A GRAPHICAL PASSWORD SCHEME FOR MOBILE DEVICES

by
Hsin-Yi Chiang

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

MASTER OF SCIENCE

School of Computer Science

at

CARLETON UNIVERSITY

Ottawa, Ontario
January, 2013

Abstract

Typing text passwords using touchscreens can be challenging on mobile devices. We designed a new graphical password scheme called ***T****ouchscreen* ***M****ulti-layered* ***D****rawing* (TMD) for use with touchscreens.

We conducted a preliminary study of existing graphical passwords on smart phones and tablets. Based on our findings, we designed a scheme that avoids the fuzzy boundaries problem without memorizing images.

TMD is a user-drawn graphical password scheme addressing these issues. With the use of *warp cells*, TMD allows users to continuously draw their passwords across multiple layers in order to create more complex passwords than normally possible on a small screen.

We compared the usability of TMD to Draw A Secret (DAS) on a tablet computer and a smart phone. Results showed that TMD passwords are more memorable and eliminated the fuzzy boundaries problem. Also, participants preferred using TMD than DAS to replace text passwords on mobile devices.

Acknowledgements

First and foremost, I would like to thank my supervisor Sonia Chiasson. This thesis would not have been possible without her excellent guidance, countless encouragements and limitless patience. Sonia, thank you very much and I am very proud to be your student.

Many thanks to the members of my committee, Tara Whalen, Tim Lethbridge and Anil Somayaji, for your guidance and support for this thesis.

I would like to thank NSERC ISSNet for funding the user studies in this thesis so I was able to gather valuable data for analysis.

I would like to thank Murray Christopherson for his help running the user study.

Thanks to all my friends for their support and help throughout the course of this thesis.

Last but not least, I would like to thank my parents. Thank you for all the support and love that you have given me.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Research Question

Mobile devices have the ability to connect to the internet and access various personalized remote services. These services often ask users to identify themselves using text passwords; this requires typing on the mobile devices. Modern mobile device interfaces are heavily graphic-oriented and touchscreens are typically used as the primary input method. Regardless of how mobile device software simulates physical keyboards, physical constraints like screen sizes make typing on touchscreens less accurate and less efficient when compared to physical keyboards [17, 59]. As a result, typing text passwords can be challenging. With this observation, the question arises: *Is there an alternative type of authentication that can be easily deployed like text passwords but without loss of usability due to the physical constraints of mobile devices?* Our goal in this thesis is to design a new graphical password scheme optimized for mobile devices with touchscreens.

1.2 Motivation

Mobile devices such as smart phones and tablet computers have evolved very quickly. Built with powerful processors and connected to high speed networks, mobile devices are capable of executing users' daily tasks such as browsing the internet, managing bank accounts, storing personal data, or socializing with others. Major mobile operating system companies such as Google and Apple have been improving the development environment for their products, encouraging the development of new applications. With the increasing number of applications and more data being exchanged,

the protection of private information is becoming very challenging.

Text-based passwords are the most popular authentication scheme for various local or remote services. Theoretically, properly defined text passwords have a password space that is sufficiently large to be considered secure [27]. However, practical deployment has some drawbacks due to human factors [58, 76]:

1. Users often choose insecure passwords; [2]
2. Users often reuse their passwords for multiple accounts [3];
3. Secure passwords are hard to remember by humans [76];
4. Users sometimes write their password down [58];

On the other hand, the scheme has some advantages which makes it the most used scheme:

1. Users are very familiar with how the scheme works;
2. It requires no special hardware to deploy;
3. A user can have multiple text passwords which are not related to each other or personally identifiable;

Using a text-based password with a regular computer is very easy because desktop and laptop computers are equipped with physical keyboards. On a standard physical keyboard, the size of each key and the layout of the keys are comfortable for most users. In addition, a physical keyboard provides tactile feedback to users. Most mobile devices nowadays are equipped with touchscreens and have no physical keyboards. Mobile devices use virtual keyboards when typing is needed; however, virtual keyboards might have different layouts. Figure 1.1 offers screenshots of the virtual keyboards of the Android and iOS operating systems. Typing with a virtual keyboard on a touchscreen has been well studied [17, 32, 59]. Results show that when typing on a touchscreen, users generally do not perform as well as they would using a physical keyboard.

(a) Android keyboard layout

(b) iOS keyboard layout

Figure 1.1: Virtual keyboard layout for mobile devices

Given the usability issues with virtual keyboards, will non-text-based passwords be a good alternative to authenticate users on mobile devices? A potential alternative is to explore the use of graphical passwords. A graphical password [8] is a secret that is entered or displayed in the form of drawings, icons or graphics. Graphical passwords are suitable candidates for several reasons:

1. Almost all mobile operating systems are graphically oriented; graphical password schemes are graphically oriented as well;

2. Touchscreens are well-suited as an input device for graphical passwords;

3. Deploying graphical passwords on mobile devices does not require additional hardware;

4. Graphical passwords are more memorable than text passwords [12];

5. Graphical passwords are harder for users to write down or share;

6. Attacks on graphical passwords must be customized to each specific scheme.

For these reasons, we chose to investigate their use on mobile devices.

1.3 Contribution

This thesis includes three main contributions:

1. A 31-user comparative study of three existing graphical password schemes that we implemented on smart phone and tablet computers;

2. The design and implementation of TMD — a new graphical password scheme specific for small touchscreens;

3. A 90-user one-week study comparing TMD to the existing Draw A Secret scheme on smart phone and tablet computers.

We conducted two formal user studies in this thesis. The first study was to identify problems that users might encounter when using graphical password schemes on mobile devices. We chose a representative scheme from three main categories [8]: *recall*, *cued-recall*, and *recognition*. 31 participants tested DAS [45], PCCP [11] and Object Recognition [39] using a smart phone or a tablet computer. The results indicated that the user-drawn graphical password scheme (DAS) was affected by the screen size due to accuracy problems. From the user responses, we saw that users did not like to remember unfamiliar images as part of their passwords (PCCP and Object Recognition).

We propose a new graphical password scheme designed to use with touchscreens; we call this scheme: ***T****ouchscreen* ***M****ulti-layered* ***D****rawing* or *TMD*. TMD is a user-drawn graphical password scheme with an interface composed of a grid of large cells that are not attached to each other. The size of the cell was intended to reduce the accuracy problem and the space between the cells was intended to eliminate the fuzzy boundaries problem. We used multiple layers of grids to allow users to create more complex passwords even on a small touchscreen. No buttons are used in the main

interface to maximize the grid size.

(3) The second study was to evaluate the usability of TMD on mobile devices by comparing it with DAS; again, we used a smart phone and a tablet computer for this study. The overall result of our second user study was favourable for TMD. First, we determined that TMD passwords were more memorable than DAS a week after they were created. Second, user responses indicated that participants were more willing to use TMD than DAS to replace text passwords on mobile devices. Third, our observations showed that TMD users did not have the fuzzy boundaries problem [24] common in DAS.

1.4 Thesis Outline

This thesis is organized as follows: In chapter two, we review prior work related to mobile device authentication and graphical passwords; in chapter three, we describe our preliminary user study testing three existing graphical passwords on smart phones and tablets; in chapter four, we describe and discuss the design of TMD; in chapter five, we describe a user study evaluating TMD; and finally, in chapter six, present some conclusions from our user studies and discuss future work.

Chapter 2

Background

In this chapter, we first talk briefly about the importance of user authentication on mobile devices. Knowing that users are typically authenticated using text passwords [16] and typing text on mobile devices using touchscreens can be difficult [17, 32, 59], we then look at some alternative solutions others have proposed to authenticate users on mobile devices without typing. Having selected graphical password schemes as our solution, we summarize the relevant graphical password literature and discuss possible attacks.

2.1 Authentication on Mobile Devices

As mobile devices become more powerful and compact, they have become a necessity for modern users. Because of the devices' portability, users are able to use them to handle their daily tasks such as managing bank accounts, accessing social media, answering personal e-mails, or connecting to a virtual private network (VPN) when they are away from their desks. Many of these tasks involve accessing of private information; therefore, mobile devices are often protected with passwords to prevent others from accessing the information. There are two cases when a mobile device user is required to be authenticated; the first case is when accessing online services through web browsers or applications and the second is when accessing local services or changing important settings. In Herley et al.'s study [38], a text password is most commonly used to authenticate users for different services. Choosing text passwords as the authentication scheme has several benefits which other schemes do not have. First of all, text passwords are very easy to implement and deploy on multiple platforms. Second, text passwords are well understood by users so the scheme has

very high usability. Third, unlike biometric passwords which are created based on users' behavioural or physical characteristics, it is very easy to create multiple text passwords. Fourth, text-based passwords do not require users to carry additional hardware such as physical tokens to authenticate. Although there are many benefits using the text-based passwords, the scheme also has some disadvantages such as: Users often choose weak passwords [38, 51]; the password is hard to remember when it is secure [76]; and users often write down their passwords [58]. To authenticate users on mobile devices locally, PINs are the most commonly used according to Clarke and Furnell's survey on mobile device authentication schemes [16]. As a subset of the text passwords, PINs are also susceptible to all the weaknesses of text-based passwords [51].

Taking the advantages of mobility, connectivity, and personalization, some services use the ownership of mobile devices as part of the authentication process. Since the operator and the owner of a mobile device can be different from each other, it is very important to authenticate the users before granting access to the services. The following are two example services that authenticate users using mobile devices.

2.1.1 Two Factor Authentication

Because mobile devices are designed as non-shareable devices, the devices are sometimes used as a factor in an authentication scheme. A few recent examples of such mechanisms are Google Gmail's 2-step verification option [31] and Mobile-OTP (mobile one time password) [49]. In addition to regular text passwords, the systems send out a single-use password to the registered mobile devices which is used to complete the authentication process. In these two examples, the users are authenticated based on ownership of the mobile device. Similar to a house key or car key, the systems cannot determine who currently has the mobile device. In the case of loss or theft, it is very important to prevent non-owners from accessing the system by additionally authenticating users directly on the mobile device.

2.1.2 Authentication for Mobile Payments

Another application that needs to authenticate users on mobile devices is a mobile payment system. Also called mobile money transfer, mobile money, or mobile wallet, this payment system uses an internet-enabled mobile device as the physical token to prove the identity of the payer. Many forms of mobile payment systems have been proposed and implemented, some examples include: SMS based transaction by Espirity [42], WAP (Wireless Application Protocol) payment by Netsize and txtNation [53,67], or NFC (Near Field Communication) payment by Google [30]. Payment details are entered on the phone by the user either by typing text (SMS payment), going to a particular web page (WAP billing) or scanning a NFC tag (NFC payment). This information is sent to the service provider through the internet and the transaction is completed based on the preregistered payment options. In these three examples, the payment accounts are protected by text passwords to prevent unauthorized access.

2.2 Text Typing on Touchscreens

Efficient text entry is a challenge because mobile devices do not use physical standard keyboards as the input interface and they have enough surface area for users to type with one or two fingers only. A common solution is to use a virtual keyboard as the main interface for inputting text. A virtual keyboard is a simulation of a physical keyboard on touchscreens. Due to size constraints on some mobile devices, virtual keyboards have not only a much smaller key size and key space (the distance between keys) but also fewer keys than desktop physical keyboards.

Later studies have shown that the size of the keys on virtual keyboards can affect the speed and the accuracy of typing [17, 32, 59]. More recent studies have shifted the focus from virtual keyboards to general soft keys (simulated buttons on touchscreens) [37,55] and similar results are concluded. Experiments by Henze et al. [37] have shown that the target size affects both the accuracy and the speed of the touches. Figure

2.1 shows the relationship between the target size and the error rate [37]. A similar study conducted by Lee and Zhai [47] determined that button sizes can affect the performance, especially when the buttons are smaller than 10 mm in width.

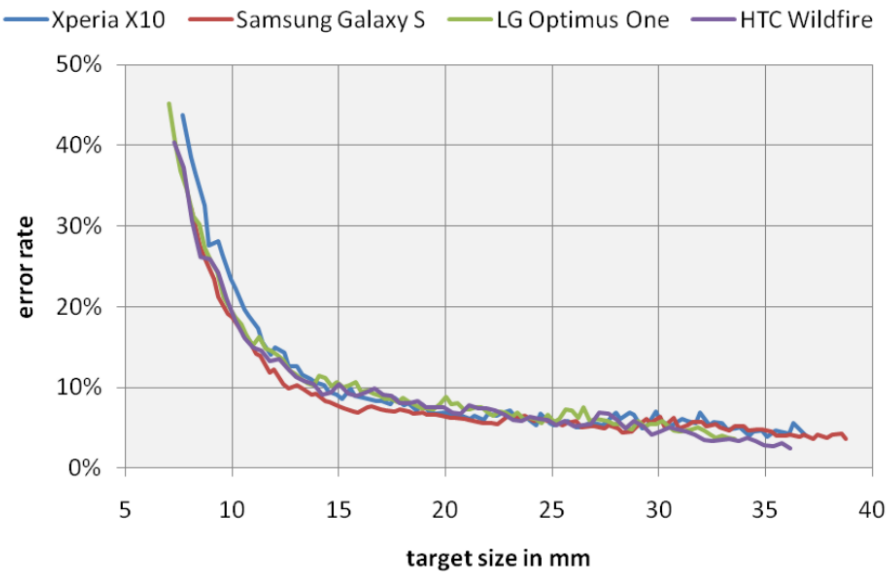


Figure 2.1: Relationship between the target size the error rate [37]

Much effort has been dedicated to increasing the usability of virtual keyboards. Perlin proposed Quikwriting [56] which combines virtual keyboards and gestures, figure 2.2 is an example of the Quikwriting interface. Another example that combines gestures and a virtual keyboard is Ward et al.'s Dasher [70]. In these proposed schemes, gestures allow users to select the letters of a word with one continuous swipe motion, deemed easier than typing individual keys.

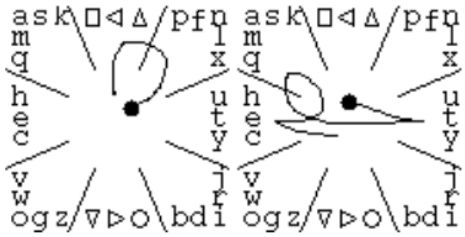


Figure 2.2: Using Quikwriting to write 'f' and 'the' [56]

Another approach to increasing usability of the virtual keyboards is to change the shape or arrangement of the keys on the virtual keyboard. Further details are available

in a survey by MacKenzie et al. [48] who compared and evaluated many proposed keyboard layouts and tried to determine the factors that affect typing speed. Zhai et al. [79] designed two virtual keyboards layouts using quantitative techniques which allowed users to type faster than using a virtual QWERTY keyboard. In addition, Faraj et al.'s [25] designed a virtual keyboard called *BigKey* which they claimed can improve typing performance. However, Gunawardana et al. [33] described in their study how key-target resizing can violate user expectations resulting low performance.

2.3 Alternative Solutions for User Authentication on Mobile Devices

Many schemes with different approaches have been proposed to authenticate users without having them type passwords. In general, there are three categories of authentication mechanisms that can be used to identify users [73]: ownership, biometric, and knowledge. In each category, the schemes use properties that are unique to each user to identify them. Table 2.1 defines and provides examples of each category. In the following subsections, we discuss some alternative solutions in each category, focusing on solutions intended for mobile devices such as tablet computers and smart phones.

Factors	**Definition**	**Examples**
Knowledge	Something the user knows	Text passwords, graphical passwords, PINs, or challenge response
Ownership	Something the user owns	ID cards, mobile phones, hardware tokens, or soft tokens
Biometric	Something the user is (physical or behavioral)	DNA, fingerprints, voice, or typing habits

Table 2.1: Authentication types

2.3.1 Knowledge-based Solutions

Mobile users often need to login to multiple accounts or the same accounts several times a day which can be inconvenient if the passwords are long and complex. One

solution to reduce the amount of typing required is to use a password manager. A password manager is a database which stores unique passwords for various accounts; it is usually guarded by a single master password [6]. The benefit of using a password manager is that users need only remember and type one password but can login to multiple websites with unique passwords. In addition, secure passwords that are strong against dictionary attacks can be used without having to remember them since the passwords are stored in the password manager. There are many commercial or open source password managers available for smart phone platforms; a survey done by Belenko and Sklyarov listed and analyzed many password managers of this kind [6]. Password managers also have some disadvantages. Studies of password managers identified potential security issues [13, 35]: First, if the master password is compromised then all the managed accounts are compromised because all of the user's passwords are typically protected by a single user-created master password; also, the strength of the password database encryption might also cause security issues [58]. In addition, Chiasson et al.'s study [13] uncovered some usability issues with password managers that might raise security concerns.

Another solution to decrease typing of passwords on mobile devices is to use graphical password authentication schemes. Unlike traditional knowledge-based authentication schemes that use alphanumeric characters to represent the password, graphical passwords use images, shapes or drawings to represent the passwords [1]. Nelson, Reed and Walling's study on human learning and memory [52] shows that pictures or images are generally more easily remembered than text. In other words, using graphics instead of text for passwords may decrease the difficulty for users to remember them. There are many types of graphical passwords and many graphical password schemes have been proposed [1]; because this is directly related to our study, we will discuss graphical passwords in more details in section 2.4.

2.3.2 Ownership-based Solutions

Bojinov and Boneh [9] proposed a mobile authentication scheme using hardware tokens. They designed two types of hardware tokens, magnetic and acoustic, that can

emit sound waves or magnetic fields. By using a mobile device's build-in microphone and compass as the receiver, users can be authenticated if the emitted sound or magnetic patterns matches the secret. The authors also discussed the possibilities of using lights (QR code) or gravity (accelerometer) as the transmission medium. The benefit of this solution is that the mobile user does not need to remember any secret to be identified. In addition, because the tokens communicate to the mobile devices through existing hardware, the solution can easily be deployed without having to modify the mobile devices.

A solution proposed by Syta, Kurkovsky and Casano [61] is to use RFID technology to authenticate users on mobile devices. Syta et al. exploit the idea of using RFID tags named RFID-AM (RFID-based Authentication Middleware), a non-contact sensor technology, as a physical token. When authenticating users, the mobile device uses its build-in sensor to detect the presence of the RFID-AM. If a RFID-AM is detected, mobile devices can determine if the current user is authorized to access the services by reading the tag contents. Also, the authors suggested that the token can be used in "continuous authentication" which continuously authenticates users for every operation. The advantages of using RFID-AM to authenticate mobile users are: the authentication process is transparent for users; no actions are required from users; RFID tags and readers are very cost-effective and reliable; and RFID-AM can authenticate users for every operation to prevent unauthorized operation. In this solution, the RFID tags used might post some security issues such as the potential for relay attacks [19, 36, 46]. A relay attack is a type of attack which combines man-in-the-middle and replay attacks. In a typical relay attack, the attacker tries to read the target RFID tag when it is outside the range of a valid reader and relay the message to a valid receiver.

2.3.3 Biometric-based Solutions

Biometric-based solutions can be divided into two subsets: physical and behavioral biometrics. Physical biometrics are based on users' physical characteristics whereas behavioral biometrics are based on users' behavior patterns (such as typing or speech

patterns).

A physical biometric solution proposed by Uchida [68] uses fingerprint identification technology to authenticate users on mobile devices. The fingerprint-based user interface, or FpUI, uses a fingerprint scanner that is attached to the mobile device to scan the user's fingerprints. Once the fingerprint information has been gathered, the data is simplified by going through a feature extraction process. The simplified data is sent to a remote server through a secure connection for matching. If a match is found in the database, then the user is granted access. In this study, Uchida also described the possibility of using FpUI as an external authenticating scheme for third party services.

Ijiri, Sakuragi and Lao [41] explored the idea of using human facial features as the key to authenticate users. Ijiri et al. designed and implemented a fully functional face verification and identification system on a mobile phone. The proposed scheme uses the algorithm described by Wu, Huang and Lao's study on face detection [74]. Wu et al.'s algorithm allows mobile phones to capture users' facial features despite the rotation, size or lighting of the face. This scheme authenticates users by scoring the likelihood that the captured face matches the record in the database. However, facial recognition technology is still imperfect; the results might be affected by facial expression, aging, marks or makeup [43].

A behavioral biometric solution was proposed by Barua [5] using voice verification to authenticate users. The system is designed to authenticate users before they attempt to dial certain restricted numbers on a mobile phone by using voiceprint as the key. Although voice recognition has been around for a while, there are still some problems with the technology. A recent survey [57] on voice recognition systems pointed out that these systems still cannot reach perfect results which means there is still a chance for the system to falsely accept or reject users especially in noisy environments where someone might use a mobile device. Another behavioral biometric solution is to use keystroke dynamics [15,77]. Keystroke dynamics is the study of the patterns or timing details when users are typing on a keyboard. Two user characteristics are measured

in this scheme: the keystroke latency (the time between two keystrokes) and hold-time (the time of a single keystroke). By analyzing the patterns, mobile applications are able to identify the users. However, studies has shown that keystroke dynamics cannot be very accurate because typing patterns do not remain stable over time [7,50].

In the this section, we discussed some solutions that have been proposed to allow users to more easily authenticate on mobile devices. Table 2.2 is a summary of the three categories of authentication schemes. From the summary, we see that token or physical biometric based scheme cannot be easily deployed on most current mobile devices because they require specific hardware. Furthermore, although appropriate in some circumstances, they are not viable in all cases. It seems that knowledge-based options remain necessary for many applications.

2.4 Graphical Passwords

We decided to explore the possibility of using graphical password schemes on mobile devices. The reasons for this decision are:

1. Graphical password schemes require only a touchscreen for input and these are available on most recently built mobile devices.

2. The process of authenticating users using graphical password is similar to text password which can be easily understood by users.

3. Graphical password schemes require minimal typing which is very suitable for touchscreens.

4. Graphical password schemes can be used on mobile devices and desktop computers, so users do not need to change the way they login for different environments.

5. Graphical passwords have memorability advantages over text passwords [52].

			Biometric	
	Knowledge	**Token**	**Physical**	**Behavioural**
Memorability	Users need to remember secrets. The capacity of human memory is limited and decays over time [58]	Users do not need to remember any secrets but must remember to carry the tokens	Users do not need to remember any secrets	Users do not need to remember any secrets
Privacy	No direct connection between users and passwords	No direct connection between users and passwords	Direct connection between users and passwords	Direct connection between the users and passwords
System Error Rate	Low, user inputs are directly compared with the database	Low, user inputs are directly compared with the database	System decisions are based on threshold values [57]	System decisions are based on threshold values [57]
Required Hardware	Requires touchscreens (graphical based), mouse (graphical based) or keyboards (text-based) for user input	Schemes require readers to read tokens (e.g., NFC, smart card reader)	Requires readers to read biometric information (e.g., fingerprint reader)	Uses existing hardware to record user input (i.e., keyboard, microphone)

Table 2.2: Summary of authentication schemes based on the categories

2.4.1 Password Spaces

Throughout this thesis, we use the term *password space* to describe the strength of passwords. In computer security, the term *password space* refers to the set of all possible combinations which a password scheme can produce. We often convert the total to base-2 and refer to the number of bits to represent the number of combinations. For example, there are 94 alphanumeric and type-able symbols on a standard

keyboard. If we were to create an 8-character text password using the keyboard, the password space would be $94^8 = 6.09 \times 10^{15}$ or approximately 52 bits. There are two types of password spaces commonly discussed in the literature. The *theoretical password space* is the number of all possible combinations of a password scheme and *effective password space* is the number of combinations that is used more often by the users. Ideally, the theoretical and effective password spaces are identical to maximize security against guessing attacks. In practice, the effective password space is usually smaller since users are unlikely to select completely random passwords. Of course, when passwords are randomly assigned, then the two spaces are the same.

2.4.2 Fitts' Law and Graphical Passwords

Proposed by Fitts [26] in 1954, Fitts' law explains the tradeoff between the speed and the accuracy of human movements. The law states that the time required for a user to reach a target depends on the size of the target and the distance between the resting position and the target. As the target becomes smaller or further away, the time needed to reach the target increases. In addition, the law also states that the accuracy of the reaches decreases if the movement speed increases or the target size decreases. Sears et al. [60] suggested that Fitts' law can be applied to selection tasks on touchscreens.

However, it is unclear whether this law applies to passwords because it contradicts some of the important security requirements with the respect to maximizing the password space. First, we encourage users to select password components that are randomly distributed across the screen. Second, we want to maximize the number of targets. This means the individual target sizes should be as small as possible while still maintaining acceptable usability of the scheme.

2.4.3 Types of Graphical Passwords

Surveys of graphical passwords schemes [1, 8] classified the schemes into three categories: recall, recognition, and cued-recall. Each category allows users to manipulate images differently, as described in table 2.3. We next describe in more detail several example schemes from each category.

Category	Method of authentication	Examples
Recall	Users remember a drawing which they have created before. Usually no hint is given.	Draw A Secret (DAS) [45], Pass-Go [63]
Recognition	Users recognize a set of objects which they selected before.	Image selection [44], pict-O-lock [40], Passfaces^{TM} [18]
Cued-recall	Users remember a sequence of points which they have chosen before. Visual cues are given as references or hints.	Background DAS [24], PassPoints [71]

Table 2.3: Types of graphical password schemes

Recall-based Graphical Password Schemes

One of the earliest and most commonly cited recall-based graphical password schemes is DAS (Draw A Secret). Proposed by Jermyn et al. in 1999 [45], DAS allows users to draw their passwords on a two-dimensional grid using one or more lines. Each grid cell is given unique coordinates which are used to encode the password from graphic to text. To transform a drawing into text, the algorithm records the sequence of grid cells crossed by the user's stroke. The start and end of the stroke are also recorded. An example is shown in figure 2.3. In this example the text password generated is: *pen-down, (2,2), (3,2), (3,3), (2,3), (2,2), (2,1), (5,5), pen-up.* In terms of weakness, DAS is known to be susceptible to dictionary attacks [54] because users tend to draw their password in predictable patterns. The password space of DAS was calculated using recursive methods, for DAS passwords with maximum length of 10, the password space is 48 bits [45].

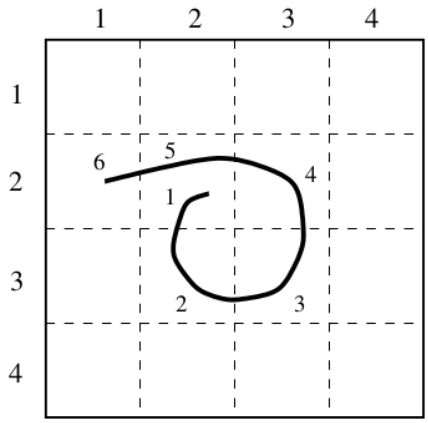


Figure 2.3: Example of DAS (Draw A Secret) on a 4×4 Grid [45]

An improved version of DAS, proposed by Thorpe and van Oorschot in 2004, is called Grid Selection [65]. In the ordinary DAS scheme, users are given a grid and they use the entire space to draw their passwords. However, user-selected passwords frequently have small stroke counts or have no strokes of length one, decreasing the password space dramatically. To reinforce the security of the scheme, Thorpe and van Oorschot proposed the *Grid Selection* the scheme that includes an additional step before drawing. As shown in figure 2.4, the size of the grid in this scheme is significantly more dense than the grid used in the DAS study [45]. Before drawing their password, users select a section of the grid as their drawing grid. In this example figure, the user selected the area created by **ps** and **pe** as the drawing grid. With this mandatory selection process, the password space of the scheme is increased.

Pass-Go was proposed by Tao and Adams in 2008 [63]. It was inspired by the old Chinese game Go due to its interface that looks like a Go board. In this scheme, the password is created by drawing on the screen like DAS; however, Pass-Go asks users draw their passwords by connecting the intersections of the grid lines. From figure 2.5, we can see the design of Pass-Go and an example password. Pass-Go also allows users to select the color of the strokes as an additional option which increases the password space. The full password space of Pass-Go on a 9×9 grid with one or eight available colors was calculated in the literature [63], the full password space of Pass-Go passwords with a length of 10 and under is 64 bits with single color and 94

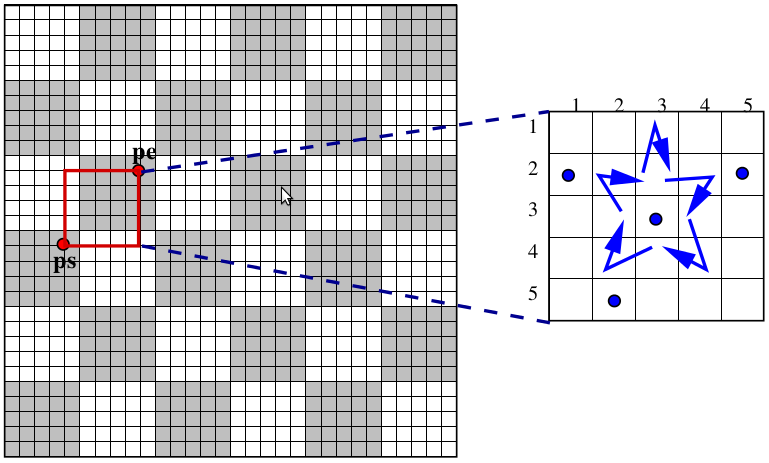


Figure 2.4: Grid selection scheme [65]

bits with eight colors. Tao and Adams argued that the full password space of Pass-Go is larger than DAS with the same grid size.

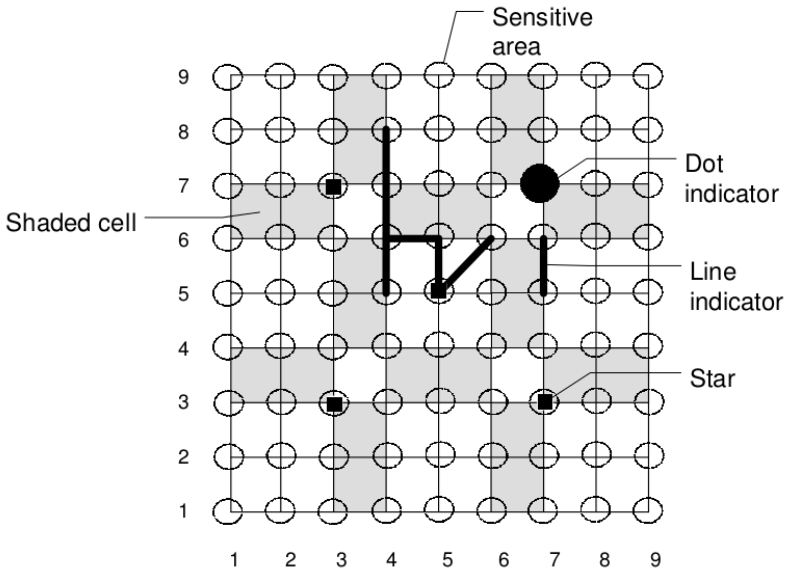
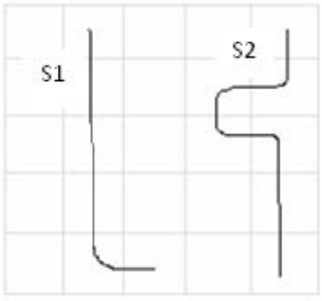


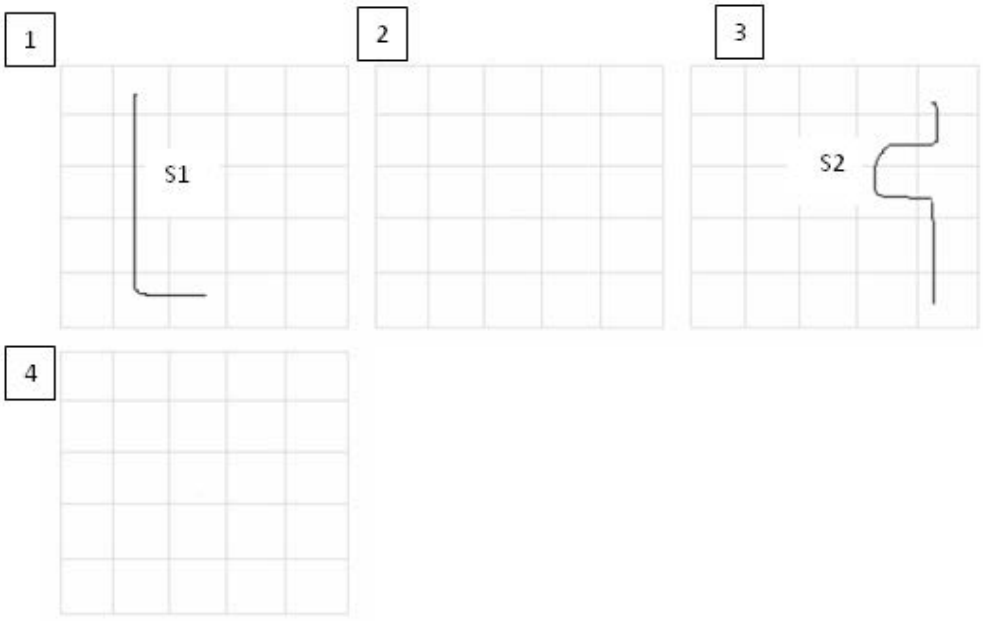
Figure 2.5: Interface of Pass-Go scheme [63]

Considering that recall-based graphical passwords are vulnerable to shoulder surfing, Zakaria et al. [78] proposed three techniques that can be used to against such attacks. Using DAS (Draw A Secret) [45] and BDAS (Background Draw A Secret, an alternative DAS which uses background images to enhance usability and security) [24] as

the test schemes, the three techniques are tested: decoy strokes, disappearing strokes, and line snaking. In each technique, the authors tried to improve security by manipulating the lines in different ways so that bystanders cannot see the password easily. The results showed that only disappearing strokes and line snaking improves the security of the schemes and disappearing strokes is the most acceptable by the users when comparing the three techniques. Figure 2.6 and 2.7 show how the disappearing stroke and the line snaking techniques work.



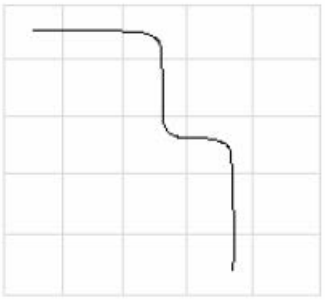
(a) The actual password



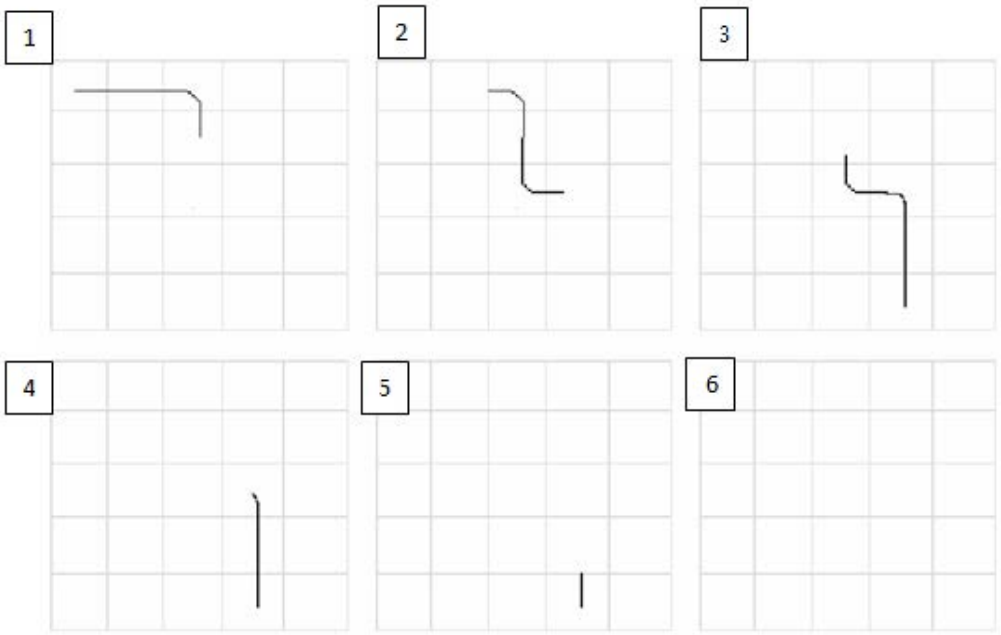
(b) Strokes are hidden after drawing

Figure 2.6: Decoy stroke defense [78]

Generally, recall-based graphical password schemes authenticate users by having them draw secret images on a grid which are then translated to a set of coordinates; usually



(a) The actual password



(b) The tail of the stroke is erased after a short time, leaving only the most recent portion of the drawing

Figure 2.7: Line snaking defense [78]

no hints are given to the users.

The Android operating system develop by Google Inc. uses graphical passwords to prevent unauthorized users from unlocking the screen of a mobile device (figure 2.8). Similar to the Pass-Go [63], Android pattern unlock scheme uses the intersections of a 2×2 grid where the user selects a series of intersections with one smooth gesture. Users are allowed to select each of the intersections at most once; however, they are allowed to go through the selected intersections in order to reach a new intersection. The

Android pattern unlock scheme has 389,112 possible combinations [4]. The scheme cannot be a replacement of text password because its password space is only $2^{18.5}$ bits long or approximately equivalent to a 5 digit PIN number. The Android pattern unlock scheme is susceptible to a smudge attack [4] which we will discuss more in section 2.4.4.

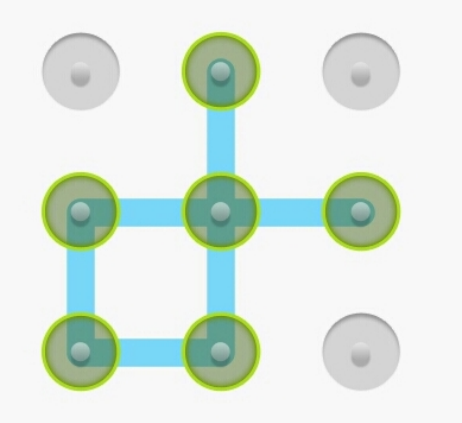


Figure 2.8: The Android pattern unlock scheme

Recognition-based Graphical Password Schemes

Passfaces^{TM} [18] is one of the most studied commercial recognition-based scheme [10,23,69]. In Passfaces^{TM}, users select faces from a series of screens. There are a total of three screens consisting of nine faces each and the user has to select their previously memorized face on each screen to be authenticated. Figure 2.9 shows an example screen for Passfaces^{TM}. Since the password space of Passfaces^{TM} is very limited ($9^3 = 729 \approx 2^{9.5}$), Passfaces^{TM} cannot be a direct replacement of text passwords but could be used as an additional security measure for an existing authentication scheme. A security risk for the scheme was discovered in Dunphy et al.'s study [23]; they discovered that it is possible for a malicious user to login based solely on the account owner's description on the faces. They suggested strategically selecting decoy faces with similar descriptions during setup to reduce the risk.

Proposed by Dhamija and Perrig in 2000 [20], Déjà Vu uses a set of *Random Art* images to authenticate users. Showed in figure 2.10, the interface panel consists of

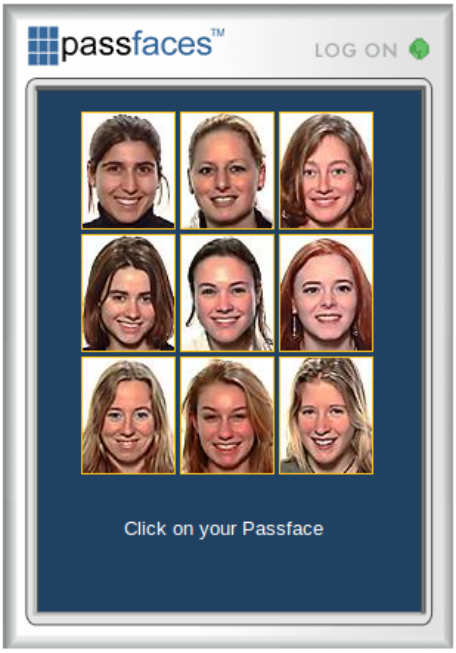


Figure 2.9: Passfaces™ Interface [18]

25 *random art* patterns. To login, users select their 5 pre-defined images from the panel. As described in the study, *random art* makes it difficult for users to write down or share passwords since the image itself does not carry any meaning. Similar to Passfaces™, the password space of Déjà Vu is only $\binom{25}{5} = 53130 \approx 2^{15.7}$ which is too small to be used as a replacement for text password.

Wiedenbeck et al. proposed a recognition-based scheme called Convex Hull Click (CHC) designed to withstand shoulder-surfing attacks [72]. The interface of the scheme consists of n icons. Within the set, there are k pre-defined icons called "pass-objects". Users click on an icon that is inside the imaginary convex hull formed by the pass-objects. Figure 2.11 shows a login screen with three pass-objects. They argue that observers are not able to determine the pass-objects which formed the convex hull, it is difficult to determine the user's passwords.

Hlywa, Biddle and Patrick [39] designed an experiment to study the relationship between image types and the usability of recognition-based graphical password schemes. They designed a graphical password scheme similar to Passfaces™ [18] but that is able to use different kinds of images. In their study, they choose three types of images:

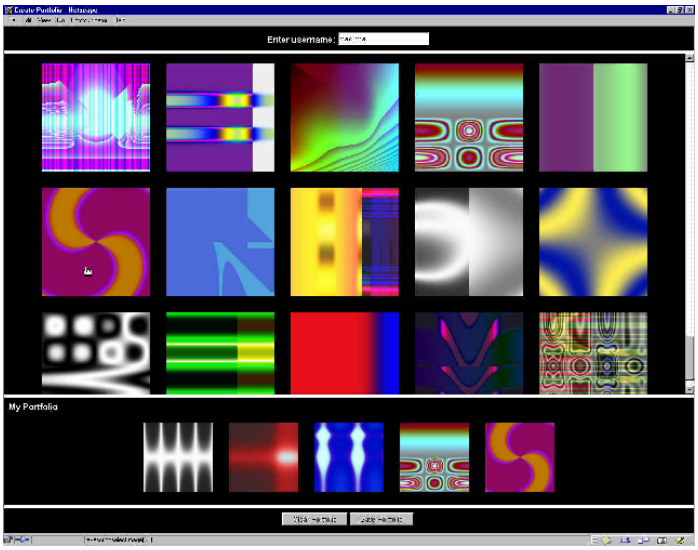


Figure 2.10: Déjà Vu interface [20]

Figure 2.11: Convex hull click with 100 icons including 3 pass-objects [72]

houses, faces and daily objects. The results of their study indicated that different types of images can indeed affect the usability of the scheme and the scheme was most usable when the set of daily object images was used. Figure 2.12 is the interface of the scheme using the set of daily object images.

Figure 2.12: A panel of object images used in Hlywa et al.'s study [39]

In general, recognition-based graphical password schemes authenticate users by asking users to differentiate secret images from decoy ones. The process usually involves users scanning through the images one by one and making a binary decision on each image. The time required to complete a login process and the strength of the password depend on the number of decoy images that are displayed.

Cued-recall based Graphical Password Schemes

Proposed by Yampolskiy in 2007 and inspired by the Traveling Salesman Problem, PassMap lets users set up their passwords by connecting or disconnecting paths between cities on a map (figure 2.13) [75]. The Travelling Salesman Problem is useful as a password scheme because it has a very large search space [34]; the search space grows

exponentially as the number of points increases. In addition, the article mentioned that it is relatively easy for humans to remember landmarks based on a well-known journey. By combining these two factors, Yampolskiy argues that PassMap is a very secure and usable scheme.

Figure 2.13: PassMap scheme [75]

PassPoints was proposed by Wiedenbeck et al. [71]. In this scheme, users select five points from a single image as their secrets and there are no restrictions on what type of the images are used. Considering that it is highly unlikely that users will be able to click on the exact pixel which they previously selected, the scheme is configured to have some tolerance on the precision of the clicks. Figure 2.14 shows an example password of the scheme; the selected points are marked with a small rectangle representing the tolerance area.

One of the biggest challenges that the scheme is facing is the hot-spot problem [21,66]. A hot-spot is a section of the image which users select more frequently than the others; an image can have multiple hot-spots. Analysis done by Thorpe and van Oorschot [66] showed that hot-spots exist in many images used in cued-recall schemes. Figure 2.15 shows the hot-spots for an image of cars. The hot-spot problem is considered a security risk for PassPoints because hot-spots can be used to create dictionaries for dictionary attacks. A dictionary attack is a form of guessing attack in which the

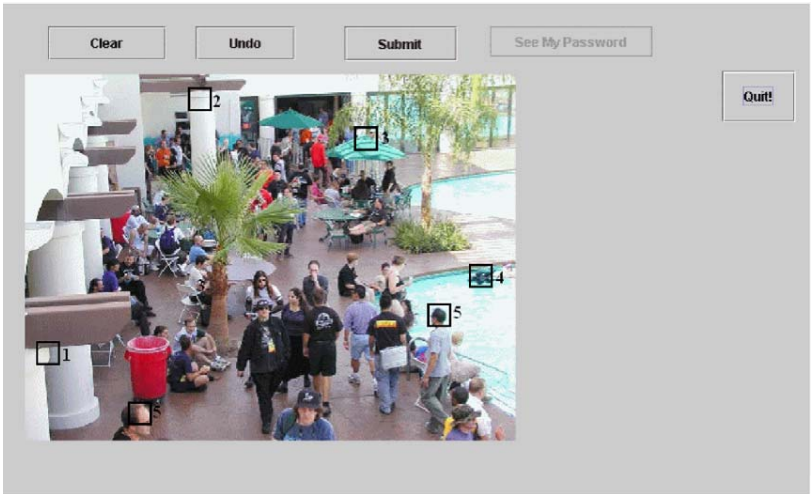


Figure 2.14: PassPoints scheme [71]

attackers guess passwords based on a list (dictionary) consisting of passwords believed to be more likely to be selected by the users.

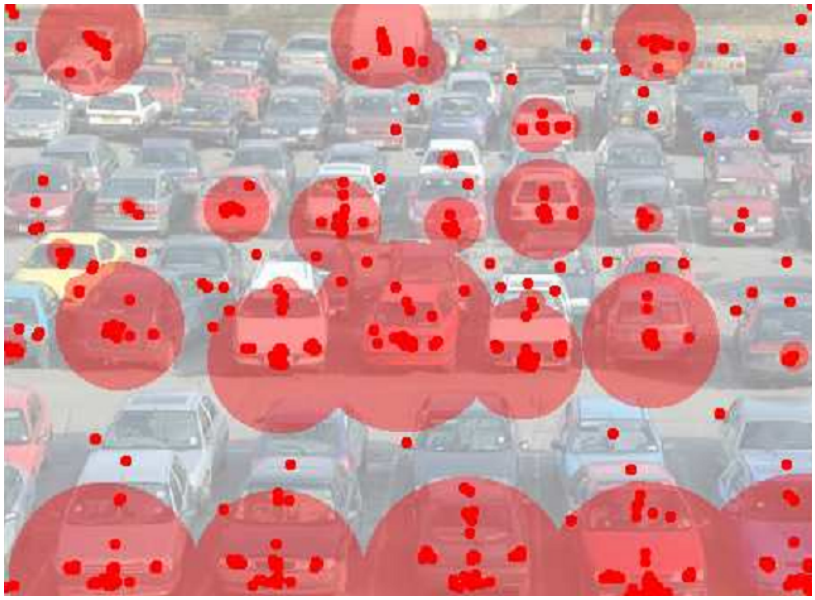


Figure 2.15: Hot-spots of a PassPoints image [66]

In order to reduce the chance of success of a dictionary attack, Cued Click Points (CCP) was proposed by Chiasson et al. in 2007 [14]. It improves security compared to PassPoints by using multiple images for a single password. When creating a CCP password, the next image is displayed depending on the coordinates of the click events.

When re-entering the password; if an incorrect point is selected, an image different from the original password is displayed. Figure 2.16 illustrates how the image selection process works.

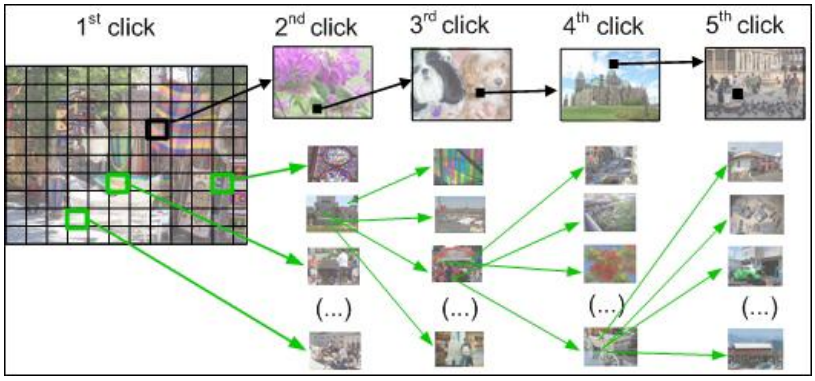


Figure 2.16: Possible image combinations in CCP [14]

The advantage of using multiple images is that it increases the complexity of dictionary attacks. To launch a dictionary attack on a PassPoint password of 5 points, the attacker only needs to analyze the hot-spots of a single image. However, to attack a CCP password of 5 points using the same method, many more pictures will have to be analyzed and the combinations of images also have to be considered.

Although CCP increases the complexity of dictionary attacks, the hot-spots on each image remain. To further increase the security of CCP, another scheme was proposed [11]. Persuasive Cued Click-Points (PCCP) tried to reduce the hot-spot problem by encouraging users to select their points more randomly. PCCP introduced a new concept called a "viewport" (figure 2.17). A viewport is a highlighted area randomly positioned on each image during the setup of passwords; users can only choose a point within the highlighted area as part of their passwords. But if users cannot find a suitable point within the viewport, the scheme allows user to shuffle the viewport to another random location. Based on a lab study [11], more PCCP click points fall outside of the predicted hot-spots than CCP.

In general, cued-recall based graphical password schemes authenticate users by asking users to select a series of points. During the login process, images are given to the users to provide visual cues or reference. Some schemes suffer from hot-spot problems

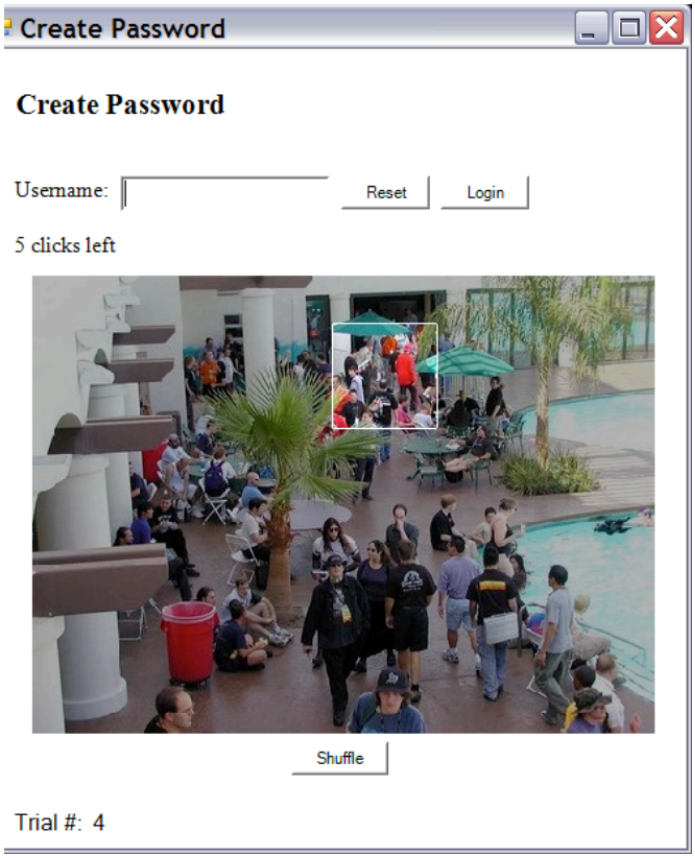


Figure 2.17: A PCCP image superimposed with the viewport [11]

but solutions are proposed to increase the security.

2.4.4 Possible Attacks on Graphical Password Schemes

The risk of dictionary attacks has been previously mentioned and applies to all schemes where users chose their own passwords and the effective password space is small. Brute force guessing attacks, where an attackers guess all possible combination, are also possible, especially when the theoretical password space is small.

Shoulder surfing is a type of social engineering where the attacker observes users' passwords by looking over their shoulders directly or using video recording devices. Tan and Czerwinski [62] showed that it is possible for an attacker to observe target words on a desktop monitor or projection screen from a distance; the success rate

increases as the size of display increases. Another study done by Tari et al. [64] showed that it is possible to observe Passfaces^{TM} passwords on desktop monitors using a shoulder surfing attack. Dunphy et al. [22] conducted a study on a recognition-based graphical password scheme to identify if the number of decoy images can affect the success rate of a shoulder surfing attack. Their result indicated that a larger number of decoy images in the scheme increases the difficulty of the attack.

The shoulder surfing problem has been addressed in many graphical password related studies [28, 72]. Our survey of the literature did not uncover any graphical password schemes which have anti-shoulder surfing mechanisms designed or tested specifically for mobile devices.

Dunphy et al. [23] studied social social engineering attacks on graphical passwords. In the study, they tested PassPoints [71] and Passfaces^{TM} [18] to see if the schemes are vulnerable to description. They discovered that it is possible for an attacker to successfully guess the passwords based on the description of the passwords.

Aviv et al. [4] examined the feasibility of smudge attacks on touchscreen devices using the Android unlock screen as the target . Smudge attacks try to uncover users' graphical password by analyzing the path of oily residues left on touchscreens. They showed that it is possible to see users' passwords by following the smudge marks even if the marks have been partially disturbed. Figure 2.18 is an example of smudge marks left on the touchscreen after unlocking an android phone.

2.5 Summary

In this chapter, we showed that typing text on mobile devices can be challenging because of small virtual keys and the same problem can be found when authenticating with text passwords. To minimize the need for typing when authenticating users on mobile devices, we looked at some possible alternative solutions to replace text passwords; the solutions use different factors including ownership, biometric and

Figure 2.18: Smudge marks on a mobile device [4]

knowledge. After reviewing these possible solutions, we decided to explore the possibility of using graphical password schemes on mobile devices because the schemes require no special hardware, have a similar login process to text passwords, can be used on multiple platforms, and have memorability advantages over text passwords. We explored some existing graphical password schemes from each of the three categories: recall, recognition, and cued-recall. At the end of this chapter, we talked about some possible attacks on graphical password schemes including shoulder surfing, social engineering and smudge attacks.

Chapter 3

Preliminary User Study

3.1 Objective

In chapter 2, we discussed many graphical password schemes that have been proposed; however, most of these schemes were designed to be used on desktop computers where the screens are large and input methods are accurate. Our goal is to design and implement a new graphical password scheme optimized for mobile devices with touchscreens. To have a better understanding of how touchscreens affect the usability of the scheme, we designed a preliminary user study testing existing schemes.

3.2 Prototype Configuration

We selected three different password schemes, each representing a different category (recall, recognition, and cued-recall). Table 3.1 summarizes the three test schemes selected. We have discussed DAS, PCCP, and object recognition in chapter 2. However, for Object Recognition, we modified the original scheme [39]; users had to select minimum 8 images from a single panel of 25 daily object images instead of picking one image from each of 6 panels of 26 daily object images.

In addition to the three test schemes, we also use two test devices each with a different screen size in order to determine the relationship between screen sizes and the usability of the schemes. Two devices were used in the study to test the usability of the schemes on different screen sizes. The first device is a 4th generation *iPod touch* by Apple Inc.; the device has a 3.5-inch widescreen multi-touch display with a 960 by 640 pixels resolution. Since we do not need to use the phone functionality in this study, an iPod

Category	**Scheme Name**	**Basic Operation**	**System Configuration**
Recall-Based	DAS (Draw A Secret) [45]	Users draw their password on a grid	Drawing on a 5 by 5 grid (75×75 pixels per cell) with a minimum length of 5 blocks; each block can be passed multiple times
Recognition Based	Object Recognition [39]	Users select at least 8 icons from a panel of 25 icons (75×75 pixels per icon)	Selecting a minimum of 8 icons from a panel of 25 icons, the order of selection matters
Cued-recall based	PCCP (Persuasive Cued Click Points) [11]	Users select a point within the viewport from each of the 5 images	Images are 451 by 331 pixels each; the viewport is 100 by 100 pixels. The tolerance of the clicks is 25 pixels

Table 3.1: The three test schemes for the preliminary study

Touch serves as a suitable replacement. The second device is a 3rd generation iPad by Apple Inc.; the device has a 9.7-inch widescreen multi-touch display with 2048 by 1536 pixel resolution. In order to ensure the two test devices render and execute the test schemes in the same way, all of the password scheme are implemented using JavaScript and Scalable Vector Graphics (SVG) technology and accessible from any of the standard web browsers. During the experiment, we used the built-in Safari browser on both devices.

Based on Herley, Florencio and Coskun's research on web password strength [27] a 20 bit password space with additional login rules (e.g., limit the number of retries) is considered sufficient to have minimum defense against web attackers. Following their suggestions, we implemented minimum password length restrictions. However, we did not implement additional login rules because our user study was conducted in a

closed lab environment and we wanted to gather information regarding login failures. The password space of each scheme, assuming the minimum length password, is as follows:

DAS Drawing on a 5 by 5 grid with a minimum length of 5 cells gives a password space of:
$(5 \times 5)^5 = 9,765,625 \approx 2^{23}$

PCCP Selecting one point from five 451 by 331 pixel images with a tolerance of 25 by 25 pixels gives a password space of:
surface area of a single image $= 451 \times 331 = 149,281$
possible selections on a single image $= 149,281/25^2 = 238.85$
password space $= 238.85^5 \approx 7.7 \times 10^{11} \approx 2^{39}$

Object Recognition Selecting a minimum of 8 icons from a panel of 25 icons gives a password space of:
choose a minimum 8 out of 25 icons $= \binom{25}{8} = 1,081,575 \approx 2^{20}$

3.3 Functionality

Figure 3.1 shows the graphical interface of the test schemes implemented for the preliminary study. DAS requires users to draw their password on the displayed grid (figure 3.1a). To record the secret in DAS, users click on the *set password* button; if the password is accepted by the system, the *set password* button will greyed out and the *check password* button will be enabled. To confirm the password, users re-draw the secret and press the *check password* button. At any given time, users may clear the screen by using the *clear screen* button or return the scheme to its initial state by using the *reset* button.

Figure 3.1b shows the interface for PCCP. In this scheme, 5 images are given to the

user in sequence. On each image, the viewport is represented by a yellow square. Users are allowed to shuffle the viewport to another random position on the image by using the *shuffle* button. To create a password, users have to pick a point within the viewport on each of the 5 images in sequence. To confirm, the same first image is displayed again without the viewport. At this stage, the *shuffle* is disabled and the *retry* button is enabled. If unable to confirm, users may restart the process with the *reset* button.

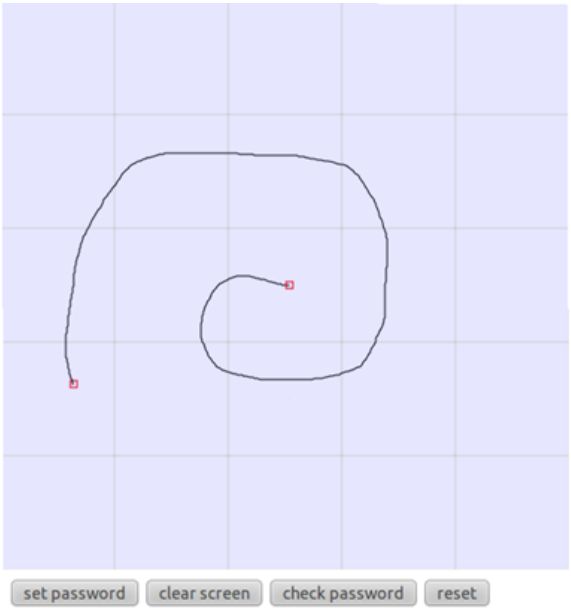
Figure 3.1c shows the interface for the Object Recognition scheme. To set up the password, users select at least eight icons as their password by highlighting the icons with clicks; pushing the *set password* button confirms the selections. If the new password is accepted by the system, icons will be shuffled to different positions, the *check password* button is enabled and the *set password* is disabled. To confirm, users re-enter the password by clicking their icons and pushing *check password*.

To capture users' behaviors during the experiment, we embedded PHP to record and upload user activities to our online database. We designed two SQL tables: one table to record all the touch events and the other table to keep all the passwords created by the users.

3.4 Participants

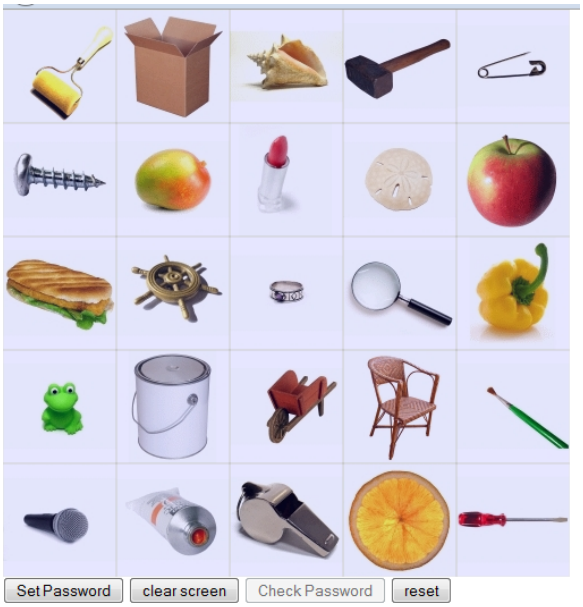
We recruited the participants from the university campus. In total, 31 participants took part, 11 were female and 20 were male. The average age of the group is 24.8 years old. The education level of the group is relatively high: 15 participants studied at the undergraduate level, 13 participants studied at the masters' level, 3 participants studied at the Ph.D. level. Thirteen participants were enrolled in computer science or related technical programs.

Of the 31 participants, 7 did not own either a tablet or a phone while 24 participants owned at least one mobile device. Regarding experience with graphical password schemes, 51% of participants have seen or used a graphical password before, and



(a) DAS

(b) PCCP



(c) Object Recognition

Figure 3.1: Graphical password schemes used in our study

almost all their experience is based on the unlock screen for the Google Android operating system.

3.5 Protocol

This experiment was approved by the Carleton University Research Ethics Board. This preliminary user study was carried out in one-hour-sessions in a lab environment. We divided our participants into two groups: one group used the smart phone and the other group used the tablet computer as the test platform; both groups tested all three schemes. We had 15 participants test on the smart phone and 16 participants on the tablet computer. Since the participants' performance is likely to improve with practice, we constructed a Latin Square for each test group (Table 3.2) to randomize the order of the password schemes seen during the experiment. A Latin Square is an n by n array in which each of n symbols appear exactly once in each row and column of the array and is used to reduce ordering effects in experiments. Each participant is assigned a testing order based on one row of the Latin Square.

Phone		
Scheme 1	**Scheme 2**	**Scheme 3**
PCCP	Object Recognition	DAS
DAS	PCCP	Object Recognition
Object Recognition	DAS	PCCP

Tablet		
Scheme 1	**Scheme 2**	**Scheme 3**
DAS	PCCP	Object Recognition
PCCP	Object Recognition	DAS
Object Recognition	DAS	PCCP

Table 3.2: Latin Square used to determine the order of the test schemes

At the beginning of the session, the participants were told that they will be testing the usability of three different graphical password schemes by creating a password with each scheme on a mobile device. The participants were told that they could create as many passwords as needed until they were confident that the password created was memorable. They were also told that they will be given a chance to practice each scheme on a desktop computer environment before proceeding to the mobile device. The remainder of the experiment is carried out with the following steps based on the

permutation given by the Latin Square:

step 1: Introduce scheme. Users were given verbal instruction on how to use the schemes.

step 2: Learn scheme. The participants practiced the scheme using a desktop computer with keyboard and mouse as the input methods. The interface and the settings of the scheme is identical to the test scheme on the mobile device; however, the icons and images used in *Object Recognition* and *PCCP* schemes were replaced with a dummy set to avoid memory interference. Users could create as many passwords as they wanted and explore for as long as they wanted. The intention was to familiarize users with the scheme so that usability problems arising during testing on the mobile device were in fact due to the form factor rather than confusion with the scheme.

step 3: Create passwords. Moving to the mobile devices, users create a password which they think they can remember. If using *PCCP*, users may shuffle the viewport as many times as they wish.

step 4: Confirm password. Users confirm the password by re-entering it again. If unable to confirm, they will be asked to create another password, returning to step 3.

step 5: Answer questionnaire. Returning to the desktop computer, users are asked to answer a questionnaire to providing feedback regarding what they think and feel about the scheme which they tested on the mobile device. The questionnaire is an online survey and consists of nine Likert scale and three open-ended questions. The list of questions can be found in Appendix A.

Step 6: Login. On the mobile device, users re-enter the password which they created previously. They may retry as many times as needed. If unable to remember their password, users could stop and move on to the next step.

Step 7: Answer questionnaire. Another questionnaire is given to the users on the desktop computer. The questionnaire consists of five Likert scale and three

open-ended questions which ask about users' perceptions of the test scheme. The list of questions can be found in Appendix B.

These steps were repeated three times, once for each of the three schemes. Upon conpletion of the three schemes, users completed an additional two questionnaires on demographics (Appendix D) and past experiences with mobile devices (Appendix C).

3.6 Results and Interpretation

In this section, we statistically and descriptively compared different data collected during the study to identify usability issues or user preferences when using graphical password schemes on mobile devices. We mainly focus on determining how screen sizes can affect the performance of schemes by comparing the creation time, login time, login success rate and password length of the same scheme but on different devices. To compare the creation time, login time and password length, we used Mixed-design ANOVA to look for overall differences and T-tests to determine where the difference occurred; Fisher's exact tests were used to compare the login success rate. For these tests, the alpha value is set to be 0.05 which means the probability that results occurred by chance are less than a 5%. We also compared the Likert scale questions in the questionnaires using Mann-Whitney U test (to compare independent ordinal data) and Friedman test (to compare paired ordinal data) to identify user preference; we used an alpha value of 0.05 for these tests as well.

3.6.1 Password Creation Time

	DAS		PCCP		Object	
	Tablet	Phone	Tablet	Phone	Tablet	Phone
Number of passwords created	16	15	16	15	16	15
Average creation time (Sec.)	29.8	34.3	62.8	74.5	59.3	56.7
Average shuffles per image	-	-	22.1	15.9	-	-

Table 3.3: Password creation

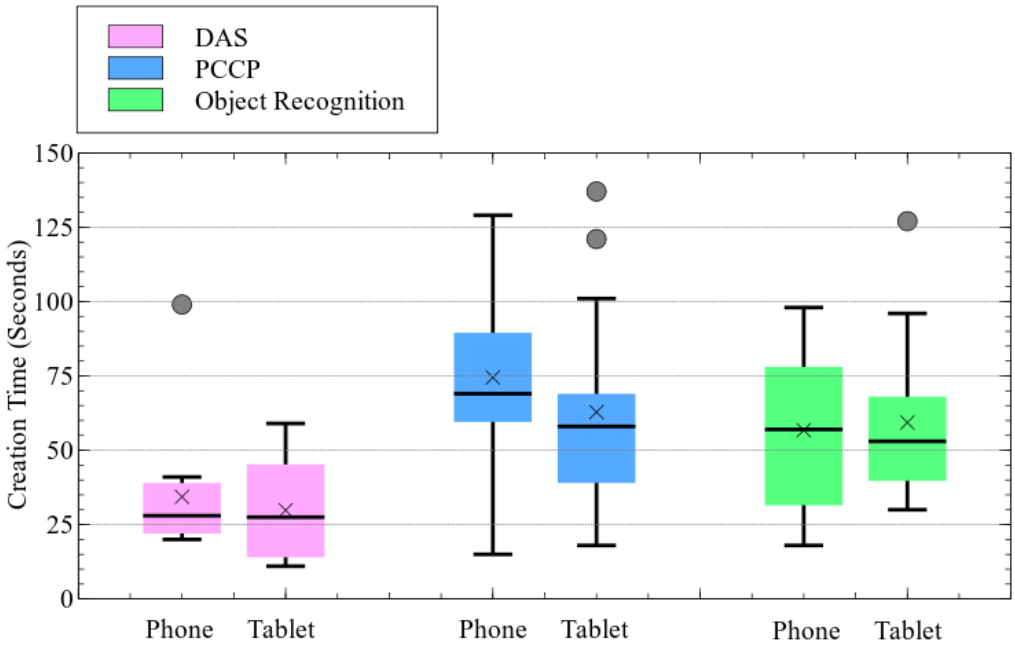


Figure 3.2: Password creation time

Table 3.3 shows the number of passwords created during the experiment and the average time required for users to successfully create a password. Figure 3.2 is the graph plotted using the creation times from each scheme. The creation time of a password is defined as the time between the first touch event and the push of the submit button. The average numbers are calculated based on the numbers that are within the standard deviation, no records was discarded in this case. The Mixed-design ANOVA test indicated no main effect of form factor on create time ($p = 0.491$, $F = 0.487$, and $df = 1$). On the other hand, the results also indicated a significant effect for the types of scheme ($p < 0.000$, $F = 17.928$, and $df = 1$). We ran paired T-tests to find the differences between schemes. There is a significant difference between the DAS-Object Recognition pair ($p < 0.001$, $t = -5.468$, and $df = 30$) and DAS-PCCP pair ($p < 0.001$, $t = -6.978$, and $df = 30$); no significant difference were found in PCCP-Object Recognition pair ($p = 0.136$, $t = -1.533$, and $df = 30$). From the tests, we see that screen size does not affect the password creation time of any scheme. However, DAS passwords can be set up in the shortest time (less than 35 seconds) while the other schemes take longer (over 55 seconds).

3.6.2 Password Length

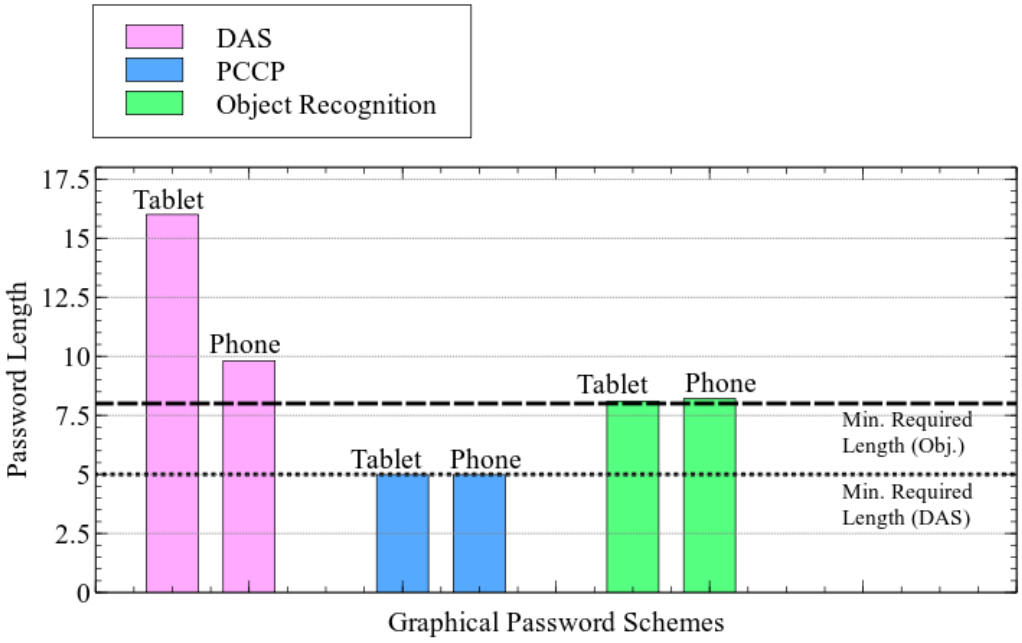


Figure 3.3: Average password length

Figure 3.3 shows the average length of the passwords that were created during the experiment. We used Mixed-design ANOVA tests to determine if there is a difference in the password length. The result showed a main effect of form factor ($p = 0.031$, $F = 5.153$, and $df = 1$). Further analysis comparing tablet versus phone for DAS ($p = 0.016$, $t = -2.553$, and $df = 29$) and Object Recognition ($p = 0.701$, $t = -0.388$, and $df = 29$) showed that DAS was the only scheme affected by form factor in terms of password length; users who used the tablet created significantly longer DAS passwords. PCCP lengths were not compared because the password length is fixed to 5 by design. From these results, we suspect that the small screen increased the difficulty for users to draw DAS passwords on the screen accurately, so users created shorter passwords. Object Recognition can be operated by just pushing the virtual buttons and was not affected by screen size. In addition, we noticed that both phone and tablet DAS users generally created passwords that are much longer than the minimum required length while Object Recognition users create passwords that just met the minimum requirement.

Login Time

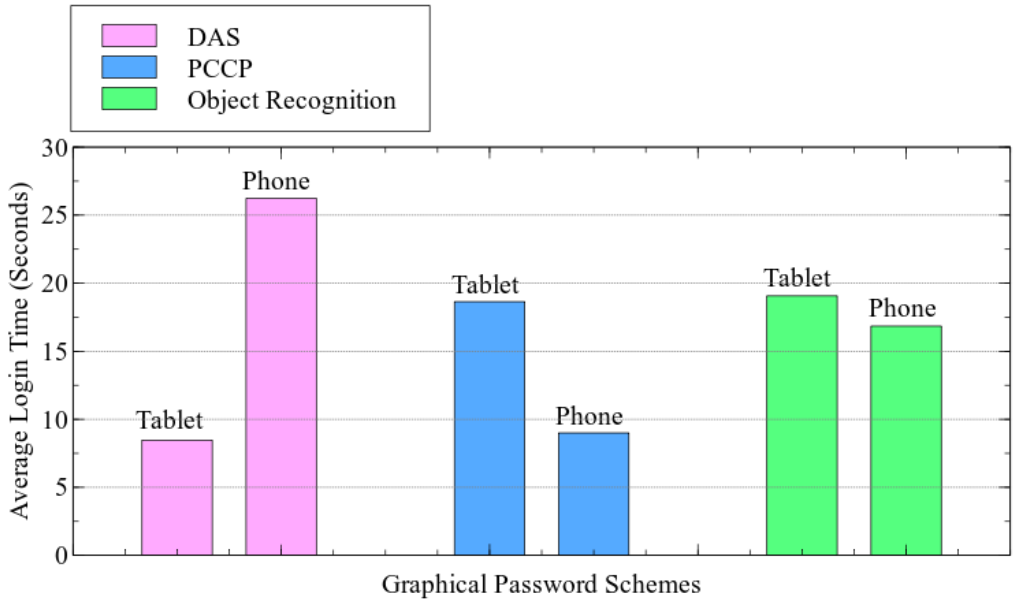


Figure 3.4: Average login time

Figure 3.4 shows the login time for successful attempts on both devices. Other than DAS on the phone, users took less than 20 seconds to login successfully on all schemes. For the DAS and Object Recognition schemes, the time of a login attempt is measured from the first touch event detected on the screen until the *check password* button is pressed; this includes the time spent clearing and starting over. On the other hand, the measurement of time for PCCP is slightly different. In PCCP, it is possible for users to notice an erroneous click before completing the login process because the scheme is designed to display pictures that did not appear in the setup process when the user selects the wrong point. Therefore, when measuring the login time for PCCP, we treated user resets as failed attempts.

The Mixed-design ANOVA test results indicated no main effect for neither the type of scheme ($p = 0.864$, $F = 0.030$, and $df = 1$) nor form factor ($p = 0.593$, $F = 0.296$, and $df = 1$) on the login time. From our results, we see that the screen size does not affect the login time for any of the three schemes. We did not compare the time that users spent on failed login attempts because this measurement is affected largely by

individual users' approaches. When users were not sure about the passwords, some users spent a long time trying to recall their password while others quickly made a guess, neither approach is really indicative of the scheme itself.

3.6.3 Login Success Rate

	DAS		PCCP		Object	
	Tablet	Phone	Tablet	Phone	Tablet	Phone
Success on the first try	100%	64.2%	86.6%	84.6%	86.6%	84.6%
Success within 3 tries	100%	92.8%	100%	100%	100%	100%

Table 3.4: Login success rate

In this preliminary study, we did not test the long term memorability of the passwords because we were focused on the effects of using graphical password schemes on mobile devices. Table 3.4 shows the login success rate of the schemes after the users complete the first questionnaire. We used Fisher's exact test to compare the login success rate between the devices within the same scheme because of the small sample size. The test results showed that DAS on tablet computer has a higher login success rate than the smart phone($p = 0.04$) on the first try; on the other hand, no significant differences were detected for the other schemes for the first attempt. On the other hand, no schemes showed significant differences for the login success rate withing three tries. In this comparison, we observed that the screen sizes only affected the recall-based scheme (DAS); recognition (Object Recognition) and cued-recall (PCCP) schemes were not affected. From our logs, we see that users made more mistakes while drawing on the small screen. We suspect it was because it is more difficult to accurately draw on the small screen accurately. The possibility that users forgot their password is unlikely because the time between creating the passwords and logging into the system is very short and most of the users could correctly enter the passwords within three tries.

3.6.4 Observations and User Feedback

Although we did not record our participants with any electronic devices during the sessions, we observed users and recorded all relevant behaviours in writing. We also took note on all the questions or opinions that the participants had during the experiment. This information can better help us to understand how users felt about the schemes when used on mobile devices. We discuss our observations for each scheme separately.

DAS

While testing DAS on the smart phone, several users complained that the canvas was too small, making it difficult to draw their secrets accurately. Interestingly, none of those participants tried to enlarge the canvas by zooming in. Another observation was that several users chose passwords that had the "fuzzy boundaries" problem. The term "fuzzy boundaries" [24] refers to a DAS password that traces the grid lines or crosses to another cell via the corner. Since passwords are recorded as a series of grid cells, users may be unaware which side of the grid line was used. As the result, users will not able to exactly replicate their passwords and the password becomes unusable. Figure 3.5 shows example passwords containing fuzzy boundaries.

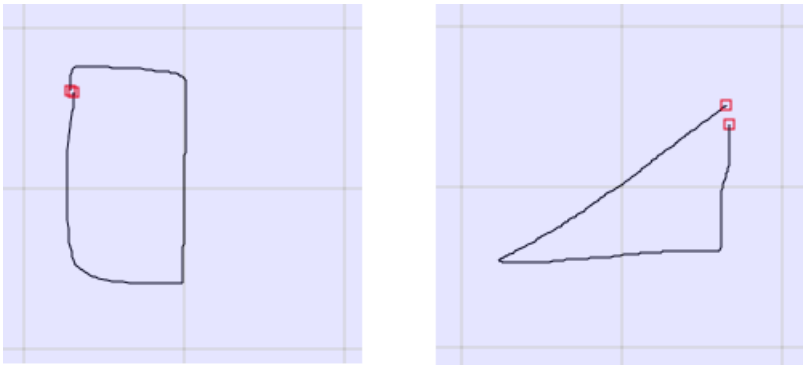


Figure 3.5: Passwords containing fuzzy boundaries

PCCP

The main observation for PCCP was regarding the shuffling of the viewport. The concept of viewport is to encourage users to create a stronger password by having them select points within the viewport as their passwords. Instead of choosing a point within the viewport, many users scanned the entire image and selected a point outside of the viewport. With the point selected, users then continuously clicked the *shuffle* button until the viewport moved to the desired location. In addition, many users actually tried to drag the viewport with their fingers because of their past experiences with the touchscreen devices.

Object Recognition

For Object Recognition, users tended to pick their icons to form a semantic pattern. After users created a password using this scheme, we asked them what rules they followed to pick the icons. Most users tried to group the icons based on their properties such as size or color. They then selected groups of icons to help with memorability. The size of the icons appeared to be sufficiently large for users to click on both devices.

3.6.5 Questionnaire Response

Another important aspect of this preliminary study is to explore how touchscreens affect user perceptions of the graphical password schemes. This is done by asking users to complete questionnaires during the different stages of the study. Listed in Appendix A and B are the questions that users answered for each scheme. The questionnaires contained Likert scale questions and open-ended questions. For the Likert scale questions, users assigned a score to each of the listed statements. The scores ranged from 1 to 10, with 1 being strongly disagree and 10 being strongly agree with the statement. We have grouped the Likert scale questions into 3 categories for discussion: form factor, graphical password schemes, and memorability.

Form Factor

For form factor, we compared smart phone versus tablet computer users' responses for each scheme. We used Mann-Whitney U test to compare the responses from the two different test groups because the groups are independent from each other and the responses are ordinal. Consistent with the previous results (section 3.6.2 and 3.6.3), we observed that screen size influences users' experiences only for DAS. The relevant Likert scale questions are provided next. We used box plot graphs to represent our data. The lower and higher whiskers represent the first and fourth quartiles excluding outliers. The box represents the second and third quartiles of which 25% of the data is in the upper half of the box and 25% of the data falls within the lower half of the box. The thick line inside the box represents the median which is the middle of a dataset. Outliers are the values that are 1.5 times greater or smaller than the upper or lower quartiles; they are represented by dots. The average value of the dataset is marked with an $\times$.

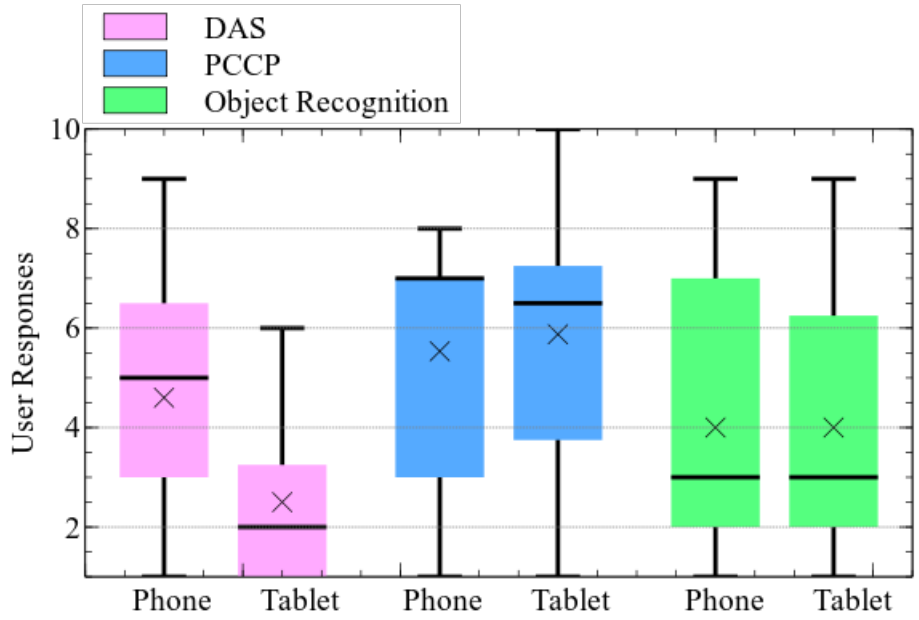


Figure 3.6: User responses to: "I find it hard to create a graphical password using this scheme" (1 = strongly disagree, 10 = strongly agree)

Figure 3.6 shows a box plot of the question *I find it hard to create a graphical password*

using this scheme. Lower scores indicate a more positive response for this question. Participants thought that DAS was more difficult to use on the small screen ($p = 0.009$, $U = 54.5$, and $z = 2.606$), but no statistically significant differences were found for PCCP ($p = 0.858$, $U = 115.5$, and $z = 0.179$) or Object Recognition ($p = 0.889$, $U = 116.5$, and $z = 0.139$). In this question, DAS scored an average of 4.6 (smart phone) and 2.5 (tablet computer); PCCP scored an average of 5.5 (smart phone) and 5.8 (tablet computer); and Object Recognition scored an average of 4.0 for both smart phone and tablet computer. Except using DAS on a tablet computer, the scores showed that participants generally found it somewhat hard to create passwords using both devices.

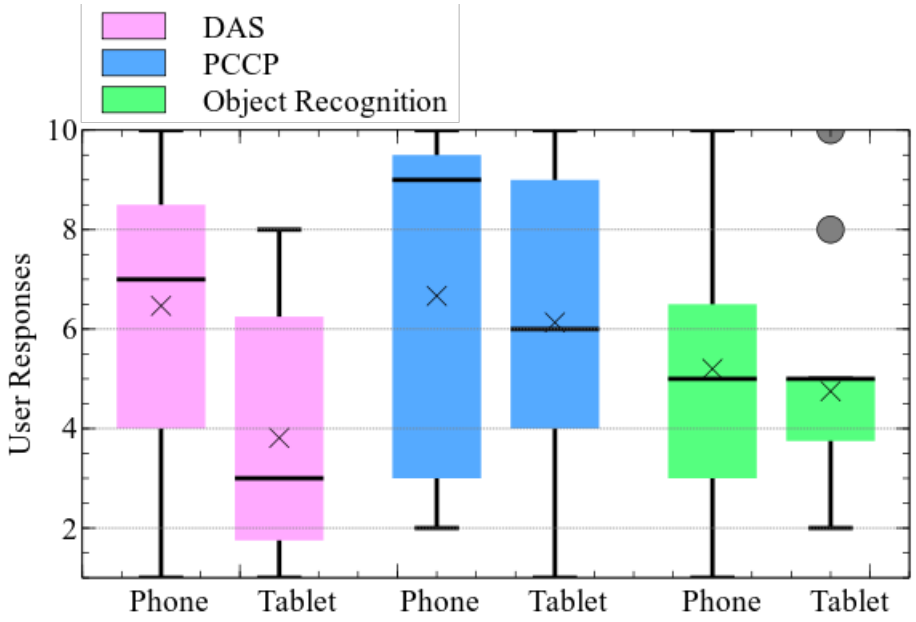


Figure 3.7: User responses to : "I think this scheme will be easier to use on a desktop computer than mobile devices" (1 = strongly disagree, 10 = strongly agree)

Figure 3.7 is a box plot of the question *I think this scheme will be easier to use on a desktop computer than mobile devices*. A lower score means a more favorable response. Similar to the previous question, smart phone participants were more likely to think that DAS ($p = 0.014$, $U = 58.5$, and $z = 2.445$) would be easier on a desktop than tablet participants. PCCP ($p = 0.559$, $U = 98.5$, and $z = 0.585$) and

Object Recognition ($p = 0.773$, $U = 111.5$, and $z = 0.341$) showed no significant differences. Except for DAS on the tablet, the average scores are between 5 and 7. The results showed that participants generally think that having a larger screen with more accurate input method might make the scheme more usable.

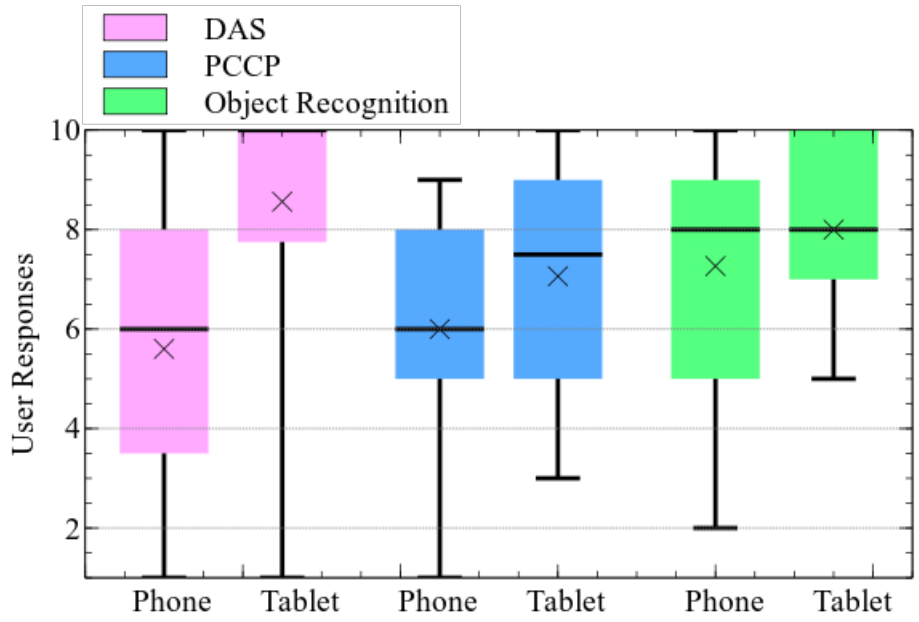


Figure 3.8: User responses to : "This scheme was easy to use given the size of the device screen" (1 = strongly disagree, 10 = strongly agree)

Figure 3.8 illustrates the question *This scheme was easy to use given the size of the device screen*. Favorable responses are represented by higher scores. Once again, participants felt that DAS is more difficult to use on the smart phone than tablet computer ($p = 0.004$, $U = 49.0$, and $z = 2.842$) while no statistically significant differences were found for PCCP ($p = 0.570$, $U = 106.0$, and $z = 0.568$) and Object Recognition ($p = 0.571$, $U = 99.0$, and $z = 0.567$). Looking at the averages, DAS scores 5.6 (smart phone) and 8.5 (tablet computer); PCCP scores 6.0 (smart phone) and 7.0 (tablet computer); and Object Recognition scores 7.2 (smart phone) and 8.0 (tablet computer). Despite the fact that participants generally felt the schemes were somewhat hard to create password (figure 3.7) and using the schemes on the desktop computer might improve the usability (figure 3.6), participants still felt that

the schemes are usable on mobile devices.

Graphical Password Schemes

We also investigated how the schemes can affect users', perception and opinion. A well designed graphical password scheme should be easy to understand and use by the users. To compare the designs of the three schemes to each other, we used two tests: Friedman test and Wilcoxon Signed Ranks test because we are comparing the responses originated from the same users but different schemes. The following are the two relevant questions.

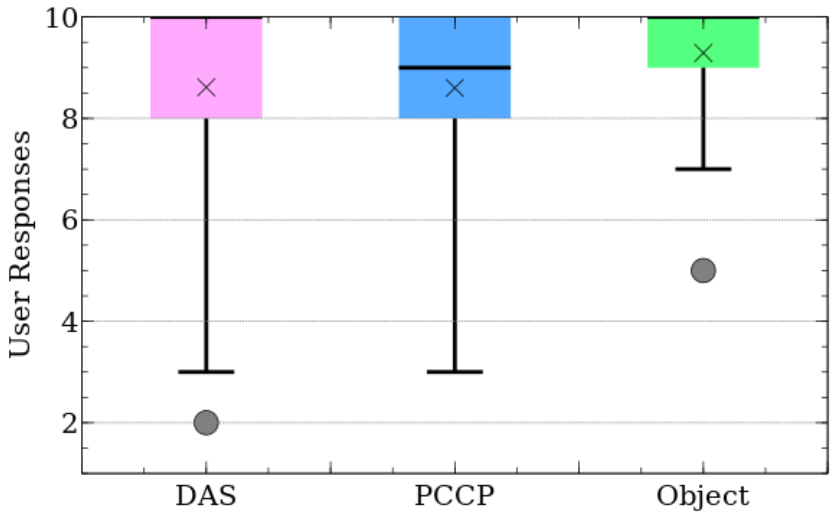


Figure 3.9: User responses to : "It was easy to understand how the scheme works" (1 = strongly disagree, 10 = strongly agree)

For any password scheme, it is very important that users easily understand how the scheme works to reduce the chance of misuse. Figure 3.9 represents the question *It was easy to understand how the scheme works*. Higher scores signify more positive responses. All three test schemes received very high average scores (DAS : 8.61, $PCCP$: 8.60 and $ObjectRecognition$: 9.29) and Friedman test showed that there is no difference between the schemes ($\chi^2 = 2.37$, $df = 2$, and $p = 0.31$) for this question.

It appears that users felt that they understood how each scheme works without any difficulties.

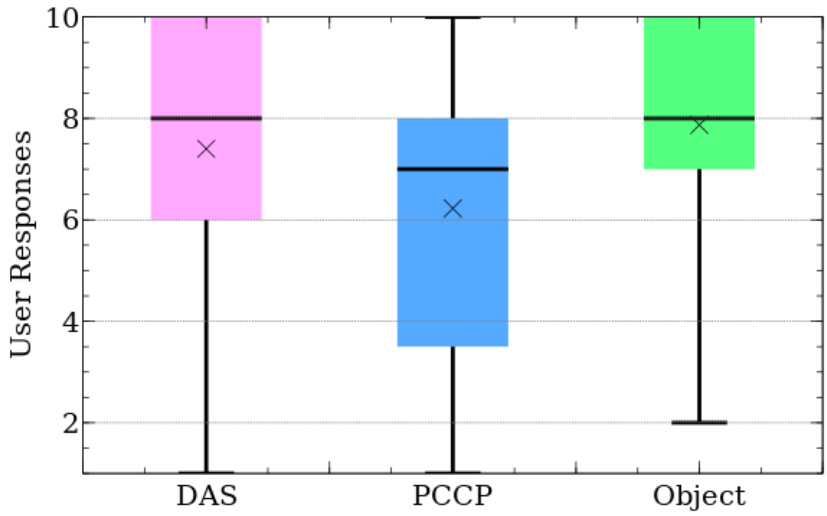


Figure 3.10: User responses to : "It was easy to set up a password" (1 = strongly disagree, 10 = strongly agree)

Figure 3.10 shows a box plot of the question *It was easy to set up a password*. Again, more favorable responses are indicated by higher scores. It is important that users are capable of setting up a password easily. Difficulties with the setup process might cause users to choose easier passwords which affect the security of the scheme. For this question, the mean scores for the three schemes are: $DAS = 7.45$, $PCCP = 6.23$ and *Object Recognition* $= 7.87$. Friedman test indicates that there is a difference between the 3 groups ($\chi^2 = 9.05$, $df = 2$, and $p = 0.01$). Further analysis using Wilcoxon's test showed that there is no significant difference between the Object Recognition/DAS pair ($p = 0.48$ and $z = -0.71$) or DAS/PCCP pair ($p = 0.06$ and $z = -1.92$) but there is a significant difference between the Object Recognition/PCCP pair ($p = 0.01$ and $z = -2.73$). From the test results, we can only conclude that participants felt that it is easier to setup the password using Object Recognition than PCCP. Based on users' responses from the open-ended question, one possible reason that made PCCP passwords hard to set up is the fact that the viewport limits their choice of points, making the setup process tedious.

Password Memorability

The memorability of the passwords can affect the security of the scheme; if a password is difficult to remember, then users might write the password down or choose weaker password which are security risks. In the questionnaires, we asked the participants questions about the memorability of the passwords. Although we did not actually test the long term memorability of the passwords, users responses can still be used as a first indication. For this group of questions, we compare schemes to each other regardless of the devices.

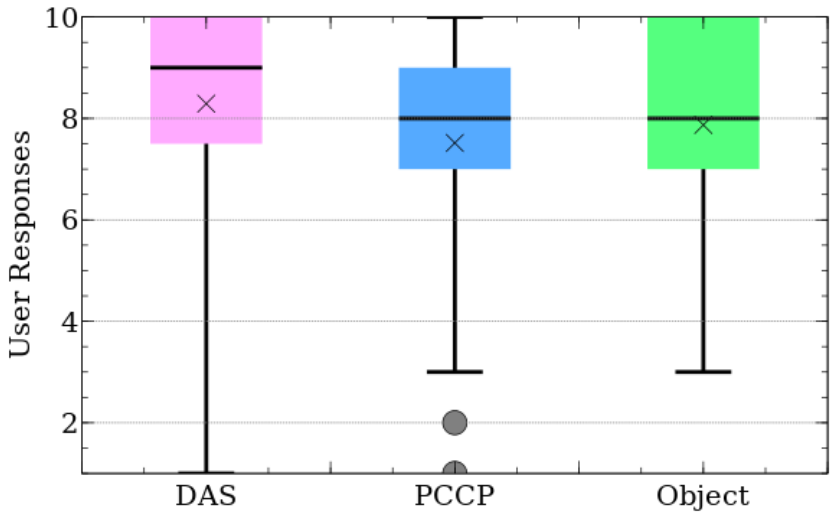


Figure 3.11: User responses to: "It was easy to remember the password" (1 = strongly disagree, 10 = strongly agree)

Figure 3.11 is the box plot of the question *It was easy to remember the password*. A score of 10 is the most favorable. In this question, the mean score of each scheme was: 8.29, 7.52 and 7.87 for DAS, PCCP and Object Recognition. Friedman test results ($\chi^2 = 1.94$, $df = 2$, and $p = 0.38$) showed that there is no significant difference between the three schemes. From these scores, participants appear confident about being able to remember passwords created using these schemes.

Figure 3.12 shows a box plot of the question *I will be able to remember more than one graphical passwords using this scheme*. Positive responses are indicated by a

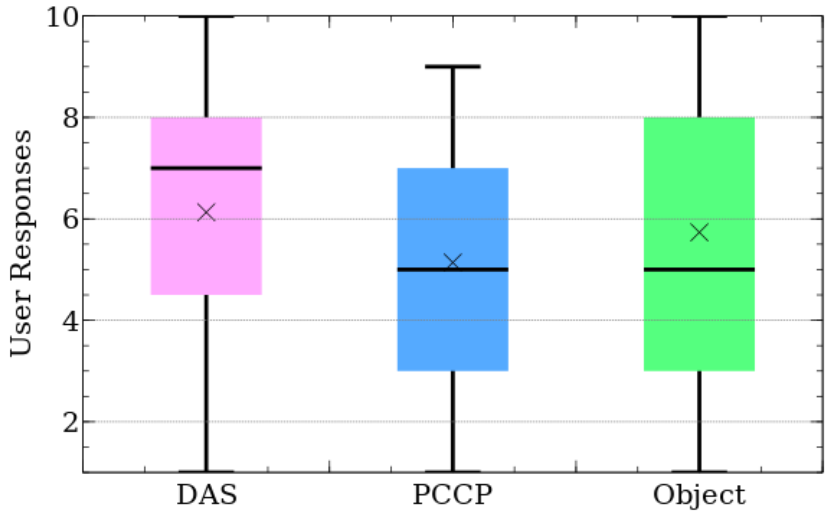


Figure 3.12: User responses to : "I will be able to remember more than one graphical passwords using this scheme" (1 = strongly disagree, 10 = strongly agree)

higher score. The mean score of each scheme is: 6.13, 5.16 and 5.71 for DAS, PCCP and Object Recognition respectively. Friedman test result ($\chi^2 = 1.87$, $df = 2$, and $p = 0.39$) showed that there is no significant difference between the three schemes. Participants seemed unsure about whether they would be able to remember multiple passwords. If we compare results from this question with the result of the question: *It was easy to remember the password* (figure 3.11), we see that participants are significantly less confident that they could remember more than one password (DAS: $p < 0.01$, $z = -4.00$; PCCP: $p = 0.01$, $z = -2.44$; Object Recognition: $p = 0.02$, $z = -2.42$).

3.6.6 Open-ended Questions

At the end of each questionnaire, we have three open-ended questions allowing users to provide further feedback about what they found easy or difficult when using the scheme. Table 3.5 is a summary of the most common issues raised by participants. In addition, participants also noted characteristics that they liked about the schemes; these are summarized in Table 3.6.

Scheme	Common Issues
DAS	• Difficult to draw the lines accurately on the small screen • Cannot draw diagonal lines • Difficult to remember the starting point of the password
PCCP	• Difficult to remember five images and the points in a short time • Hard to select memorable points within the viewport • Hard to click on the desired points precisely
Object Recognition	• Hard to remember many objects in a short time • Difficult to differentiate similar images on a small screen • Difficult to find objects that share common properties to use as passwords

Table 3.5: Common issues raised by participants

Scheme	Common Issues
DAS	• Not having to type • Easy to remember the password
PCCP	• Not having to type, clicking is efficient
Object Recognition	• Not having to type, clicking is efficient • Hard to miss the clicking target

Table 3.6: Characteristics liked by participants

3.7 Conclusions Drawn from the Preliminary Study

The most important conclusion drawn from the preliminary study is the relationship between usability and touchscreen sizes for different schemes. We learned that the size of the touchscreen significantly affects DAS because it requires more precision. On the other hand, the click-based password schemes PCCP and Object Recognition were not affected by the screen sizes. Furthermore, participants generally feel that

PCCP and Object Recognition passwords are hard to remember because they are forced to quickly memorize images which they have not seen before.

3.8 Limitation of the Study

We asked each participant to test three different schemes. This might affect the results of the study because participants may rate the schemes based on comparisons between the schemes rather than each individually. We use Latin Squares to vary the order of presentation and minimize the effects, but individual differences may still have occurred. Lastly, the experiment was done in a controlled environment in which some external factors that might affect the schemes (e.g., standing or walking while holding the device, additional noise and distractions, or sub-optimal lighting conditions) are eliminated.

3.9 Design Goals for the New Scheme

Learning from the results, we selected to use DAS as the base of our new scheme because the participants created longest passwords (comparing to the minimum required length; section 3.6.2) using this scheme. In addition, participants generally think that DAS passwords are easier to remember because they do not need to memorize new images quickly. With that said, DAS suffers from accuracy problems when used on small screens (section 3.6.6 and 3.6.2) and has the fuzzy boundaries problem if not explained to the users specifically (section 3.6.4). If we can use the advantages and eliminate usability issues of DAS on mobile devices, the new graphical password scheme might be more usable on mobile devices than the existing ones.

Chapter 4

Design of the *Touchscreen Multi-layered Drawing* (TMD) Authentication Scheme

Based on our preliminary study, we concluded that one of the major problems of user-drawn graphical passwords on touchscreens is the accuracy problem. Furthermore, we also discovered that users disliked having to memorize unfamiliar images or icons. With that in mind, we designed a graphical password scheme that has larger target areas and does not force the users to remember additional images or icons.

4.1 The Interface

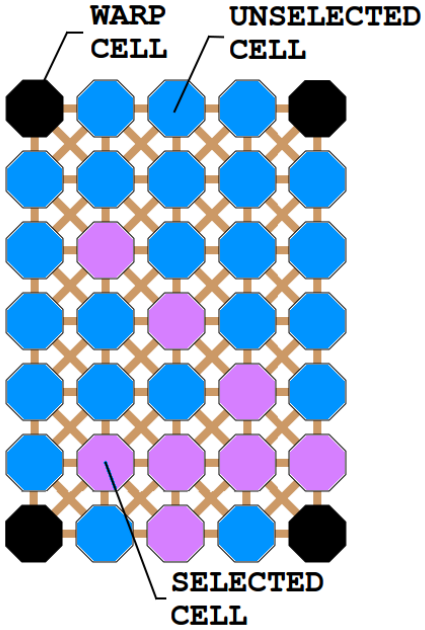
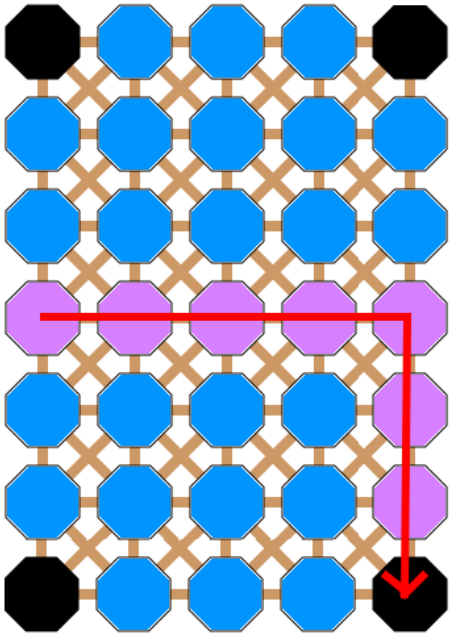


Figure 4.1: Password entry

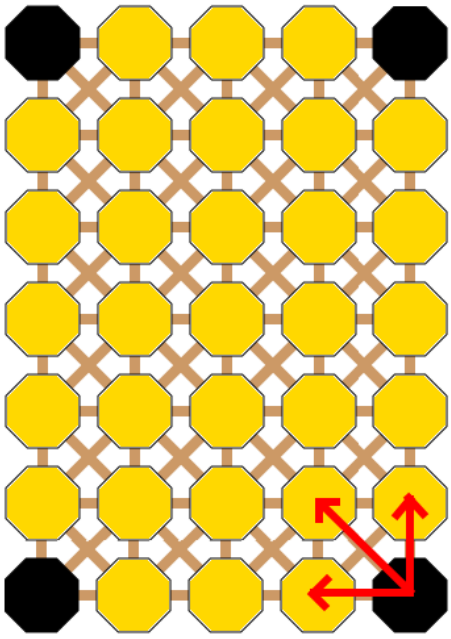
Similar to other recall-based graphical password schemes which ask users to draw their secret on a grid, TMD requires users to draw their secrets by selecting series of adjacent cells. Figure 4.1 provides a screenshot of the interface. The TMD interface consists of cells that are not attached to each other, eliminating the "fuzzy boundaries" problem described in section 3.6.4. The figure also shows that the TMD interface consists of three types of "cells": *Unselected*, *Selected* and *Warp* cells.

Initially, every cell on grid except the four corners are unselected; the four corners are warp cells. To create a password, users start by choosing any unselected cell as their starting point. If a warp cell is selected at this time, the scheme ignores the selection and records the first unselected cell chosen instead. Once the initial cell is selected, users can make the password longer by choosing any unselected adjacent cell as the next cell in the password; the color of the cell changes to indicate the cell has be selected. Users are allowed to traverse over cells which have been selected previously; however, going over the selected cells does not get recorded again as part of the password path.

As the name suggests, TMD allows users to draw their secrets across multiple "layers". This feature allows us to increase the size of the target area without affecting the password space. When the user's password reaches a new layer, the scheme resets all the selected cells on the screen back to the unselected state and changes the color of the unselected cell to notify the users that they have moved to the next layer. The transfer of layers is triggered when the user's password reaches one of the four warp cells located at the four corners. Figure 4.2 illustrates how a user reaches a warp cell (figure 4.2a) and gets transferred to the next layer (figure 4.2b). Selection of the cells must be done within a single dragging gesture. As soon as the user lifts their fingers from the screen, a confirmation screen is displayed (figure 4.3) to allow users to either start over or submit the passwords. For password creation, the users are required to enter the same password twice to set the password.



(a) The user has reached a warp cell when entering the password



(b) The scheme displays the next layer and the user may continue the password on any of the 3 indicated cells

Figure 4.2: Moving from one layer to the next layer in TMD

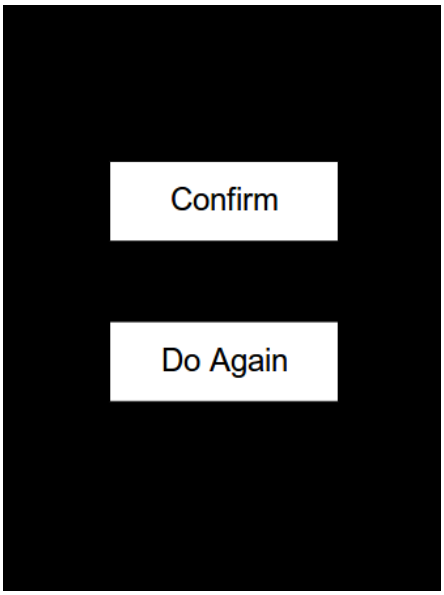


Figure 4.3: TMD Confirmation screen seen during password creation or login

4.2 Encoding of the TMD Passwords

Similar to DAS [45] or Pass-Go [63], passwords created using TMD are encoded using an alpha-numerical representation of each cell. In TMD, each of the non-warp cells is assigned a value used to encode the password; all warp cells are represented by the character "W" instead of a number. Figure 4.4 shows the alphanumerical representation of the cells. To encode a password, simply concatenate the alphanumerical text of each cell separated by a comma in the order which they were selected by the user. For example the encoding of the password in figure 4.2a is *(15,16,17,18,19,24,29,W)*. As soon as the scheme moves to the next layer (figure 4.2b), the next cell attached to the end of the password is one of *(,33)*, *(,28)* or *(,29)*.

4.3 System Rules

To make the TMD scheme more complete, the following rules are set:

- The length of the password is the total number of selected cells on all layers excluding the warp cells;

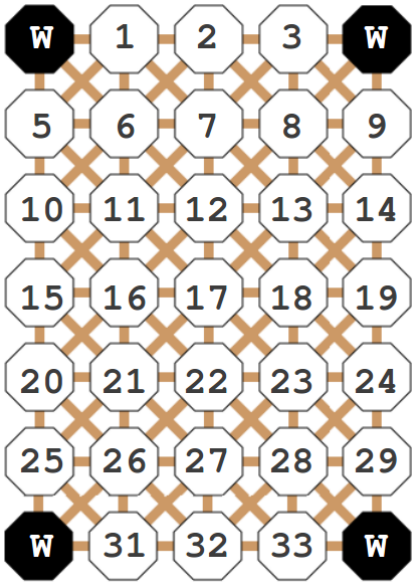


Figure 4.4: TMD encoding

- The depth of the password equals the number of times the path reaches one of the four warp cells. The depth of the password is 0 at the initial state;
- When the stroke reaches a warp cell, the depth of the password increments;
- The first cell selected for a passwords has to be a non-warp cell.
- If the first cell selected is a warp cell, the scheme starts recording only when they reaches the first unselected cell;
- The confirmation page is displayed after the first touch event has ended.

4.4 Theoretical Password Space Lower Bound of TMD

The calculation of the lower bound of the password space of TMD is very similar to the ones described by Jermyn et al. [45] and Tao et al. [63]; we used a recursive method to calculate the lower bound of the TMD password space. The following lower bound calculation is based on the assumption that users only create passwords which do not use warp cell (i.e., password depth = 0)

We first define the following function:

$f(n) =$ *The lower bound of possible combinations of passwords with length n*

Now, consider the base case when password length is equal to 1, because there are 31 possible choices (figure 4.1), we can define our base case:

$$f(1) = 31$$

Increasing the length of the password to 2, there will be **at least** 4 possible choices for our next selected cell depending on the location of the initial cell. The fewest choices occur when we select a cell on the edge of the grid and adjacent to a warp cell. Therefore, the lower bound of the password space of length = 2 can be defined as:

$$f(2) = f(1) \times 4$$

Since TMD allows users to go through the selected cell in order to reach an unselected cell, the function remains true as long as there are at least 4 unselected cells remaining on the grid. We can generalize our function:

$$f(n) = f(n-1) \times 4, n = 2...28$$

For the password space of passwords with a length of 29, 30, 31, we define the following function to account for the smaller number of remaining choices on this layer:

$$f(29) = f(28) \times 3$$
$$f(30) = f(29) \times 2$$
$$f(31) = f(30) \times 1$$

To calculate the overall lower bound of the password space of passwords with depth=0, we get:

$$
\begin{aligned}
\sum_{i=1}^{31} f(i) &= f(1) + \sum_{s=2}^{28} f(s) + f(29) + f(30) + f(31) \\
&= 31 + ((31 \times 4^1) + (31 \times 4^2) + ... + (31 \times 4^{27})) + f(28) \times 3 + f(29) \times 2 + f(30) \times 1 \\
&= 31 + 31 \times (4^1 + 4^2 + ... + 4^{27}) + f(28) \times 15 \\
&= 31 + 31 \times (\sum_{s=1}^{27} 4^s) + f(28) \times 15 \\
&= 31 + 31 \times (\sum_{s=0}^{27} 4^s - 1) + 31 \times 4^{27} \times 15 \\
&= 31 \times [1 + (\frac{4^{28} - 1}{4 - 1} - 1) + (4^{27} \times 15)] \\
&\approx 31 \times [2.4 \times 10^{16} + 2.7 \times 10^{17}] \\
&\approx 31 \times 2.94 \times 10^{17} \\
&\approx 9.11 \times 10^{18} \\
&\approx 2^{62}
\end{aligned}
$$

From the above calculation, the lower bound of the password space is 2^{62} for passwords of 1 to 31 cells in length without using warp cells. Assuming l is the lower bound of the password and d is the depth of password, for each additional layer used in the password, the lower bound of theoretical password space should be at least:

$$l = 2^{62} \times d$$

4.5 Resistance to Shoulder Surfing Attacks

One of the common weaknesses of graphical passwords is susceptibility to a shoulder-surfing attack. With DAS and Pass-Go, the entire password is visible during password setup or login. In TMD, the use of multiple layers not only increases the password space but also reduces the chance of shoulder-surfers observing the entire password because only part of the password is visible at a time. Although users can decide to use only one layer for their password which exposes the entire password, this can easily be prevented by setting up a password policy. Another design feature intended to increase protection against shoulder surfing is to allow users to travel through cells that were previously selected. This design not only gives users more freedom in terms of choosing passwords but also creates a one-to-many relationship between the pattern visible on the screen and the encoding of the passwords. With this one-to-many relationship, seeing a screen does not uniquely identify the password (or portion thereof). Figure 4.5 is an example password that can be made out of 48 different combinations. These features should be combined with additional login policies such as "the three strike" rule in order to maximize the resistance to shoulder surfing attacks.

4.6 Summary

In this chapter, we explained the design of *Touchscreen Multi-layered Drawing*, including the interface layout, functionality, usage, and encoding schema. We tried to improve the accuracy on a small screen by using large colored cells. We have also tried to eliminate the fuzzy boundaries problem by adding space between the cells. In order to determine the usability of the scheme, we designed a comparative user study in which we compare TMD to DAS using different devices. This study is described in chapter 5.

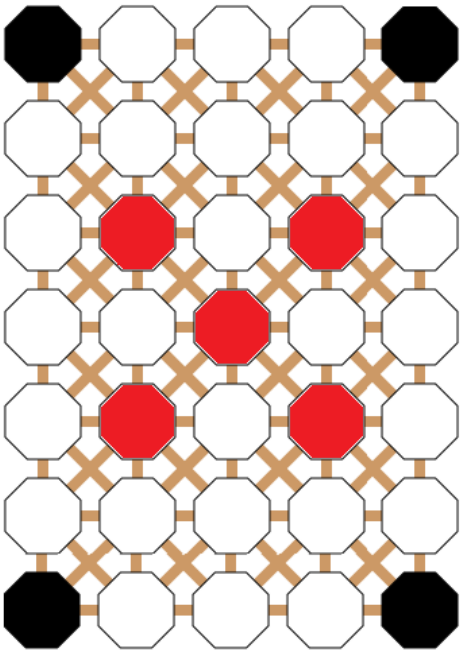


Figure 4.5: An example of a TMD password

Chapter 5

User Study Comparing TMD and DAS

5.1 Objective

We conducted a 2×2 between-subject user study in order to assess how usable Touchscreen Multilayer Drawing (TMD) is on mobile devices. In this study, we compared several aspects, such as password length, password creation time, password memorability, and password login time for TMD and DAS on smart phones and tablet computers. We then analysed TMD password patterns and distribution for password security. Finally, we analysed the answers from questionnaires to have a better understanding of the participants' perceptions on TMD.

5.2 Prototype Configuration

We selected DAS in our comparison because it also uses recall-based graphical passwords. Similar to the preliminary study, we tested our schemes on two devices with different screen sizes. The first device is a 4th generation *iPod touch* by Apple Inc.; the device has a 3.5-inch widescreen multi-touch display with a 960 by 640 pixels resolution. This is identical to iPhone 4 except it lacks phone capabilities which were unnecessary in our study. The second device is a 3rd generation iPad by Apple Inc.; the device has a 9.7-inch widescreen multi-touch display with 2048 by 1536 pixel resolution.

We set the minimum acceptable password length for TMD to be 10 cells long and DAS to be 5 squares long. We implemented the minimum length restriction for both schemes based on Herley et al.'s study [27] suggesting that password schemes should

have a minimum password space of 20 bits with additional login rules in order to have sufficient protection against online brute force attacks. We did not implement additional login rules because it was out of the scope of this study. The password space for each scheme is calculated as follows:

TMD We used the lower bound calculation described in section 4.4. Drawing on a 5×7 grid with a minimum length of 10 cells gives a password space of:
$(7 * 5 - 4) * 4^9 = 31 * 262144 = 8126464 \approx 2^{22.96}$

DAS Drawing on a 5×7 grid with a minimum length of 5 cells gives a password space of:
$(5 * 7)^5 = 52521875 \approx 2^{25.64}$

5.3 Functionality

We implemented TMD and DAS as web pages using JavaScript and Scalable Vector Graphics (SVG) technology. We embedded PHP scripts in the web pages to record user activities during the experiment. The activities included time spent to setup a password, time spent entering a password, number of retries/clears before sending the password for verification, the length of password created, and the date and time of each login attempt. All the collected data are stored in an online SQL database for analysis.

Figure 5.1 is the initial page displayed at the beginning of the test for both TMD and DAS. On those pages, users enter their username and click on either the *create* or *login* button to proceed.

Figure 5.2a is the main interface of TMD. We used a 5×7 grid in this test because this is the best fit for the size of the smart phone screen where the display area is limited. As described in chapter 4, a confirmation screen is used to allow the users to send or redraw the password (figure 5.2b). There is no limit on how many times an user can redraw the password.

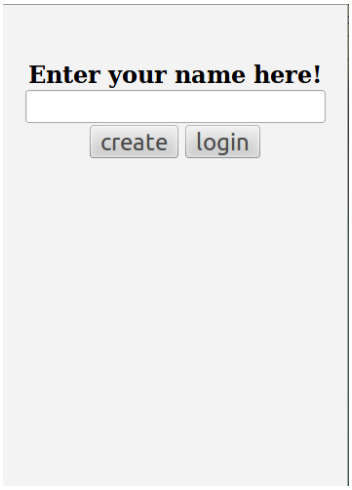
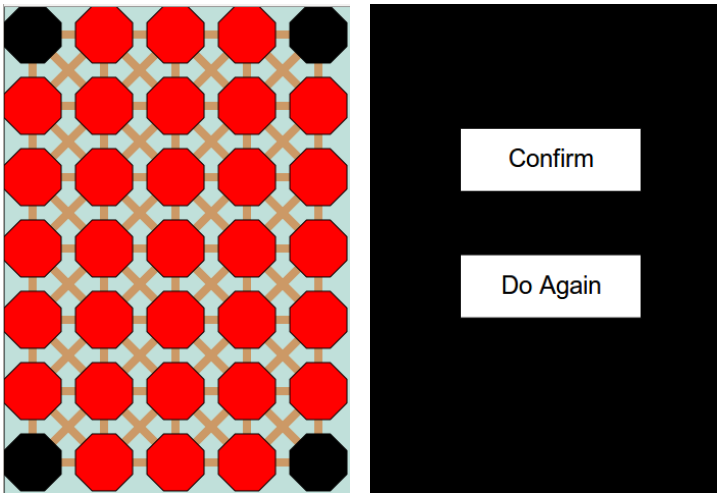


Figure 5.1: The initial page of TMD and DAS



(a) Main interface (b) Confirmation page

Figure 5.2: TMD Interface

Figure 5.3 is the main interface of DAS. In order to match the configuration of TMD, we also used a 5×7 grid for the users to enter their passwords. On this page, users may clear the screen by using the *clear* button or send their password by using the *send* button. While entering the password, users are allowed to clear the drawing as many times as desired. An explicit send button was needed to signify that drawing the password was finished beecause it could consist of multiple strokes.

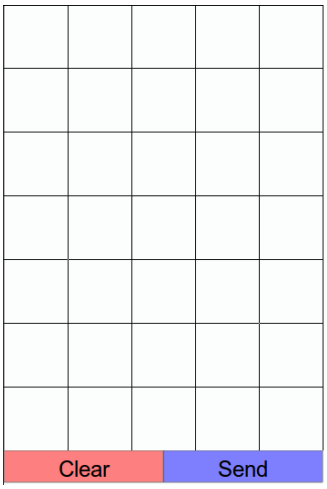


Figure 5.3: DAS interface

5.4 Participants

We recruited 90 participants from the university campus. There were 46 females and 44 males; the average age of the group is 23 years old. Among these participants, 13 (14.4%) studied at Ph.D. level, 13 (14.4%) studied at masters' level, 59 (65.5%) studied at undergraduate level, and 5 (5.5%) did not answer the question. In addition, 72 participants (80%) owned at least one smart phone for at least six months and 18 participants (20%) owned at least one tablet computer for at least six months.

Regarding their experience with graphical password schemes, 57 participants (63%) had seen a graphical password before and 29 (32%) had used a graphical password scheme before. Of these, almost all the participants reported experience with the unlock screen of the Google Android operating system.

5.5 Protocol

This experiment was approved by Carleton University Research Ethics Board. The study used a 2×2 design, with participants randomly assigned to one of the four groups testing TMD on iPod, DAS on iPod, TMD on iPad, and DAS on iPad; there were 22, 23, 23 and 21 participants per group respectively. The user study was carried

out in two thirty-minute sessions scheduled 5-10 days apart in a lab environment.

5.5.1 Session 1

In the first session, the participants were told that they will be testing the usability of a graphical password scheme on a mobile device. They were asked to create a password which they think is safe and memorable. If the participant had no further questions, the remainder of the first session was carried out with the following steps:

Step 1: Introduce the scheme. Participants were given verbal instruction on how to use the scheme.

Step 2: Create password. On their assigned device, users created a password which they thought they would remember. They may try as many times as necessary.

Step 3: Confirm password. Users confirmed the password by re-entering it again. If unable to confirm, they were asked to create another password, returning to step 2.

Step 4: Answer questionnaire. On a desktop computer, users answered a questionnaire to provide feedback regarding their opinion and perceptions of their assigned scheme. The questionnaire was programmed as an online survey and consisted of eight Likert scale and three open-ended questions. The list of questions can be found in Appendix E.

5.5.2 Session 2

At the beginning of the second session, the participants were asked to login using the password created in the first session; they had three chances to enter the password correctly. They were also told that there will be no penalty if they could not get the password right within three tries. The rest of the second session was carried out with the following steps:

Step 1: Login On the mobile device, users re-enter the password which they created previously. If unable to login within three tries, users stop and move on to the next step.

Step 2: Answer questionnaires. Three questionnaires were given to the users on the desktop computer. The first questionnaire was about the user's experience; it consisted of Likert scale and open-ended questions. The list of questions can be found in Appendix F. The other two questionnaires were on demographics (Appendix D) and past experiences with mobile devices (Appendix G).

5.6 Results and Interpretation

In this section, we compared the data collected from TMD and DAS to determine the usability of TMD on mobile devices. The compared data includes password creation time, password length, login time, login success rate, and questionnaire responses. We used two-way ANOVA for the initial test and T-tests for between group tests to compare password creation time, password length and login time. For the login success rates, we used Fisher's Exact test. We also looked at the questionnaires to see what participants like or dislike about the schemes; we used Mann-Whitney U test to test Likert scale questions. For all the statistical tests, we set the alpha value to be 0.05 which means there is only 5% probability that the results can occur by chance.

5.6.1 Password Creation Time

Figure 5.4 shows the password creation time for each group (TMD on smart phone, TMD on tablet computer, DAS on smart phone, and DAS on tablet computer). The password creation time is measured from the time when the *Create* button is pushed until the time which the password has been confirmed and sent to the database for matching. Participants in all groups in general could complete the password creation process within a minute which we think was reasonable. Comparing the creation time using two-way ANOVA, the results showed no significant difference between the

devices ($p = 0.692$, $F = 0.158$, and $df = 1$) or the schemes ($p = 0.167$, $F = 1.939$, and $df = 1$).

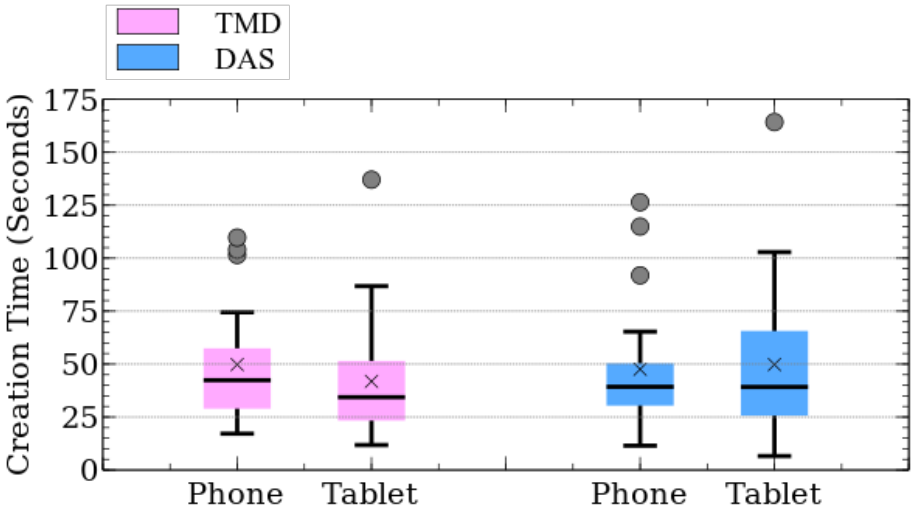


Figure 5.4: Password creation time

5.6.2 Password Length and Depth

Figure 5.5 illustrates the average password length for each test group. The average password length of each group is greater than 16 blocks/cells long which is at least 1.6 times longer than the minimum length requirement for both schemes (TMD requires minimum 10 cells and DAS requires minimum 5 blocks). Two-way ANOVA results showed that there was no significant difference in length between the devices ($p = 0.600$, $F = 0.277$, and $df = 1$) or schemes ($p = 0.352$, $F = 0.877$, and $df = 1$).

In the design of TMD, we incorporated the concept of *password depth*, i.e., the number of layers used in a password. By default, the password depth is set to 0 at the initial state and incremented when users passed though a warp cell. Figure 5.6 displayed the average password depth in this study. On both devices, the average password depths are over 1 (span over two panels) which indicated that the users were actually using this feature when creating the passwords. T-test results showed that there is

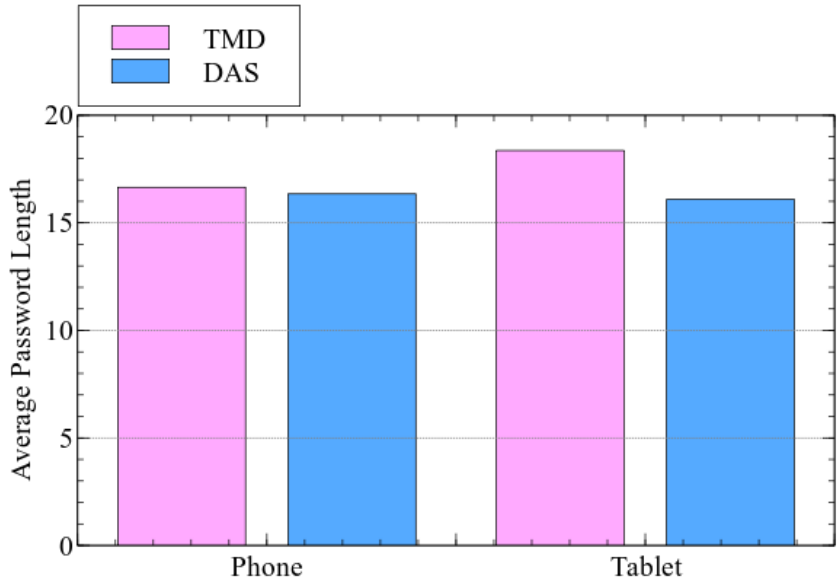


Figure 5.5: Average password length

no significant difference in depth between the devices ($p = 0.208$, $t = -1.28$, and $df = 43$).

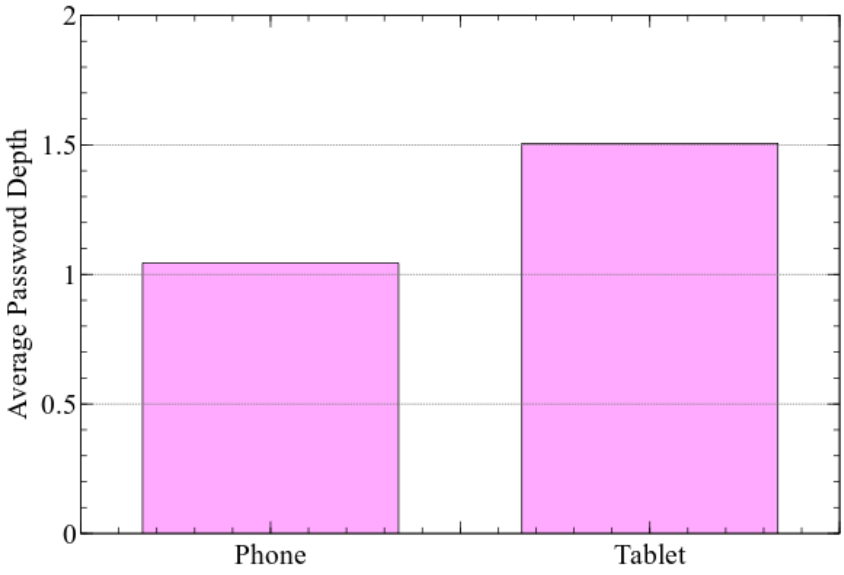


Figure 5.6: Average password depth for TMD

5.6.3 Login Time (2nd Session)

Figure 5.7 shows the average login time of a successful attempt for all groups approximately a week after password setup. The time of a successful login attempt starts when the *login* button on the initial page is pressed until the password is sent off for verification. Two-way ANOVA test results showed no significant difference in login time between the devices ($p = 0.869$, $F = 0.027$, and $df = 1$) or schemes ($p = 0.310$, $F = 1.046$, and $df = 1$). The average login time for all the groups is between 15 and 18 seconds. Forget et al.'s [29] experiment on text passwords reports an average of 8.7 seconds to enter a 8 character text password using a desktop computer. Login times in our study are longer but we expect these time to decrease once participants become more familiar with TMD and their password. Furthermore, no participant complained that login took too long during the study.

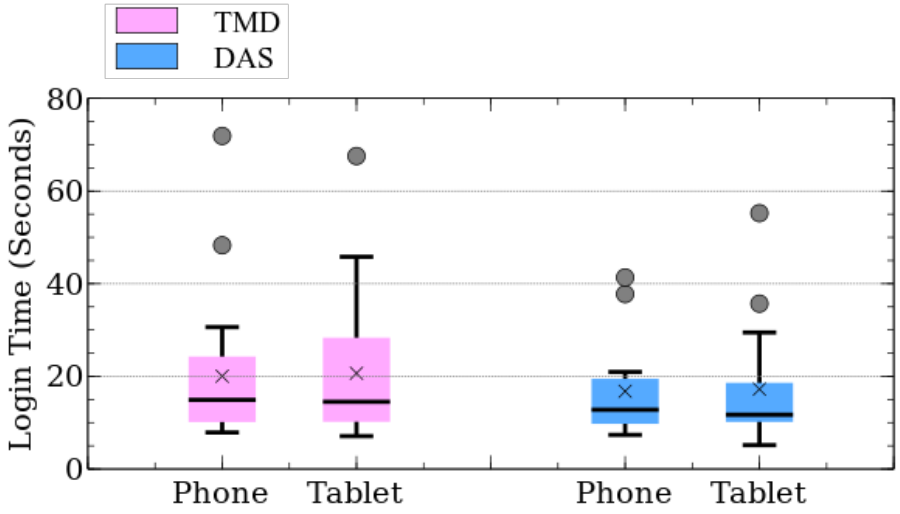


Figure 5.7: Average login time of the 2nd session

5.6.4 Login Success Rate (2nd Session)

Figure 5.1 shows the login success rate for the schemes. A week after password setup, TMD shows a login success rate of at least 95% within the first 3 tries whereas DAS

only has a 71% success rate. We used one-sided Fisher's Exact test to verify our hypothesis that TMD has a better login success rate between than DAS. For logging in successfully without any mistakes (first attempt), test results showed that TMD has a higher login success rate than DAS on the tablet computer ($p = 0.017$) but no difference when used on the smart phone ($p = 0.16$). For logging in successfully within 3 tries, test results showed that TMD has a higher login success rate than DAS on both tablet computer ($p = 0.04$) and smart phone ($p < 0.01$). These results suggested that TMD passwords were more memorable than DAS passwords especially if users are allowed a few attempts.

	TMD		DAS	
	Phone	Tablet	Phone	Tablet
Success on the first try	86.36%	86.36%	66.67%	57.14%
Success within 3 tries	100%	95.45%	71.43%	71.43%

Table 5.1: Login success rate

5.6.5 Observations and User Feedback

During this study, we observed and recorded noteworthy behaviours. In addition, we noted any feedback or questions that the participants had during the two sessions. This information gave us insight on how to improve the design of our scheme or the study in the future.

TMD

The first thing we noticed with TMD was the absence of the fuzzy boundaries problem. Our observations indicated that participants tended to use more vertical and horizontal strokes in their passwords than diagonal strokes. However, for those who used diagonal lines in the passwords, the participants had no problem confirming the passwords. Some participants complained that they could remember the shape of their password but were not sure which cell was their starting point in the second session. Unlike DAS passwords which relied solely on shapes, some TMD users used

the unique color from each panel to help memorize their passwords, providing us with positive feedback on this feature.

DAS

Some participants who used DAS on iPod complained that it was hard to draw the lines accurately because the line was covered by the participants' own fingers. As in the preliminary study (section 3.6.4), the fuzzy boundaries problem affected many participants and they could not correctly confirm their passwords. Also, similar to TMD, some participants said that they had problems remembering the starting point of their passwords in the second session.

5.6.6 Questionnaire Response

The user perception of the graphical password scheme is an important factor which affects usability. In both sessions, we asked users to complete questionnaires to provide us with feedback. Appendix E and F list the questions we asked the users; the questionnaires contains two types of questions: Likert scale and open-ended questions. For the Likert scale questions, we asked users to give a score to each of the statement listed. The scores ranged from 1 to 5, with 1 being strongly disagree and 5 being strongly agree. We used Mann-Whitney U tests to compare the Likert scale questions between different test groups. We grouped the Likert scale questions into 3 categories for discussion: form factor, graphical password scheme, and password memorability.

Form Factor

For form factor, we compare responses between the smart phone and tablet computer groups for each scheme. Consistent with the preliminary study (sections 3.6.5, 3.6.3, and 3.6.2), participants generally felt that DAS is harder to use with a small screen. However, the size of the screen did not affect the participants' perception about TMD.

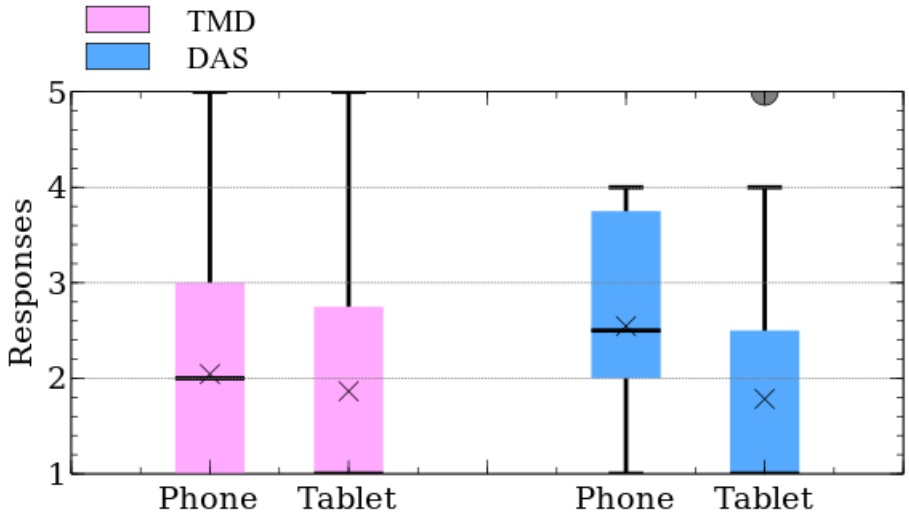


Figure 5.8: User responses to: "The size of the screen on this device makes the scheme hard to use" (1 = strongly disagree, 5 = strongly agree)

Figure 5.8 illustrates the box plot of the question *The size of the screen on this device makes the scheme hard to use*. Favourable responses are represented by lower scores. A Mann-Whitney U test indicated that DAS users generally found it more difficult to use the scheme on a small screen ($p = 0.021$, $U = 154.0$, and $z = 2.304$) while TMD users in general did not feel that the screen size can affects the usability ($p = 0.553$, $U = 228.0$, and $z = 0.593$). Average scores for each test group were 2.0 (TMD on smart phone), 1.8 (TMD on tablet computer), 2.5 (DAS on smart phone), and 1.7 (DAS on tablet computer). The scores indicate that TMD was generally easy to use regardless the size of the screens. On the other hand, users felt that the small screen made DAS more difficult to use.

Figure 5.9 shows the box plot of the question *I find it hard to create a graphical password using this scheme without making any mistakes*. In this question, Mann-Whitney U test results showed there is no significant different between different devices when using TMD ($p = 0.573$, $U = 228.5$, and $z = 0.564$) or DAS ($p = 0.327$, $U = 210.5$, and $z = 0.979$). The phrasing of this question meant that a response of 1 was most positive. The average score of the test groups is between 2.3 and 2.8 indicating

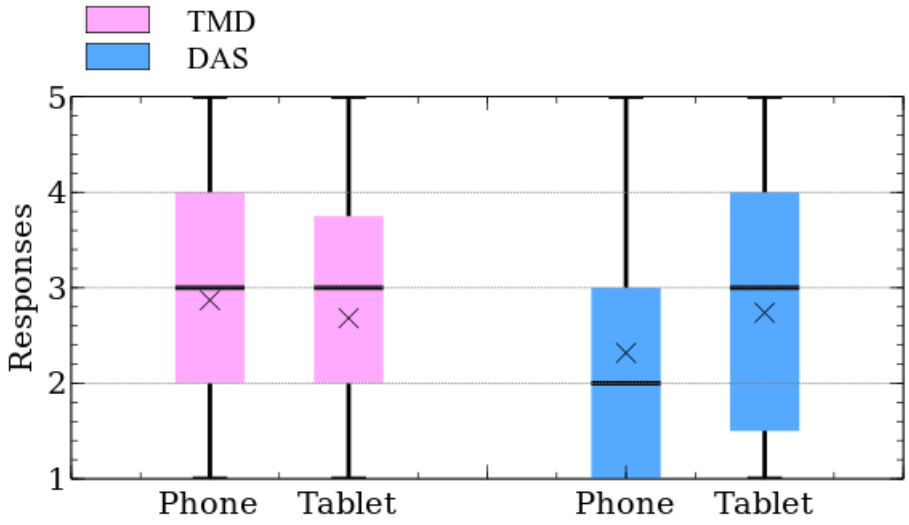


Figure 5.9: User responses to: "I find it hard to create a graphical password using this scheme without making any mistakes" (1 = strongly disagree, 5 = strongly agree)

that participants generally found it neither easy or difficult to create new graphical passwords.

Graphical Password Scheme

The design of the graphical password scheme has a direct impact on users' perception and opinion. A good graphical password scheme should be easy to understand and use so that the users are willing to use it. The following is a list of relevant questions which we asked the participants in this study. In this section we compare responses between TMD and DAS regardless of form factor.

Figure 5.10 is the box plot of the question *It was easy to understand how the scheme works*. Positive responses are indicated by higher scores. Mann-Whitney U test showed no significant difference between TMD and DAS ($p = 0.517$, $U = 941.5$, and $z = 0.649$). The average scores for the two schemes are both 4.6, showing that participants felt that the schemes are extremely easy to learn.

Figure 5.11 illustrates the box plot of the question *I am more willing to use this*

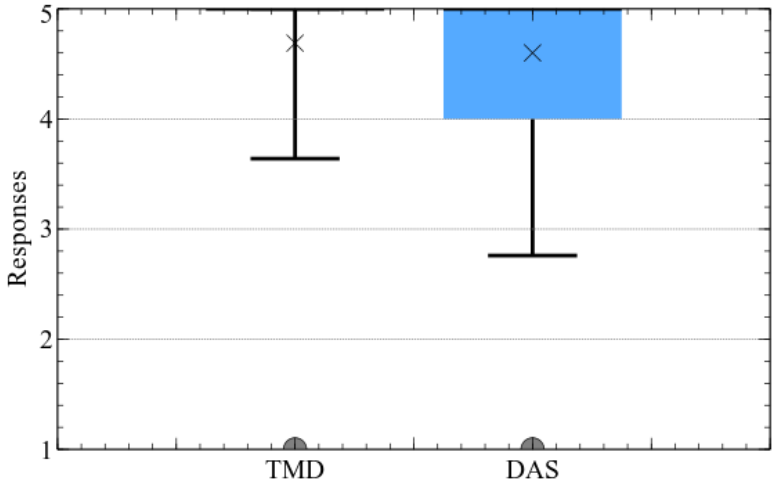


Figure 5.10: User responses to: "It was easy to understand how the scheme works" (1 = strongly disagree, 5 = strongly agree)

password scheme than traditional text-based passwords on this device. More favorable responses are the higher scores. In this question, the statistical test showed that participants are more willing to use TMD than DAS ($p = 0.048$, $U = 771.0$, and $z = 1.979$) to replace traditional text-based passwords. TMD scored an average of 3.8 (median = 4) and DAS scored an average 3.3 (median = 3) in this question, showing that participants generally would prefer to use TMD than DAS to replace text passwords on a touchscreen device.

Figure 5.12 shows the box plot of the question *I would use this graphical password for my important accounts (e.g., online banking).* A higher score is more favorable in this question. The test results for this question showed that participants gave TMD significantly higher scores than DAS ($p = 0.013$, $U = 673.0$, and $z = 2.496$). The average scores for TMD and DAS in this question are 3.6 and 2.9. The scores showed that users generally felt that TMD passwords can provide sufficient protection for their important accounts whereas DAS might not.

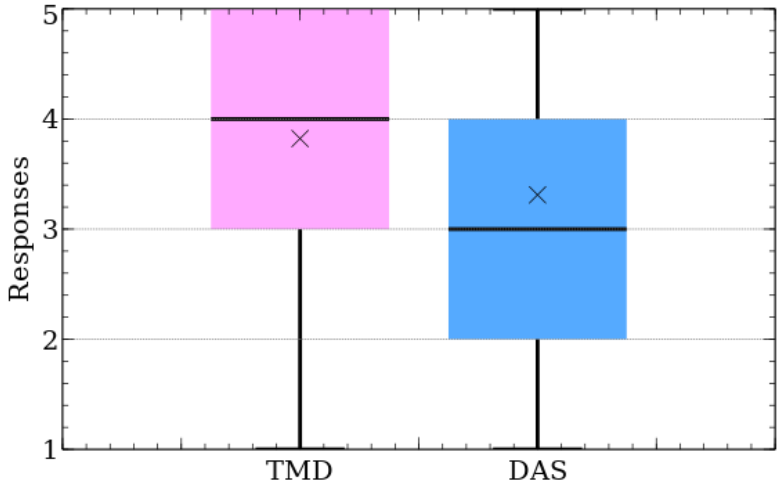


Figure 5.11: User responses to: "I am more willing to use this password scheme than traditional text-based passwords on this device" (1 = strongly disagree, 5 = strongly agree)

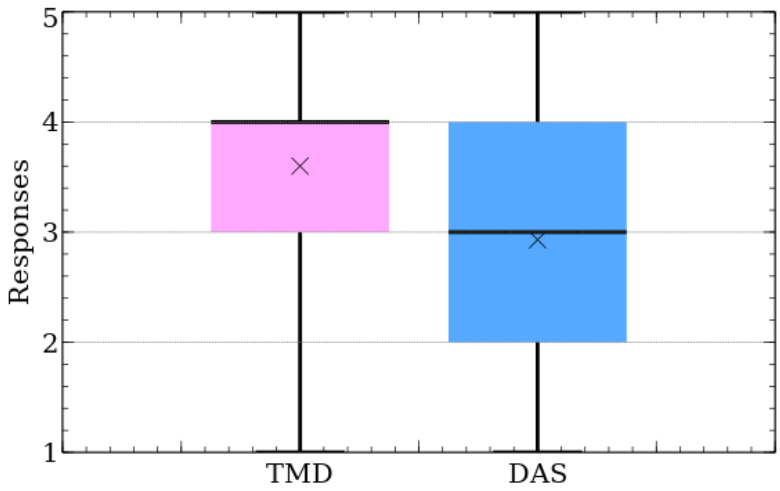


Figure 5.12: User responses to: "I would use this graphical password for my important accounts (e.g., online banking)" (1 = strongly disagree, 5 = strongly agree)

Graphical Password Memorability

The ability to create memorable and secure passwords is also important for graphical password schemes. Passwords that are easy to remember can reduce security risks such as writing down or reuse of passwords. Although actual password memorability

has been looked at in section 5.6.4, the questionnaire questions can still provide us with useful information about users' perception. In this section we compare TMD and DAS regardless of device.

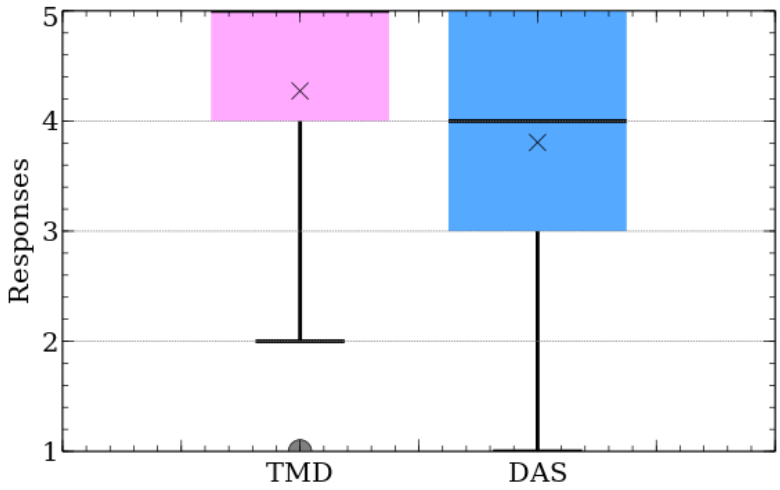


Figure 5.13: User responses to: "It was easy to remember the password" (1 = strongly disagree, 5 = strongly agree)

Figure 5.13 is the box plot of the question *It was easy to remember the password* which we asked the participants in session 2. Higher scores are more favorable for this question. The average score for TMD is 4.2 (median = 5)and DAS is 3.8 (median = 4), indicating that the participants felt that passwords were memorable. Mann-Whitney U test results showed that there is no significant difference between the two schemes ($p = 0.272$, $U = 782.0$, and $z = 1.099$). Although DAS participants thought that memorizing the passwords was easy, this is inconsistent with the login success rate discussed in section 5.6.4, which showed that they had significantly more difficulty than TMD users.

Figure 5.14 shows the box plot of the question *I will be able to remember more than one graphical password using this scheme*. Positive responses are indicated by higher score. Statistical test results showed no significant difference between TMD and DAS ($p = 0.404$, $U = 790.0$, and $z = 1.834$). The average scores for TMD and DAS are 3.6 (median = 4) and 3.3 (median = 3) indicating that the participants are mildly

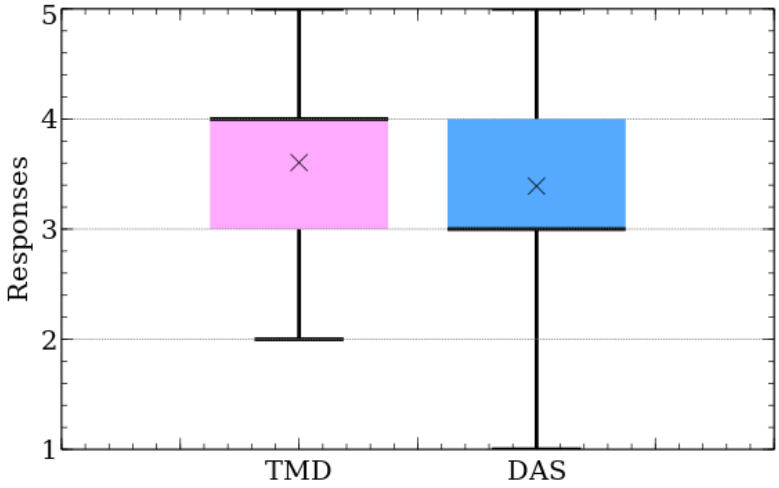


Figure 5.14: User responses to: "I will be able to remember more than one graphical password using this scheme" (1 = strongly disagree, 5 = strongly agree)

confident that they might be able to remember more than one password using the same scheme.

5.6.7 Open-ended Questions

At the end of both sessions, we asked the participants to provide us with feedback on what they liked or disliked about the scheme they just tested. We have summarized the most significant negative issues raised by the participants in table 5.2. A number of noteworthy positive qualities of the schemes were also mentioned by the participants; table 5.3 lists these qualities.

The responses from open-ended questions showed that both TMD and DAS shared some good qualities such as input speed and drawing of the passwords. Interestingly, the things which the participant did not like about the two schemes are very different. In TMD, the complaints where more focused on the operation system or hardware problems such as the friction of the screen surface or accidentally sliding out the top menu in iOS. In DAS, the complaints were more focused on the design of the scheme and its use on a small touchscreen.

Scheme	Common Negative Issues
TMD	• The friction created by the long stroke made it difficult to draw • It was hard to think of a pattern which uses only one line • Accidentally activating the top panel of the iOS
DAS	• Difficult to draw the lines accurately on the small screen • Cannot draw diagonal lines • Difficult to remember the starting point of the password

Table 5.2: Common negative issues raised by participants

Scheme	Common Positive Characteristics
TMD	• It is faster enter TMD passwords than text passwords • Not having to type the passwords • The password can be entered with one fluid motion
DAS	• Not having to type the passwords • Able to associate shapes or images with the passwords • It is faster enter DAS passwords than text passwords

Table 5.3: Common positive characteristics mentioned by participants

5.7 TMD password patterns and distribution

We collected 45 TMD passwords in total and examined these passwords for distinctive patterns. We described these patterns in table 5.4. These patterns represent broad categories and would also be present to some degree in random passwords. Some of these patterns are on a single layer or across multiple layers; example passwords for each pattern are available in appendix H. Previous studies have already shown that DAS passwords contain patterns [54]; as the result, we only focus on a preliminary analysis on TMD in this section.

We visually inspected each password and classified it into the most fitting category. Passwords that did not fall into one of the six identified patterns were classified as

"abstract", meaning that they had no discernible pattern. For passwords which use multiple layers, we superimpose all the layers before we inspect the passwords. If a password qualified for more than one category, the category with the largest order number (as specified in table 5.4) will claim the password.

Figure 5.15 shows the distribution of each pattern in this study. Other than the abstract drawing, the top three most popular categories are: *Along the edges*, *Simple Shapes*, and *Back-trace*; these three categories make up 42.1% of all the passwords collected in this study. Similar analysis was done on other graphical password schemes by Tao et al. [63], van Oorschot et al. [54], and Chiasson et al. [12]. We did not compare our results with other studies because TMD is a scheme which uses multiple layers, making the password patterns unique from other schemes. As suggested by van Oorschot and Thorpe's study [54], the predictability of the passwords can be used to prioritize the list of passwords used in a dictionary attack so this issue will need further exploration in TMD. We believed that by adjusting the password policy of TMD and providing guidance on password selection, we can reduce the concentration of the patterns. However, this requires further studies to prove or disprove our assumption.

Category	**Order**	**Definition**
Recognizable symbols	1	Symbols which are well known to others such as the English alphabet, Arabic numbers, or mathematical operators
Back-trace	2	The path of the password on the current layer is identical to the previous layer but the direction of the path is reversed
Recognizable patterns	3	Recognizable paths such as spiral or zigzag patterns
Symmetric	4	Shapes that are symmetric about an axis, the axis can be vertical or horizontal
Along the edges	5	Uses only the cells on the edges of the grid
Simple shapes	6	Closed simple polygon shapes
Abstract	-	Passwords that do not follow any obvious patterns

Table 5.4: Different categories of password patterns

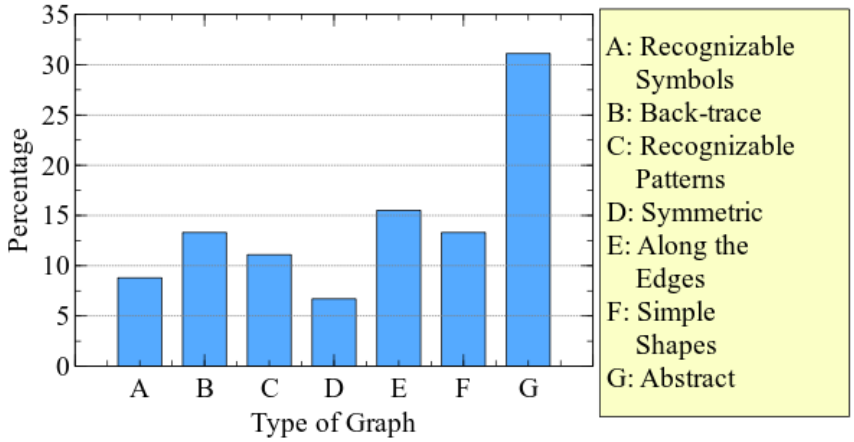


Figure 5.15: Distribution of password patterns

In addition to the password patterns, we also looked at the distribution of the starting points of the passwords. Similar to the password patterns, the distribution of the starting points can also be used by the attacker to create a more efficient list for dictionary attacks. Figure 5.16 shows the distribution of the 45 starting points collected. Given the number of cells, we would expect approximately half of starting points to be on an edge if the distribution was random. From our analysis, 93% of participants picked cells that are on the edges of the grid as starting points. Within the starting points on the grid edge, 88.1% are next to a warp cell. The lack of visual reference on the interface might have caused this concentration of starting points. Adding additional visual references in the scheme and studying their effect of the distribution of starting points should be included in future work.

5.8 Improved Encoding

During the course of our analysis, we discovered an encoding problem. Although we do not believe that it impacted our results, we discuss it as a cautionary note to anyone implementing such schemes. In order to maintain the size of the password space and the security of the scheme, each unique TMD password should have one and only one corresponding string representing it. However, we discovered that in our prototype it is possible to find two different TMD passwords with the same encoded string. This

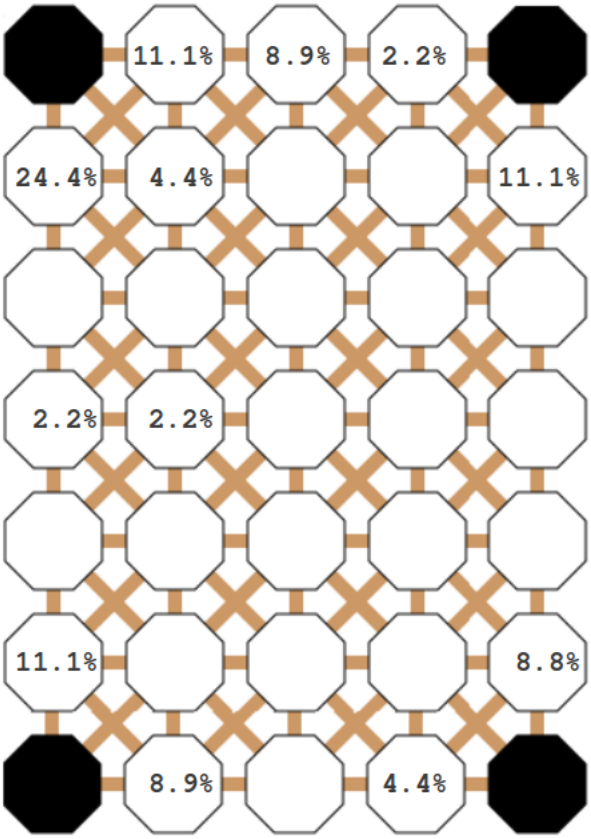
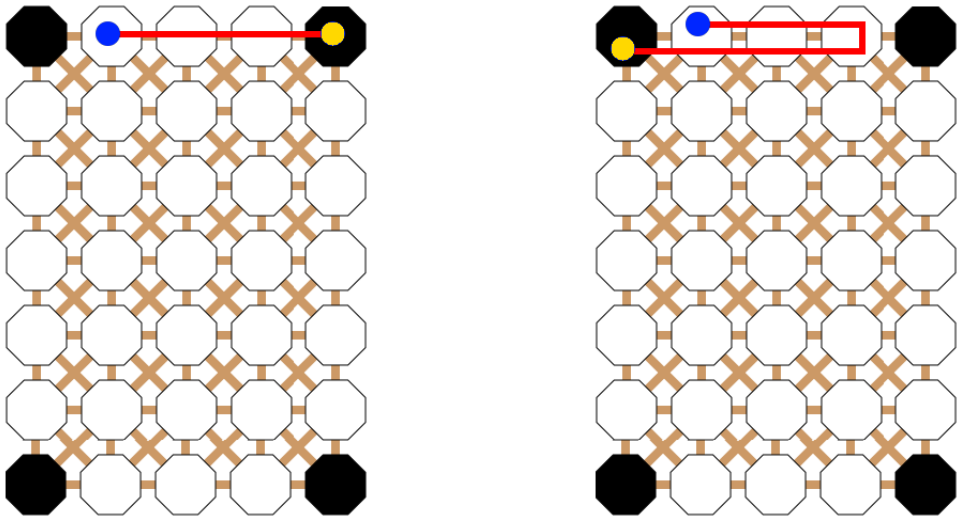


Figure 5.16: Distribution of the starting points of the passwords

occurs because all four warp cells share the same alpha-numerical representation. As an example, figure 5.17 shows two different TMD passwords that have the same encoded string: *(1,2,3,W)*. This problem can easily be corrected by giving each warp cell a unique alpha-numerical representation (figure 5.18).

5.9 Limitation of the Study

Although this study was carefully prepared, some tradeoffs were made. The study only asked users to remember the password for about a week before they had re-login. A week offers a reasonable first measure of memorability but further exploration is needed. The test groups contain about 20 participants each, from a university environment; this may not be fully representative of the mobile user population. The participants used the scheme in a controlled environment which might eliminate



(a) (b)

Figure 5.17: Two TMD passwords which share the same encoded string (blue dots indicate the starting point and yellow dots indicate the ending point)

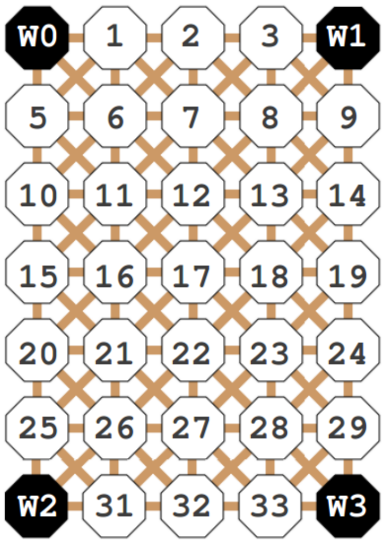


Figure 5.18: Improved TMD encoding

some of the factors that can affect the usability of the graphical password schemes. This was a necessary first step in evaluation, but further studies should explore more realistic scenarios, such as having the passwords protect real accounts, being used on different platforms, having different environments or conditions, and having multiple passwords to remember.

5.10 Discussion

In this study, our data indicated a high concentration of starting points which might decrease the security of the scheme. Learning from other similar schemes [24], adding background images to serve as visual references might help users to select their starting points. However, since users did not like to memorize unfamiliar images as part of their password in our preliminary study; an alternative solution is to allow users upload their own images. The down side of allowing users to use their own images is that they might use an image containing obvious cues. Another possible visual cue is to make certain cells have different colors. However, the number of reference cells can also affect the usability and the memorability of the scheme. If there are only a few reference cells, we might still find a concentration of starting points. On the other hand, if we place too many reference cells, users might be distracted and forget their starting points.

One possible reason why we had many password patterns is because we did not instruct users on how to create a secure TMD password during the experiment. Similar to text passwords, if users do not have knowledge of what is a secure password, they are more likely to choose a password which is a common dictionary word [2]. Therefore, deployment of TMD should include a set of instructions on what is a secure TMD password and include a strong password policy which reinforces these guidelines. Some possible policies might include encouraging users to use multiple layers in their passwords, limiting the number of cells in the password that are on the edges of the grid, or asking users to go through preselected cells at least once. By adding such rules, the memorability of the scheme might decreased and should be further evaluated.

We have discussed some measures which we can take to make the scheme more secure; however, the usability of the scheme might decrease if we force more restrictions upon the users. At the end, regardless what methods we decide to use to make the scheme stronger against attacks, we need to carefully plan our strategy so there is a balance between security and usability.

It is also worth hightlighting the features of TMD that were successful and that make TMD a usable scheme. One of these qualities is the concept of warp cells and multiple layers. During our test, users had no problem understanding the concept of layers and how to reach the next layers by using warp cells. The visual design of the scheme is very intuitive, making the scheme easy to understand and use. This simplicity encouraged users to create longer passwords than the minimum required length. Over 95% of the participants were able to remember the password after a week even though they have never used the scheme before. On the contrary, only 71% of the participants were able to remember their DAS passwords which is significantly less than TMD. Another advantage of TMD is that it is compatible with existing services that use text password to authenticate users. TMD converts the graphical password into a long string of characters locally before sending the data to the servers, so it is possible to deploy TMD to an existing service without having to modify back-end databases.

5.11 Conclusions from the Study

In this study, we found that TMD has some advantages over DAS. First, TMD passwords were more memorable than DAS passwords after one week. Second, TMD is easier to use on a touchscreen when compared with text passwords or DAS. Third, TMD offered more confidence for users than DAS when asked if they were willing to use this scheme to protect important accounts. Finally, TMD eliminated the fuzzy boundaries problem that users experienced with DAS. In all other measures, TMD performed at least as well as DAS. Based on this evidence, we feel that TMD is a more usable graphical password scheme for touchscreens than DAS.

Chapter 6

Conclusion and Future Work

In this chapter, we summarize our contributions and our findings. At the end of this chapter, we discuss some potential future work to improve the scheme.

6.1 Summary of Contributions

In this thesis, we:

1. Conducted a 31 user comparative study of three existing graphical password schemes which we implemented on smart phone and tablet computers;

2. Designed and implemented TMD — a new graphical password scheme specific for small touchscreens;

3. Conducted a 90 user one-week study comparing TMD to the existing Draw A Secret (DAS) scheme on smart phone and tablet computers.

We conducted a preliminary user study to test existing graphical password schemes on mobile devices to have a better understanding of how touchscreens can affect their usability. In this preliminary study, 31 participants tested DAS [45], PCCP [11], and Object Recognition [39] using either an iPad or an iPod Touch. The schemes were instrumented to record users' interaction and input for analysis. In addition, questionnaires were given to the participants to provide us with feedback.

Data from the preliminary study indicated that DAS was the only scheme affected by the screen size. With the small screen, users not only created shorter passwords during setup but also made more mistakes when logging in. From the questionnaires

we learned two things: first, the participants did not like to use DAS on a small screen because it was difficult to accurately enter passwords. Second, participants did not like to memorize unfamiliar images as part of their passwords. From our observations, we realized that many DAS users suffered from the fuzzy boundaries problem [76].

We designed TMD based on the results from the preliminary study; it is a user-drawn graphical password scheme. The interface of TMD is composed of cells which are not attached to each other. The large cells were intended to reduce errors caused by accuracy problems and the space between the cells were intended to eliminate the fuzzy boundaries problem. Different from other recall-based schemes, some features were added to maximize the grid size while maintaining a large theoretical password space: first, the main interface screen does not have any buttons; the scheme can sense the end of a password entry when users lift their fingers. Second, TMD introduced the concept of layers; each layer is identified using a different color. With multiple layers, the length of the password is bounded by the device memory or system configuration but not the screen size.

To measure the usability of TMD on mobile devices, we conducted another user study where participants tested TMD or DAS using an iPad or iPod Touch; 90 participants took part in this study. The study was divided into two sessions that were 5 to 10 days apart; users were asked to create a graphical password in the first session and asked to login using their passwords in the second session. In both sessions, the performance of these participants were recorded for analysis using PHP scripts and SQL databases and online questionnaires were given to gather their feedback.

6.2 Summary of Results

We discovered several advantages of TMD over DAS. Statistical data showed that TMD passwords are more memorable than DAS passwords; more than 95% of the TMD users could remember the password after a week while only 71% of the DAS users could do the same. The questionnaire responses indicated that participants are more willing to use TMD than DAS to replace text passwords on mobile devices.

Lastly, we observed that TMD users did not encounter the fuzzy boundaries problem. The analysis of password patterns and distributions showed that TMD passwords may be predictable; 68% of the passwords contain recognizable patterns and 93% of the passwords start from the edge of the grid. However, the number of sample used in the password analysis was very limited (only 45 TMD passwords were collected) so further exploration is recommended. Adding visual references and improving the password policy might reduce the predictability of passwords.

6.3 Future Work

Future work should focus on the security aspects of the scheme. We identify three general directions for such future work. A larger scale user study should be conducted to collect more samples to help in analysing the patterns and the distributions of the passwords. The same data can also help us to identify possible attacks on TMD which eventually can help us to improve the security of the scheme. In addition, a larger scale user study can help us to better evaluate password memorability, scheme design, and suitability for different form factors. Another interesting topic for the future work is to assess TMD's resistance to shoulder surfing attacks under different environmental conditions. A password policy is an important part of any password schemes when user choice of passwords is allowed. However, a strong password policy may reduce the usability of the scheme if it is not carefully designed. We believe that users are more likely to remember their passwords if they had input into their selection, but realized that they will need some guidance and restrictions to ensure the security of the system. An interesting area to explore is how to develop a strong password policy which can increase security without sacrificing the usability of the scheme.

Bibliography

[1] Muhammad Daniel Hafiz Abdullah, Abdul Hanan Abdullah, Norafida Ithnin, and Hazinah Kutty Mammi. Towards identifying usability and security features of graphical password in knowledge based authentication technique. In *Proceedings of the 2008 Second Asia International Conference on Modelling & Simulation (AMS)*, AMS '08, pages 396–403, Washington, DC, USA, 2008. IEEE Computer Society.

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

[3] 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.

[4] Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX conference on Offensive technologies*, WOOT'10, pages 1–7, Berkeley, CA, USA, 2010. USENIX Association.

[5] Susamma Barua. Authentication of cellular users through voice verification. In *Proceedings of IEEE International Conference on System, Man, and Cybernetics*, volume 1, pages 420–245, 2000.

[6] Andrey Belenko and Dmitry Sklyarov. "secure password managers" and "military-grade encryption" on smartphones: Oh, really? Technical report, Elcomsoft Co.Ltd., http://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf, 2012.

[7] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Transation Information System Security*, 5(4):367–397, November 2002.

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

[9] Hristo Bojinov and Dan Boneh. Mobile token-based authentication on a budget. In *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications*, HotMobile '11, pages 14–19, New York, NY, USA, 2011. ACM.

[10] S. Brostoff and M. A. Sasse. Are passfaces more usable than passwords? A field trial investigation. In *Proceedings of HCI*, pages 405–424, 2000.

[11] 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.

[12] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. User interface design affects security: patterns in click-based graphical passwords. *The International Journal of Information Security*, 8(6):387–398, October 2009.

[13] Sonia Chiasson, P. C. Van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *In Proceedings of the 15th USENIX Security Symposium*, pages 1–16, 2006.

[14] Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. Graphical password authentication using cued click points. In *ESORICS*, pages 359–374, 2007.

[15] N. L. Clarke and S. M. Furnell. Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*, 6(1):1–14, December 2006.

[16] Nathan L. Clarke and Steven Furnell. Authentication of users on mobile telephones - a survey of attitudes and practices. *Computers & Security*, 24(7):519–527, 2005.

[17] M.F. Coleman, B.A. Loring, and M.E. Wiklund. User performance on typing tasks involving reduced-size, touch screen keyboards. In *Vehicle Navigation and Information Systems Conference, 1991*, volume 2, pages 543 – 549, oct. 1991.

[18] Passfaces Corporation. The science behind passfaces. `http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf`. Accessed June, 2012.

[19] George C. Dalton, II, Kenneth S. Edge, Robert F. Mills, and Richard A. Raines. Analysing security risks in computer and radio frequency identification (rfid) networks using attack and protection trees. *International Journal of Network Security*, 5(2/3):87–95, March 2010.

[20] Rachna Dhamija and Adrian Perrig. Déjà 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.

[21] 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.

[22] Paul Dunphy, Andreas P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 3:1–3:12, New York, NY, USA, 2010. ACM.

[23] Paul Dunphy, James Nicholson, and Patrick Olivier. Securing passfaces for description. In *Proceedings of the 4th symposium on Usable privacy and security*, SOUPS '08, pages 24–35, New York, NY, USA, 2008. ACM.

[24] 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.

[25] Khaldoun Al Faraj, Mustapha Mojahid, and Nadine Vigouroux. Bigkey: A virtual keyboard for mobile devices. In Julie A. Jacko, editor, *Human-Computer Interaction. Ambient, Ubiquitous and Intelligent Interaction, 13th International Conference, HCI International 2009, San Diego, CA, USA, July 19-24, 2009, Proceedings, Part III*, volume 5612 of *Lecture Notes in Computer Science*, pages 3–10. Springer, 2009.

[26] P. M. Fitts. The information capacity of the human motor system in controlling the amplitude of movement. *Journal of Experimental PSychology*, 74:381–391, 1954.

[27] D. Florencio, C. Herley, and B. Coskun. Do strong web passwords accomplish anything? In *the 2nd USENIX workshop on hot topics in security*, pages 1–6, 2007.

[28] Alain Forget, Sonia Chiasson, and Robert Biddle. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 1107–1110, New York, NY, USA, 2010. ACM.

[29] Alain Forget, Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. Improving text passwords through persuasion. In *Proceedings of the 4th symposium on Usable privacy and security*, SOUPS '08, pages 1–12, New York, NY, USA, 2008. ACM.

[30] Google. `http://www.google.com/wallet/`. Accessed October, 2012.

[31] Google. 2-step verification. `http://support.google.com/accounts/bin/topic.py?hl=en&topic=28786&parent=2373945&ctx=topic`. Accessed June, 2012.

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

[33] Asela Gunawardana, Tim Paek, and Christopher Meek. Usability guided key-target resizing for soft keyboards. In *Proceedings of the 15th international conference on Intelligent user interfaces*, IUI '10, pages 111–118, New York, NY, USA, 2010. ACM.

[34] D. R. Hains, L. D. Whitley, and A. E. Howe. Revisiting the big valley search space structure in the TSP. *Journal of the Operational Research Society*, 62(2):305–312, 2011.

[35] J. Alex Halderman, Brent Waters, and Edward W. Felten. A convenient method for securely managing passwords. In *Proceedings of the 14th International World Wide Web Conference (WWW*, pages 471–479, 2005.

[36] Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.

[37] Niels Henze, Enrico Rukzio, and Susanne Boll. 100,000,000 taps: analysis and improvement of touch performance in the large. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11, pages 133–142, New York, NY, USA, 2011. ACM.

[38] C. Herley, P.C. van Oorschot, and A.S. Patrick. Passwords: If we're so smart, why are we still using them? In *Financial Cryptography and Data Security, LNCS 5628, Springer*, 2009.

[39] 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.

[40] Dawei Hong, Shushuang Man, Barbra Hawes, and Manton M. Matthews. A graphical password scheme strongly resistant to spyware. In *Security and Management*, pages 94–100, 2004.

[41] Yoshihisa Ijiri, Miharu Sakuragi, and Shihong Lao. Security management for mobile devices by face recognition. In *Proceedings of the 7th International Conference on Mobile Data Management*, MDM '06, pages 49–, Washington, DC, USA, 2006. IEEE Computer Society.

[42] Espirity Inc. `http://iparked.ca/iParkedBrochure.pdf`. Accessed October, 2012.

[43] Anil K Jain, Brendan Klare, and Unsang Park. Face recognition: Some challenges in forensics. *Change*, pages 726–733, 2011.

[44] Wayne A. Jansen. Authenticating Mobile Device Users Through Image Selection. *Data Security*, 2004.

[45] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Avi Rubin. The design and analysis of graphical passwords. In *8th USENIX Security Symposium*, pages 1–14, 1999.

[46] Benjamin Khoo, Peter Harris, and Syed Abbas Husain. Security risk analysis of rfid technology: a rfid tag life cycle approach. In *Proceedings of the 2009 conference on Wireless Telecommunications Symposium*, WTS'09, pages 371–377, Piscataway, NJ, USA, 2009. IEEE Press.

[47] Seungyon Lee and Shumin Zhai. The performance of touch screen soft buttons. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 309–318, New York, NY, USA, 2009. ACM.

[48] Scott I. MacKenzie and William R. Soukoreff. Text Entry for Mobile Computing: Models and Methods,Theory and Practice. *Human-Computer Interaction*, 17(2 & 3):147–198, 2002.

[49] Mobile-OTP. Mobile one time passwords. `http://motp.sourceforge.net/`. Accessed June, 2012.

[50] Fabian Monrose and Aviel D. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*, 16(4):351–359, 2000.

[51] Robert Morris, Robert Morris, Ken Thompson, and Ken Thompson. Password security: A case history. *Communications of the ACM*, 22:594–597, 1979.

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

[53] Netsize. `http://www.netsize.com/Products_mPayment-WAP-Web-billing.htm`. Accessed October, 2012.

[54] 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.

[55] Pekka Parhi, Amy K. Karlson, and Benjamin B. Bederson. Target size study for one-handed thumb use on small touchscreen devices. In *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, MobileHCI '06, pages 203–210, New York, NY, USA, 2006. ACM.

[56] Ken Perlin. Quikwriting: Continuous stylus-based text entry. In *UIST '98: Proceedings of the 11th annual ACM symposium on User interface software and technology*, pages 215–216. ACM Press, 1998.

[57] Zia Saquib, Nirmala Salam, Rekha Nair, and Nipun Pandey. Voiceprint recognition systems for remote authentication - a survey. *Internal Journal of Hybrid Information Technology*, 4(2):79–98, 2011.

[58] M. A. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3):122–131, July 2001.

[59] 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*, 12:17–22, 1993.

[60] Andrew Sears and Ben Shneiderman. High precision touchscreens: design strategies and comparisons with a mouse. *International Journal of Man-Machine Studies*, 34(4):593–613, April 1991.

[61] Ewa Syta, Stan Kurkovsky, and Bernardo Casano. Rfid-based authentication middleware for mobile devices. In *Proceedings of the 2010 43rd Hawaii International Conference on System Sciences*, HICSS '10, pages 1–10, Washington, DC, USA, 2010. IEEE Computer Society.

[62] Desney S. Tan and Mary Czerwinski. Information voyeurism: social impact of physically large displays on information privacy. In Gilbert Cockton and Panu Korhonen, editors, *Extended abstracts of the 2003 Conference on Human Factors in Computing Systems, CHI 2003, Ft. Lauderdale, Florida, USA, April 5-10, 2003*, pages 748–749. ACM, 2003.

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

[64] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords.

In Lorrie Faith Cranor, editor, *Proceedings of the 2nd Symposium on Usable Privacy and Security, SOUPS 2006, Pittsburgh, Pennsylvania, USA, July 12-14, 2006*, volume 149 of *ACM International Conference Proceeding Series*, pages 56–66. ACM, 2006.

[65] Julie Thorpe and P. C. van Oorschot. Towards secure design choices for implementing graphical passwords. In *Proceedings of the 20th Annual Computer Security Applications Conference*, ACSAC '04, pages 50–60, Washington, DC, USA, 2004. IEEE Computer Society.

[66] 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.

[67] txtNation. `http://www.mfusion.com/solutions/wap/billing`. Accessed October, 2012.

[68] Kaoru Uchida. Fingerprint-based user-friendly interface and pocket-pid for mobile authentication. *Pattern Recognition, International Conference on*, 4:4205, 2000.

[69] T. Valentine. Memory for passfaces after a long delay. Technical report, Goldsmiths College, University of London, 1999.

[70] David J. Ward, Alan F. Blackwell, and David J. C. MacKay. Dasher - a data entry interface using continuous gestures and language models. In *Proceedings of the 13th annual ACM symposium on User interface software and technology*, UIST '00, pages 129–137, New York, NY, USA, 2000. ACM.

[71] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Passpoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Study*, 63(1-2):102–127, July 2005.

[72] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*, AVI '06, pages 177–184, New York, NY, USA, 2006. ACM.

[73] Wikipedia. Multi-factor authentication. `http://en.wikipedia.org/wiki/Multi-factor_authentication`. Accessed June, 2012.

[74] Bo Wu, Haizhou AI, Chang Huang, and Shihong Lao. Fast rotation invariant multi-view face detection based on real adaboost. *Automatic Face and Gesture Recognition, IEEE International Conference on*, 0:79, 2004.

[75] R.V. Yampolskly. User authentication via behavior based passwords. In *Systems, Applications and Technology Conference, 2007. LISAT 2007. IEEE Long Island*, pages 1–8. IEEE, May 2007.

[76] 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.

[77] Saira Zahid, Muhammad Shahzad, Syed Ali Khayam, and Muddassar Farooq. Keystroke-based user identification on smart phones. In *RAID*, pages 224–243, 2009.

[78] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, pages 6:1–6:12, New York, NY, USA, 2011. ACM.

[79] 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

First Questionnaire (Preliminary Study)

1. It was easy to set up a password

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

2. It was easy to understand how the scheme works

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

3. If I didn't use this scheme for a few weeks, I would still remember how to use this scheme

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

4. I think this password scheme is hard to break by bad guys

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

5. It is easier to make mistakes when setting up a password using this scheme than traditional text-based passwords

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

6. I find it hard to create a graphical password using this scheme

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

7. I am more willing to use this password scheme than traditional text-based password

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

8. I think this scheme will be easier to use on a desktop computer than mobile devices

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

9. I would like to have some feedback from the mobile device (vibrate or sound) when I input something

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

10. What do you find the most difficult when setting up the password using this scheme?

11. What did you find easiest when re-entering a password using this scheme?

12. Do you have any other feedback about using this scheme on your mobile device?

Appendix B

Second Questionnaire (Preliminary Study)

1. It was easy to remember the password

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

2. It is easier to remember a new graphical password in this scheme than a new text-based password

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

3. This scheme was easy to use given the size of my mobile device screen.

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

4. I think this scheme will be easier to use if I have a more accurate input method (e.g., using a touch screen pen)

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

5. I will be able to remember more than one graphical password using this scheme

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

6. What do you find the most difficult when re-entering a password using this scheme?

7. What did you find easiest when re-entering a password using this scheme

8. Do you have any other feed back about using this scheme on your mobile device?

Appendix C

Questionnaire for User Experience (Preliminary Study)

1. Do you own a smart phone?(if answered No, skip to question 10)

   ☐ Yes ☐ No

2. What type(s) of input methods does your phone have?

   ☐ Touch Screen ☐ Physical Keyboard ☐ Voice Recognition ☐ Others:

3. What operating system(s) is your smart phone running?

   ☐ Android ☐ iOS ☐ Symbian ☐ BlackBerry ☐ Windows Mobile ☐ Others:

4. How long have you been using a smart phone?

   Years: Months:

5. When do you enter a username/password on your smart phone?

   ☐ Never

   ☐ Only once because I store all passwords on my smart phone

   ☐ I only type some of my important passwords (e.g., online banking)each time I wish to log in

   ☐ I type all my passwords each time I wish to log in

6. How often do you enter a username/password on your smart phone?

   ☐ At least once a day ☐ Several times a week ☐ Once a week ☐ Less than

once a week

7. I often make mistakes when typing my username/password on my smart phone (please circle)

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

8. Where do you use your smart phone the most often?

   ☐ Home
   ☐ School
   ☐ Work place
   ☐ Public Place
   ☐ while traveling/commuting
   ☐ Others:

9. How do you usually operate your smart phone?

   ☐ Hold the device with one hand, operate the device with the other hand
   ☐ Use the same hand to hold and operate the device
   ☐ Depends (please specify):

10. Do you own a tablet computer?(if answered No, skip to question 18)

    ☐ Yes ☐ No

11. What type(s) of input methods does your tablet computer have?

    ☐ Touch Screen ☐ Physical Keyboard ☐ Voice Recognition ☐ Others:

12. What operating system(s) is your tablet computer running?

    ☐ Android ☐ iOS ☐ Symbian ☐ BlackBerry ☐ Windows Mobile ☐ Others:

13. How long have you been using a tablet computer?

    Years: Months:

14. When do you enter a username/password on your tablet computer?

    ☐ Never

    ☐ Only once because I store all passwords on my tablet computer

    ☐ I only type some of my important passwords (e.g., online banking)each time I wish to log in

    ☐ I type all my passwords each time I wish to log in

15. How often do you enter a username/password on your tablet computer?

    ☐ At least once a day ☐ Several times a week ☐ Once a week ☐ Less than once a week

16. I often make mistakes when typing my username/password on my tablet computer (please circle)

Strongly Disagree										Strongly Agree
	1	2	3	4	5	6	7	8	9	10

17. Where do you use your tablet computer the most often?

    ☐ Home
    ☐ School
    ☐ Work place
    ☐ Public Place
    ☐ while traveling/commuting
    ☐ Others:

18. How do you usually operate your tablet computer?

    ☐ Hold the device with one hand, operate the device with the other hand
    ☐ Use the same hand to hold and operate the device
    ☐ Depends (please specify):

19. Have you seen a graphical password before?

☐ Yes ☐ No

20. If Yes, where did you see it (please specify)?

21. If Yes, how often to do use it?

Appendix D

Questionnaire for User Background (Preliminary and Main Study)

This information will be held completely confidential. (Please, do not put your name on this form!)

Age: _____ years

Gender: male female

At what level are you studying?

Undergraduate Masters Ph.D. Other

What year of study are you in? _____

In what academic program are you enrolled?

Have you ever used a graphical password before?

Have you ever been in a graphical password study before? If so, please describe the study.

Appendix E

First Questionnaire (Main Study)

1. It was easy to understand how the scheme works

Strongly Disagree					Strongly Agree
1	2	3	4	5	

2. I would use this graphical password for my important accounts (e.g. Online banking)

Strongly Disagree					Strongly Agree
1	2	3	4	5	

3. I am more willing to use this password scheme than traditional text-based password on this device

Strongly Disagree					Strongly Agree
1	2	3	4	5	

4. The size of the screen on this device makes the scheme hard to use

Strongly Disagree					Strongly Agree
1	2	3	4	5	

5. I think this scheme will be easier to use if I have a more accurate input method (e.g., with a touch screen pen)

Strongly Disagree					Strongly Agree
1	2	3	4	5	

6. It takes too much time to enter a password using this scheme

Strongly Disagree					Strongly Agree
1	2	3	4	5	

7. I would like to have more feedback from the device (vibrate or sound) when I input something

Strongly Disagree					Strongly Agree
1	2	3	4	5	

8. What do you find the most difficult when setting up the password using this scheme?

9. What did you find easiest when re-entering a password using this scheme?

10. Do you have any other feedback about using this scheme on your mobile device?

Appendix F

Second Questionnaire (Main Study)

1. It was easy to remember the password

Strongly Disagree					Strongly Agree
1	2	3	4	5	

2. This scheme was easy to use given the size of screen of the test device

Strongly Disagree					Strongly Agree
1	2	3	4	5	

3. The password is easy to see if someone is peeking

Strongly Disagree					Strongly Agree
1	2	3	4	5	

4. I think the passwords of this scheme are hard to guess by others

Strongly Disagree					Strongly Agree
1	2	3	4	5	

5. It takes too long to enter a password using this scheme

Strongly Disagree					Strongly Agree
1	2	3	4	5	

6. I will be able to remember more than one graphical password using this scheme

Strongly Disagree					Strongly Agree
1	2	3	4	5	

7. What do you find the most difficult when re-entering a password using this scheme?

8. What did you find easiest when re-entering a password using this scheme

9. Do you have any other feed back about using this scheme on your mobile device?

Appendix G

Questionnaire for User Experience (Main Study)

1. Do you own a smart phone?(if answered No, skip to question 9)

   ☐ Yes ☐ No

2. What type(s) of input methods does your phone have?

   ☐ Touch Screen ☐ Physical Keyboard ☐ Voice Recognition ☐ Others:

3. What operating system(s) is your smart phone running?

   ☐ Android ☐ iOS ☐ Symbian ☐ BlackBerry ☐ Windows Mobile ☐ Others:

4. How long have you been using a smart phone?

   Years: Months:

5. When I type my passwords, I hide them from nearby observers

   ☐ Never

   ☐ Only the important ones such as my online banking accounts

   ☐ Always

   ☐ Other:

6. How often do you enter a username/password on your smart phone?

   ☐ At least once a day ☐ Several times a week ☐ Once a week ☐ Less than once a week

7. I often make mistakes when typing my username/password on my smart phone (please circle)

Strongly Disagree					Strongly Agree
1	2	3	4	5	

8. Where do you use your smart phone the most often?

   ☐ Home
   ☐ School
   ☐ Work place
   ☐ Public Place
   ☐ while traveling/commuting
   ☐ Others:

9. Do you own a tablet computer?(if answered No, skip to question 17)

   ☐ Yes ☐ No

10. What type(s) of input methods does your phone have?

    ☐ Touch Screen ☐ Physical Keyboard ☐ Voice Recognition ☐ Others:

11. What operating system(s) is your tablet computer running?

    ☐ Android ☐ iOS ☐ Symbian ☐ BlackBerry ☐ Windows Mobile ☐ Others:

12. How long have you been using a tablet computer?

    Years: Months:

13. When I type my passwords, I hide them from nearby observers

    ☐ Never

    ☐ Only the important ones such as my online banking accounts

    ☐ Always

☐ Other:

14. How often do you enter a username/password on your tablet computer?

    ☐ At least once a day ☐ Several times a week ☐ Once a week ☐ Less than once a week

15. I often make mistakes when typing my username/password on my tablet computer (please circle)

Strongly Disagree					Strongly Agree
1	2	3	4	5	

16. Where do you use your tablet computer the most often?

    ☐ Home
    ☐ School
    ☐ Work place
    ☐ Public Place
    ☐ while traveling/commuting
    ☐ Others:

17. Have you seen a graphical password before?

    ☐ Yes ☐ No

18. If Yes, where did you see it (please specify)?

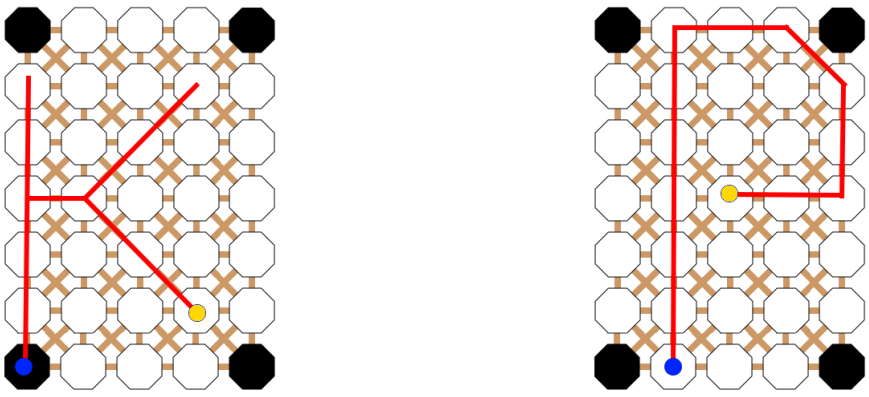
19. If Yes, how often to do use it?

Appendix H

Example TMD Passwords

The following are some example TMD passwords collected during the study. In these figures, blue dots indicate the starting point and yellow dots indicate the ending point of a password. Patterns that uses multiple multiple layers are surrounded by a black border.

Recognizable Symbols: symbols which are well known to others such as the English alphabet, Arabic numbers, or mathematical operators.



(a) (b)

Figure H.1: Examples of "recognizable symbol" passwords

Back-trace: the path of the password on the current layer is identical to the previous layer but the direction of the path is reversed.

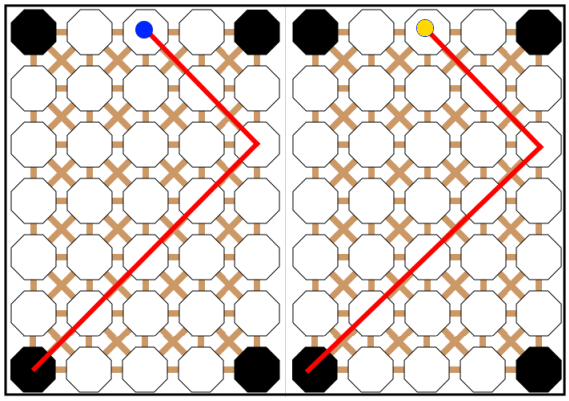
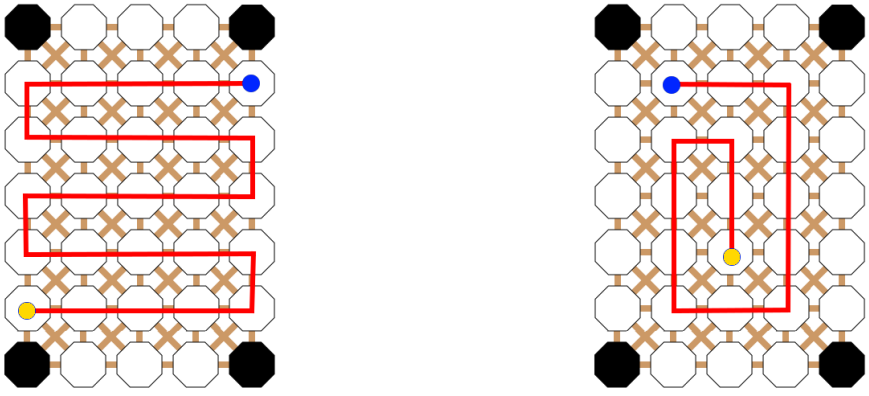


Figure H.2: Example of a "back-trace" password

Recognizable patterns: recognizable paths such as spiral or zigzag patterns.



(a) (b)

Figure H.3: Examples of "recognizable pattern" passwords

Symmetric: shapes that are symmetric about an axis, the axis can be vertical or horizontal.

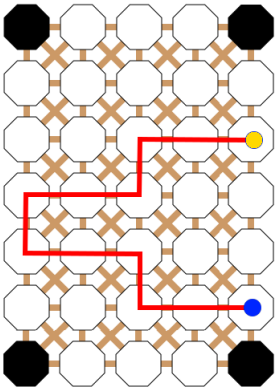
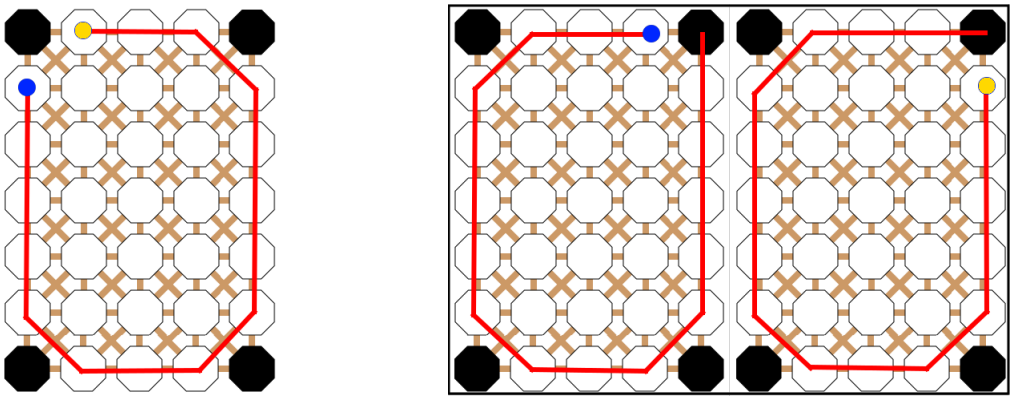


Figure H.4: Example of a "symmetric" password

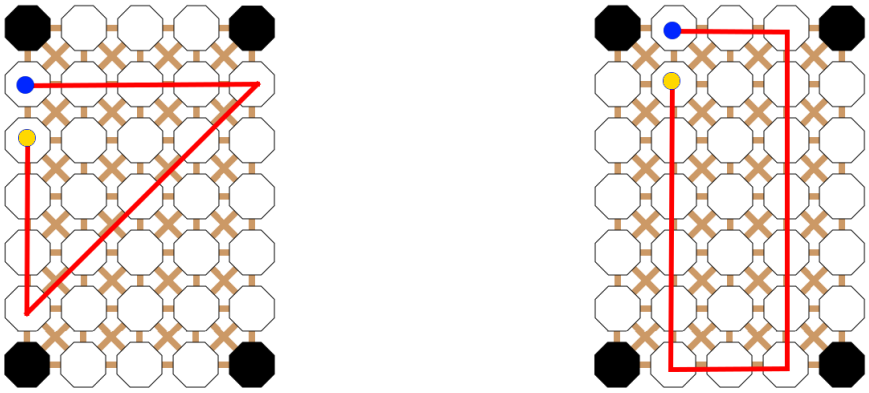
Along the edges: used only the cells on the edge of the grid.



(a) (b)

Figure H.5: Examples of "along the edges" passwords

Simple shapes: closed simple polygon shapes.



(a) (b)

Figure H.6: Examples of “simple shapes” passwords