Honours Project Report

Graphical Password Authentication for Secure Social Networks

Dorothy Emma Mhlanga

Supervised by: Dr Anne Kayem

	Category	Min	Max	Chosen
1	Requirement Analysis and Design	0	20	0
2	Theoretical Analysis	0	25	0
3	Experiment Design and Execution	0	20	15
4	System Development and Implementation	0	15	15
5	Results, Findings and Conclusion	10	20	15
6	Aim Formulation and Background Work	10	15	15
7	Quality of Report Writing and Presentation	10		10
8	Adherence to Project Proposal and Quality of Deliverables	10		10
9	Overall General Project Evaluation	0	10	0
Total marks		**80**		**80**

Department of Computer Science

University of Cape Town

2013

Abstract

All access control systems have some means of preventing unwanted access while allowing valid users entrance, be it via barriers, keys or passwords. In the case of electronic systems, access control has mainly been implemented via the use of a combination of a unique user identifier and either a secret numeric or alphanumeric password. These text based password schemes have been affected by a myriad of problems especially concerning their vulnerability to attacks and the difficulty of remembering them as a secure password should at a minimum be comprised of eight unique characters. One alternative that has been gaining prominence due to its potential to be a viable replacement for text passwords has been graphical passwords.

The aim of this research is to evaluate the viability of text based password schemes as an alternative to text passwords for the authentication of social networks. To this end, two graphical password schemes based on Recall and Cued-Recall were implemented and a user evaluation on the two systems and an existing text system was conducted.

The results from the user study provided significant insight into current user practises with text based passwords, and also into the potential reactions of user to a graphical password scheme. The majority of the users by a slight margin, stated that they would use a graphical password scheme to authenticate their social networking sites. The idea of graphical passwords is one that intrigued the users and with continued improvement and enhancements, graphical passwords could be a viable alternative to text passwords.

Acknowledgements

This project would not have been possible without the help of a collective group of people

Firstly I would really like to thank mama na daddy Mhlanga who have been the best parents a person could have. Their constant and ready support of me and their encouragement are what have helped see this project to fruition. My sisters I thank for their humorous support and cheering. And thank you to all my friends and family for their support.

I would like to thank my project partner Lebogang Mametja who has not only been a great team member but also a very dear and valued friend.

I would also like to thank Rotondwa Wayne Ratshidaho from BSG for all his insight and help with understanding the Hackmi2 framework.

Finally I would like to especially thank my project supervisor Dr. Anne Kayem for her guidance and direction throughout the duration of the project.

Contents

List of Figures and Tables

Figures

Table

1. Introduction

All access control systems have some means of preventing unwanted access while allowing valid users entrance, be it via barriers, keys or passwords. In the case of electronic systems, access control has mainly been implemented via the use of a combination of a unique user identifier and either a secret numeric or alphanumeric password. These text based password schemes have been affected by a myriad of problems especially concerning their vulnerability to attacks and the difficulty associated with remembering them as a secure password should at a minimum be comprised of eight unique characters. Several alternatives to text-based password schemes have been proposed. One alternative that has been gaining in prominence due to its potential to be a viable replacement for text passwords has been graphical passwords. This project seeks to implement a graphical password scheme and to evaluate whether they are a viable alternative to text passwords.

1.1 Motivation

Research has shown that text passwords are becoming more and more inefficient as a means of system authentication. The main challenge posed by text passwords for users, is the amount of memory load required in order to remember a secure text password. Added to this, as most users make use of several applications that require authentication information before granting access, creating and remembering a unique secure password for each of these applications becomes a challenge. Another challenge with using text password is that as they have been in use for a very long time, several attacks against them have been developed and implemented. As a result it is not surprising to often read articles about how a user's password was hacked and their system compromised. With text passwords being used to secure low security and high security applications, their vulnerability poses a serious threat to all password users. To this end it is essential to find a viable alternative to text passwords in order to ensure the continued safety and security of the respective applications.

It was these and other identified problems that prompted researchers to explore alternatives to text passwords. Several different non-text authentication methods have been proposed and some have gone on to be implemented. Biometric authentication procedures aim to use unalterable individual characteristics as a way of authenticating a user. These individual characteristics could include using fingerprint information and eye identification information for example. While this is a potentially more secure means of authentication, as the required information is not very simple to forge, biometric systems are slow to be adopted due to the high costs associated with implementing them. Apart from the high costs, some applications do not easily lend themselves for use with biometric authentication. An example of this would be a web based application. For fingerprint authentication, it would require each user to have additional hardware to conduct the fingerprint scanning. Other authentication methods have been evaluated and similarly to biometric authentication methods, they have been slow to be adopted due to either the costs associated with using them or the extra technology requirements that will be involved with their use.

Graphical passwords are gaining in prominence as alternatives to text passwords because unlike the other proposed alternatives, they seem to be the most simple to implement whilst also imposing a limited amount of overhead. Also pivotal to the attraction of graphical

passwords as a possible solution is the fact that based on neurological studies and mathematical they are supposed to be easier to remember than text passwords and also they are supposed to be more secure, respectively. A graphical password is a password scheme that has a visual element associated with it for example an image or a drawing.

It is based on this information that the topic of this project came to be determined. The aim of the research is to evaluate the viability of graphical password schemes as an alternative to text passwords. To this end, two graphical password schemes based on Recall and Cued-Recall were implemented and a user evaluation on the two systems and an existing text system was conducted. In the proposal to this project, it had been our intention to implement a third graphical password scheme based on Recognition, however as the scope of the project was further refined, it was decided to focus on the two aforementioned password schemes and leave the investigation of the remaining password scheme as future work.

1.2 Research Questions

While the overall goal of this project was to evaluate the viability of graphical passwords as an alternative to text passwords, it was essential to refine the scope of the project into specific questions and goals. One of the gaps in the existing literature on graphical passwords is information on the performance of a graphical password scheme on its intended domain. Most research studies only evaluate the graphical password scheme in controlled lab environments and not in its intended real world applications. This means that for some of the studies there is little evidence to prove the ecological validity of their results. This project aims to work towards filling this gap by evaluating the graphical password schemes in their intended final domain, which in this case is a social networking site. The research questions for this project were refined into two main questions of interest, namely:

1. **Which category of graphical password schemes is best suited for social networks: schemes based on recall, cued-recall?**
2. **Are graphical password schemes a viable alternative to text-based schemes as a means of providing authentication for secure social networks?**

1.3 Legal and ethical considerations

A significant portion of this project will involve having users evaluate the system. To this end it was necessary to obtain the relevant ethical clearance to allow human subjects to test the system. Ethical clearance was obtained from the University's Faculty of Science Research Ethics Committee. During user testing the user would be provided with an informed consent form to ensure that they consented to participating in the study.

1.4 Structure of the report

This project has been divided into four distinct chapters each detailing an aspect of the project development. The **Background chapter** explores in detail the challenges facing text-based password schemes and the development of graphical passwords as a proposed alternative. Current research into the main implementations and knowledge on graphical passwords is also explored in this section.

The **System Design** chapter details and examines the decisions that went into the design of the system. In particular this section details the system requirements and the proposed system design to cater to these needs.

Following this section is the **System Implementation** chapter. This chapter shows the final system that was implemented and examines the tools and techniques that were employed to implement the system. The challenges and the solutions that were implemented and managed during this implementation section are also detailed.

After the system implementation, the next section presented is the **System Evaluation** chapter. In this chapter the experiment design, the user testing and the results of the user study are presented. The results of the testing are then analysed with respect to the initial research questions of the project.

Finally the **Conclusion** chapter of the project is presented. This chapter simply summarises the development of the project and offers a few comments on the potential for graphical passwords. The remainder of the paper is comprised of references and appendixes

2. Background

As the use of computer systems becomes ever more ubiquitous, the need to secure these systems becomes even more critical. Currently the most common way to conduct user authentication is through the use of text-based passwords. However these passwords have been shown to have several usability challenges as well as being vulnerable to attacks e.g dictionary attacks. Altenatives to using text-based passwords for authentication have been proposed. One alternative to text-based passwords has been the use of graphical passwords. Instead of using alphanumeric characters to create a password, graphical passwords make use of images and drawings. Similarly to text-based passwords, graphical passwords are a knowledge-based authentication system in which users enter a shared secret as evidence of their identity (Biddle, Chiasson, & Van Oorschot, 2012). The main motivation behind graphical passwords is the promise of the increased memorability and usability of these passwords. These graphical passwords are anticipated to be more robust than text-based passwords. Several studies have shown that humans remember images more easily compared to text (Yan, Blackwell, Anderson, & Grant, 2004). Graphical passwords hope to leverage visual information and in turn make it easier for users to select more secure passwords.

Initially, researchers did not anticipate that the challenges faced with text-based passwords would also be found in graphical passwords (Oorschot & Thorpe, 2008). However, it was soon discovered that some of the challenges regarding password use were common to both text-based and graphical passwords. In particular issues concerning memorability of the password, password strength and susceptibility to dictionary attacks (Oorschot & Thorpe, 2008). New research is now focused on building on existing knowledge in order to create stronger graphical passwords. Graphical passwords can be categorised under three main schemes, recognition, recall and cued recall (Zakaria, Griffiths, Brostoff, & Yan, 2011). The study of these three main schemes and determining which of them allows for the strongest passwords as well as usability is an active area of research.

Having only been introduced in 1999, graphical passwords are still a fairly young area of research. In this section, an overview and analysis of the aforementioned three main types of graphical password schemes available will be conducted with a special focus on the Cued-Recall system, PassPoints, of which this research is based.

2.1 Graphical Password Systems

2.1.1 Recall Based Schemes

Recall based graphical password schemes are authentication procedures that require the users to reproduce something that was created earlier during registration. These password schemes are often referred to as *drawmetric* password schemes as the users are required to draw their password, for example drawing images or characters to make up their password (De Anglei et al, 2005). The recall aspect of this type of password system stems from the fact that the users have to reproduce their created drawing each time from memory with no aids, in order to gain access to the desired system. Recall is a challenging memory task as the users have no

prompts to aid in their remembrance of the password. This makes recall based password schemes more taxing in terms of memory load as compared to the other two prominent password types which all make use of some sort of memory aid. Text passwords can be classified as recall based systems. This is simply because like the drawing passwords, the user is expected to re-enter the password solely from memory.

Interestingly, it has been proposed and some studies have shown that with both text and drawing password users have devised innovative ways to obtain memory prompts (Chaisson et al, 2009). In the case of text passwords, users sometimes use the name of the site or the function of the site as its password. For example for a work password, the user could use a password like *password123*. In the case of the drawing password, if users can find a symbol or an image to represent the site, this could be used as a cue. For example, drawing the letter W, as the password for a work related website.

Recall based password schemes are known to be vulnerable to a number of attacks. The general security concern for all graphical passwords applies also to recall based systems. This concern is the major vulnerability of the password schemes to shoulder surfing attacks. Several studies have been conducted in order to explore different mitigation techniques in order to make drawing graphical password schemes more secure. While susceptible to shoulder surfing attacks, drawing password schemes are more robust against dictionary attacks. This is because in a system where the user is presented with a blank canvas for example, it is difficult to predict what kind of an image they could produce. This is unlike cued recall or recognition based password schemes where the user is provided is provided with a cue, making it easier for attackers to attempt to guess at the password

The first implementation of a recall based graphical password scheme is thought to be Draw-a-Secret (DAS). The authentication process consists of a user drawing their password on an N * N grid (Jerymn L Mayer et al, 2009). Dunphy and Yan J, 2009, considered DAS to be a system worthy of extensive study for a couple of reasons. One such reason, being that DAS has a theoretical password space which is larger than that of most text password scheme.

Various studies have been conducted on this system; however, to date DAS has only been tested through paper prototypes. As such, little can be said on its usability or practical security due to this lack of implementation and suitable user studies (Biddle R et al, 2012).

2.1.2 Recognition Based Schemes

Recognition based systems are password systems where the user is initially presented with a catalogue of images. From this catalogue the user is expected to select a specific number of images to make up their password (Biddle et al., 2012). During the authentication process, the user goes through a series of rounds, in which they are presented with a set of images, one from their password and the rest being decoy images; they are then required to select one which appears in their catalogue of images from the decoy images (De Angeli, Coventry, Johnson, & Renaud, 2005). After successfully navigating all the required rounds, the user is granted access to the system. Studies have shown that humans have a strong ability to successfully recognize and identify images; this makes recognition based systems effective in terms of remembering the password. Recognition based systems make use of a variety of image types including, human portraits, nature and artwork.

One of the main difficulties associated with using recognition based systems is that they have a small theoretical password space. The strength of these passwords is comparable to a 4 or 5 digit pin code (Biddle et al., 2012). These are widely known to be insecure as current knowledge recommends that for a text-based password to be considered strong it should have a minimum length of 8 characters (Cheswick, 2012). As a result many recognition based graphical passwords are not considered to be suitable alternatives to text-based passwords.

Other challenges to using recognition based password systems are that, they are susceptible to shoulder surfing attacks. Recognition based systems are particularly susceptible to shoulder surfing attacks because it would be easy for a would-be attacker to observe the image selected on each round of the login (Biddle et al., 2012). This is also a challenge because the number of images that are presented to the user are few and therefore this may mean that each image will have a relatively large display place on the screen, making them even simpler to observe (Biddle et al., 2012). A few mechanisms have been proposed as a possible means to counter this. One such mechanism is to request that the user, instead of clicking on the specific image in their portfolio, rather do some action based on the location of the image (Biddle et al., 2012). So for example the system may request that for a specific login session the user selects an image that is below and to the left of their password image. This solution has been implemented with varying success.

An implementation of a recognition based graphical password system is the Passfaces authentication system. Passfaces relies on the user being able to recognize a predetermined set of faces (De Angeli et al., 2005). At password creation the user is asked to select a set of faces to comprise their password. During login the user is presented with a set of decoy images and one image from their password set. Once the user successfully navigates the rounds of testing, they are granted access. Another system implementing recognition based graphical passwords is Deja-vu. Deja-vu makes use of abstract art images instead of faces. This system is considered to be more secure than Passfaces due to the difficulty in communicating them to third parties (Biddle et al., 2012). So for example, a human face is easier to describe than a piece of abstract art. This means that the system is more resistant to social engineering attacks as compared to Cued-Recall based systems.

Apart from suffering from the traditional security challenges that affect all graphical passwords, recognition based systems, particularly Passfaces, have other security challenges unique to them. These include the security risk posed by the development and use of hot-images (Duggan et al., 2012). Hot-images refer to the emergence of popular images that users are likely to include as part of their password set

2.1.3 Cued-Recall Based Schemes

This project will involve the design, implementation and testing of the Cued-Recall graphical password system, ClickPoints. The ClickPoints system is based on the original implementation of a graphical password scheme known as PassPoints. Recall based graphical password systems are systems where the user is presented with graphical information to remember and then during authentication they are requested to restate this information (Bower, 2000). With cued-recall the user is also presented with graphical information to remember, however during authentication, the user is provided with cues to aid their memory. In graphical passwords, cued-recall based password systems are systems

where the user is provided with an image and then asked to select specific parts of the image to use as their password (Forget, Chiasson, & Biddle, 2010). The user is provided with a graphical cue that triggers the user's memory of his/her password (Forget et al., 2010). The aim of using cued-recall is to reduce the memory load on the users whilst at the same time enabling them to make use of stronger more challenging passwords. Cued-recall graphical passwords (locimetric passwords) are easier to remember than pure recall passwords (Biddle et al., 2012).

Cued-recall graphical passwords fall into a subclass of graphical passwords commonly known as click-based passwords (Masrom, Towhidi, & Lashkari, 2009). One key example of a cued-recall graphical password system is PassPoints. In PassPoints, a password is made up of 5 points that a user selects on different places on an image (Van Oorschot, Salehi-Abari, & Thorpe, 2010). During authentication, a user is presented with the same image and requested to enter the password by clicking the 5 points selected during password creation.

Compared to other graphical password systems PassPoints is a strong system as it has a larger password space which makes it more resistant to attacks (Biddle et al., 2012). This and the fact that the system makes use of cued-recall make up two of the major benefits of using PassPoints. Other studies of PassPoints have shown that it has a high usability, requiring a small amount of time to create the password and allowing for fast login in times (Zakaria et al., 2011).

Similarly to all passwords schemes, cued-recall graphical passwords are susceptible to certain security threats. In an attempt to make using cued-recall graphical passwords safer, researchers have come up with improvements and extensions to make these systems more secure. An example of this is the Background Draw-A-Secret Password (BDAS) (Yan et al., 2004). Draw-A-Secret was the first graphical password to be proposed and it works by requiring the user to draw their password using either a mouse or a stylus. This password is then stored on the system and during authentication, the user is asked to reproduce this image from memory. BDAS extended the Draw-A-Secret scheme by adding a background image to it (Dunphy & Yan, 2007). The background image acted as a cue to aid users in remembering where they had drawn their images. It also served to make the passwords more secure by increasing the theoretical password space (Yan et al., 2004).

A major threat for cued-recall graphical schemes is that of shoulder-surfing (Forget et al., 2010; Tari, Ozok, & Holden, 2006). Shoulder surfing occurs when an observer is able to obtain the password of the user by observing them as they enter the passwords. Text-based passwords are not very susceptible to this type of attack because as users enter the password, asterisks are used by the system to hide the password from anyone who may be observing (Duggan, Johnson, & Grawemeyer, 2012). Graphical passwords however, by nature of using images, tend to keep the image on the screen. It is then often simple for an observer to watch and learn the passwords by observing the points on the image that the user would have selected (Masrom et al., 2009).

Cued-Recall graphical passwords are also susceptible to social engineering attacks. Social engineering attacks are an attack where the user is tricked into revealing their password to a stranger (Biddle et al., 2012). For example, in the case of PassPoints, a user may reveal their password to an external party by describing on which places on the image they placed their 5 points.

Several improvements to PassPoints have been proposed. One such improvement on PassPoints is a system called Cued-Gaze Points. This system instead of making use of a

mouse to enter the password makes use of the user's eye gaze. The advantage of using this system is that it is more capable of resisting shoulder surfing attacks (Forget et al., 2010). One major limitation of this solution is that gaze based input mechanisms are still expensive and therefore implemented only in a few places. Another challenge of implementing this solution is that there is a trade-off between usability and security. To benefit from the added security, users have to endure long password creation and login times because gaze based systems have to be recalibrated for each user, which takes time (Forget et al., 2010) Other attacks that cued-graphical passwords are susceptible to are dictionary and phishing attacks as well as susceptibility to hotspots.

This project aims at the development, implementation and testing of a version of PassPoints named ClickPoints, with the ultimate goal being to answer the stated research questions of determining whether ClickPoints is both a suitable alternative to text passwords and whether it is applicable in the setting of social networking sites.

2.2 The Case for Graphical Passwords

Graphical passwords are anticipated to have several benefits and enhancements over the current text based password schemes that are currently in use. The main anticipated benefits of graphical passwords are examined in this section.

2.2.1 Increased Memorability

People have a tendency of using insecure passwords and this results from long term memory limitations. It is challenging for users to remember pseudo-random passwords over time (Wiedenbeck et al, 2006). The Power Law of Forgetting has shown that after learning something new, people undergo a period of rapid forgetting and then over time they gradually lose the rest of the learned material. As a result of this, users have come up with several innovative but usually insecure ways of coping with remembering their various passwords. These methods include selecting short and easy to remember passwords, which are in turn easily discoverable by dictionary attacks. Other coping strategies include writing the passwords down, recycling passwords over multiple systems or sharing passwords with a trusted individual.

Graphical Passwords are supposed to be easier to remember than text based passwords. Unlike text passwords they engage more of the users' information processing capabilities. Research into the workings of human memory has shown that humans have a greater ability to remember visual information as opposed to simply strings of text. One of the most widely accepted theories is the dual-coding theory. This theory suggests that in the human mind verbal (word based) and non-verbal (image-based) are processed and represented in a different way in the brain (Widenbeck et al, 2006). Text is thought to be represented symbolically where symbols are given meaning cognitively associated with the text. Images on the other hand are stored in a way that retains the perceptual features that are seen and they are assigned meaning based on what is being observed.

Therefore with a graphical password scheme users are more likely to remember specific parts of images if they focused on them. As a result of this, graphical password schemes require the users to exert less effort to remember as opposed to the effort required to remember an equally strong text-based password.

Evaluated amongst themselves, the different password schemes have varying ease of memorability. Recognition and Cued-Recall graphical schemes both provide the user with some form of a visual cue. This is different from Recall based schemes which like text-based passwords rely solely on the users recall abilities. Therefore, Recognition and Cued-Recall password schemes have a higher memorability as compared to pure Recall based password schemes. Several theories have been put forward to explain the difference between recognition based memory tasks and recall based memory tasks (Widenbeck et al, 2009). The question is whether the two tasks are distinct and unique process or whether they are similar and only differ in the difficulty in retrieval. As mentioned prior, it is however a generally accepted fact that having a visual cue is an easier memory task as compared to relying on pure recall.

2.2.2 Larger Password Space

One of the key anticipated benefits to stem from the use of graphical password is the potential to have a larger password space compared to text-based password schemes while at the same time exerting a lower demand on the users memory load. An intricate image has the potential to allow for many unique memorable points. In the case of PassPoints, even when only using 5 click points, the available password space is large.

One example would be to look at an image that is 330 * 260mm. If we assume that a quarter of the image consists of memorable spaces and that a tolerance of 6 * 6 mm is used, then this results in 590 memorable tolerance regions (Wiednebeck et al 2005). Using a 5 clicks PassPoints system, this would result in $590^5 = 7.15 * 10^{13}$ possibly memorable passwords (Wiednebeck et al 2005. This is a password space that is larger than that available for an 8 character password created over a 64 character alphabet. Therefore attacking a ClickPoints system via a brute force attack would be harder and require more resources than the effort required guessing a random Unix password.

2.2.3 Security in Graphical Passwords

The main aim of introducing graphical passwords was in the hope of creating an authentication mechanism what would be more secure and offer greater usability than what is currently offered by text-based graphical passwords (Biddle et al., 2012). While graphical passwords offer solutions to some of the challenges of text-based passwords, they are far from being a clear superior alternative. This is due in part to the fact that graphical passwords are still relatively new and therefore need to be studied further. It is also due to the fact that there are new security concerns specific to them.

One of the problems with passwords, both graphical and text-based stems from the way users select them (Duggan et al., 2012; Wiedenbeck, Waters, Birget, Brodskiy, & Memon, 2005). People tend to select weak passwords and this is mainly because these passwords are easier to remember (Chiasson, Forget, Biddle, & van Oorschot, 2008; & Li, 2012). Studies have also shown that the particular system and the personal user motivation play a significant role in influencing the type of password that a user selects. For example, for a system that secures banking information, users would be more motivated to select more difficult passwords. While for systems that secure for instance general mail, the reverse may be true. Cued-graphical passwords have a key advantage over this challenge in that the way these systems are structured using images, users are automatically selecting stronger passwords than the equivalent text-based version (Duggan et al., 2012).

While cued-recall password systems allow the user to create a strong password, a challenge that arises from this is how to authenticate that password. In the case of ClickPoints the system uses a predetermined algorithm to determine whether the entered points, if not on the exact same spot as the original password are within an acceptable range to the original click point. This algorithm will impact the security of the system. If the acceptable range is too small, then the user may fail or have trouble logging in, if on the other hand the range is too large, then the system is more vulnerable to attacks.

Graphical passwords are especially vulnerable to two types of attacks, guessing attacks and capture attacks (Biddle et al., 2012). Guessing attacks are attacks whereby an external party attempts to guess the correct password. A common method of doing this is through dictionary attacks. In a dictionary attack, the system attempts to guess the correct password by comparing it to a set of stored passwords. The success of dictionary attacks on graphical passwords is an area that needs further study. Capture attacks are attacks whereby an external party attempts to capture the full or sections of the password. This can be done through shoulder surfing or phishing attacks.

Several mitigation techniques have been developed to counter these attacks. In the case of guessing attacks, one such technique is password lock-out (Van Oorschot et al., 2010). Lock-out allows the user a limited number of chances to enter the password correctly. If the user fails on all attempts then the account locks the user out and requests that the user goes through a password recovery process in order to verify them. This technique has been implemented with some success for graphical passwords. It effectively counters dictionary attacks by limiting the number of guesses that can be entered (Van Oorschot et al., 2010). In the case of capture attacks techniques such as using eye-glaze as an input mechanisms have been implemented in an attempt to secure the password (Bicakci, Atalay, Yuceel, Gurbaslar, & Erdeniz, 2009; Bulling, Alt, & Schmidt, 2012; Gao, Guo, Chen, Wang, & Liu, 2008; Zakaria et al., 2011). Another technique has been to use the keyboard as an alternative input mechanism to the mouse (Tari et al., 2006).

When people process images they tend to view the image in terms of characteristics like light or dark, foregrounded or back grounded information (Bower, 2000). As people tend to have similar image processing mechanisms, this results in the emergence of hot-spots for cued-recall click-based passwords and hot images for recognition based passwords (Meng & Li, 2012). Hot-spots or hot-images refers to sections in an image or images that are most likely to be chosen by a large number of users. Hot spots/images present an area of weakness for graphical passwords. It makes the systems more prone to brute-force attacks based on educated guesses of hot spots (Meng & Li, 2012). In an experiment by (van Oorschot & Thorpe, 2011), they generated a "human seeded" attack on a system protected using

PassPoints. Within a hundred guesses, they were able to predict 4% of the passwords (van Oorschot & Thorpe, 2011). A human seeded attack can be described as an attack that is based on data collected from people (van Oorschot & Thorpe, 2011). This serves to highlight how significant the challenge of hot spots/images is in the security of graphical passwords.

Using icons is one method that has been proposed to counter hot-spots in click-based systems. Instead of using one image to create the password in, the user is presented with a large set of small icons. The rationale behind this is that with more options to choose from, the emergence of hot-spots will be reduced (Meng & Li, 2012). Also using multiple smaller images will increase the password space allowing for stronger passwords to be created. One counter against this solution is that similarly to the hot-spots on one image, there will be icons that will become hot-icons. With this in consideration, it is recommended that the best implementation of this version of a click-based system would be to assign the user with random icons selected by the computer. This will undoubtedly reduce the emergence of hot-icons. In recognition-based systems, the counter to the emergence of hot-images is to have the system be comprised of abstract images and similarly to click-based systems, to have the system generate the password.

Unfortunately with graphical passwords, most of the usability tests have been conducted in the lab and few out in the field (Biddle et al., 2012). The main challenge of this is that it is difficult to conduct conclusive comparisons between text-based passwords and graphical passwords. As result researchers are unable to conclusive declare graphical passwords as being superior to text-based passwords. When implementing a graphical password scheme, it is essential to keep all these challenges in mind in order to aid the creation of a truly secure system.

2.3 Evaluation

Graphical passwords still suffer from several implementation challenges. However there are techniques that have been employed in an attempt to make them more secure. Users also have a responsibility to securely manage and protect their passwords (Moglen, 2013). One study showed that given more information on how to create stronger passwords, some users do create stronger passwords (Moglen, 2013). A counter study to this showed that the number of users who ended up adopting the system was low (Moglen, 2013). This was due to non-compliance and frustration on the user's part on the difficulty of remembering the stronger passwords.

Users can aid their memory of graphical passwords by creating picture stories (mnemonics). This system works well especially for recognition based systems where the user is not provided with a cue to aid their memory (Biddle et al., 2012). Graphical passwords have a lot of potential to offer enhanced protection and usability as compared to text-based passwords. Additional field studies of graphical passwords are required to enable for comparisons of their performance versus that of text-based passwords. This will allow for the strengthening of existing graphical password solutions and ultimately adopting them as a superior alternative to text-based passwords.

Security, especially cyber security is one of the major concerns of our time (Bishop, 2003). With access to sensitive information like personal records and banking details being secured

by passwords, it is very critical that these passwords be as secure as possible whilst also being convenient for the user. Text-based passwords have been shown to have several usability challenges. It is therefore essential to develop alternatives to these passwords that can be more secure.

To this end this paper has looked at the implementation of graphical passwords in particular recognition-based and click-based graphical passwords. The strengths and the weaknesses of either system were evaluated with special focus on the security and usability of each. One key factor that was noted in this research is the critical need for further examination and testing of graphical password systems. This is especially important as passwords are used to secure more and more of our everyday computer systems.

3. System Design

The main aim of this research project is to develop and implement a version of the PassPoints authentication system, ClickPoints, on a social networking site, in order to examine whether graphical passwords are a suitable alternative to text-based passwords in the specified context. To this end a combination of the Waterfall and Agile software engineering techniques were employed to aid in the design and implementation of the system. The Waterfall design strategy follows a set set of steps, namely requirement analysis – system design – implementation – testing – deployment and maintenance. This process is implemented to ensure that the system is working efficiently before it is used for user testing. As the project aims to evaluate the viability of picture passwords both in terms of usability and security, the design of the project had to cater to both these requirements.

3.2 System Requirements

3.2.1 Usability Requirements

- Ease of Use

  The system should be simple for the users to understand and not require the users to have excessive extra training to enable them to be able to use the system. This is so that they can be similar to text based passwords which are relatively simple to learn how to use.

- Speed Requirements

  As the system will be tested in an environment of social networking sites, which are environments that are accessed often and require quick login, the ClickPoints system should also adhere to this specification.

3.2.2 Security Requirements

- Authentication method

  The system should be able to correctly identify a specific user and grant access to the system only when the user has correctly entered the required authentication information.

- Cryptographic encryption

  The system should also guarantee basic privacy and security of the user's personal details. This can be achieved via a number of techniques including using cryptographic encryption to secure the passwords or password databases

3.3 Overview of Pass Points

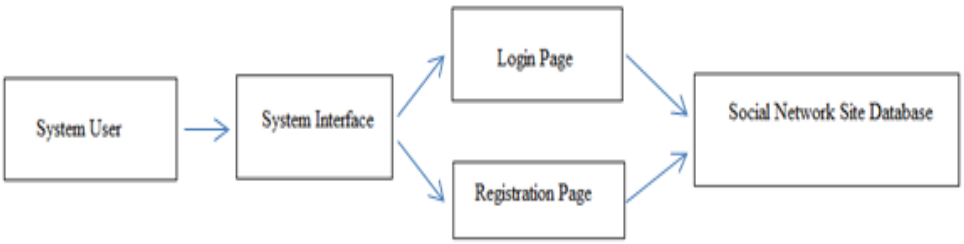


Figure 1: Wireframe Diagram of ClickPoints authentication system

The cued-recall graphical password scheme that we will be implementing will be based on the original implementation of PassPoints with a few modifications added to ensure it suits the intended application of a social network site.

Figure 3 shows some of the key features of the ClickPoints graphical password system and how these features interact and relate to each other. As previously mentioned in the system requirements, the main features of ClickPoints will be the user interface which will directly impact the usability of the system and the security of the system which will be directly impacted by the security procedures utilised in the system.

The user will primarily be interacting with two main interfaces, namely the login page and the registration page. The registration page is of significant importance as this is where the user will be able to create and set their password. First the user should select a unique user name to accompany their picture password. Once this is done the system will allow the user to select an image from a set of pre-determined images presented to them. After this selection, the user should then select the 5 points to make up their password. The system will require the user to re-enter the password to ensure that they are able to use the system and test out the limitations of the tolerance regions. Once this is done, the user should be able to press login, and if the two passwords were matching, the user will be authenticated and logged into the system. The login screen will be in communication with the database of the social network site. The user name and the selected click points are sent to the data base and stored there.

The second interface that the user will be interacting with is the login screen of the system. With this interface the user will be required to enter their user name, then if they are able to correctly select 5 points within an acceptable tolerance to the original points they selected, then they are granted access into the social networking site. Similarly with the registration page, the login page interacts with the server for the social networking site. A request is sent to the server with the username and the entered points, the server then evaluates the entered details and determines whether to grant access or not. If access is not granted, an error message is presented to the user informing them of the error. For both the login and registration pages, the users will be provided with a means to clear any errors they would have made with entering the password and given the opportunity to try again.

Both the login and the registration page interact with the social networking database. This database is responsible for the secure storage of the user's personal details including the user name, the image selected for the password and the 5 chosen pass points. It is imperative that the database be secure to guarantee the security of the users' information.

3.4 Key Design Considerations

3.3.1 Image Tolerance

A key design feature of ClickPoints relates to the tolerance that is used on the system. Tolerance refers to how the system determines if a given point is in an acceptable range to the original click point. This design feature should be handled very carefully as it has implications for both the strength of the password selected and the usability of the system. The effect on the strength of the password occurs in that the smaller the acceptable range, the harder it is for a would-be attacker to correctly guess the required password. This however has an inverse relationship with regards to the usability of the system. The lower the acceptable tolerance, the lower the usability of the system as the users will be required to be very accurate with their given points.

Different studies have recommended varying levels of tolerance, with one study even recommending using a 9 * 9 pixel range. For the purposes of this system however, a tolerance of 19 * 19 pixels will be used. This figure was derived from (Chaisson et al, 2007) implementation of PassPoints.

For the purposes of this design of ClickPoints, no grid overlay will be inserted above the image. This is because of several resulting constraints including that of lowering the password space. If grids are inserted over the image, though this will make selecting points and remembering the given squares much simpler for the user, it in turn reduces the number of possible passwords that can be created as they will be limited to the grid dimensions. Also implementing a grid system introduces the challenge of how to handle grid edge points. This implementation will make use of the Euclidean distance to calculate the distance between two points.

3.3.2 Images

The size and type of image used for authentication in ClickPoints are carefully selected as they affect both the usability of the system and the security of the passwords created. The key aspects that are considered are the image size and the image type.

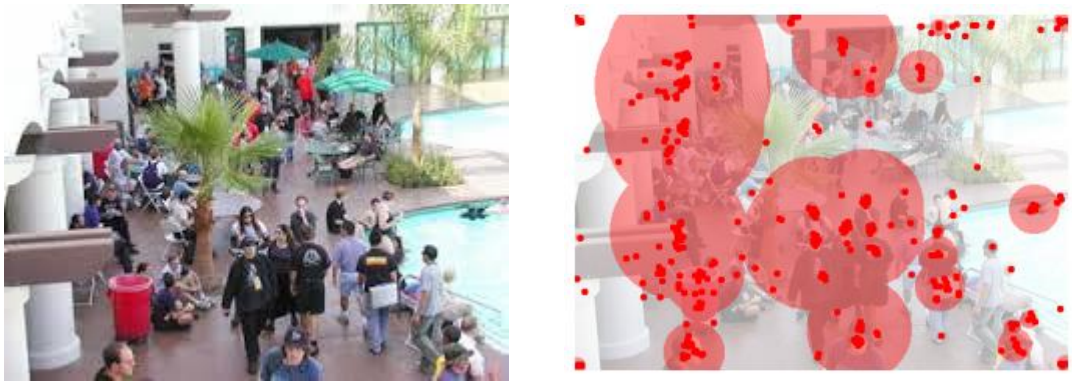
Image Size

The original implementation of PassPoints used images of dimension 451 * 331 pixels. This size was deemed adequate as it allowed for a reasonably sized image that

would display on the screen. The smaller size of the image also lowered its susceptibility to shoulder surfing attacks. Using a grid square of 20 * 20 and 5 click points results in a password space of $373^5 = 7.2 * 10^{12}$.

Image Type

Research into the user choice of passwords in a PassPoints authentication system has shown a correlation between the type of image used and both the memorability and the strength of passwords generated. Different categories of images for example, human portraits or abstract art were shown to present different usability responses from the users. Also as picture passwords are known to be susceptible to hot spots, careful consideration has to be undertaken into the type of image that is used. This is because there are certain images that are more vulnerable to the development of hot spots than others. Another factor that was considered in the design of the system was whether or not to allow users to provide their own images for the password. After evaluation and research into other implementations of PassPoints this option was rejected. Since the system requires that the images be of a specific format and size, it would require a lot more administration on the users' part in order to provide a system approved image. As this would affect the usability of the system, it was decided to provide the users with a set of images from which to choose from.



a ***b***

Figure 2: Sample pictures used for ClickPoints authentication. Figure a shows poolside scene. Figure b shows hot spot areas

3.5 Hackmi2

One of the aims of this project is to examine and evaluate whether graphical password schemes are a viable alternative to text-based passwords for secure authentication to social networking sites. To this end it was imperative to have a social networking site in which to test the graphical password authentication. This would also allow for the password schemes

to be tested in a realistic real world environment. The social networking site that was used to test the password schemes is a site named Hackmi2. Several considerations went into the selection of Hackmi2 as the testing platform. The main motivator behind the use of Hackmi2 is that it is a social networking site in which we have full access and permissions. As such implementing the ClickPoints login will be possible. Another positive factor of using Hackmi2 lies in the fact that as this is a test social networking site, obtaining legal and ethical clearance for testing on this platform is relatively simple. This is because the users do not have to reveal any personal information, for example, as would be needed if using their personal profiles.

Hackmi2 is a social networking site that was developed in 2012 for the purposes of testing security in social networking sites. The HackMi2 social networking site was developed using Elgg v1.8.8 framework, an open source social networking engine. It is a cross platform system written in PHP. Our implementation of the graphical password schemes will be conducted using Java. This is mainly because Elgg provides functionality to embed Java applets into its pages through the use of Plugins. This will enable the graphical password scheme to be used on HackMi2.

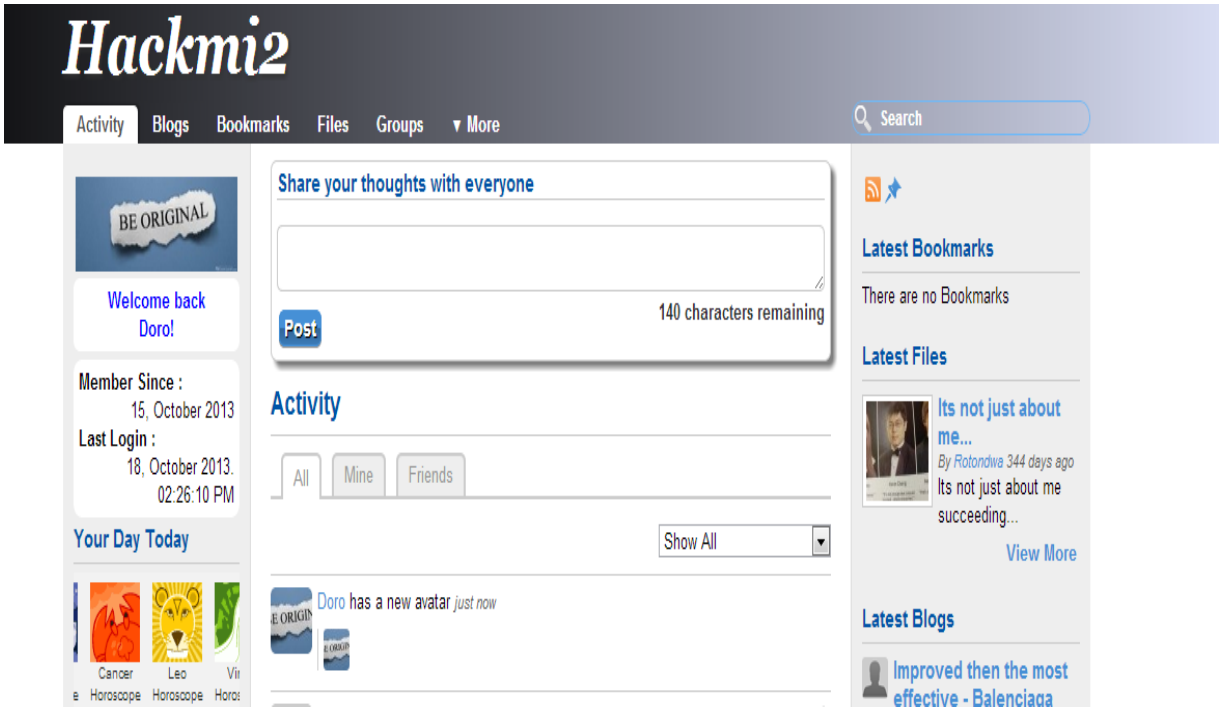


Figure 3: Screenshot of test Social Networking Site, HackMi2

3.6 Evaluation

In this section a description of the design and the design decisions that went into this implementation of ClickPoints have been designed. The key design considerations of the system namely, the tolerance level used, the images used and the social networking engine used were presented. It is anticipated that through following the guidelines stated in this design section, a fully functional version of ClickPoints, implemented on a social networking

site should be produced. After fully evaluating and designing the system, the next stage of the project involves the actual implementation of the design decisions.

4. System Implementation

In this section, the tools and the techniques used to bring the design of the system into fruition are presented. Three programming languages, Java, JavaScript and PHP were used to implement the system. Java was used for the development of the ClickPoints application while JavaScript and PHP were used for the social networking site.

4.1 Tools and techniques

4.1.1 ClickPoints - Java Applet

4.1.1.1 System Overview

As the final destination for the ClickPoints authentication system was for an online social networking site, it seemed prudent to develop the system as a Java Applet. A java applet is an application that is written in java and is deployed as byte code. It can be launched from a web page which is then executed within the Java Virtual Machine and can be run in a process that is stand-alone from the browser. The benefits of using a java applet include firstly that applets run at faster speeds than most complied languages. Also applets have the capability of providing interactive features for web pages. For example, java applets are able to record mouse input, like clicks. This was essential for a system such as ClickPoints as accurate recording of mouse input is central to the success of the program. Also as java's bytecode is cross-platform, the applets are able to be displayed in many different browsers. Again this was also important as social networking sites by nature need to be able to run on different web browsers. After the development of the application, the next stage was to embed the app in the home screen of the social networking site, offering an alternative way to log in as compared to the existing text-based login.

Applet Security

In order to guarantee the authenticity of the applet, the applet was signed by the developer's details. The users of the system were then informed of this and told to allow their browsers to run the application. In the event of commercial deployment, an independent certificate authority server would be utilised.

Registering a new user

On the home page of the java applet, the user is presented with a screen and the option to either login with existing user details, or to register a new account in order to gain access to the system. After selecting the register button, the user is navigated to the second stage of the registration process

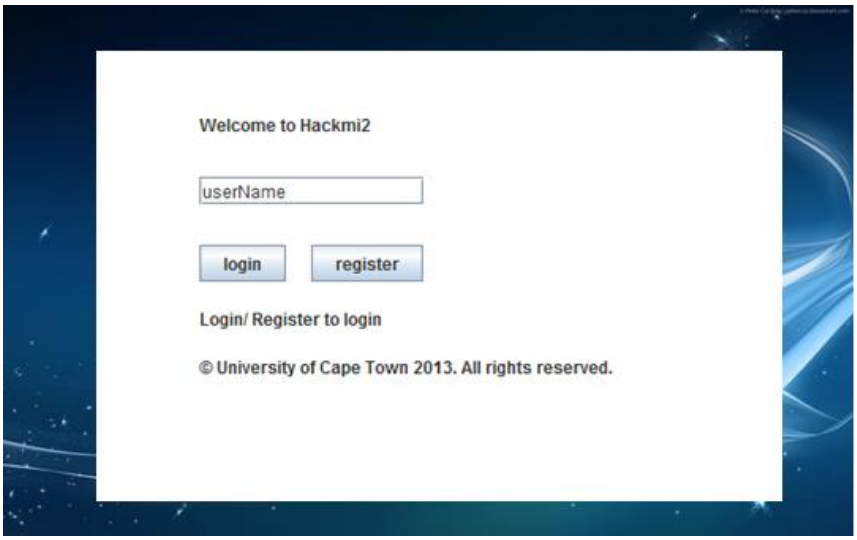


Figure 4: Step 1 of the registration process

In the second stage of the registration, the user is presented with the three from which to create a password on. The user is required to click on the desired image which will then navigate then to that last stage of the registration process

Figure 5: Step 2 of the registration process

In the last stage of the registration process, the user is required to enter a user name of their choice and then select 5 points on the image to make up their password. After entering the pass points for the first time, the verify button is then activated and the user is required to re-enter their selected points. If the re-entered points are within the pre-defined tolerance level, the user is presented with a button to log into the system. This step ensures firstly that the user is able to correctly re-select their chosen points but it also acts as a memory prompt to help the users better remember their selected password.

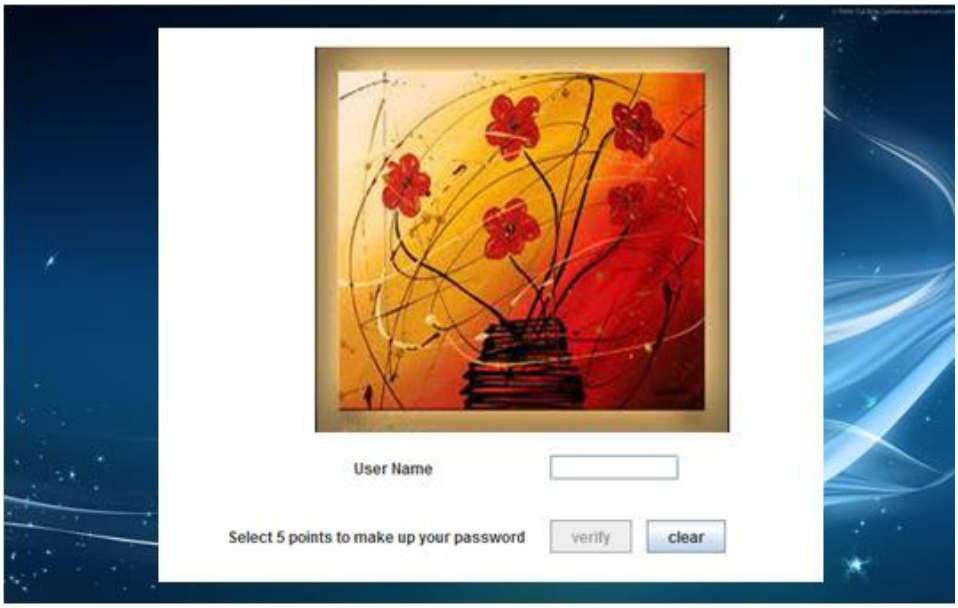


Figure 6: Final Step of the registration process

Before the system navigates the user to the social networking site, the selected user name and the selected ClickPoints along with the timestamp are recorded. These details are then added to the database of user names and passwords

Login into the system

Figure 7: Login step 2

If the user enters a valid user name from the home screen, they are then navigated to this second page of the login process where they are required to re-select their chosen pass points. If they successfully select the exact points or points within the acceptable defined tolerance they are granted access to the social networking site.

System Security Checks

In order to ensure that the system authentication was functioning properly and not allowing false authentication, several security measures were implemented in the system including

- Ensuring that only users with verified user names and pass points were logged in
- Requiring the user to verify their pass points before being allowed to register a new pass word
- At each login, each pass point was examined to ensure that it was within the acceptable range. If one point is not within the correct range, or if the points are entered in incorrect order, access to the system is not granted
- A record of each all login activity was recorded to allow for verification

4.1.1.2 System Provided Images

a ***b*** ***c***

Figure 8: A selection of 3 images used as potential cues for passwords

Figure 3 shows the three images presented to the users as options for their password. The images were limited to three in order to allow for better monitoring and analysing of the password choice amongst the users. Each image was carefully selected based on existing psychological research and intuition. The aim was to select images that would represent three distinct categories of images. There has been debate amongst researchers of Cued-recall based graphical password schemes as to which is the most appropriate type of image for said system. The considerations that ought to go into the selection of the image include the potential the image affords the user of choosing unique click points.

In order to adhere to the original implementation, the images were scaled to 451 * 331 pixels respectively. Figure 8 *image a* shows an image of a human portrait. Figure 8 *image b* shows an image of abstract art. Figure 8 *image c* shows an image of a landscape.

4.1.1.3 Password Tolerance

The authentication of the user and the verification of the user's entered password occur at two stages in the system. Initially it occurs during registration where the user is required to verify their chosen click points, and then it occurs each time during login. As stated in the design chapter, it was decided that instead of delimiting the image by superimposing a grid over it, the user would be allowed to select any point as their password. A predetermined radius surrounding the original click point would constitute the tolerance region.

When the user attempts to log into the system, two methods are utilised to determine whether the point falls within the acceptable tolerance. The first method *distance*() calculates the distance between the original click point and newly entered point. The distance is calculated using the Euclidean distance formulae. Once the distance has been calculated, a new method *inRange()* is invoked. This method checks whether the provided distance lies within the acceptable tolerance range. Some research on systems similar to ClickPoints recommended using a discretization algorithm in order to calculate the tolerance. As we wanted to perform analysis on the created passwords, using a discretization algorithm would not have been feasible. This is because for the analysis we would want to extract the original co-ordinates that the users selected.

Based on research and available literature, the first tolerance range was implemented at 20 * 20 pixels. As a result if a user entered a point that was within 20 pixels range from the original click point, irrespective of orientation, they would be granted access to the system.

Once the system was implemented, the next stage in the waterfall methodology that was being followed was to test the system. This testing comprised of testing the system for any bugs and ensuring that it was working efficiently. It was during this testing stage, that it became apparent that the 20 * 20 pixel range that was being utilised was not user friendly. Unless the entered click points were exactly or only miniscule distance away from the original click point, the system would state incorrect password and deny access to the social networking site. This rendered the system virtually unusable, and keeping in mind that the system would need to be relatively simple to use when implemented on a social networking site, it was therefore necessary to adjust the implemented tolerance level. After several rounds of testing, it was decided to increase the tolerance from 20 * 20 pixels to 40 * 40 pixels. This tolerance level performed better during testing trials and allowed for a bit more leeway with each entered point.

4.1.1.3 Authentication Information Storage

In order to be able to authenticate users, the system had to store a set of user details. Apart from the conventional user details that any authentication system requires, this implementation of ClickPoints required additional details to be stored. For each user,

the image selected for the password and the co-ordinates for the 5 pass points were stored.

After selecting a user name, an image and the 5 click points this user information was recorded and stored on the system. The user name and the image were stored as simple text. The 5 pass points were stored as x and y co-ordinates named from a - e, with each letter representing one pair of co-ordinates. The rationale behind storing the pass points as co-ordinates was that this would enable the system to store a record of the original click points selected, and then at each login attempt, each point would be compared against the original click point to determine whether it was within the specified range of tolerance.

To ensure for a thorough evaluation of the system, it was essential to record the user's activities on the site. Of particular interest to this project were the login details of each participant. To this end, the system was designed to record in file specific information about each login attempt namely

- User Name
- Login Date and Time
- Number of Login Attempts
- Login successful or not successful
- ClickPoints Image Selected
- Number of times the password was reset

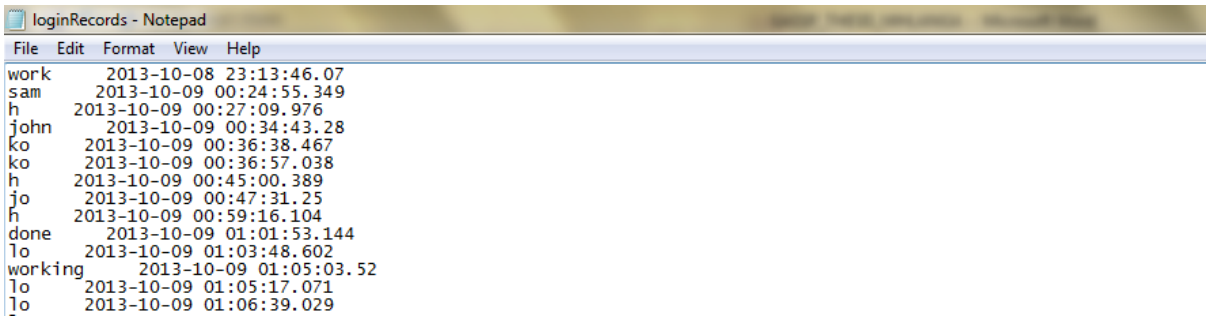


Figure 9: Sample of Login records log

4.2.1 Text-based Password Scheme

One of the key goals of this project was centred on determining whether graphical password schemes are a viable alternative to text based password schemes for authenticating social networks. Therefore, apart from the ClickPoints and Pluto graphical password schemes, it was essential to have a text-based authentication system in order to allow for comparing and contrasting between the systems. To this end a text-based login system was also used on the test social networking site.

Registering a new user

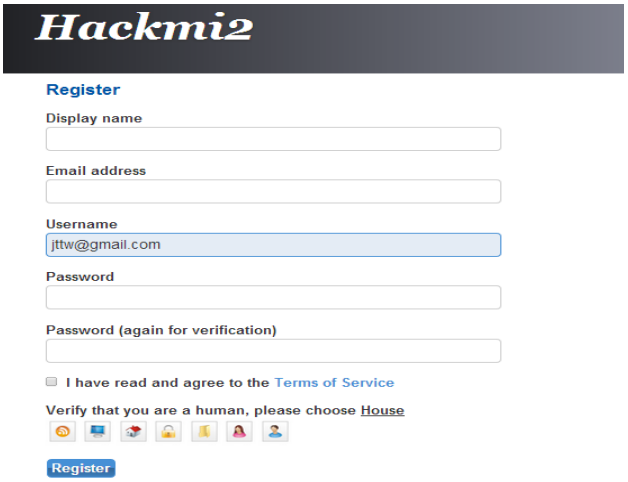


Figure 10: Sample of text-based registration page

Figure 4 shows the registration page of the text-based system. The user is required to select and enter among other information a text password. The system imposes some general constraints to the type of passwords that users can create; this is in accordance to most major authentication systems that prompt users to select stronger passwords. In the case of this text based system, the user is required to create a password that is at least 6 characters long. After entering a system approved user name and password combination, the user is required to confirm their account details by logging into their personal email to verify their account. Once the user clicks on this link they are granted access to the system.

Login into the system

To log into the system, the user is required to enter either their username or email and their text password. If these are correctly entered the user is granted access to the social networking site. The user is given the opportunity to reset their password in the eventuality of them forgetting their password. For them to be allowed to re-set their password, the system will send them a time limited link to access their account and from there re-set the password.

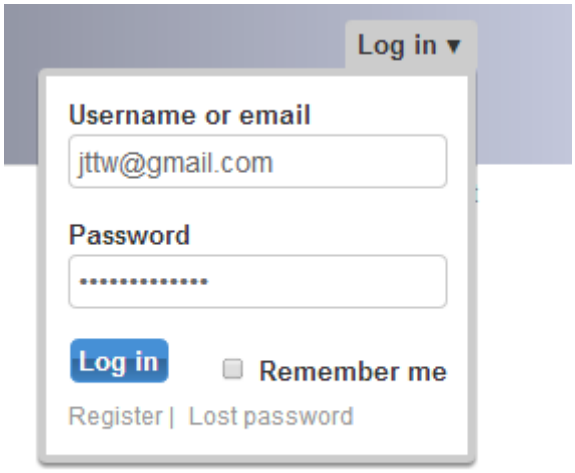


Figure 11: Sample of text-based login page

System Security Checks

The Elgg framework came with some pre-installed security measures to ensure that only correctly authenticated users would be granted into the system. Some of these measures include

- Ensuring that only users with verified user names and passwords were logged
- Requiring the user to verify their pass word before being allowed to register a new pass word
- Email verification for registration of a new user

4.3.2 Integrating onto Hackmi2

After implementing the java applet the next stage was to integrate the java applet with the Hackmi2 social networking site.

4.3.2.1 JPatchWork for Elgg 1.8

The Hackmi2 engine Elgg, comes with the capability of installing plugins. These plugins can be used to extend and customise the functionality of the created social networking site. The JPatchWork version 1 plugin for Elgg 1.8 was utilized to extend the existing capabilities of Hackmi2 to include the functionality of displaying java applets. The JPatchWork plugin facilitates for the embedding of Java applets into Elgg.

For the plugin to work on Elgg, the client side needs to have the java runtime environment installed in their browser. If the java runtime environment is not installed, the java applets will not work and the browser will display a blank screen where the graphical password schemes ought to be.

The installation procedure for JPatchWork was twofold. The first stage required that the JPatchWork folder be copied into a specified directory in on the server hosting Hackmi2. The second stage of the installation was to enable the plugin in the admin section of Hackmi2. JPatchWork includes a sample applet and also a little game for demonstration purposes. This enabled us to verify that installing java applets on Hackmi2 was feasible.

4.3.2.2 Web Services API

In order to cater for the communication between the user and the Hackmi2 site, it was necessary to implement a web service API. A web service is a means of communication over the world wide web of two devices. Elgg uses an Apache web server which provides a framework for building web services. According to the Elgg documentation, though the API is called RESTful, it is in fact a REST/RPC hybrid which is similar to the APIs provided by other social networking sites like Twitter and Flickr.

To allow for the communication between the user and the social networking site, through the java applet it was necessary to specify a new API. A rest API for logging in and setting a new password was created. The three requirements for creating an API for an Elgg site are exposing the methods, setting up the API authentication and setting up the user authentication. The *expose_function()* was the function that was used in order to expose certain methods. The web services API framework has three different default response formats. These are XML, JSON and serialized PHP.

The *expose_function()* was used to expose the login and the registration functionality. The defined web API is used to call the login and registrations functionality. What this does is that it then takes the username, the password, the selected image and the elgg security token. These are then exchanged during the communication with the server.

Elgg has in built security measures it implements in order to secure the site. One of these security measures is Hackmi2's built in anti – CSRF (cross-site request forgery) mechanisms. It does this by using anti-CSRF tokens in its forms. As a result of this, elgg requires that each action should be accompanied by a security token. The system works by generating a private token every time a web form is created. This new token is based on the initial token, a site secret, a timestamp, the user agent and a session identifier. The token is kept as hidden information on the page. Once the form is submitted the current token is checked against the hidden token in the form. If the timestamp is less than an hour old then then it is then it is secure.

4.3.2.3 Communicating with the server

The fact that the java app could communicate with java script was exploited in order to facilitate for sending the information to the server. The java applet would collect the

user name and the generated password In the event of a login attempt, the generated username and password are stored temporarily. JavaScript was then used to query the database and obtain information about the username and password. The first check was to establish whether the username exists in the database. If the username exists, then the password would be checked to establish whether it falls within the predetermined tolerance. If it does, then user is has been successfully authenticated they are then redirected to their account home page. In the case of the username not existing in the database or an incorrect password has been entered, JavaScript is again taken advantage of to catch the error from the server and display the error message on the information box on the applet.

4.3.2.4 Database

The Elgg database is the primary storage area for the user details stored by the system. The Elgg database is a MySQL database. A MySQL database had to be created to store the information. In each entry in the database, the user name and the password of the user were stored. The user name was stored as a string, while the pass points were stored as x,y double pairs for each selected pass point. The database that was used was a secure database as to gain access to the data; a user would need to the secure shell (SSH) network protocol to access the local host machine where the database was stored. Access to this was protected with secure user authentication.

4.3.2.5 Implementing graphical password scheme login

Once the communication with the server and the java plugin implemented and tested, the next stage was to add the java applet onto the social networking site. Porting the site from the java applet and onto the social networking site, required that the authentication procedure of the applet had to be modified in order to cater to the Hackmi2 framework. While the login procedure for the java applet involved a two-step procedure and the use of two screens, for Hackmi2 this was reworked into a one screen process. On the Hackmi2 implemented graphical password scheme, the user is required to enter their user name and their password and then click the login button. As this is similar to the existing text-based login screen, this was done in order to create an equal platform in which to test the two systems. If the picture password appeared to deliberately require more effort than the text system, this would influence the results of the user testing. Similarly to the login process, the registration process for a new password was reduced from a three stage process involving three different screens to a one page process.

The existing home page for Hackmi2 had the text-based login in the top right corner, leaving much of the home page blank. This was convenient as to implement the graphical password schemes it was simply a case of inserting the java applet on the home page. As a result the user could log into the system using either the text-based system or via the graphical password scheme. To create a graphical password scheme, the user first had to create a text-based password scheme to gain access to the system, once inside

they would navigate to the settings section of their user profile; under this section they could create a new graphical password. In the event of forgetting their password, they could also navigate to this page in order to reset their password.

4.3 Issues

During the implementation of the java applet and especially during the porting of the applet onto Hackmi2, several challenges presented themselves. With each challenge that presented itself, a solution or a work around was implemented in order to have a fully functional system.

Signing the java applet

The first challenge that was encountered with the functioning of the java applet had to do with the access permissions. Since web applications require that java applets be signed by a verified certificate board, Hackmi2 would not allow our application to run as it was not signed. The solution to this was to sign the application with the developer's details. As a result of this the user is informed that running the application will be at their own risk as the applet has an unverified certificate. In the event of the system being deployed in a commercial setting, then an authorised signature will be obtained.

Class definition errors

One of the major challenges we faced was with a class definition error the applet produced once on Hackmi2. The error resulted from our attempt to use the Gson library. In order to convert java objects into their JSON representation, the Gson library is used. However when we attempted to use the library, a java.lang.NoClassDefFoundError occurred. This problem took several days to solve. Eventually a work around solution was discovered. Instead of using this class to first convert the java objects, JavaScript was used directly to communicate with the server bypassing the need for this conversion library.

Recording login details

In order to be able to successfully evaluate the system, it was essential to record the details pertaining to the user's use of the system. While this had been implemented on the java applet by writing to a text file within the java code, this solution was not directly applicable once the applet was on the social networking site. The eventual solution to this challenge was to include within the web page, php code to record the each login attempt whether successful or not and to write this data to a text file stored on the server.

4.4 Discussion

In this section, the implementation details of the ClickPoints system have been presented with particular focus on the development of the java application and the porting of the application from a standalone applet to integrating it with the social networking site, Hackmi2. As

detailed in this section, a number of adjustments had to be made to the standalone java applet to ensure that it could function correctly on Hackmi2. A complete and functional version of the ClickPoints graphical authentication system was implemented on a social networking site as per the initial requirements of the project. This meets one of the goals of the project which is to have a working graphical password scheme on which to test our research questions.

Through the implementation of the system and with the benefit of hindsight, several important lessons with regards to project implementation and web application development were learnt. The major learning point was that for the purpose of web applications, it is better to use java script for the development of small to medium size web apps. The benefits of using java script are many including increased speed and also less use of memory as the language is by nature very light weight. Java Applets on the other hand have a lot of restrictions associated with them and also require external libraries to facilitate for their communication with the web services, for example, the case with using the Gson library. That being said the eventual system implemented on Hackmi2 is capable of authenticating users to the social networking site via either a graphical password scheme or a regular text-based password scheme.

5. System Evaluation

After the design and implementation of the system, the next stage was to conduct the system evaluation. This section details the testing methodologies and strategies that were employed. An evaluation and discussion of the test results will also be presented. The evaluation of the system was a key component of the project as the results obtained from this section are pivotal to answering the research questions and objectives of this project.

5.1 Testing strategy

In order to efficiently evaluate the system for both usability and security, it was essential to structure the usability study in a manner that would obtain the required metrics. According to experts, usability testing measures a human made products ability to meet its intended purpose. In this light we intended to evaluate the overall system under four main broad areas, namely

- Efficiency

  The different graphical password schemes would need to be evaluated for overall efficiency. Under this topic the testing aim is to determine whether the system works as intended, whether it does so in a reasonable amount of time and whether it is secure

- Recall

  The different password schemes would be evaluated to determine which password scheme facilitates for the most recall and is the simplest to remember.

- Emotional response

  One factor that determines the success of any system is how the users respond to the system. To this end, the testing would seek to determine how the users interacted with the system and to evaluate whether they felt competent or not when using the system.

- Security

  The key aspect to any authentication system is whether or not it is secure. To this end the testing would seek to evaluate the security of the system by looking at the strength of the passwords created and the vulnerability of the system to attackers

A two stage usability study to compare the three implementations of passwords schemes: ClickPoints, Pluto and the text-based password scheme was designed based on prior research and common industry practices. The first stage of testing comprised of a lab study to evaluate and compare the robustness of the different password schemes to guessing and capture attacks. A pre-study questionnaire was distributed in order to elicit the participant's current strategies when using text passwords. Issues such as how often the users forgot their

passwords and whether they made use of coping strategies such as writing down the passwords in order to aid their memory was examined.

The next stage of testing comprised of a field web-based study to evaluate and compare the usability across the three implemented schemes. Then finally a post-study questionnaire was distributed to the users in order to gather their opinions on their experiences with the password schemes and their preference. The questionnaire would also seek to examine how the users interacted with and managed their graphical passwords. In order to encourage continued participation from the users, each person that completed the lab session or the field was offered a small incentive for their time.

5.2 Evaluation Tools and Techniques

Several methodologies and tools were employed in order to evaluate the system. The aim of the testing was to collect both qualitative and quantitative data about the usability of the system. For the testing we used a combination of information gathering tools including controlled experiments and questionnaires. The lab study was the session that comprised of controlled experiments. These experiments were set up in order to test specific security functionalities of the system, specifically robustness to attacks. Though controlled, these experiments allowed us to collect quantitative data about the performance of the different password schemes.

For the field study we employed a technique known as Hallway testing. Hallway testing is a testing methodology where a varied sample of individuals irrespective of geographic location and time differences are asked to evaluate the system. In this case, the testing methodology simulated a social network environment whereby individuals are located in different locations and make use of the system at different times.

At the end of both the lab and the field testing experiments, the users were asked to complete a questionnaire. The choice of using a questionnaire was made based on the fact that they are quick and simple to implement and also they allow for the extraction of both quantitative and qualitative data from the users. To construct the questionnaire, research was conducted on how questions in questionnaires ought to be asked and structured. This in turn would ensure that the users were posed with the right questions in order to evaluate the system.

5.2 Lab Session

The controlled experiments in the lab session were divided into two sessions. The first session involved introducing the participants to the idea of graphical passwords and assisting them with creating their graphical passwords and with the initial login to the system. The aim of this section, apart from initial introduction, was to allow us to measure metrics such as the time taken to create a new password and the memorability of the passwords after a short time.

The second section of the lab study involved testing the system for robustness against attacks. The following attacks were tested on the system.

Guessing attacks

Guessing attacks are attacks on the system where the potential attacker attempts to guess the users password. This guessing can be a brute force attack, where passwords are attempted at random, or they can be comprised of informed guesses, for example when the user's personal details are known. In this experiment brute force attacks were attempted as these are the most fundamental of all guessing attacks.

- Dictionary attacks

  Dictionary attacks are brute force attacks where a dictionary of passwords is attempted in the hope of finding a match. In this experiment, to test for dictionary attacks, the user selected passwords were all complied, and then based on their selected passwords, if the passwords were in the vicinity of the anticipated hot spots of the image; this password was deemed vulnerable to dictionary attacks.

Capture attacks

Capture attacks are attacks on the system where the potential attacker attempts to obtain the users password by some malicious and deceptive means. There are several capture attacks currently in use on text-based passwords. However for this experiment we decided to examine the two capture attacks; the first is one that graphical passwords have been shown to be most vulnerable to while text passwords have been shown to be robust against the same attack. The second capture attack is the opposite to the first one in that graphical passwords have been reported to be robust against this attack while text passwords have been shown to be vulnerable.is one that text passwords have been shown to be most vulnerable to.

- Shoulder surfing

  Shoulder surfing attacks, are attacks where by the potential system intruder attempts to observe the user as they enter their password. Then based on their observation, they attempt to login to the system. In this experiment, we tested two participants at the time. Both participants were given the opportunity to act as the attacker. Each participant was asked to observe as the other participant entered their password onto the system. After observing the password being entered, they were then asked to try and login to the other participants account. The results from these tests would then be used to determine how vulnerable a specific scheme was to shoulder surfing.

- Social engineering

  Social engineering attacks are attacks whereby the user is tricked into revealing their password. There are several different techniques of conducting social engineering attacks including using malicious email links and spyware. In this experiment, to test for vulnerability to social engineering, each user was asked to describe their password to another participant. If based on the description, a participant was able to

successfully login to another account, this would highlight the systems vulnerability to social engineering attacks. Text passwords are especially vulnerable to this as the given instructions are specific and accurate, graphical passwords on the other hand were of interest to examine how attackers would potentially attempt to approach this situation.

5.3 Field Session

An online field study was conducted to allow the users to access and use the social networking site under realistic conditions, similar to the social networking sites they currently use. Users would be sent text and email prompts to remind them to login into the system. The goal of the field testing was to evaluate the usability of the system and the memorability of the passwords by monitoring specific metrics including how often a password was rest, the number of login attempts and the login time. In order to record these metrics, the password schemes were designed to record in a file each login attempt, success, fail, password reset and the time that these occurred. The two graphical password schemes in particular would be evaluated under four main observational areas namely

Following this, the two graphical schemes would be compared against each other over four core usability features namely ease of use, ease to create, ease to learn and ease to memorize. For ease of use, the test would seek to examine how simple it was for the participants to use the graphical password scheme. For ease to create, the test would be seeking to evaluate how simple it was for the users to create their first graphical password. Ease to learn and ease to memorize tests would seek to evaluate how simple it was for the users to learn how each system function and how simple it was to remember the graphical passwords.

- **Ease of use**

  For ease of use, the testing would seek to establish from the user's opinion how simple and user friendly they found the overall graphical password systems. This information would be obtained from the post-study questionnaire that the users would complete. This would provide qualitative about their opinions on the system.

- **Ease to create**

  For ease to create the testing would seek to measure both how long and in the users opinion how simple it was for them to create a new graphical password for both the ClickPoints system and the Pluto system. This information would be collected from the system records and also from the questionnaire. To observe how simple it was for the user to create a password, the number of times they created a password during initial login would also be recorded. In terms of data collected, this would be qualitative and quantitative data.

- **Ease to learn**

  For ease to create, the testing would seek to measure if the users found the graphical password system easier than the text based system to learn how to use. To record this metric, the users responses to the questionnaire would be evaluated, also the amount of time it took them to feel familiar with the system.

- **Ease to memorize**

  The aim of examining the ease to memorize aspect of each graphical password scheme is to determine which of the two schemes result in less work for the user in order to remember their password. To determine this, the user's responses to the questionnaires would be evaluated and also the number of times a user had to rest their password was also evaluated.

5.4 Target Users (Participants)

In order to test the system in the context of a social networking site which caters to a variety of individuals, the participants of the study were chosen carefully to attempt to represent this diversity. The participants were composed of a mix of male and female students at the University of Cape Town. The ages of the participants ranged between 20 – 25 years. The expertise level and familiarity with technology was also varied with the pool of participants consisting of a variety of professions from computer science students to art students.

5.6 Test results

The following section details the data that was collected during the lab and the field testing sessions.

5.6.1 Lab test

Time taken to create a new Password

Table 1 shows the average number of tries the participants required in order to be able log into the system. As shown in the table users on average required at least 3 attempts in order to be able to successfully create a new password for the ClickPoints graphical password system. This corresponded to the users taking on average in excess of 3 minutes to create a ClickPoints password. The Pluto graphical password scheme and the text based password scheme required between 2 to 1 attempts respectively. For the Pluto password scheme, the users on average took about a minute to successfully create a new password. The text based password scheme required the least number of attempts with most users intuitively knowing how to create a basic 6 character password, which was the system requirement. On average the users took less than a minute to create a text based password.

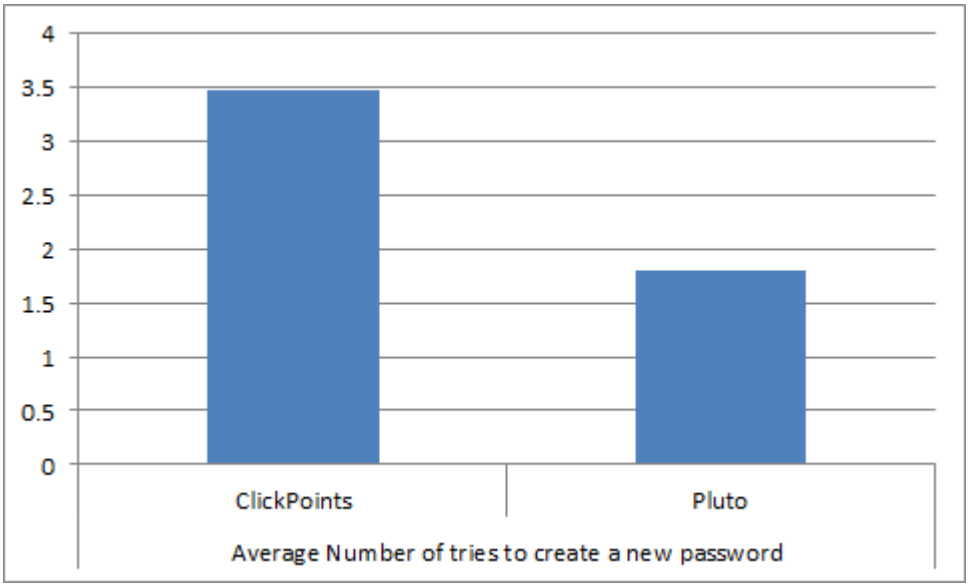


Table 1: Table showing the average number of attempts to create a new password

Social Engineering attacks

The three password schemes were tested for their susceptibility to social engineering attacks. Text based passwords proved to be very vulnerable to social engineering attacks with all the passwords able to correctly enter the password once given the instructions. The two graphical password schemes had significantly lower vulnerability to these attacks than the text version. The Pluto password scheme proved to be twice as vulnerable as the ClickPoints password scheme. However both systems were still over 60% more robust against social engineering attacks than text passwords.

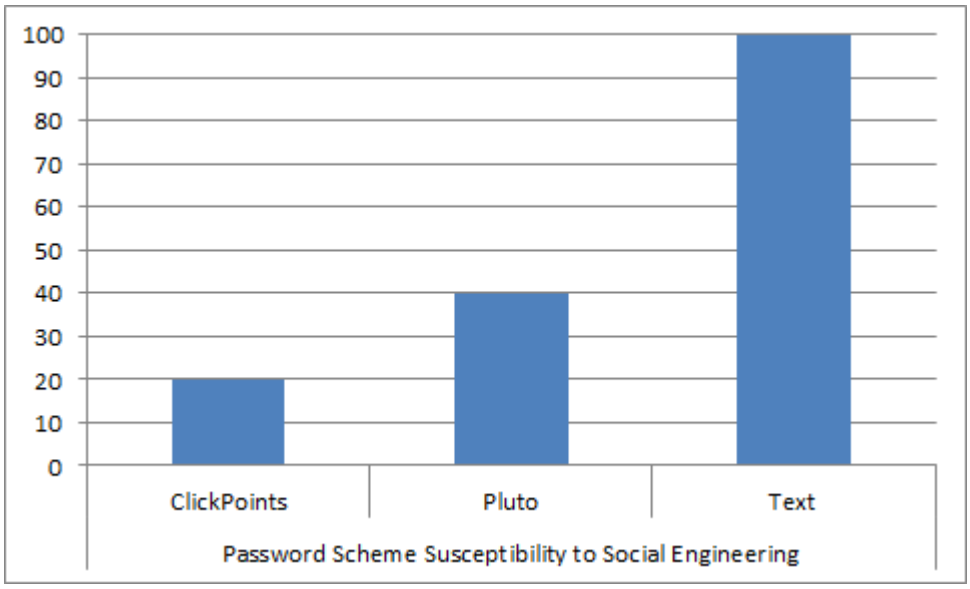


Table 2: Table showing the average susceptibility of a password scheme to social engineering attacks at a %

Shoulder Surfing Attacks

When tested for robustness against shoulder surfing attacks, the two graphical password schemes proved to very vulnerable to these types of attacks. The Pluto password scheme was very vulnerable to these attacks with most user selected passwords being easily obtained by an attacker. On the contrary, the ClickPoints password scheme though still susceptible to shoulder surfing, was more robust with fewer than 70% of the passwords being guessed via shoulder surfing. The text-based passwords proved to be very robust against shoulder surfing with none of the attackers being able to glean the password from observation.

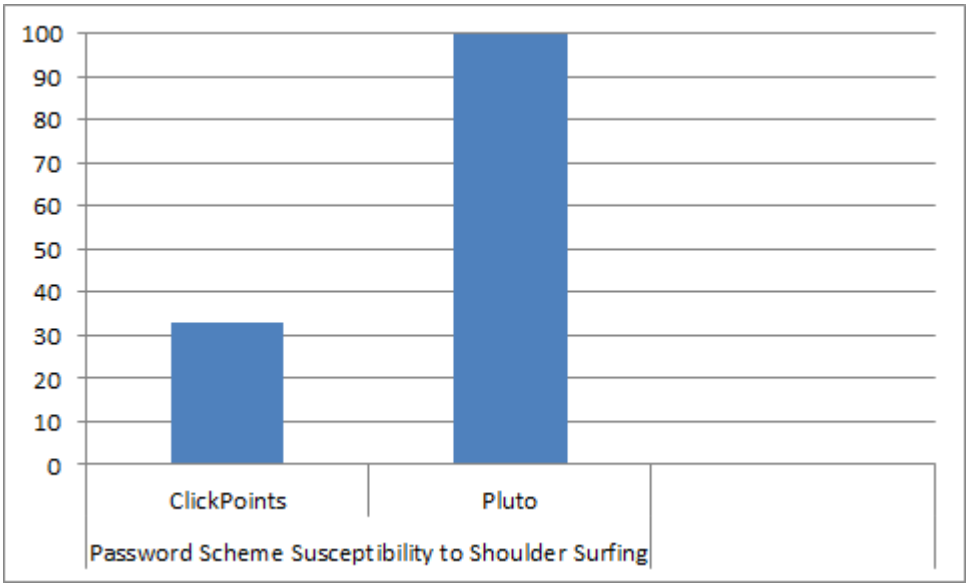


Table 3: Table showing the average susceptibility of a password to shoulder surfing

Dictionary Attack

The results from the dictionary attack tests were very varied between the three password schemes. The ClickPoints graphical password scheme seemed to be the least vulnerable to dictionary attacks with only 40% of the passwords being obtainable by running a dictionary attack on the scheme. The Pluto scheme was slightly more vulnerable than the ClickPoints system with about 60% of its passwords being obtainable by a running an exhaustive search. The text based password scheme was also very vulnerable to dictionary attacks.

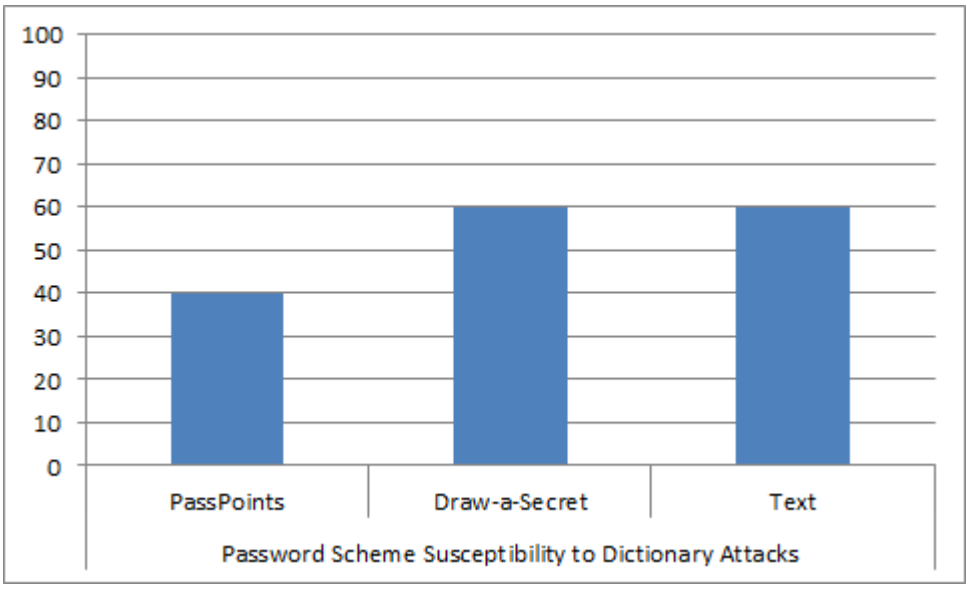


Table 4: Table showing the average susceptibility of a password scheme to dictionary attacks

Questionnaire

A questionnaire was distributed to the participants after the completion of the lab session exercises. The questionnaire was comprised of 11 questions designed to establish the participant's general practises with text based passwords and also to obtain their opinion on the new passwords schemes they had recently been exposed to. The first questions designed to test the user's practises with passwords revealed that the majority of the participants were prone to succumbing to the risky password use and maintenance strategies that most people use. When asked whether they used different passwords for different applications 80% of the participants responded in the positive, while the remaining 20% said no. However the following question which asked them whether they used simple variants of their passwords e.g. sam1, sam12, sam123, for the different applications, 85% of the participants said yes. This shows that while they use different passwords for different applications, it does not necessarily mean that the password is unique or that it is very secure.

The next sets of questions were designed to discover the techniques that the users employed in order to aid their memory of the passwords. When asked whether they used their web browser to remember the passwords to sites they visited, 75% of the users said yes. The next question which asked whether the users wrote down their passwords either on paper or electronically to aid their memory, again 75% responded in the affirmative. When asked whether during password creation, the users made use of personal information e.g. birthdays, family names etc., the response was split in the middle with 50% saying yes they did while the rest said no. It was found that none of the users made use of dedicated secure password storage software to aid their memory.

The last set of questions inquired into the participant's opinions of the graphical password schemes they had been exposed to. When asked which graphical password

scheme they found the easiest to create and the easiest to remember, the responses were split 65 to 35% with the former saying the drawing password was the simplest and the rest saying the ClickPoints system was the simplest to use. 10% of the respondents stated that they were neutral and found both systems equal in terms of usability and memorability

5.6.2 Field Test

Efficiency

Time to create/login password

Table 5 shows the average time taken by the participants to create a new password for the different password schemes. On average, the graphical password schemes required more than a minute for a participant to be able to successfully create a password. The majority of the participants reported that the graphical password schemes took required more than 2 minutes in order for a person to successfully create a password. On the contrary, most of the participants reported that the text based passwords took less than a minute to create with the exception of one user who struggled with creating a system approved password.

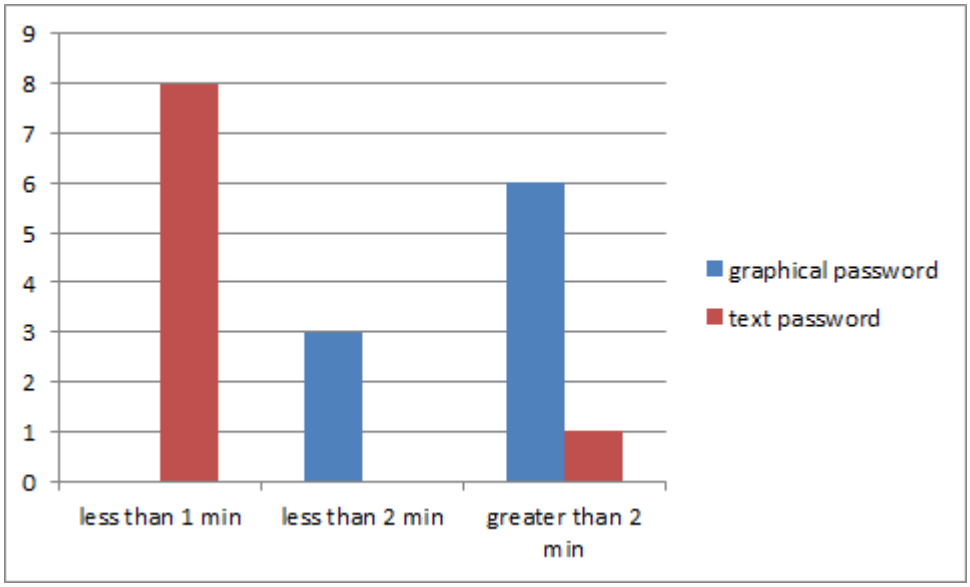


Table 5: Table showing the average time taken to create a graphical password and a text based password

Error Rates

Login success rate

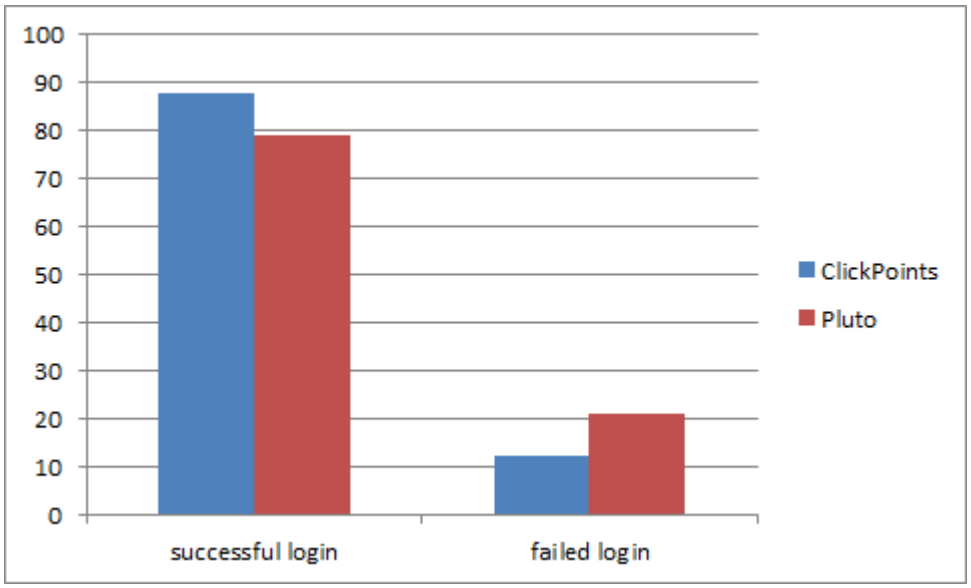


Table 6: Table showing the average login success and error rates between the two graphical password schemes

Table 6 shows the average login success and error rates between the two graphical password schemes. As shown in the table, the ClickPoints graphical password scheme had a slightly higher average rate of successful logins as opposed to Pluto. Correspondingly, ClickPoints had fewer recorded failed logins as opposed to Pluto.

Reset Passwords

Both graphical password schemes, ClickPoints and Pluto recorded the same number of password resets with each scheme having two password resets respectively. As this was viewed as one indicator of the memorability of each of the password schemes, this result implies that the ClickPoints and Pluto system have about the same memorability rates. The text password schemes recorded a high memorability rate as only 3 participants reset their passwords.

ClickPoints –selection for password

Figure 4 shows the hot spots that emerged on each of the available system images. The hot spots were determined based on the most popular selected points for each image. Figure 4 *image b* was the most popular image for the password. The hotspot points that emerged for this image were the centres of the flowers. Most users that selected this image as their password selected a varied sequence of the each of the

flower centres. The next popular image for passwords was Figure 4 *image a*, the human portrait. With this image the hot spot areas developed around the eyes, ears, nose and teeth. These areas seemed to easily afford themselves for a password as most users selected a combination of these for their password. The least popular image of the system was Figure *4 image c*. This image was selected by less than 30% of the participants. When selected, the hot spots developed around the text on the password and on the brighter spots of the image. Figure 4 *image c* resulted in the most secure passwords as the selected points were not as obviously or easily intuitive as the other two images.

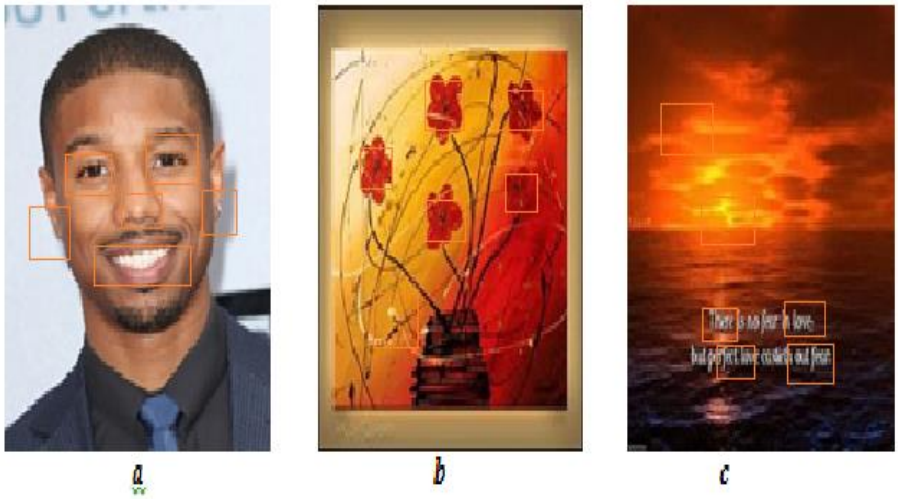


Figure 11: Figure showing the hotspots discovered on the images

Questionnaire

The first set of questions on the questionnaire was designed to extract the participant's opinions on their experience with the graphical password schemes. The first question which asked whether the participants would use graphical passwords to authenticate their Facebook account, 57% of the participants responded in the negative. Similarly when asked whether they thought graphical passwords were easier to easier to manage 78% of the participants said that they thought graphical passwords were more demanding to manage. When asked which password scheme they found the simplest to remember, the users selected ClickPoints as the more user friendly system.

When asked to select a password scheme between the text, ClickPoints and Pluto to use for their social networking accounts, the majority of the participants selected the text system. In terms of perceived security of the password schemes, just over 63% of the participants stated that they thought that graphical password schemes were more secure than text passwords. Some of the participants further elaborated on how they arrived to that conclusion.

5.7 Discussion

The results from the user testing provide for the basis of evaluating the graphical password schemes and determining their suitability for social networking sites.

Lab Session

During the lab session the users were first introduced to the idea of graphical passwords and the system was tested for robustness against certain attacks. All of the users were curious and interested in the graphical password schemes.

Based on their responses from the questionnaire, the users were found to have adopted the most common and insecure means of managing text passwords. This includes the practice of writing passwords down and using a variation of one core password for a variety of applications. The main reason for this as established from the user study and prior research is that there exists now an information overload with the amount of passwords that users are required to remember for different passwords. Also the restrictions that most sites are imposing on the passwords that can be created are also adding to this information overload.

The time taken and the number of tries needed to create a graphical password was recorded. As shown in the results the ClickPoints system required on average more than 3 tries before a user could successfully create a password. This is much more than the average two tries a user needed to create the Pluto password and the one try that was average for the text based passwords. One possible explanation for this is that ClickPoints password scheme was very novel to the users as opposed to the drawing password and the text password. With the Pluto system, most users have been exposed to a system familiar to this which is the grid lock screen available on most smart screen. This may have contributed to them understanding more quickly what was required of them than with the ClickPoints system.

The results from the robustness checks were very varied. As anticipated, the two graphical password schemes were very susceptible to shoulder surfing attacks. Since picture passwords have the asterisks to mask user input, this makes it difficult for an attacker to observe the entered password without having to watch the users' keyboard strokes. As most people are quick with typing, and also from repeated use and experience, users tend to enter their passwords quickly, this further reduces the possibility of being able to successfully deduce a text password from shoulder surfing attacks. Graphical passwords are yet to have a general and acceptable defence to this and hence it is easy for a would-be attacker to directly observe the password being input. In this lab session, the ClickPoints system seemed to be only slightly more robust to shoulder surfing attacks than the Pluto system. A possible explanation for this is that while with the drawing system, if a user is able correctly observe the pattern of the drawn password, they are almost guaranteed to be able to successfully enter it. With the ClickPoints system however, even if the attacker successfully observers the sequence of the entered password, upon input, if they are within the general vicinity of the original click point, but outside of the acceptable tolerance level, then they still fail to login. This to a certain extent is a deference that ClickPoints naturally has to shoulder surfing attacks.

The test for robustness to social engineering attacks produced results similar to the ones for shoulder surfing for the two graphical password schemes. The Pluto system was twice as vulnerable to social engineering attacks as opposed to the ClickPoints system. Some of the passwords that the users created for the Pluto system were based on elements that most people are familiar with, for example, the users would create passwords of box shapes or line

shapes or letter shapes. This meant that when describing their password to other users, the listening person could understand and visualize what the password was supposed to look like. This resulted in more people being able to correctly enter these passwords. With the ClickPoints system however, some of the users found it difficult to describe their passwords because for some of the points, they could not give an accurate description of where it was on the image. For example with the landscape image, it was difficult for the users to describe which point on the horizon exactly their pass point was located. This in turn resulted in fewer people being able to log into a system based on these descriptions. It is essential to note that though the graphical password schemes were susceptible to social engineering attacks, their levels of vulnerability to this attack were significantly lower than those of text passwords. This is because with a text password, a user can spell out their password and the attacker will know exactly what input and in what manner they are expected to input it. This makes both graphical passwords schemes significantly more robust in this instance as compared to text passwords.

When tested for susceptibility to dictionary attacks, the graphical password schemes were found to have vulnerabilities. In the case of the ClickPoints system, the development of the password hotspots are prime targets for dictionary attacks. Text based password schemes have had several studies to examine their robustness against dictionary attacks. Several strategies have been employed to attempt to make text based authentication systems more robust against dictionary attacks. These mitigations techniques include prompting the users to select stronger passwords and also limiting the number of attempts that a user can have before a system automatically locks them out. These are techniques that can be translated with some modification to graphical password schemes.

After the lab session the users were given a questionnaire to complete. The aim of the questionnaire was to elicit the participant's responses and opinions to the password schemes they had been introduced to. When asked which password scheme they found the most simple to use, the responses were split with most users saying the drawing password scheme was the easiest to use. Some of the reasons that the users gave for preferring the Pluto system was that the ClickPoints required more memory effort in order to remember exactly where the original point had been placed. As previously hypothesized, this could be because the users may have had some prior basis for how the Pluto system would work as opposed to the ClickPoints system which was a completely new idea.

Field Session

The results from the field study had significant ecological validity as they attempted to simulate how an average user would login and access their social networking site. The first test was to examine the amount of time it took for users to create a new password. As evidenced by the results, the participants found the graphical password schemes to require on average more than 2 minutes creating a password, which is more than twice the amount of time needed to create a text password. This is a significant usability issue because it requires more effort on the users which it had been hoped graphical passwords would do the opposite and require less effort from the users.

The next metrics that were evaluated were the recorded error rates during the duration of the field study. The two graphical password schemes were compared against each other to evaluate which system had the most successful login rate. As evidenced by the results, the ClickPoints system had slightly more successful logins as opposed to the Pluto system. There are several reasons as to why this was the case. One of the reasons may be that the

allowed tolerance for password was generous and as such the users were allowed more leeway with pass points that were not in exactly the original spot. Some of the users complained that the challenge they faced with the Pluto system was that it was difficult with their laptops to be able to control their drawing strokes. This challenge was not there for the ClickPoints system as the users only had to click a specific point. Quite possibly the participants may have performed better is they had had mouse input. Also the Pluto system maybe better suited for touch input as opposed to input from other devices in terms of facilitating for more accurate password input.

In terms of the number of times the users reset their passwords, both the ClickPoints and the Pluto system recorded the same number of password reset. Since the number was very low, this could be seen as an indication of the memorability of the created passwords. However it is important to take into consideration that as these were the only graphical passwords that the users had, that element of uniqueness may have prompted their remembrance of said password. Given a multitude of graphical passwords to remember the results may have been different.

As shown in the ClickPoints system, the image that was the most popular for creating a password on was the image of the abstract art. The image with the next highest popularity was the image of the human portrait with the landscape image being the least popular. One clear reason as to why the abstract image was the more popular is that it intuitively presents the user with five click points required by the system, in the form of the 5 flower centres. In terms of memorability also, the users stated that it was simple to remember the points and also to re-enter them as all they would need to do would be to aim for the centre of the centre of the flower. This would result in most entered points always falling within the acceptable tolerance. The human portrait was the second most popular and this is possibly similar to the flower image, it presented the users with fairly intuitive click points, in the form of distinct spots on the image, like the pupils, the tip of the nose and the teeth. In contrast to the flower and portrait image, the landscape image did not present the user with immediate distinct click point areas. Also because much of the image was the same hue and tone, it was difficult for the users to remember exactly which point on the image they had placed their click points. As a result, even though most of the entered click points were within the general vicinity of the original click point, they tended to fall just outside of the acceptable tolerance. This suggests that for future graphical password schemes, if the intended target platform has a low security requirement, then images like the abstract art and human portraits would be more appropriate. Then for systems with a high security requirement, it would be more prudent to supply the users with more images of landscapes as these tend to both facilitate for the creation of stronger passwords and a stronger defence against dictionary attacks.

After the field study was completed, the users were required to complete a questionnaire in which they were asked to document their experiences with the graphical password schemes. The majority of the users stated that given the option, they would not user either graphical password scheme to login to their social networking sites. Most stated a preference for the text based systems. Some of the reasons for this included the facts that the users found both creating and logging into the social networking site to take at least twice as much time as the time required by a text system. This seems to indicate that graphical password schemes still require more improvements and refinements in terms of efficiency in order for them to be competitive to text based password schemes. The majority of the participants stated that in their opinion they did thought that graphical passwords were more secure than text based password schemes. In terms of remembrance, the ClickPoints system seemed to be the easiest to use with over 57% finding this password scheme easier to remember than that Pluto

system or the text passwords. A possible explanation for this could be that as graphical ClickPoints system uses more visual information than the text system, it makes it easier to remember.

The majority of the participants stated in their questionnaire responses that they did not find the graphical passwords to be easy to remember especially when compared to text passwords. Some of the complaints around the ClickPoints system were centred on the fact that the password had to first be within the acceptable tolerance, and then the pass points also had to be entered in the correct sequence. Some of the users employed a variety of strategies to aid their remembrance of the password schemes. One user stated that to remember their password, they picked literal points on the image, for example, for the ClickPoints system; they picked an ear while on the Pluto system they used an L shape.

One of the final questions in the questionnaire required the users to raise any concerns that they had about the use of graphical passwords. Some of the main complaints were that the graphical passwords did not seem secure as a person could easily detect the password from looking over someone's shoulder. Also for the ClickPoints system, some of the users complained that the tolerance level was too strict which made the using the system frustrating. Also the limited choice of images for ClickPoints was an issue for some of the users.

Due to some of the challenges faced and the limitations of this study, it is important to take these results in context. Some of the limitations faced were that the number of participants used to test the system was limited; therefore these results should not be extrapolated to represent the general population.

Based on the results of the testing it would seem that the users prefer using text passwords to graphical passwords. While a slight majority of the users stated that they would use graphical password schemes for authenticating their social networking sites, the users still had a few reservations. In response to the second research question, it would seem that at present though offering more security, graphical passwords still have a lot more improvements and enhancements to undergo before they can be a viable alternative to text-based passwords as a means of providing authentication to social networking sites. When comparing the two graphical password schemes ClickPoints and Pluto together, the ClickPoints system performed slightly better than the Pluto system. One factor that impacted this result was the input mechanism, which for the Pluto systems seems more suited for touch input. Therefore in terms of efficiency, cued-recall based password schemes seem better suited for social networks, if only mainly in terms of input methodology.

5.8 Future work

As graphical password schemes are young area of research and therefore few systems have actually been implemented and tested, this results in a large scope for possible future work. After evaluating the system and based on user responses the most practical and interesting topic of future work would be to attempt to improve on the current graphical password schemes on hackmi2 with particular focus being on ways to address the usability and security concerns that the users raised. In the case of ClickPoints this would involve looking at

Changing tolerance levels

In further research into the topic, one area of focus could be examining the effect of different tolerance levels on both the strength of the created passwords and the usability of the system. In this implementation of ClickPoints, only one tolerance level was tested. This could be enhanced by testing a variety of tolerance levels. This would result in the discovery of a tolerance level that has the best combination between security and usability being implemented.

Increasing image database

Also in this implementation of ClickPoints, due to the need to collect as much information as possible from our limited pool of participants, the number of image choice in the system was limited to three. Further work on this aspect of the project would involve increasing the pool of images the users are allowed to select from and also implementing the feature that allows users to use their own personal images fir the background image. The benefit of this work would be an increased understanding of the implications that choice and the image have on both the memorability and the strength of the passwords created.

Enhancing the user testing

Due to limited resources and access, the user evaluation was conducted with a limited number of participants. In the case of a system like ClickPoints where user opinion is central to the option of the technology, it is essential to test such a system with as many users as possible. This allows for the development of the best system possible as many of the usability issues are bound to be discovered due to the size and variety of testers.

Also this project focused on one implementation of a cued-recall graphical scheme. However there are several types of cued-recall based systems that would be of interest to explore their applicability for social networking sites. For example a system such as Persuasive Cued Click Points would be interesting to conduct user testing on and to see whether uses could actually be guided as in text-based systems to create more random passwords.

6. Conclusion

As the world becomes more and more digitalized, the issue of secure authentication has grown in prominence and importance. Currently, most systems use a combination of a unique user identifier and either a numeric or an alphanumeric set of characters as the password. This system has been in use for a very long time and as a result it has been closely studied and many attacks and vulnerabilities to the system have been discovered. Graphical passwords have been proposed as an alternative to text-based passwords. This project facilitated for an implementation of a graphical password scheme, ClickPoints onto a social networking site, Hackmi2. The aim of the project was twofold, first to determine which graphical password scheme is most suitable for use on social networking sites and second to determine whether graphical password schemes are a viable alternative to text-based password.

To this end, a cued-based recall graphical password scheme, ClickPoints, was developed based on the original implementation of ClickPoints. Particular attention was paid to the password tolerance set and to the images used for the system as these are the two core features of such a password scheme. After the implementation of the password scheme, a user evaluation was conducted in order to determine the functionality of the system and to attempt to answer the stated research questions of this project. The system was evaluated against another graphical password scheme, Pluto and a text based system.

The results from the user study provided significant insight into current user practises with text based passwords, and also into the potential reactions of user to a graphical password scheme. The majority of the users, though they were interested in the idea of graphical passwords, did not immediately want to adopt them for use for social networking sites. A variety of explanations were offered up for this, including the sentiment and evidence that graphical password schemes require more time for users to create a new password and to log into the system. As the majority of the users did not perceive graphical passwords to be more secure than text based passwords, the extra work and effort needed to use graphical password schemes was deemed unnecessary.

The field of graphical passwords is still relatively new and more research into their functions still needs to be established. There is a vast potential for improvements into the memorability, manageability and usability of these graphical password schemes. This project has helped lay the foundation for the development of these improvements, enabling future researchers to build upon this research. Text based passwords are fast becoming an insecure and archaic means of system authentication, it is therefore essential to continue to explore potential alternatives, like graphical passwords, that could provide for more security and ease of use.

7. References

Bicakci, K., Atalay, N. B., Yuceel, M., Gurbaslar, H., & Erdeniz, B. (2009). Towards usable solutions to graphical password hotspot problem. *Computer Software and Applications Conference, 2009. COMPSAC'09. 33rd Annual IEEE International, , 2* 318-323.

Biddle, R., Chiasson, S., & Van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR), 44*(4), 19.

Bishop, M. (2003). What is computer security? *Security & Privacy, IEEE, 1*(1), 67-69.

Bower, G. H. (2000). A brief history of memory research. *The Oxford Handbook of Memory,* , 3-32.

Bulling, A., Alt, F., & Schmidt, A. (2012). Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems*, 3011-3020.

Cheswick, W. (2012). Rethinking passwords. *Queue*, *10*(12), 50.

Chiasson, S., Forget, A., Biddle, R., & van Oorschot, P. C. (2008). Influencing users towards better passwords: Persuasive cued click-points. *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1*, 121-130.

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1), 128-152.

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human-Computer Studies, 70*(6), 415-431.

Dunphy, P., & Yan, J. (2007). Do background images improve draw a secret graphical passwords? *Proceedings of the 14th ACM Conference on Computer and Communications Security*, 36-47.

Forget, A., Chiasson, S., & Biddle, R. (2010). Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, 1107-1110.

Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008). Yagp: Yet another graphical password strategy. *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*, 121-129.

Masrom, M., Towhidi, F., & Lashkari, A. H. (2009). Pure and cued recall-based graphical user authentication. *Application of Information and Communication Technologies, 2009. AICT 2009. International Conference On*, 1-6.

Meng, Y., & Li, W. (2012). Evaluating the effect of user guidelines on creating click-draw based graphical passwords. *Proceedings of the 2012 ACM Research in Applied Computation Symposium*, 322-327.

Moglen, E. (2013). The tangled web we have woven. *Communications of the ACM, 56*(2), 20-22.

Oorschot, P. v., & Thorpe, J. (2008). On predictive models and user-drawn graphical passwords. *ACM Transactions on Information and System Security (TISSEC), 10*(4), 5.

Tari, F., Ozok, A., & Holden, S. H. (2006). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. *Proceedings of the Second Symposium on Usable Privacy and Security*, 56-66.

Van Oorschot, P. C., Salehi-Abari, A., & Thorpe, J. (2010). Purely automated attacks on passpoints-style graphical passwords. *Information Forensics and Security, IEEE Transactions On, 5*(3), 393-405.

van Oorschot, P. C., & Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords. *Journal of Computer Security, 19*(4), 669-702.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: Effects of tolerance and image choice. *Proceedings of the 2005 Symposium on Usable Privacy and Security*, 1-12.

Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: Empirical results. *Security & Privacy, IEEE, 2*(5), 25-31.

Zakaria, N. H., Griffiths, D., Brostoff, S., & Yan, J. (2011). Shoulder surfing defence for recall-based graphical passwords. *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 6.

8. Appendices

Questionnaire Lab Session

1. Have you ever forgotten a password?

   _____

2. Do you reuse your password for different applications e.g. UCT access, email, Facebook, etc.?

   _____

3. Do you use simple variants of your password for different applications e.g. sam1, sam12, sam123?

   _____

4. Do you use your web browser to remember your passwords for certain sites?

   _____

5. Do you ever write down your passwords, either on paper or electronically to help you remember them?

   _____

6. When creating a new password, do you make use of personal information? e.g. birthdays or names of family members

   _____

7. Do you make use of dedicated secure password storage software?

   _____

8. Do you have more than 10 unique passwords that you make use of?

   _____

9. Are you a member of 10 or more sites that require you to login in to them?

   _____

10. Which password scheme did you find the easiest to create?

    _____

11. In your opinion which password scheme had the easiest password to remember?

    _____

Questionnaire Post Field Session

1. Would you use a graphical password to authenticate a social network site, for example your Facebook account?

   _____

2. In your opinion which password scheme had the easiest password to remember?

   _____

3. Do you think graphical passwords are easier to manage as compared to text based passwords?

   _____

4. What methods did you use to help you remember your graphical password?

   _____

5. If you had to choose a password scheme for your Facebook account, from the three that you have been using, which one would you pick?

   _____

6. Do you think graphical passwords take longer to create than a text password?

   _____

7. How long do you think it took to create your graphical password? 1-2min 3-4min 5-6min

   _____

8. How long do you think it takes to create a text password? 1-2min, 3-4min, 5-6min

   _____

9. Do you think it takes longer to login with a graphical password scheme as opposed to a text based password scheme?

   _____

10. How long do you think it took you to login with a graphical password scheme? 1-2min, 3-4min, 5-6min

    _____

11. How long do you think it took you to login with a text password scheme? 1-2min, 3-4min, 5-6min

    _____

Text-based passwords

1. How many times did you have to reset your text passwords?

   _____

2. Did you make any mistakes entering your text passwords and if so how many?

   _____

3. How secure do you think your text password is?

INFORMED CONSENT FORM

Graphical Authentication for Secure Social Networks

Investigators:	Dorothy Mhlanga	mhldor003@myuct.ac.za	0790511129
	Lebogang Mametja	mmtleb002@myuct.ac.za	0769989404
Supervisor:	Dr. Anne Kayem	akayem@cs.uct.ac.za	0216502664

You are being invited to take part in a research study. Before you decide to participate in this study, it is important that you understand why the research is being done and what it will involve. Please take the time to read the following information carefully. Please ask the researchers if there is anything that is not clear of if you need more information.

Purpose of the Research

This study is designed to compare two graphical password schemes to each other and to text-based password schemes to evaluate usability, and robustness to guessing and capture attacks. All testing will be done on a prototype social networking platform called HackMi2 (http://hackmi2.cs.uct.ac.za/).

Description of Subject Involvement

The study will consist of a two-hour lab session and a four-week online study. If you agree to be part of the study, we will ask you to take part in tasks that include:

1. Answering questions about your current strategies when using text passwords, and about your experience and preferences on your use of graphical passwords (lab)
2. Participating in activities that will test the system for robustness against attacks (lab)
3. Logging onto the social networking site three-five times a week for four weeks (online)

Risks and Discomforts

Potential risks or discomforts include feeling frustrated from forgetting your password.

Confidentiality and Anonymity

We will make every effort to protect your privacy. We will not use your name or any other identifying details in any of the research reports. We plan to publish the results of this study, but will not include any information that would identify you. The results will be published in the form of a research paper and may be published in a professional journal or presented at professional meetings.

Compensation

You will be compensated with a small gift for your participation.

Withdrawal without Prejudice

Participation in this study is voluntary; refusal to participate will involve no penalty. You are free to withdraw consent and discontinue participation in this project at any time without prejudice or penalty. You are also free to refuse to answer any question we might ask you.

Ethics Approval

This study has been approved by the Faculty of Science Research Ethics Committee of the University of Cape Town. If you have questions about your rights as a research participant; or wish to obtain information, ask questions or discuss any concerns about this study with someone other than the researchers, please contact the Chair of the Faculty of Science Research Ethics Committee at 021 650 2786 or via email at richard.hill@uct.ac.za.

Consent

By signing this consent form, I confirm that I have read and understood the information and have had the opportunity to ask questions. I understand that my participation is voluntary and that I am free to withdraw at any time, without giving a reason and without cost. I voluntarily agree to take part in this study.

Name (please print)	**Signature**	**Date**