 6

- [ ] Dragging (Single Touch)
- [ ] Dragging (Multi Touch)
- [ ] Clicking (Single Touch)
- [ ] Clicking (Multi Touch)
- [ ] Rotating(Single Touch)
- [ ] Rotating(Multi Touch)

**24 [3]What do you like about this graphical password scheme?**

Please write your answer here:

**25 [4]What do you dislike about this graphical password scheme?**

Please write your answer here:

**26 [8]**

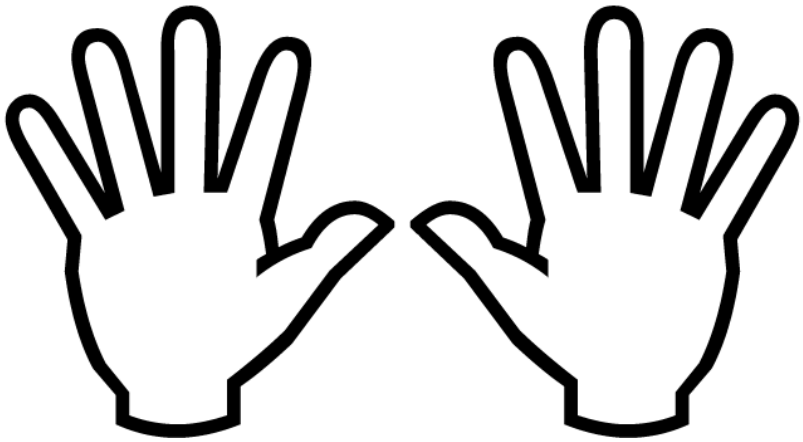
**Do you have any comments/feedback?**

Please write your answer here:

# Appendix C

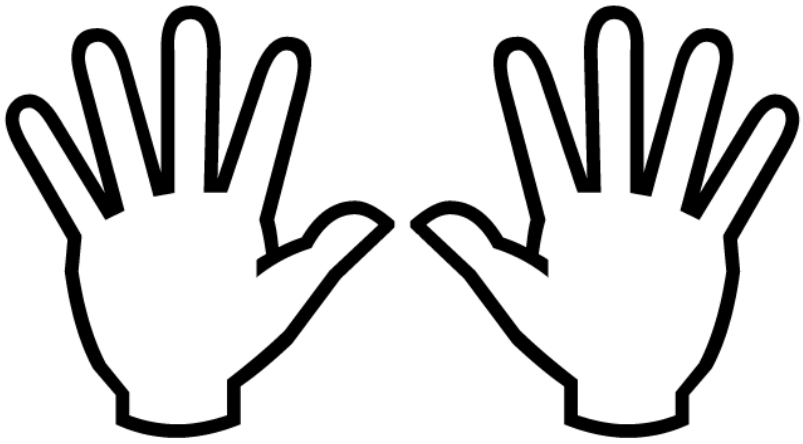
## Fingers Utilized

Device:
Creation



| | | |
|---|---|---|
| Selection: | Single touch | Multi-touch |
| Movement: | Single Drag | Multi-drag |

Login



| | | |
|---|---|---|
| Selection: | Single touch | Multi-touch |
| Movement: | Single Drag | Multi-drag |

# Appendix D

## Main Study: Informed Consent Form

**Main Study: Informed Consent Form**

*The purpose of an informed consent is to ensure that you understand the purpose of the study and the nature of your involvement. The informed consent has to provide sufficient information such that you have the opportunity to determine whether you wish to participate in the study.*

*Study Title:* Gesture Password Study


*Research Personnel:*

| | |
|---|---|
| Investigator: | Shahshuja Shahzada, shahshuja.shahzada@carleton.ca |
| Faculty Advisors: | Dr. Robert Biddle, robert_biddle@carleton.ca |
| | Dr. Sonia Chiasson, chiasson@scs.carleton.ca |


*Purpose:* The purpose of this study is to investigate the usability of a gesture based password scheme on mobile devices.

*Task Requirements:* The study involves registering, logging on and commenting on a couple of websites. Participants will also be asked to complete a few questionnaires. The study should take less than an hour during the course of three sessions.

*Potential Risk/Discomfort:* There is no known risk/discomfort greater than those encountered by participants in similar aspects of their everyday life.

*Anonymity/Confidentiality:* The data will be kept anonymous and confidential. Only the research personnel directly involved with this experiment will have access to the data.

*Right to Withdraw:* You are allowed not to answer any question(s) that you choose to omit. You have the right to withdraw from this experiment at any time without penalty.

*Ethical Concerns:*
If you have any ethical concerns about this study, you may contact:
Professor Andy Adler, Chair of Research Ethics Board Carleton University Research Office Carleton University 1125 Colonel By Drive, Ottawa, Ontario, K1S 5B6 Telephone: (613) 520-2517 or E-mail: ethics@carleton.ca

---

*I have read the above description of the experiment and understand the conditions of my participation. My signature indicates that I agree to participate in this experiment and this in no way constitutes a waiver of my rights.*

| Name of Participant | Signature of Participant | Date |
|---|---|---|

| Name of Researcher | Signature of Researcher | Date |
|---|---|---|

# Appendix E

# Main Study: Questionnaire

## Main Study: Questionnaire

*Please note that some questions are identical by design. Questions are repeated for each password scheme and during different sessions. The online version of the questionnaire clearly outlines these separations.*

## Session 1

**Please enter your username**

Please write your answer here

**Pin Questions**

Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, and 10=Strongly Agree)

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| I found this password scheme easy to understand | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Entering my password was easy to do | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I found it easy to remember my password | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I found this password scheme useful | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be hard for someone to guess my password | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be difficult for someone to see my password | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I found using this scheme to be enjoyable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| The size of the screen makes the scheme difficult to use | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would use this scheme on multiple devices | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be tedious to use this scheme on a daily basis | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would use this scheme for my email | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would not use this scheme for important accounts (online banking) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would be able to enter my password without looking | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be challenging to remember multiple passwords on this scheme | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

**Please enter your username**

Please write your answer here:

## Gesture Questions

Please choose the most appropriate number of each statement, which corresponds most closely to your desired response. (1=Strongly Disagree, and 10=Strongly Agree)

Please choose the appropriate response for each item:

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| I found this password scheme easy to understand | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| Entering my password was easy to do | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I found it easy to remember my password | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I found this password scheme useful | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be hard for someone to guess my password | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be difficult for someone to see my password | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I found using this scheme to be enjoyable | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| The size of the screen makes the scheme difficult to use | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would use this scheme on multiple devices | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be tedious to use this scheme on a daily basis | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would use this scheme for my email | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would not use this scheme for important accounts (online banking) | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| I would be able to enter my password without looking | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |
| It would be challenging to remember multiple passwords on this scheme | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

## Demographics Section:
## Please select your gender

Please choose **only one** of the following:

- ◯ Female
- ◯ Male

## Please enter your age

Please write your answer here:

## Please enter your occupation

Please write your answer here:

### If you are a student, at what level are you studying?

Please choose **only one** of the following:

- ◯ Highschool
- ◯ Undergraduate
- ◯ Masters
- ◯ Ph.D.
- ◯ N/A
- ◯ Other

## How often do you enter a password

Please choose **only one** of the following:

- ◯ Never
- ◯ 1-3 times a day
- ◯ 4-6 times a day
- ◯ 7-9 times a day

- ◯ 10-12 times a day
- ◯ More than 12 times a day
- ◯ Other

## Do you enjoy entering your passwords?

Please choose **only one** of the following:

- ◯ Yes
- ◯ No
-

## Are you right or left handed?

Please choose **only one** of the following:

- ◯ Right Handed
- ◯ Left Handed
- ◯ Other

## Which password scheme was faster?

Please choose **only one** of the following:

- ◯ Pin password
- ◯ Gesture password
- ◯ Neither

## Which password scheme was easier to remember?

Please choose **only one** of the following:

- ◯ Pin password

- ◯ Gesture password
- ◯ Neither

## What did you dislike about the gesture password scheme?

Please write your answer here:

## What did you like about the gesture password scheme?

Please write your answer here:

## What did you dislike about the pin password scheme?

Please write your answer here:

## What did you like about the pin password scheme?

Please write your answer here:

## Session 2

**Please enter your username**

Please write your answer here:

**Which password scheme was faster? (for login)**

Please choose **only one** of the following:

- ○ Pin password
- ○ Gesture password
- ○ Neither

**Which password scheme was easier to remember?**

Please choose **only one** of the following:

- ○ Pin password
- ○ Gesture password
- ○ Neither

**What did you dislike about the gesture password?**

Please write your answer here:

**What did you like about the gesture password?**

Please write your answer here:

**What did you dislike about the pin password?**

Please write your answer here:

**What did you like about the pin password?**

Please write your answer here:

## Session 3

**Please enter your username**

Please write your answer here:

**What password scheme was faster? (for login)**

Please choose **only one** of the following:

- ○ Pin password
- ○ Gesture password
- ○ Neither

**Which password scheme was easier to remember?**

Please choose **only one** of the following:

- ○ Pin password
- ○ Gesture password
- ○ Neither

**Do you have any other feedback about the two different password schemes?**

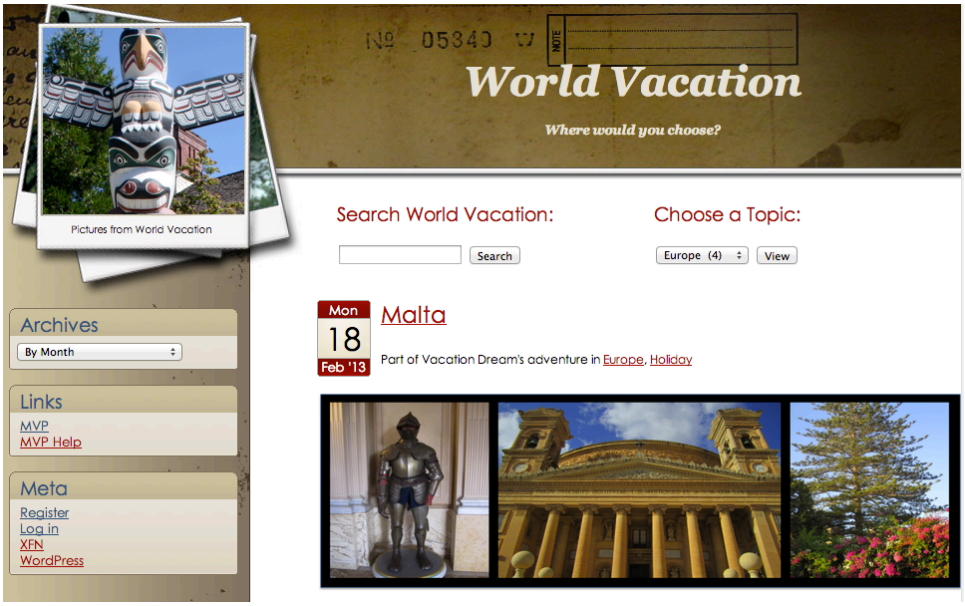
Please write your answer here:

# Appendix F

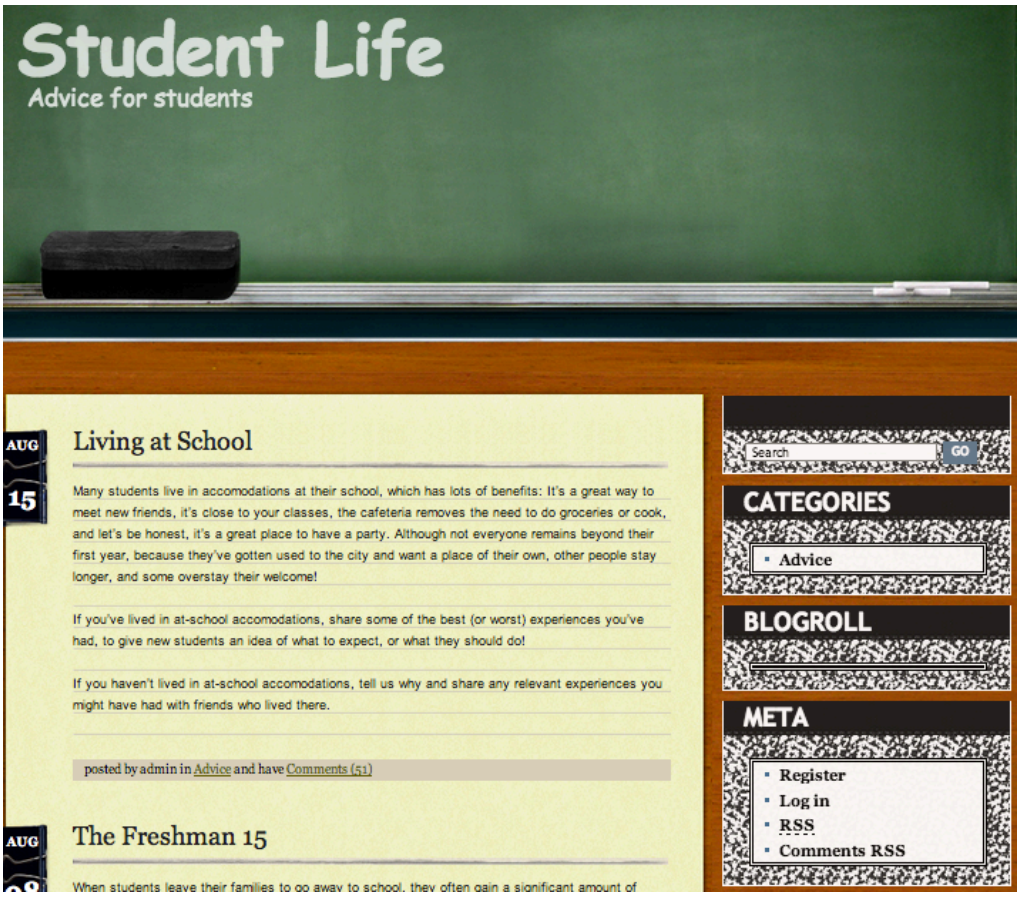
## Main Study: Websites

Study Websites

World Vacation:




Student Life:



# Appendix G

## Preliminary Study: Ethics Clearance Form

Carleton University
Canada's Capital University

**Carleton University Research Office**
Research Ethics Board
1325 Dunton Tower
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada
Tel: 613-520-2517
ethics@carleton.ca

## Ethics Clearance Form

This is to certify that the Carleton University Research Ethics Board has examined the application for ethical clearance. The REB found the research project to meet appropriate ethical standards as outlined in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition* and, the *Carleton University Policies and Procedures for the Ethical Conduct of Research*.

**X New clearance**
**□ Renewal of original clearance** **Original date of clearance:**

| | |
|---|---|
| Date of clearance | **18 July 2013** |
| Researcher | **Shahshuja Shahzada, Master's student** |
| Department | **School of Information technology, Human Computer Interaction** |
| Supervisor | **Prof. Robert Biddle and Prof. Sonia Chiasson, School of Computer Science** |
| Project number | **14-0451** |
| Title of project | **An evaluation of multi-touch passwords** |

Clearance expires: **31 May 2014**

**All researchers are governed by the following conditions:**

**Annual Status Report:** You are required to submit an Annual Status Report to either renew clearance or close the file. Failure to submit the Annual Status Report will result in the immediate suspension of the project. Funded projects will have accounts suspended until the report is submitted and approved.

**Changes to the project:** Any changes to the project must be submitted to the Carleton University Research Ethics Board for approval. All changes must be approved prior to the continuance of the research.

**Adverse events:** Should any participant suffer adversely from their participation in the project you are required to report the matter to the Carleton University Research Ethics Board. You must submit a written record of the event and indicate what steps you have taken to resolve the situation.

**Suspension or termination of clearance:** Failure to conduct the research in accordance with the principles of the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition* and the *Carleton University Policies and Procedures for the Ethical Conduct of Research* may result in the suspension or termination of the research project.

Andy Adler, Chair
Carleton University Research Ethics Board

Louise Heslop, Vice-Chair
Carleton University Research Ethics Board

## Appendix H

## Main Study: Ethics Clearance Form

Carleton University
Canada's Capital University

**Carleton University Research Office**
Research Ethics Board
1325 Dunton Tower
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada
Tel: 613-520-2517
ethics@carleton.ca

## Ethics Clearance Form

This is to certify that the Carleton University Research Ethics Board has examined the application for ethical clearance. The REB found the research project to meet appropriate ethical standards as outlined in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition* and, the *Carleton University Policies and Procedures for the Ethical Conduct of Research*.

**X New clearance**
**□ Renewal of original clearance** **Original date of clearance:**

| | |
|---|---|
| Date of clearance | **11 November 2013** |
| Researcher | **Shahshuja Shahzada, Master's student** |
| Department | **School of Computer Science** |
| Supervisor | **Prof. Robert Biddle and Prof. Sonia Chiasson, School of Computer Science** |
| Project number | **100601** |
| Title of project | **Gesture Password Study** |

Clearance expires: **31 May 2014**

**All researchers are governed by the following conditions:**

**Annual Status Report:** You are required to submit an Annual Status Report to either renew clearance or close the file. Failure to submit the Annual Status Report will result in the immediate suspension of the project. Funded projects will have accounts suspended until the report is submitted and approved.

**Changes to the project:** Any changes to the project must be submitted to the Carleton University Research Ethics Board for approval. All changes must be approved prior to the continuance of the research.

**Adverse events:** Should any participant suffer adversely from their participation in the project you are required to report the matter to the Carleton University Research Ethics Board. You must submit a written record of the event and indicate what steps you have taken to resolve the situation.

**Suspension or termination of clearance:** Failure to conduct the research in accordance with the principles of the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition* and the *Carleton University Policies and Procedures for the Ethical Conduct of Research* may result in the suspension or termination of the research project.

Andy Adler, Chair
Carleton University Research Ethics Board

Louise Heslop, Vice-Chair
Carleton University Research Ethics Board