A STUDY OF GRAPHICAL ALTERNATIVES FOR USER AUTHENTICATION

MOHD ZALISHAM JALI

Ph.D. 2011

A STUDY OF GRAPHICAL ALTERNATIVES FOR USER AUTHENTICATION

by

MOHD ZALISHAM JALI

A thesis submitted to the University of Plymouth
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing and Mathematics
Faculty of Science and Technology

July 2011

Abstract

A Study of Graphical Alternatives for User Authentication

MOHD ZALISHAM JALI (Dip, BSc, MSc)

Authenticating users by means of passwords is still the dominant form of authentication despite its recognised weaknesses. To solve this, authenticating users with images or pictures (i.e. graphical passwords) is proposed as one possible alternative as it is claimed that pictures are easy to remember, easy to use and has considerable security. Reviewing literature from the last twenty years found that few graphical password schemes have successfully been applied as the primary user authentication mechanism, with many studies reporting that their proposed scheme was better than their predecessors and they normally compared their scheme with the traditional password-based. In addition, opportunities for further research in areas such as image selection, image storage and retrieval, memorability (i.e. the user's ability to remember passwords), predictability, applicability to multiple platforms, as well as users' familiarity are still widely possible.

Motivated by the above findings and hoping to reduce the aforementioned issues, this thesis reports upon a series of graphical password studies by comparing existing methods, developing a novel alternative scheme, and introducing guidance for users before they start selecting their password. Specifically, two studies comparing graphical password methods were conducted with the specific aims to evaluate users' familiarity and perception towards graphical methods and to examine the performance of graphical methods in the web environment. To investigate the feasibility of combining two graphical methods, a novel graphical method known as EGAS (Enhanced Graphical Authentication System) was developed and tested in terms of its ease of use, ideal secret combination, ideal login strategies, effect of using smaller tolerances (i.e. areas where the click is still accepted) as well as users' familiarity. In addition, graphical password guidelines (GPG) were introduced and deployed within the EGAS prototype, in order to evaluate their potential to assist users in creating appropriate password choices.

From these studies, the thesis provides an alternative classification for graphical password methods by looking at the users' tasks when authenticating into the system; namely click-based, choice-based, draw-based and hybrid. Findings from comparative studies revealed that although a number of participants stated that they were aware of the existence of graphical passwords, they actually had little understanding of the methods involved. Moreover, the methods of selecting a series of images (i.e. choice-based) and clicking on the image (i.e. click-based) are actually possible to be used for web-based authentication due to both of them reporting complementary results. With respect to EGAS, the studies have shown that combining two graphical methods is possible and does not introduce negative effects upon the resulting usability. User familiarity with the EGAS software prototype was also improved as they used the software for periods of time, with improvement shown in login time, accuracy and login failures.

With the above findings, the research proposes that users' familiarity is one of the key elements in deploying any graphical method, and appropriate HCI guidelines should be considered and employed during development of the scheme. Additionally, employing the guidelines within the graphical method and not treating them as a separate entity in user authentication is also recommended. Other than that, elements such as reducing predictability, testing with multiple usage scenarios and platforms, as well as flexibility with respect to tolerance should be the focus for future research.

Contents

List of Appdendices

List of Tables

List of Figures

Acknowledgement

During the journey of this degree, I am truly indebted to the persons whom always giving me courage and supports as well as advice, comment and feedback.

This thesis is dedicated to Che Zamilah bt Daud, Jali bin Jusoh, Mohd Zalisman and Mohd Zalizmim.

I wish to acknowledge and gives thanks to my beloved wife, who scarifies her work life, who always be the first person of hearing my 'crazy' ideas, who always prepares countless coffee and tea and most importantly, gave us two princes; Ahmad Ukyle and Umar Yusuf during this PhD journey.

I would also like to express thanks and appreciation to my employer, Universiti Sains Islam Malaysia (USIM) and the government of Malaysia for sponsoring my studies. Without their financial support, I believe I unable to come, gain experience and finally completed the degree.

To all the participants, I wish all of you many thanks for your time, feedback, comment and suggestions.

Finally and always, I am truly grateful to my supervisors, Prof Steven Furnell and Assoc Prof Paul Dowland for their professional support and academic guidance. To all of you out there (you know who you are), thanks indeed for your endless support and advice.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee. This study was financed by the Higher Education of Malaysia, under the scheme known as Skim Latihan Akademik Bumiputra (SLAB) in collaboration with the Islamic Science University of Malaysia (USIM). Relevant seminars and conferences were regularly attended at which work was often presented and several papers were published and prepared for publication.

Word count of the main body of thesis (Chapters 1 to 7): 30, 141

Signed _____

Date _____

1. Introduction

1.1 Motivations

With more resources (i.e. information and services) are going online, the need for control and protection for users to access such resources are critical. It is anticipated that one of many steps to achieve such protection are known as authentication and authorisation. While the general role of authentication is to identify users' credential, authorisation on the other hand deals with controlling users' behaviour or right to access resources once they are authenticated.

This thesis studies alternative user authentication. Generally, user authentication can be explained as a process of proving who the user is to the resources. The identification of users is vital to enable right users using the right resources, as well as means for protection for both users and resources (i.e. ensure the safety of the resources).

While locks (i.e. padlocks) can be said as the most popular mean of protection for drawers, cabinets and cupboards; the use of username and passwords are still dominating and most convenient for assessing resources [150]. As time goes on, the usage of such technology is no longer suitable as literatures regarding password implementation and usage revealed that using long and complex combinations of passwords can cause problems with ease of use and memorability, and using simple passwords can result in a range of security problems (refer to Chapter Two for further details).

As the consequences, alternative technologies such as the use of token, biometric, cognitive passwords as well as using single sign-on and public key cryptography are gaining much attention to replace and overcoming problems in the password-based authentication. It is anticipated that each of these technologies has their own weaknesses and strengths. For example, using token could add the level of safety but in reality; carrying out token sometimes 'unpleasant' and losing them could make the

authentication more difficult. Similarly, although the use of biometric can be considered as the most secured way to authenticate, it is surely problematic if the database for storing biometric data is hacked or compromised.

Thus, observation was made to identify potential alternatives for password-based authentication, by which the use of images (known as 'graphical passwords') was found. Having identified the possibility of images as a potential alternative, the study started with a number of questions in mind, as explained below.

a) Why images are said to be better than words/phrases?
b) What is the status or state of the art of graphical passwords?

The above questions were answered by reviewing literatures. Search on literatures using the term 'picture superiority effect' and 'graphical password' had found many useful and significant studies related to advantages of pictures/images compared with words/phrases and state of graphical passwords to date. Having understood the state of graphical passwords and their role as the alternative user authentication, a number of other questions arose:

a) In graphical passwords studies, why are the proposed systems compared with password-based methods?
b) Are users really aware/familiar with graphical passwords methods or they just confused with the use of images in the password-based authentication?
c) Why there are so few graphical password schemes successfully implemented as the main method of user authentication?

d) Having identified the core problem pertaining to graphical passwords, is there any opportunity for further enhancement?

1.2 Aims of the research

Based upon the aforementioned research questions, the aims of the research are as follows:

1. To investigate the state of the art of authentication using images (i.e. graphical passwords),
2. To investigate the usability of available graphical methods,
3. To develop a novel method and then evaluate its suitability as an alternative user authentication method and
4. To examine the use of guidance for helping users to create secure graphical secrets.

1.3 Methodology

The study tackled the aforementioned aims by implementing three approaches. The first approach was making two comparative evaluations towards graphical methods. The first study compared three major graphical schemes, with the objective of obtaining users' familiarity of graphical methods and their perception towards security and usability. The second study compared two graphical methods with the objective of evaluating the practicality of both methods in a web environment.

The second approach was to develop a novel alternative graphical method, which balanced the strength and weaknesses of methods based upon clicking on an image and selecting a series of images. Evaluations were made with the specific objectives of identifying usability problems, users' familiarity, ideal combination of click and image and the effect of using a smaller tolerance during clicking. With

the aim of reducing users' insecure behaviour when creating their graphical passwords, the third approach was to implement a set of graphical guidelines. These guidelines were deployed within the enhanced method and displayed to users before they started to select their secrets. An evaluation was made with an objective of assessing its feasibility during password creation. Figure 1-1 illustratively summarises the three approaches in an attempt to achieve the aforementioned aims and objectives.

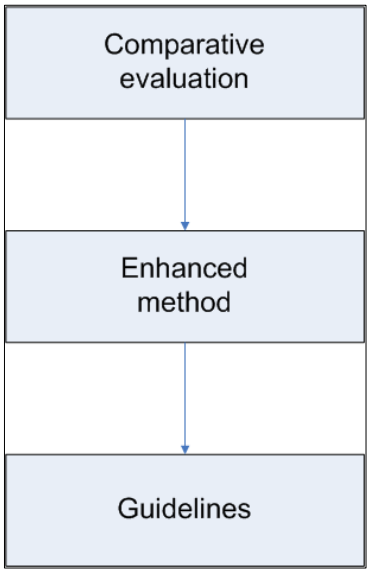

Figure 1-1 : Research approach

For each study, graphical software prototypes that were similar to the original graphical schemes were developed, and tested by participants. A mixture of internal[1] and external[2] usability studies was implemented in order to achieve the aims and objectives for each evaluation. Since one-to-one usability study was chosen to be the main research method for obtaining data, the majority of the participants were drawn from the university staff (e.g. students, lecturers, administrators), who were obtained through an open call for volunteers.

[1] Controlled usability study (i.e. participants needed to complete current task before proceed to the next)
[2] Independent usability study (i.e. participants were asked to use the software prototype and all of their interaction activities were recorded within the software prototype)

To assess the long-term ease of use of the enhanced method, additional participants were recruited by the author. Due to the criteria used for usability performance, participants were only tested with their short term recall and recognition.

Unless otherwise stated, the usability performance studies used within the thesis were based on five main elements; namely number of attempts, accuracy, pattern, timing and users' feedback. The number of attempts looks at participants' failure and success rates during both registration and login tasks while timing reports the time needed for these tasks. Pattern discusses the occurrences of pattern, with accuracy mainly focussing on the participants' ability to click on their secret and finally users' feedback reports participants' perception of the approach. Figure 1-2 illustratively summarises the methodology applied throughout all studies within the thesis; starting from the literature search up to the analysis and reporting of each study.

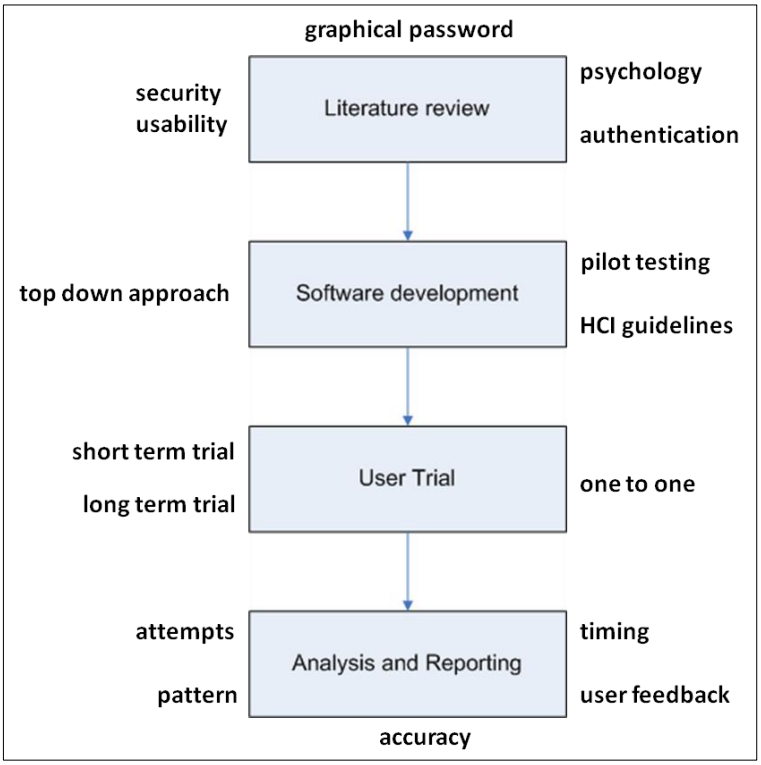

Figure 1-2 : Research methodology

1.4 Research output

The list below presents the research output and a copy of each publication is attached in Appendix E.

a) Jali, M. Z., Furnell, S., Dowland, P. & Reid, F. (2008) 'A survey of user opinions and preference towards graphical authentications', in Bleimann, U.G., Dowland, P., Furnell, S. and Grout, V. (eds.). *Proceedings of the Fourth Collaborative Research Symposium on Security, E-Learning, Internet and Networking (SEIN 2008)*. Wrexham, UK 5-8 November 2008. University of Plymouth, pp. 11-20.

b) Jali, M. Z., Furnell, S. & Dowland, P. (2009) 'Evaluating web-based user authentication using graphical techniques', in Furnell, S. and Clarke, N. (eds.). *Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance (HAISA 2009)*. Athens, Greece 25-26 June 2009. University of Plymouth, pp. 108-118.

c) Jali, M. Z., Furnell, S. M. & Dowland, P. S. (2010) 'Assessing image-based authentication techniques in a web-based environment'. *Information Management & Computer Security*, 18 (1). pp 43-53.

d) Jali, M. Z., Furnell, S. M. & Dowland, P. S. (2011) 'Quantifying the effect of graphical password guidelines for better security'. *Future Challenges in Security and Privacy for Academia and Industry (SEC 2011)*, Lucerne, Switzerland, 7-9 June 2011.

1.5 Research contributions

The lists below identify contributions made from the conduct of all studies within the thesis.

a) Alternative classifications of graphical schemes based upon the authentication process from a user perspective are described and reviewed.
b) Comparative evaluations which provide the basis for comparing graphical methods are discussed and explained.
c) Combinations of graphical methods are possible and do not impact on user performance.
d) Graphical Password Guidelines (GPG) for helping users before they start choosing their secrets are introduced and evaluated.
e) Usability performance measures (e.g. number of attempts, timing, pattern, accuracy and users' feedback) are useful for evaluating usability criteria within the scope of authentication using images, as well as within the scope of knowledge-based authentication.
f) Conducting comparative evaluation, developing enhanced method and introducing guidelines are identified as complementary to current authentication using images.

1.6 Thesis structure

Chapter 2 discusses the basic principles pertaining to user authentication with particular attention to knowledge-based authentication (or 'what the user knows'). The popularity of password-based authentication is highlighted, studies related to password-based security are reviewed with the aim of identifying password problems, and finally methods for strengthening passwords and alternative knowledge-based authentication approaches are discussed.

Chapter 3 reviews the development of authentication using images or graphical passwords. Alternative classifications based upon user actions when authenticating are presented, with other studies, issues and opportunities related to authentication using images are discussed.

Chapter 4 presents the comparative evaluations studying user familiarity using three graphical methods and their perception towards usability and security issues, and then later presenting the second comparative study evaluating two graphical methods and their effectiveness to be used as a method of web-based authentication.

The initial design and implementation of a new method, the Enhanced Graphical Authentication System (EGAS), is reported in Chapter 5. Evaluation of EGAS, with particular attention to identifying the usability and suitability of login authentication based upon four proposed scenarios, are the main focus of this chapter. Chapter 6 then reports upon an improved design and implementation of EGAS. This chapter also presents the results of an assessment of the feasibility of introducing guidelines to users as well as user familiarity, the optimal combination of click and image and the effect of using smaller tolerance are discussed and reported.

Chapter 7 summarises all findings from the studies reported within the thesis and finally acknowledges the weaknesses and limitations of the studies, along with the potential for future research.

2. A Review of User Authentication Technologies

2.1 Authentication

There is a considerable variety of user authentication techniques available although the username/password combination is still the most widely used method. O' Gorman [148] explained user authentication methods into something the user knows (knowledge-based), something the user has (possession-based) and something the user is (biometric-based). For the knowledge-based approach, users have something that they must remember; this is usually a pin or password. For possession-based methods, users have some form of device (e.g. smart cards or 'USB' devices) and for biometric-based methods, users commonly have to use a physiological characteristic (e.g. their face, finger, thumb, iris etc.) in order to be authenticated.

The thesis mainly discusses knowledge-based authentication method, with some consideration of the other methods. Specifically, this chapter highlights past and present studies related to the usage of passwords, with the ultimate aim to seek for contributors in password problems.

2.2 Security and Usability (i.e. Usable Security)

Security and usability are two different research domains with each having their own purpose and functionality. While usability is to ensure the ease-of-use of the products [1, 2], security on the other hand deals with the safety of the products or services. With respect to user authentication methods, it is obvious that both have a vital role. This is because if the authentication methods are designed with a high level of security at the expense of usability, it can be just as unusable as one designed with usability in mind but without appropriate security measures.

Karat et al. [3] outlined four main reasons why designing usable security products were difficult to achieve. First, it was anticipated that the risk for security was relatively high compared to the risk of

usability. Second, usability was not the major design objective compared with security. Third, many of the security applications were developed by highly trained and well-skilled technical users while the end-users were those who have various levels of knowledge. As a result, advanced features were not used because of a lack of understanding. Fourth, was with regard to changes to the policy, rules, regulations and requirements of the organization, which sometimes made the design for usability difficult.

Both security and usability need to be considered when designing security products, however it is difficult to achieve both. The ideal trade off is to design products that have level of security and to still be usable for a wide range of users. It has been reported that research on usable security has starting to attract interest from many security researchers and obvious example of works can be found in the book edited by Cranor and Garfinkel, [4]. This thesis gives more focus upon usability (i.e. with consideration on security in mind) as it is anticipated that design with usability is better than design with security

2.3 Password-based Authentication

This section explains the reasons for the popularity of password-based authentication, reviews a number of password security studies with the aim of identifying key problems and finally gives a number of solutions for strengthening the method.

2.3.1 Password popularity

The use of passwords is the most commonly used form of user authentication. Using passwords as the mean for authentication requires no additional hardware and can be easily deployed as well as being quick to use. In addition, passwords are familiar to the user since most computers are equipped with a

keyboard (in contrast with techniques requiring dedicated resources – e.g. fingerprint sensor, camera etc.).

2.3.2 Password problems

The following section highlights a collection of studies reviewing the issues related to password security.

Among the earliest attempts to investigate password vulnerability was the study by Morris and Thompson, in 1979 [5]. They implemented a dictionary search and character string searches to guess users passwords. The former took less time compared with the latter approach and managed to guess one third of users' password. With the character string search method, it was found that out of 3289 passwords with no constraints during password creation, 86% were less than six characters long and found in dictionaries or name lists.

Klien [6] conducted an experiment to crack UNIX users' passwords and reported that he managed to crack up to 25% of users' passwords from a total set of 13,797 accounts. Klein suggested that users should change their passwords periodically, add more constrains to the password itself (i.e. combining both numeric and special characters) and that a password based system should use a password checker. Over a three years period, Bishop and Klien [7] later reported that they were able to crack approximately 40% of users' passwords. They also proposed a Protective Password Checker (PPC). PPC checks every character inserted by users whilst typing their password and determines the appropriateness of it based upon the password creation rules setup within the system.

Spafford [8] discussed four criteria for making users' passwords secure. These were through users' education, system-generated passwords assigned to users, scanning users' passwords periodically and finally discarding users' weak passwords during registration; with each of the criteria having their own strengths and weaknesses. From the collected 13,787 users' passwords, it was reported that the average length of users' password was 6.8 characters. Comparing the collected passwords with various dictionaries, it was reported that 20% of users' passwords were found.

Identifying human and organisational factor that contributed to the security and usability of password-based authentication system were studied by Adams et al., [9]. Two studies were implemented, combining an online questionnaire (139 respondents) and later a semi-structured interview (30 users). They reported that users had to remember many passwords (averagely four), which resulted in reduced memorability, users writing down their passwords and using easy to guess passwords. Users had also shown limited awareness about security as they misunderstood the level of information sensitivity within their organisation and had not given serious attention towards security. The authors claimed that users insecure practices were actually influenced from the employed security mechanism (i.e. both implementation and design), not on the user itself.

Cartens et al. [10] conducted a survey and evaluated the human impact of password practices. They asked participants the type of password each participant had, total number of password they needed to remember and frequency of forgetting their passwords. From the collected data, they summarised that users' memorability (ability to recall their password correctly) was reduced over time and the amount of time they spent at work had a direct influence with their memorability capabilities where they unable to apply using different passwords for different sites and use easy to guess passwords.

Schneier [11] analysed MySpace[3] users' passwords and found nearly 65% of the users' passwords were 8 characters long or less. He also reported that some users had passwords that were more than nine characters long, but these passwords were easy to predict. 81% of users' passwords were combination of letters and numbers, with only 1.3% and 9.6% of users' passwords formed using number only and letters only respectively. Although not worrying, users still formed simple and easy to guess password as the author revealed the top 20 common passwords included 'password1' and 'abc123'. However, one positive finding with his analysis was that less than 4% of users' passwords were found in the dictionary.

Singh et al. [12] investigated PIN sharing (in a banking context). One of many password guidelines which says 'password should not or never be shared to anyone' were violated as it was found sharing of pin between couples (e.g. spouse, partner) and between people of certain disability with their carers or retail clerk were common practices.

Florencio and Herley [13] investigated users' password habits on the web. With nearly half a million users monitored over a three month period, they revealed that users have an average password length of 6.5 characters (i.e. the same across 3.9 different sites). The study also revealed that users have, on average, 25 accounts that require a password, requiring an average of 8 passwords to be entered per day. They also reported that users often forgot their passwords and would use less secure passwords unless they were specifically asked not to do so.

Zhang et al. [14] investigated the impact of having multiple passwords. Participants in their study (grouped into conditions named 'first letter', 'password rule' and 'control rule') had to create four unique passwords associated to four different accounts and needed to log back into each of their account after 7 days. From the collected data, the authors concluded the major reason for recall error was due to

[3] http://www.myspace.com

the interference (i.e. not using right password on the right account), with other minor reasons including number requirement errors (i.e. omitting or adding number or special characters), case errors (i.e. not using uppercase or lowercase rightly) and errors caused by forgetting the password itself.

Hoonakker et al. [15] examined end-users' password practices by using a combination of structured interview and web-based survey methods. They started their study by interviewing a number of people over the phone and from results of the focus group, the authors then conducted a web-based survey by questioning employees of a large organisation. With a total of 836 respondents, the authors claim that the human is 'the weakest link' as they found participants use the same password all the time, use simple passwords, re-use their old passwords regularly, write down their passwords (either on paper or electronically without any protection) and shared their passwords with others.

Bonneau and Preibusch [16] investigated password implementations of 150 websites. They reported many of the surveyed websites still did not encrypt users' password during transmission, store users' passwords in plain text and provide little or no protection towards brute-force attack. By first investigating users' password for lower security site and then, comparing with their high-security site, the authors managed to prove that users use similar or reuse their passwords across many accounts.

Inglesant and Sasse [17] investigated the problems faced by users to cope with password policies setup in their organisation and the ways they coped with it. Using a diary study (participants needed to record their action when logging into their account) and a debrief interview, the authors found that users rarely changed their passwords unless asked to do so, users had problem to create new passwords which comply with their organisation's policy and as the result, users tended to forget their password and wrote it down. The authors suggested that policies should be designed based upon HCI principles in order to assist users for better password creation.

With the advances in technologies, the username and password authentication is somewhat vulnerable to various means such as dictionary attacks, spyware (programs that are illegitimately installed in the user's computer and as a result, take control of certain tasks), shoulder surfing and even social engineering. As a result of these vulnerabilities, a range of guidelines have been suggested with the most cited guideline from the US Department of Defence, [143], with the other guidelines can be found in [142, 144].

Briefly, users are advised to change their passwords regularly (e.g. once a week, twice a week or even once a day). However, because it is often hard for them to remember all of their passwords, they tend to use the same passwords for many services or applications. On top of that, users are encouraged to use different passwords for different applications or services. As a result of using different passwords for different services, they tend to use simple, short and memorable ones, as they claimed it was easy for them to remember.

Users are also advised to increase the complexity of their passwords by combining numbers, text and special characters and using at least eight characters when creating their passwords. An example of these include "I_qw1(**)-", "Manchester_**&Nadn##1" and "kjknsa&ah3anz))". These passwords are no doubt secure because they are not in the dictionary. However, such passwords could result in problems of memorability and usability. As a result, users tend to write their passwords somewhere so that they could access it or in the case of forgotten.

Of all the studies explained in this section, it can be suggested that the problems associated with password security could be caused by three key-players; namely the ***user***, ***organisation*** and ***developer***. Figure 2-1 illustrates the relationship between these three entities and their contributions to the password security problem. The main contributor is users as they reuse their passwords, share with others, writing down and create easy to guess passwords. In addition, the organisation could contribute to the password problem as they create 'hard to follow' standard and policy such as frequency of password changing and

the passwords themselves. Finally, the developer could also contribute to the password problem if they practice poor design (e.g. poor user interface and poor data storage) during development of the authentication applications.

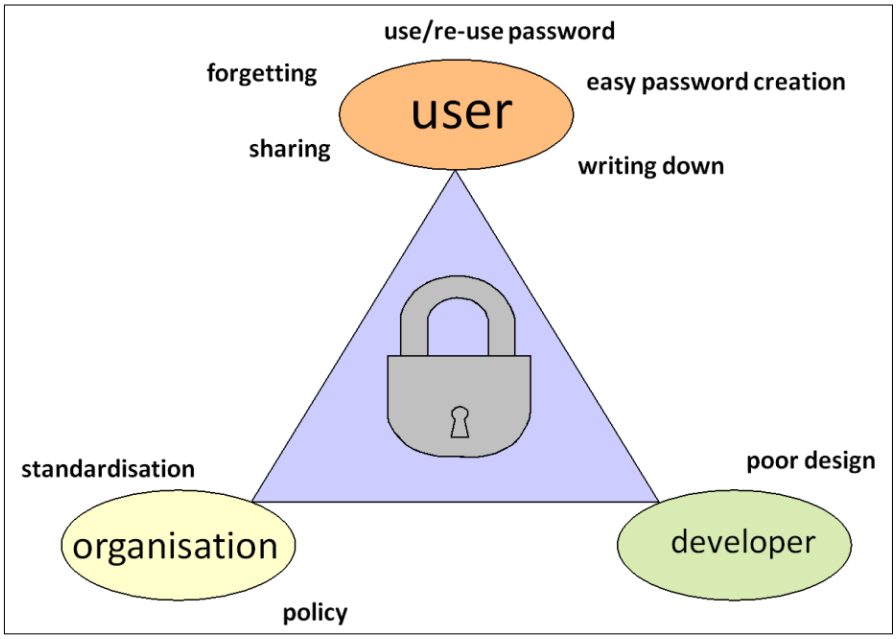

Figure 2-1: Password problem contributors.

2.3.3 Strengthening password-based authentication

The following section provides examples of strengthening password-based authentication and reducing users' load from memorising and recalling long and complex passwords.

Federated identity or similarly **Open ID** is a mechanism for users to authenticate using a single digital identity in order to use websites or applications in the web[4]. By using an open ID, users do not need to remember many username and passwords. For example, if user A already has an account with Google (e.g. Google ID and password), they can use the same Google ID and password to login to other

[4] http://en.wikipedia.org/wiki/Federated_identity

websites or web applications, provided that those particular websites or web applications participate in this scheme. In addition, **Single Sign-On** (SSO) is a scheme that requires users to only log into services once (by using an SSO identity) and automatically allow to use or login to other services without further authentication. SSO claimed could reduce the hassle of inserting the same credential for same identity and could reduce the problem of having multiple passwords. Examples of SSO technology include Kerberos[5], Microsoft passport[6] and Liberty Alliance[7].

System generated passwords were introduced to address the problem of weak passwords created by users. Upon registration, the user is assigned a random password generated by the systems or services. Another method is known as the **One Time Password** (OTP). The idea behind OTP is that passwords created by users are seeded (e.g. hash functions or mathematical formulas) to generate another passwords; which is better and computationally infeasible to crack. Normally, OTP is combined with other methods to create multi-factor authentication, which is more secure and robust.

Another user-centric approach is to use a **mnemonic** passphrase. Using this approach, users are advised to create their passwords by remembering sequences of phrases that they are familiar with. For example, the user could create their password 'IlMUfcaOTs' where each character is derived from the first letter of the phrase 'I love Manchester United football club and Old Trafford stadium'.

The mnemonic approach has attracted much interest from authentication researchers, with conflicting results. Yan et al. [18] conducted a study to evaluate the memorability and security of normal passwords, mnemonic passwords and random passwords. Overall, they found the mnemonic passwords were much stronger and memorable than normal passwords and as strong as the random passwords. Kuo et al. [19] conducted an online survey to investigate the mnemonics phrase-based passwords chosen by users. They

[5] http://www.kerberos.org
[6] http://www.passport.net
[7] http://www.projectliberty.org

found that the majority of users created their passwords from music lyrics, movies, literature and television shows, which could be vulnerable if password cracking dictionaries were developed based upon these. Keith et al. [20] conducted an empirical study investigating users' experience and satisfactions with regards to passphrases. Overall they concluded that users with passphrases experienced higher unsuccessful login errors due to memory recall failure, had more failed login attempts due to typographical errors and rated the passphrases method less favourably compared to the conventional password.

2.4 Alternatives to Password-based Authentication

One possible alternative to password-based authentication is the approach known as the **challenge-response approach**. This means users have to verify their identity by supplying secrets which only the user knows. Two common types are 'cognitive' and 'associative'. In the cognitive-type technique, the two most common types of questions used are fact-based and opinion-based. Normally, these questions are related to human daily life and experiences. Examples of the questions (adapted from [21]) are as follows:

a) What is your mother maiden name? (fact-based)
b) What is your telephone number? (fact-based)
c) What is your favourite dessert? (opinion-based)
d) What is your favourite colour? (opinion-based)

In the associative-based technique, users have to answer the associative pair of the given phrases. With this technique there are no right or wrong answers since different users might have different answers or opinions. Examples of questions are as follows:

a) Blue (common associative are sky, sea and Chelsea FC)

b) Red (common associative are traffic light, Man United, Liverpool and cherry)

c) House (common associative are bungalow, double-storeys and terrace)

d) Library (common associative are books, music and old transcripts)

Zhivan and Haga [22] studied the level of users' recall rate by testing and comparing the challenge-response authentication with three other conventional passwords; namely self-generated, system-generated and self-generated passphrases. They reported the cognitive-based password was 74% accurately matched when recalled meanwhile the associative-based password yielded 69%. Burnell et al. [21] carried out a study to test users' recall rates and guessability (i.e. ability to be guessed by an impostor). They reported that conventional passwords had relatively high recall rates and low guessability. The cognitive-based password yielded high recall rates and high guessability, with the associative-based password low for both guessability and recall.

Another variation with the challenge-response method is the **preference-based approach**, particularly developed for the case of password reset. In the scheme by Jakobsson et al. [23], users are prompted with 6 categories to choose from and for each category, 14 items are randomly displayed to them. From all of the listed items in all of the categories, users need to choose and rank 8 items which they 'like' and 8 items in which they 'dislike'. In the event of password reset, users are prompted with a series of their chosen lists and all they have to do is to answer either 'like' or 'dislike' for each of the displayed items.

Using **images** is also proposed as a possible alternative to strengthen the passwords. To date, images are used to assist users to recall their passwords and as the cue for identifying the authenticity of web sites and users (e.g. Yahoo Mail and Facebook[8]). In addition, having an image as part of the password has

[8] http://www.facebook.com

also been implemented (e.g. Alliance Online Banking[9], see Figure 2-2) and there are online authentication systems using images where users need to click on image-style keyboards in order to reduce the threat of keylogging. (i.e. Citibank online banking[10], see Figure 2-3 and ING Direct[11]).

Two factor authentications (T-FA) could be described as a scheme where users have to go through two types of authentication methods. For example, users need to insert their password and later on they have to scan their eyes. By using T-FA, it could tighten the level of security since it combine two different authentication methods. Examples of two factor authentication are combining card with pin (e.g. withdrawing money from the ATM), combining password with token (e.g. online banking) and combining pin with the biometric (e.g. entering secure building).

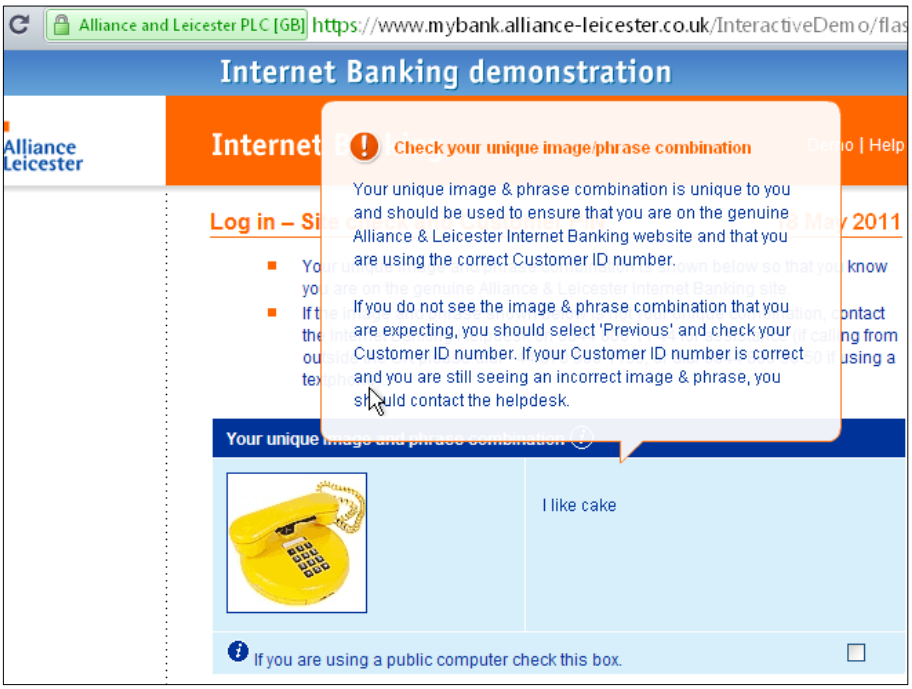

Figure 2-2: Alliance and Leicester online banking

[9] https://www.mybank.alliance-leicester.co.uk/InteractiveDemo/flashdemo/D2a.htm
[10] http://www.citibank.com.my
[11] https://secure.ingdirect.co.uk/InitialINGDirect.html

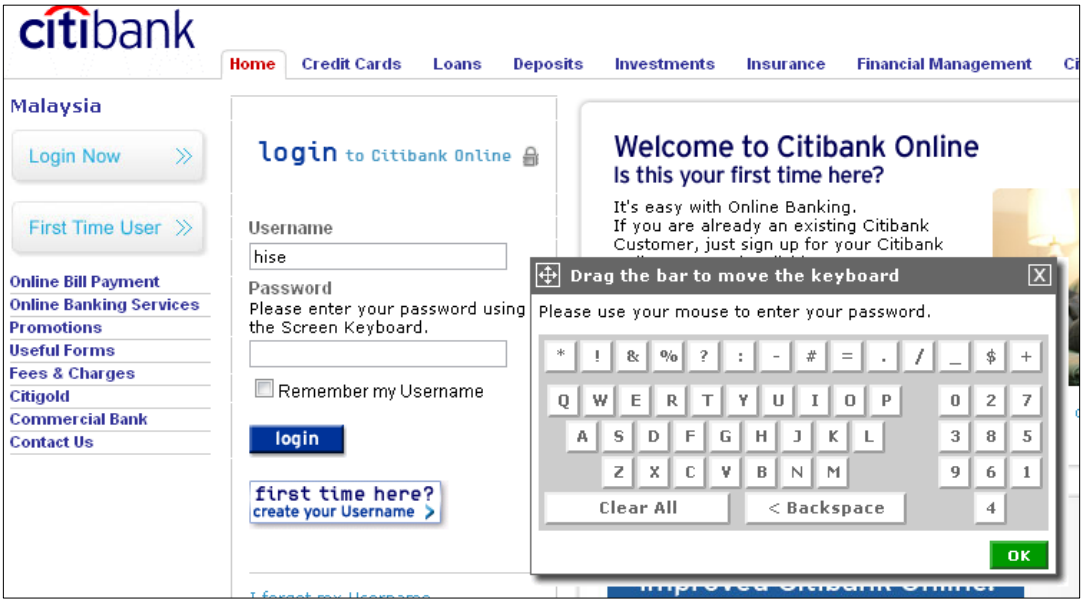

Figure 2-3: Citibank online banking authentication challenge

Another variation is using **biometric**. Biometric in user authentication could be explained as the process of verifying user's identity by means of psychological or behavioral characters. The psychological characters refer to the physical attributes such as fingerprint, face, iris and body shape while the behavioral characters refer to the users' actions such as the way they speaking, typing or drawing. The biometric processes begin when users' characteristics are captured into the system. Normally, these data will go through to the process known as the data extraction phase where only relevant samples will be stored into the designated database. During login, users once again have to supply their characters and these characters will be compared with the existing one in the database. If the patterns match, user will be allowed to enter the system but otherwise, he has to do it again.

Normal issues or problems associated with this scheme are FAR (False Acceptance Rate) and FRR (False Rejection Rate). FAR refers to the condition where impostors are falsely accepted by the system whereas FRR refers to the condition where the registered users rejected by the system. Biometric authentication could potentially be used in the applications like verifying users' identity for passports and airport check-in, entry to secure buildings such as government and private buildings and also verifying identity of nationality.

Other approaches for strengthening password-based authentication include improving the **design of user interface** for user authentication applications [24], **limiting the use of popular passwords** chosen by users [25] and using a **persuasive approach** to assist users to create better passwords [26, 27].

2.5 Conclusions

This chapter reviewed user authentication, with particular focus on the password-based authentication. The popularity of using passwords, studies related to password security, ways to strengthen the method as well as alternatives to password authentication were briefly discussed and reviewed.

Previous studies with password security have focused upon the strength of the password by examining how passwords were formed or created, the length of the password itself and how breakable (i.e. ability to be cracked/guessed) the password itself is with the available known vulnerabilities such as keylogging[12], malware[13], as well as social engineering[14] and shoulder surfing[15]. Then, the focus has changed where studies on examining effect and impact of having password were conducted and investigated. Overall, it can be concluded that the problem of password security have prevailed for many years and despite their shortcomings are still the most common and preferred method of authentication.

Having understood the major principles of user authentication methods, problems pertaining to the predominant password-based method, and the opportunities for alternative user authentication, this thesis proceeds to investigate graphical techniques as an alternative for user authentication. The graphical techniques (i.e. user authentication using images) were chosen as the main interest since they have

[12] A computer program to record users' typing pattern (keystroke)
[13] Malicious program which used to obtain users' passwords and damage computer systems
[14] Act of manipulating people in order to reveal their passwords/secrets.
[15] Looking over to someone shoulder/ recording in order to obtain information (i.e. passwords)

demonstrated that they can be used as a possible alternative for the current username/password technique. This is due to the nature of the technique that needs no additional hardware (i.e. can be deployed straight away). More importantly, as the technique uses images/pictures, it could address the problem of memorability in the username/password method. Studies have shown that users were better at recognising and memorising images than remembering long and complex words/phrases [28-35]. In addition, the graphical technique was chosen as it was an interesting research area which can be combined with other sciences (e.g. computer vision, computer graphics, Human Computer Interface (HCI)) and psychology research areas (e.g. memory, vision, human aspects). The details of graphical techniques highlighting their history, trends, issues and opportunities are explained in the next chapter.

3. Graphical Authentication Approaches

3.1 Introduction

Before explaining the current state of graphical techniques as one of the possible alternatives for user authentication, numbers of psychological studies explaining the 'picture superiority effects' towards words and verbal are presented in the next paragraphs.

Shepard [151] conducted a study to examine the level of recognition for pictures. He used 600 pictures where each of them was displayed for a few seconds to the participants. Later on, participants were asked to recognise and determine whether the displayed images were original (images that on the list during initial experiment) or fake (images that not on the list during initial experiment). Overall, it was reported that participants managed to recognise 98% of the images.

In 1968, Nickerson [152] conducted a study to determine the effect of long term recognition memory towards pictorial materials. In his study, a total of 200 images were used in which each of the images was displayed for 5 seconds. During the test, participants had to determine the displayed images either 'old' (displayed to them during the first task) or 'new' (only displayed to them during the test). The testing were implemented in four phases; namely day 1, day 7, day 28 and day 360. Overall, the results showed that the probability of success rate decreased from day 1 up until to the day 360. However, considering the factors such as time (up to a year) and the way the experiment was conducted, they concluded that the long term recognition memory for pictorial images were still better than words.

Standings et al., [153] conducted 4 experiments to examine the relationship between perception and memory. The first two experiments were about memory recognition for pictures. Experiment 1 used 1100 pictures taken from the magazines, with Experiment 2 used 2560 pictures obtained from the photographers (both amateur and professional). Overall, they found that participants scored up to 95% success for Experiment 1 and for Experiment 2, participants still scored 85% recognition success even after 4 days time. The last two experiments were about the effect of duration and the effect of reversing

and orienting the pictures during viewing. From the results, it were summarized that participants still managed to score above 90% success rate even the images were reversed. However, with regard to the image orientation, participants scored slightly low (average of 55%). On the whole, they concluded that participants managed to obtain higher success rate for picture recognition.

In 1973, Standings [154] investigated the memory capacity and retrieval speed for both pictures and words. There were a total of 4 experiments conducted and he summarised that for both memory capacity and retrieval speed, using pictures were still superior to the words or verbal. This proven when using larger set of images (he used up to 1000 images), changing the method of recognition (images were displayed sequentially rather than simultaneously) and finally different forms of testing (using visual words, normal picture and auditory words), participants still performed significantly well.

The above psychological studies have given an insight to the claim that using images/pictures were superior to using words, with regard to recognising and memorizing. With respect to using images during authentication, the first clearly distinguishable graphical authentication approach (GA) was proposed in 1991 by King [36] who discussed the rebus password. Rebus means using association of pictures in order to aid users remembering a sequence of nonsense passwords[16].

The next section highlights GA schemes based upon four categorisations, followed by other GA studies from the collected literature. Issues relating to GA and opportunities for future studies are reviewed later, with concluding remarks given in the last section of this chapter. Alternative information relating to GA can be found in [37-40].

[16] http://oxforddictionaries.com/definition/rebus

3.2 Graphical authentication schemes

Based upon user memory tasks, GA can normally be classified into two; namely recognition-based and recall-based, with a further classification of cued-recall sitting between the two. Looking upon users' action when they authenticate into the system, this thesis classifies GA into four main categories; namely ***click-based***, ***choice-based***, ***draw-based*** and ***hybrid***. Click-based requires users to click anywhere they prefer in a given image. These secret click points are the users' 'password'. The choice-based approach requires users to select their chosen images from a set of decoy images. The image selection can be continued for several rounds depending on the system settings, while the draw-based method requires users to draw their secret on the provided grid/screen. In this case, the drawing is interpreted as the password in order to be authenticated. The graphical schemes are grouped into hybrid-based method if they combined at least two of the aforementioned categories.

Figures 3-1 to 3-3 illustrate three main methods of authentication using images, with an example of secret created/chosen/drawn from the user is given. Within this section, a graphical scheme within their classification is introduced and if exist, their enhancement studies are reviewed and explained.

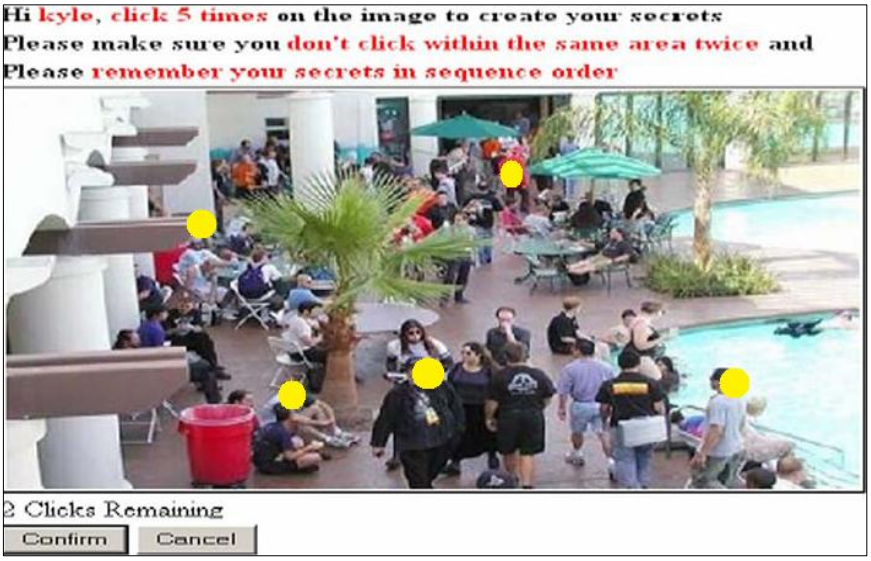

Figure 3-1: Example of the click-based graphical method

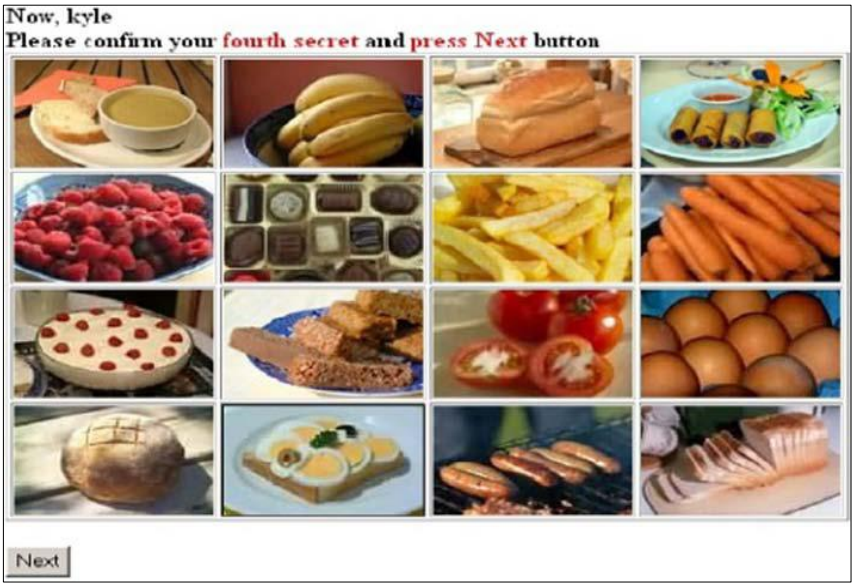

Figure 3-2: Example of the choice-based graphical method

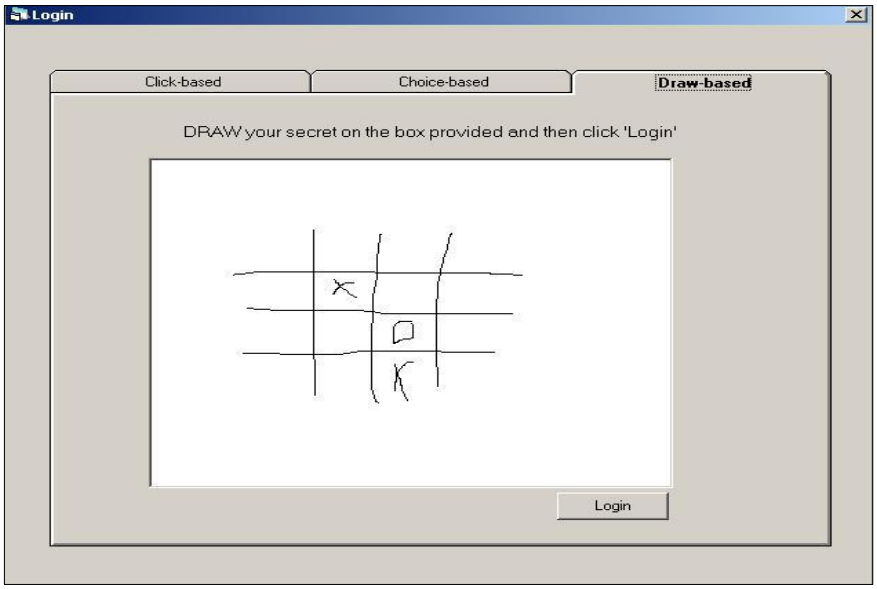

Figure 3-3: Example of the draw-based graphical method

3.2.1 Click-based Schemes

Blonder [41] patented one graphical password scheme. In the scheme, users click or tap on the predetermined areas of the given image. The predetermined areas in this case mean that the passwords are already defined within the system (see Figure 3-4). Since users could only click or tap on the predetermined areas, it is anticipated that the passwords are uncomplicated for attackers to crack/guess.

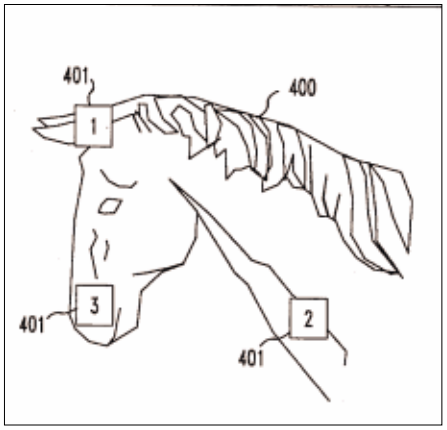

Figure 3-4:Example of image in Blonder's graphical scheme

To overcome the problem in [41], Wiedenbeck et al. [43] introduced Passpoint in which users can choose any image they prefer and the system does not need any predefined click-region or well-marked boundaries. A prototype of Passpoint (see Figure 3-5) was developed and compared with conventional alphanumeric passwords to evaluate their effectiveness (i.e. memorisation) and efficiency (i.e. error rate). From the results of 40 participants, it was reported that the alphanumeric group produced fewer mistakes compared with the graphical group, with the graphical group having problems entering their password correctly and remembering the sequence of click points. However, during the login phase, the graphical group made fewer mistakes and they could enter their password correctly.

Wiedenbeck et al. [44] investigated the effect of tolerance (i.e. areas the click is still accepted) and image choice with their Passpoint system. Two tolerances were tested; namely 10x10 pixels and 14x14 pixels. From the results, it was found that the majority of the participants had problems authenticating when a smaller tolerance was used (i.e. 10x10 pixels). For the image choice study, four types of images were used ; namely an image of people walking around a swimming pool in a hotel, an image of children painting a mural, an image of a map of Philadelphia and an image of teapots. From the total of 83 participants participated, they reported no significant difference obtained from these images.

Figure 3-5: Passpoint scheme

Chiasson et al. [45] conducted an empirical (controlled lab) study of Passpoint where 43 participants were asked to test 17 different images (including 4 images from the original Passpoint study). From the results, they reported the success rates were high, the timing were reasonable and participants had favourable opinions towards the scheme. They also stated that the choice of images had an impact on user performance where participants performed extremely well with the image size of 19x19 pixels. In the long-term study, two different images were used (i.e. pool and cars) with two different tolerances (i.e. 13x13 pixels and 19x19 pixels) settings. They reported that the Passpoint was practically usable, participants had problem when they had to remember more than one graphical passwords and the security of Passpoint was questionable due to the secrets (i.e. passwords) created by participants.

Another graphical scheme within this method is named Jiminy, by Renaud and De Angeli [42]. Jiminy is a paper-based mechanism designed originally to be a tool for recording a password but later on, extended to be used as web authentication. Evaluation of Jiminy found that users had difficulty to pin-point particular positions in the given image, with the hypothesis that image of map should perform better (i.e. in terms of memorability and predictability) as compared with image of room was rejected. During the thesis is written, no other study is found with respect to Jiminy scheme.

3.2.2 Choice-based Schemes

The most common choice-based method is Passfaces [46]. In this scheme, users need to choose from images of faces in order to be authenticated. The process of choosing faces is repeated for several rounds to ensure the password space is large enough. In laboratory studies carried out by Valentine [140, 141], it was reported that users of Passfaces were able to remember their passwords better than users with conventional passwords. The Passfaces system was also investigated by Brostoff and Sasse [139]. They reported that Passfaces users took longer to login as compared with the password users, they did not like using Passfaces as the main login material and the level of remembrance (memorability) and recall were similar to those reported for conventional passwords.

Figure 3-6: Example of the Passfaces scheme used in [50]

Djamila & Perrig [47] introduced Dejavu (see Figure 3-7). Dejavu uses images from Andrej Bauer's random art algorithm, where strings are converted into the abstract images. When compared with conventional pins and passwords, they concluded Dejavu had advantages in terms of ease of use and that it was suitable to be used within an environment where text input was difficult or limited. It was also

reported that users found difficulty recognising their chosen images and the scheme itself was vulnerable to social engineering, shoulder surfing as well as intersection attack (i.e. occurs when users' real and decoy images are selected within the same set of image pool).

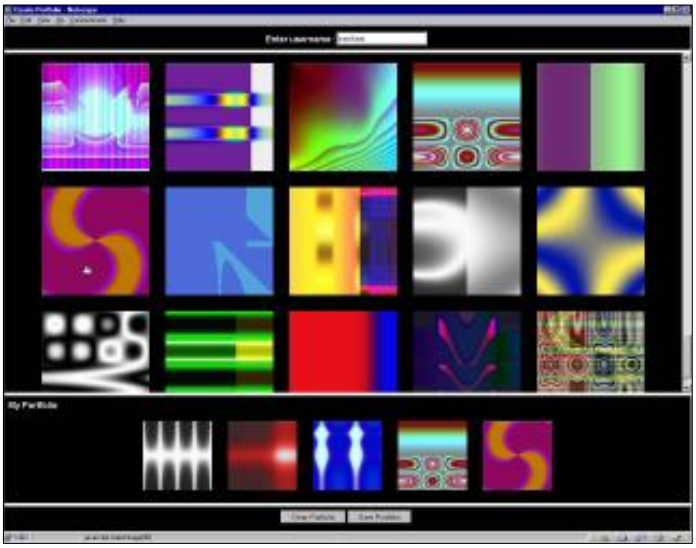

Figure 3-7: Dejavu graphical scheme

Man et al. [48] introduced WIW (name borrowed from the popular 'Where is Waldo'). The authors claimed that by using WIW, it is relatively difficult for attackers to see users' secrets, even with the aid of a hidden camera. Another scheme which claims to be resistant to shoulder surfer is in [49]. The scheme works as explained below:

a) To register, users choose their secret images (pass-image).
b) For each pass-image, the system will display the variations associated with it. For example, if users choose a **face** as their pass-images, the associated variations could be **sad**, **happy**, **angry** and **frown**.
c) Users give/enter meaningful words (pass-strings) for each of the displayed variations. The pass-string should be in the form of both numbers and letters and easy to recall.

d) To login, users need to find their pass-image and identify the type of its variation. Once found, they need to insert the pass-string associated with that variation.

Davis et al. [50] studied user choice of images. Two types of scheme used in their study were known as ‘Face’ (originated from Passfaces) and their own scheme called ‘Story’ (see Figure 3-8). The study reported that users preferred to choose faces that represented similarity with their own ethnicity, and that users tended to choose faces representing the opposite gender to them. The study suggested that the ‘Face’ scheme would be guessable if attackers know who the user was, especially his/her gender and ethnicity. As an alternative, the ‘Story’ scheme offered better security since user chosen images were random and not related to them.

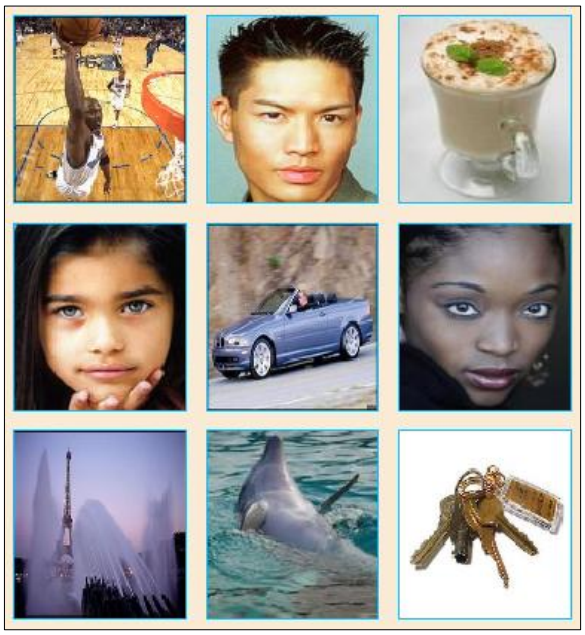

Figure 3-8: Story graphical scheme

Passimages by Charruau et al. [51] was developed to be used in a web-based environment. In order to be authenticated, users had to correctly choose six images from amongst a set of decoy images. They conducted a lab study to compare their scheme with the conventional password and reported that the

majority of the participants were able to login to their required website by using Passimages (see Figure 3-9).

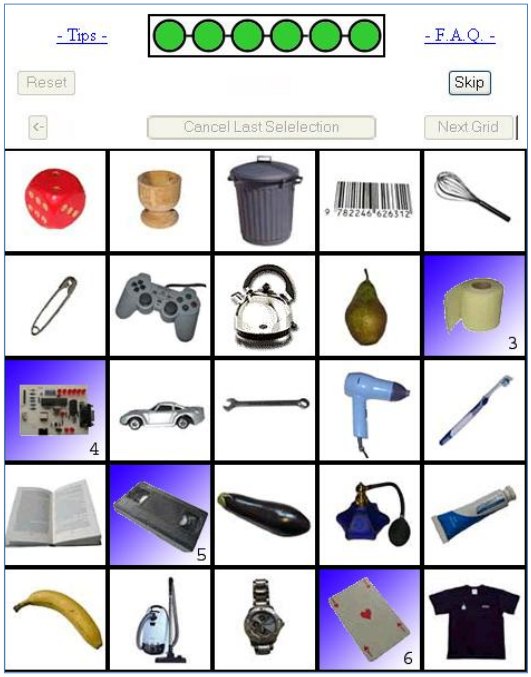

Figure 3-9: Original Passimages graphical scheme

Visual Identification Protocol (VIP) is another graphical scheme originally developed by De Angeli et al. [52]. VIP is a graphical scheme built mainly to be used in the self-service environment. For evaluation, they developed and compared three varieties of VIP (each of them had a different function and security scoring) with the prototype of a conventional ATM PIN-style (see Figure 3-10). They concluded that VIP could provide an alternative for conventional ATM PIN-style as participants made fewer errors and they could remember their secret images after periods of time. De Angeli et al. [53] carried out an extended usability study on the enhanced version of VIP and reported that the enhanced VIP offered better usability and security compared with their previous study. Another variation of this scheme is in [54], where image of faces were used.

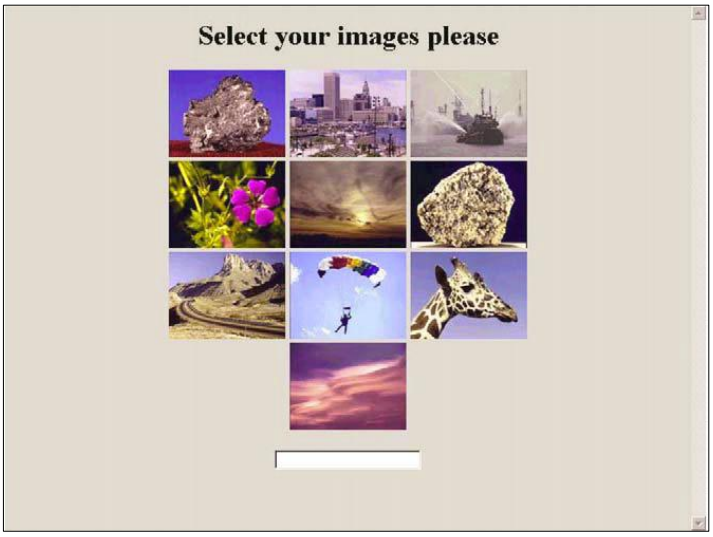

Figure 3-10: Example of interface from the VIP graphical scheme

Motivated by the schema of visual memory, Harada et al. [55] introduced a graphical scheme where users' secret images are transformed into 'unclear images' by means of image processing techniques. During login, users secret images are not displayed, instead they need to identify their 'unclear images' in order to be authenticated. A similar variation on this scheme is discussed in [56], with Hasegawa et al. [57] applying the technique of discrete wavelength where high frequency of users' secret images are embedded into low frequency of decoy image.

Weinshall [58] introduced a graphical authentication scheme that was claimed safe against spyware and shoulder surfing. Users of this scheme have to learn to differentiate between their chosen images with a large set of common images (shared among registered users and displayed during login). First, the login panel displaying common images are displayed to the users. Here, users should find the blinking cursor which is normally positioned at the top, upper left of the login panel. Below are steps to authenticate using this scheme:

a) If users find the current location highlighted by the cursor is their chosen image, they have to move one down. Otherwise, they have to move to the right.

b) They should stop when the cursor reaches the bottom or the right of the login screen. Then, they have to record the ‘random number’ displayed next to the image in the box provided.

c) This process will happen for several rounds and if users correctly entered their ‘random number’, they are allowed to login.

The Weinshall scheme (see Figure 3-11) relies upon the user’s natural cognitive abilities, without any assistance from external computational devices. Golle and Wagner [59] in their study showed that such a scheme was weak, unsecure and guessable.

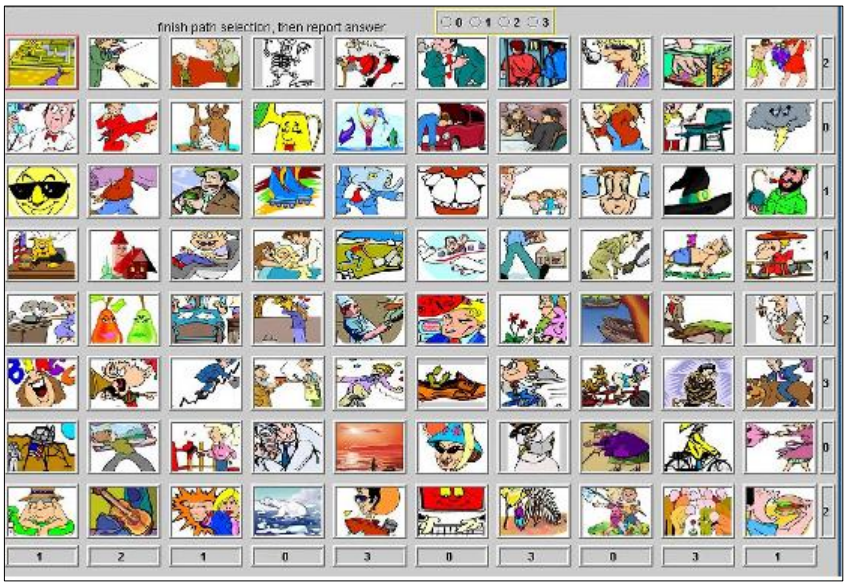

Figure 3-11: Weinshall graphical scheme

Wiedenbeck et al. [60] presented the design and evaluation of a game-like graphical password system - Convex Hull Click (CHC). The initial idea of this was already explained by Sobrado and Birget [61]. By definition, Convex Hull is the area encompassed by the edges joining a set of three or more points (see Figure 3-12). To login, users do not need to click on their actual secrets; they just click on the area in the

convex hull. Users needed to find their secrets and click in the area formed by three or four of their secrets. 15 participants used the prototype in two separate sessions; during training and after one week. From the results obtained during testing and interview, they reported that users took a longer time to familiarise themselves with this concept and interestingly after practice and training, they felt that CHC was fun, easy to learn and remember. More importantly, users found the approach useful and could be used to counter the shoulder-surfing problem.

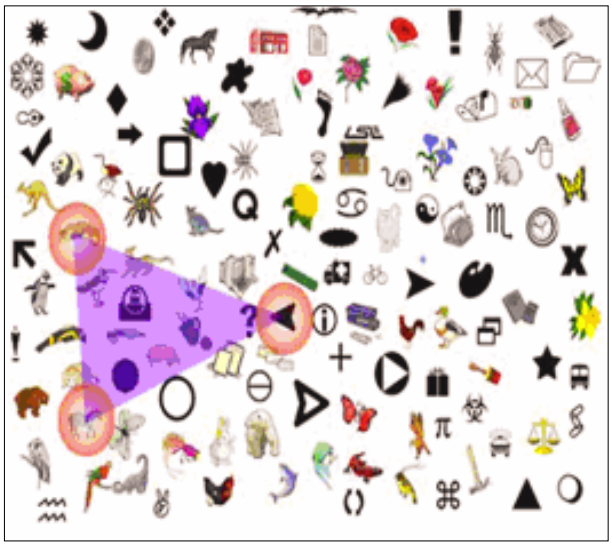

Figure 3-12: Convex hull of Sobrado and Birget

Hinds & Ekwueme [62] described another variation for this group known as 'ToonPasswords'. In this scheme, users have to remember three cartoon characters; from Walt Disney movies, television cartoons and finally from story book and nursery rhyme characters. To login, users have to undergo three rounds of authentication. For each round, users need to choose their secret among the decoy secrets arranged in four rows (where each row had ten images). They claimed that by having lots of images, it was relatively 'difficult' for an impostor to conduct an attack. Moreover, to prevent shoulder surfing, participants' secrets were not highlighted during the login process. To test their scheme, a method of cognitive walkthrough was used and tested by more than 60 college students. From the findings, it was found that users did not have problems when choosing their secret, the rate of users remembering their secret after

thirty days were good and there was good user acceptance for using cartoon characters as secrets/passwords.

Apart from the above schemes, graphical schemes based upon image of users' handwriting are also reported in [63] and [64]. In addition, there are other graphical schemes including 'jetafida' by Eljetlawi and Ithnin [65], graphical scheme by Komanduri and Hutchings [66], graphical password which uses an image of random geometric shapes [67] and the use of colour to group images for quicker login time [68].

As the conclusion within this section, it can be reviewed that each researcher normally comes out with their own ideas, and claim that their scheme was better than their predecessor. Hence, it is relatively difficult to claim that their scheme address the current weakness of their predecessor since no comparative evaluation was made. To address this, it is suggested that study within this ambiguity need to be conducted.

3.2.3 Draw-based Schemes

The initial idea behind this method was to build a graphical authentication system that could be used in a restrictive environment which limited users' input methods such as PDAs and smart phones. With that in mind, Jermyn et al. [69] introduced Draw-A-Secret (DAS). In DAS (see Figure 3-13), users draw their password in order to be authenticated. While the scheme itself offered a potential solution, study reported that the scheme suffered from problems of mismatch during reproduction of their drawings.

Nali & Thorpe [70] studied user choices of drawing using DAS. The study was carried out in order to obtain; user understanding of the instructions, user choice of the start and end point and finally, user choice of drawing. There were sixteen participants who each had to carry out two tasks. From the survey results, it was found that the instructions were well understood, the location of start and end point of each stroke were scattered across the grid and the participants drew various images such as symmetric shapes, letters and numbers.

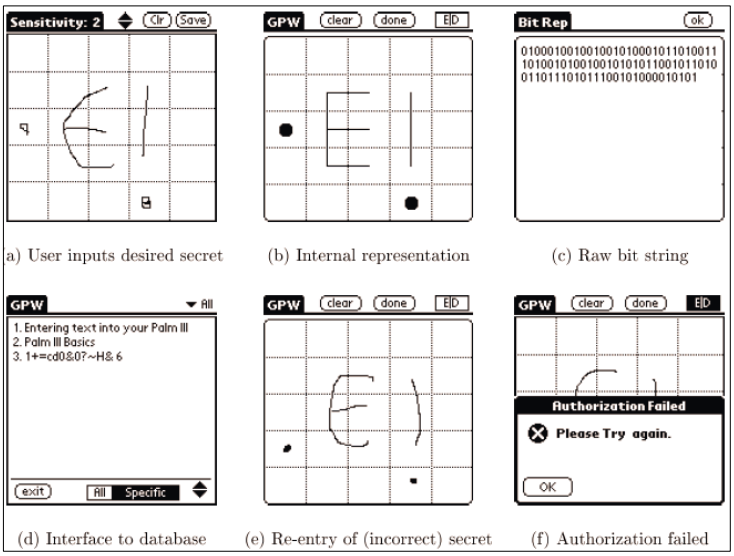

Figure 3-13: DAS scheme in Jermyn et al.

Malek et al. [71] introduced another variation called the Haptic-based graphical password. In this scheme, users draw their secrets on a layout grid referred to as the 'passgrid' (see Figure 3-14). For example, the user wanted to draw their passgrid and decided to start from point A to B, then to C and lastly moves back to A. During the drawing, they make sure that they make 'pressure' on any points they decided on earlier. By making such 'pressure' on the points in which only they know, the authors claimed it was hard for attackers to break it. In addition, by recording drawing 'pressure', the authors claimed they could produce even bigger and safer passwords. In order to evaluate the scheme, they developed two prototypes; using 5x5 grids and 8x8 grids. From the 18 participants, they determined that

users found it easy to recall and repeat their drawing with the smaller grid. However, the larger grid was more secure as it had larger areas.

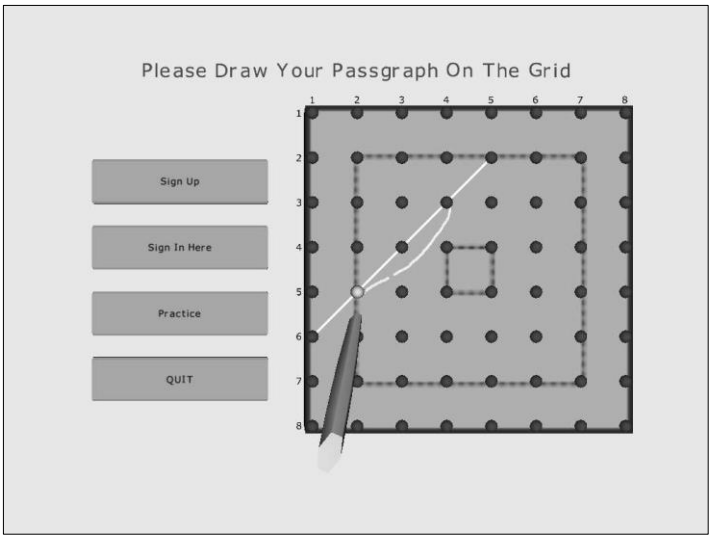

Figure 3-14: Haptic-based graphical scheme

Tao [38] introduced Pass-Go. This scheme was inspired by the traditional Chinese game GO[17]. In this scheme, users needed to click on the intersection of a given grid. This scheme claimed to be better than the original scheme proposed in [69] because it could offer a larger password space, improved usability (i.e. users just need to click on points in the grid, thus eliminating the tolerance problem) and could be adapted to various platforms. To enhance security, Pass-Go included an indicator and colour scheme where eight different colours were used. For evaluation, a prototype was developed and implemented in a web environment (see Figure 3-15). In total, there were 167 volunteers (majority students) who participated over a three month period. From the results, it was reported that users thought the indicator could reduce the shoulder-surfing problem and users also agreed the use of different colours could strengthen their password. However, users who used their laptop sometimes had problems selecting the password and sometimes they had problems drawing the curve. Enhanced versions of this scheme are discussed in [72] and [73], claiming to be better in terms of usability and security.

[17] http://en.wikipedia.org/wiki/Go_(game)

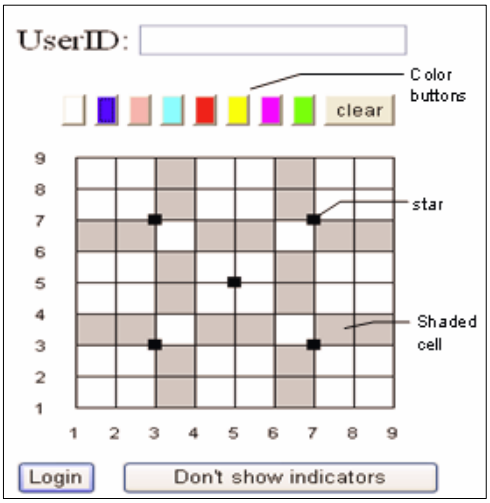

Figure 3-15: Pass-Go scheme

Dunphy & Yan [74] introduced another variation for DAS, known as Background Draw-A-Secret (BDAS). The idea behind BDAS is to eliminate user error when entering their secret drawings. This is done by drawing their secret on the canvas overlaid with a grid (see Figure 3-16). It is claimed that this offered better usability compared to the original method. In their lab study, a total of 46 volunteers participated who used both DAS and BDAS for approximately one week. From the initial usability lab study comparing BDAS with DAS, it was reported that BDAS had better password quality (produced strong passwords) and offered memorable password similar to the original DAS. A further variation of BDAS is known as the Qualitative DAS (QDAS) by Lin et al. [75], which used qualitative spatial relations and dynamic grid transformation for better precision during secret entry.

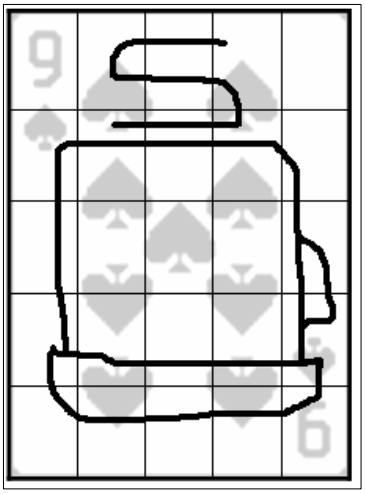

Figure 3-16: BDAS Graphical scheme in Dunphy & Yan

Motivated to improve the original DAS scheme, Gao et al. [76] introduced a scheme called Yet-Another-Graphical-Password (YAGP), this claimed to offer better usability and security in terms of free drawing position on the grid, strong resistance to shoulder surfing (as users' drawn secret are analysed beforehand) and a slightly larger password space. Evaluation was made with 30 participants and it was reported that 20 out of the 30 participants managed to redraw their secrets after 2 days, with 13 out of the 15 participants managed to redraw their secrets after two weeks.

3.2.4 Hybrid Schemes

Influenced with the approach of association, Li et al. [77] introduced a graphical scheme which combined the method of loci, a mnemonics technique for encouraging users to better remember their secrets. It was claimed that the use of these three steps could reduce the problems of shoulder surfing since users of the scheme went through three main steps, with these steps associated with each other. First, users need to choose one secret image as background image. To choose their second secret image, users need to click on any area of their secret background, in which a series of images will later appear for them to choose. Once finished selecting their second image, another set of images will appear and users need to choose their third secret image.

Zhao and Li [78] proposed another graphical scheme which they claimed was resilient to the risks from spyware, eavesdropping and shoulder-surfing. The scheme known as S3PAS (Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme), combining both textual and graphical images (see Figure 3-17). Users of this scheme have two types of passwords; one fixed password which only they know (e.g. Staff number, Library ID) and one random password which is created during the login. To login, users will be displayed with the login screen which consists of the image of characters

displayed randomly for every round and two text boxes for inserting fixed and random password. First, users need to input the fixed passwords. To get the random password, first they need to find their fixed textual passwords represented in a graphic. Here, users' random passwords are actually obtained in the triangle area formed by the three of their fixed passwords. After identifying their random password, users have to insert it in the text box provided. The process would continue for several rounds and if users correctly enter both of their passwords, they would be allowed to login. To simplify the above explanation, suppose Alice enters ABCD as her fixed password. Therefore, her random passwords would be any characters in the triangle area formed by ABC, BCD, CDA and DAB (the lengths of random password will be determined by the length of fixed password). To ensure reliability and demonstrate what they had claimed, they developed three variations for this scheme. These includes using three-set scheme to reduce border problem, a rule-based scheme to prevent users having three fixed passwords, and using a purely graphical scheme to increase the password space.

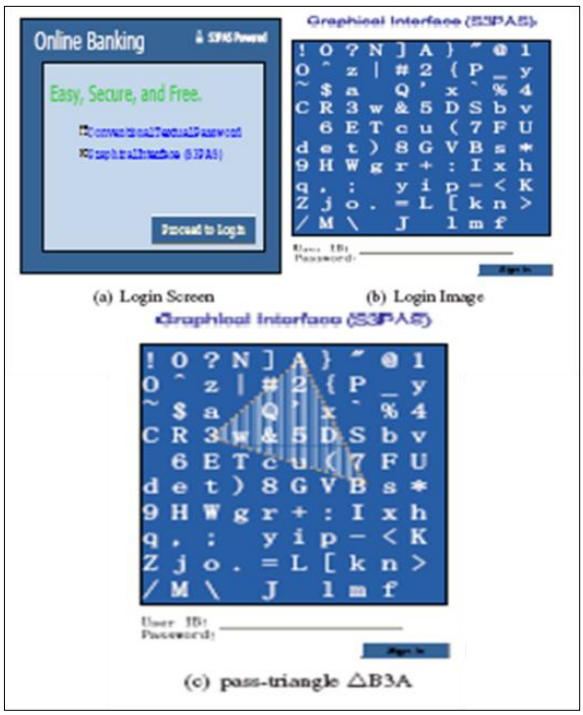

Figure 3-17: S3PAS graphical scheme

Minne et al. [79] carried out a study to evaluate the effect of using various interfaces - AuthentiGraph. In general, Authentigraph is another variation that was introduced in [80]. It uses a combination of

bitmapped data, mouse points and keystrokes. To login, users give the server the exact co-ordinates of their chosen images, in which the chosen images are displayed together with other random decoy images for every challenge round. Then, the server would map the information supplied by the user to form a password string. They developed three experiments (using quarter screen size, half screen size and full screen size), and each of the experiments consisted of five interfaces. From the 20 participants, they reported that they preferred using the half screen design with the type of interface where characters were grouped into a specific region and coloured randomly during each round. This was due to the fact that participants performed the login task faster and recognised the characters more easily.

Chiasson et al. [81] introduced another graphical scheme in which they claimed to combine the ideas from *Passpoints*, *Passfaces* and *Story*. This scheme differs from Passpoints because instead of clicking entire password in one image, users need to click only one point for each of the given images. The way the next image will be displayed is determined by user's click point of the current image (see Figure 3-18). In this scheme, they improved two aspects of usability; preventing users from clicking all passwords on one image (eliminate the problem of forgetting click points), and providing feedback at the early stage of login, rather than at the end of the login session. In the lab study of 24 participants, it was concluded that participants did not have problem inserting their passwords correctly, they were happy with this scheme and some of them preferred this new scheme when compared with Passpoint.

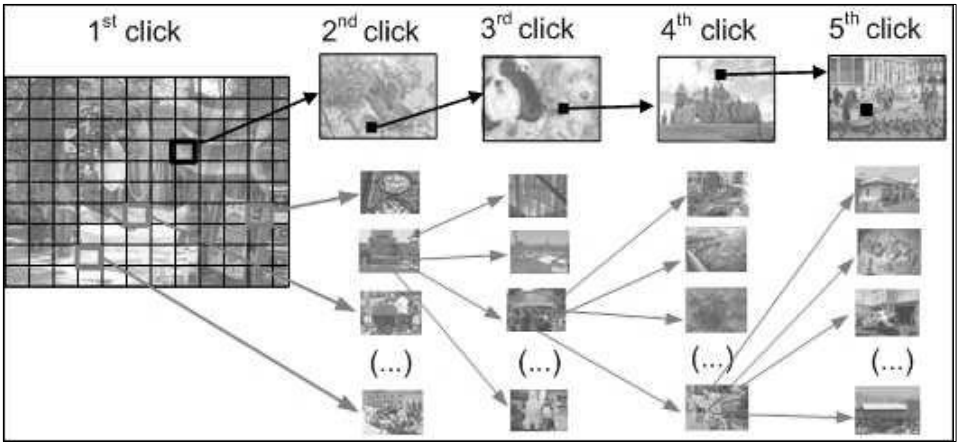

Figure 3-18: CCP graphical scheme

Using a persuasive technique to encourage users to create better secrets, Chiasson et al. [82] extended the CCP scheme and introduced a graphical scheme known as Persuasive Cued-Click Points (PCCP). PCCP was tested in the lab study environment where a total of 39 users participated. To create the password, users were only allowed to click within the box known as the 'viewpoint' (see Figure 3-19). The viewpoint was supposed to prevent the hot-spot problem (i.e. areas of interest of many users). If they are not satisfied with the area suggested by the viewpoint, they were allowed to re-position the viewpoint until they were satisfied with it. The effectiveness and efficiency of PCCP was determined by comparing the results of PCCP lab experiments with the results from their previous studies. Overall, they claimed that helping users to choose better passwords (in their case using persuasive technique) was one useful approach in order to address the problem of users creating predictable secrets.

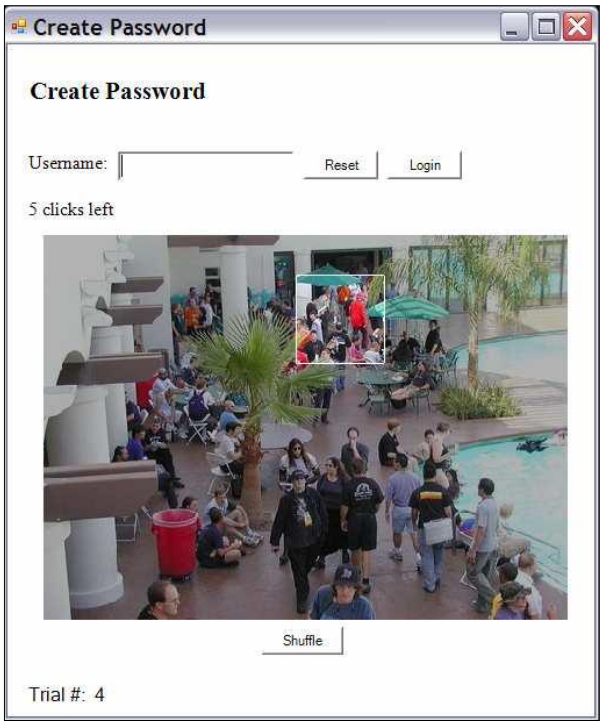

Figure 3-19: PCCP scheme by Chiasson et al.

Other graphical schemes within this category are InkClick, which combines the benefit of CCP scheme and Inkblot[18] [83], CDS, combining the method of DAS with a story sequence in [84] and Forget et al. [85] who investigated the viability of gaze (i.e. eyes) as the main input for graphical schemes.

3.3 A brief review of other graphical authentication studies

This section reviews other studies related to GA that were not discussed in the earlier section (since majority of studies within this section are indirectly related with the aforementioned graphical schemes). There are a number of studies related to **reviewing and surveying GA**. Examples are from Suo et al. [86] who surveyed GA schemes and classified GA schemes into two approaches; namely recognition-based and recall-based. Surveying usability features was also done in [87], a survey on both usability and security features [88], survey on users' familiarity and perceptions [89], review on shoulder surfing resistant schemes by Lashkari et al., [90], survey on the recognition-based algorithm [91] and an extensive review on GA by Biddle et al., [92].

To further enhance graphical schemes in both usability and security, it is found that many studies reported a **variety of approaches and solutions**. Example of these include: investigating suitable image to be used in the graphical schemes (see Table 3-1), examining the effect of using music during registration [147], using music or sound as an alternative for images for disabled users [95], guidelines for developing graphical schemes [96], and introducing algorithms for selecting distraction or decoy images [97].

Studies related to the **effect of having more than one graphical password** for both short-term and long-term duration are also reported. Examples are that from Moncur and Leplatre [99] and Everitt et al.

[18] http://research.microsoft.com/apps/pubs/default.aspx?id=70086

[100] for the choice-based method, with Chiasson et al. [101] for the click-based method. Other studies related to GA are that from Megaleas et al. [102] who proposed graphical secret representation for storage, measuring the entropy of GA strength by Rass et al., [103] and investigating image size differences in [104].

Researchers	Image Type
Real User Corporation [46]	Human faces
Djamila and Perrig [47]	Abstract images
Pierce et al. [80]	Letters and alphabets
Davis et al. [50]	Sequence of story – varieties
Tullis and Tedesco[93]	Personal photos
Harada et al. [55]	Varieties – all images are transformed into 'unclear' form
Hinds and Ekwueme [62]	Cartoon characters
Renaud and Olsen [63]	User handwriting
Lin et al. [67]	Track of geometric shapes
Hayashi et al. [94]	Varieties – user needs to identify 'degraded or distorted' images during login
Gao and Liu [98]	CAPTCHA – varieties
Gao et al. [68]	Varieties but introduce colour for image grouping
Hasegawa et al. [55]	Varieties – real image is embedded into the decoy image

Table 3-1: Study on image type in GA

Studies regarding **the use of images or pictures** are also reported. Examples are by Brossoff et al. [105] who studied the feasibility of a graphical one time PIN system, study of the graphical challenge-response authentication method by Renaud and Just [106] and graphical CAPTCHA in [98]. Combining image or graphical schemes to create **multi-factor authentication** is also studied. Examples are in Al-Sulaiman and Saddik [107] who combined biometric, text and graphical password, Sabzevar and Stavrou [108] attempted to combine images with a handheld device and combining image and text as in [109, 110].

Various **vulnerabilities and attack techniques** have also been investigated including: Hayashi et al. [111] who discussed an educated guess, Peach et al [112] explained the heuristic attack, Salehi Abari et al. [113] discussed an automated attack, with improvements of the method discussed in [114] and exploiting the click-based method by using eye tracking or gaze movement in [115]. Gathering data from

a small number of participants and using this data to crack larger numbers of participants secrets was also presented in [116], the vulnerability of attack known as description in [117], shoulder surfing study [118] and investigation on the secrets created by users in [93, 119-123].

3.4 Effective Level of Security

While the preceding sections within this chapter mainly gave focus upon on the ease of use (i.e. usability), this section highlights entropy of the GA for measuring the effective level of security. Entropy within the GA can be said as equivalent of a traditional password's "key space" i.e. the number of characters in the password (i.e. password lengths) multiplied by the range of allowed password characters/symbols, expressed in bits. Table 3-2 highlights the prediction of entropy calculation for a number of graphical schemes, compared with the 'entropy' of traditional password authentication.

From the table 3-2, it was found that most of the choice-based graphical schemes were merely weak as their entropy predictions were small (when compared to the traditional passwords of length five). Possible ways to address this are increasing the number of decoy images and the number of authentication rounds. However, this could reduce the ease of use of the method as it would take long time to login. The click-based graphical scheme (i.e. Passpoint scheme) was comparable with the traditional passwords of length six; with the scheme of hybrid (i.e. Zhao and Li [77]) could be said as providing effective security as their scheme was comparable with the passwords of length seven or eight. To enable usable and secure graphical scheme, it is suggested that combination of methods should be implemented (as shown in the thesis).

Graphical Scheme	Entropy (bits)
Passfaces [139] Authentication round = 4 (9 images per round) Target = 1 image per round Decoy = 8 images per round	4 * ($\log_2$ 9) = 12.68
VIP [52] Authentication round = 1 (10 images in total) Target = 4 images Decoy = 6 images	4 * ($\log_2$ 10) = 13.28
Passimages [51] Authentication round = 4 (25 images per round) Target = 6 images Decoy = 94 images	4 * ($\log_2$ 25) = 18.58
Passpoint [43] Authentication round = 1 Target = 5 clicks Image size, I = 450x330 Tolerance, T = 20x20 Password space = (I / T) ~ 371 (points to click)	5 * ($\log_2$ 371) = 42.67
Zhao and Li [77] Target = 4 clicks, 4 colours & 4 objects Assuming password space = 300 (points to click)	4 * ($\log_2$ 300*4*4) = 48.92
By using, All standard keyboard characters (n=94) Entropy per characters ($\log_2$ n) = 6.55 bits	Length of the passwords = 5 Therefore, entropy of passwords (5*6.55) = 32.75 Length of the passwords = 6 Therefore, entropy of passwords (6*6.55) = 39.30 Length of the passwords = 7 Therefore, entropy of passwords (7*6.55) = 45.85 Length of the passwords = 8 Therefore, entropy of passwords (8*6.55) = 52.40

Table 3-2: Entropy prediction of GA schemes

3.5 Issues and Opportunities

Following the review of GA approaches in the preceding sections, the issues that need further research can be briefly summarised into six major areas:

a) Memorability,
b) Secret entry and storage,
c) Image selection,
d) User familiarity,
e) Platform specific (e.g. mobile, desktop, etc.) and
f) Predictability.

Memorability deals with how secrets are memorised and recalled, applied to both short term and long-term. Many studies reported positive outcome with respect to single graphical password memorability [47, 51, 53, 124], with studies by Chiasson et al. [101] and Moncur and Leplatre [99] reporting positive results and a study by Everitt et al. [100] reporting negative results for having more graphical passwords secrets. As less study found to have investigated the long-term memorability effect, it is expected that study within this domain will continue.

User accuracy during secret entry is important, particularly with the click and draw-based methods since it is impossible for users to click/draw in an identical manner to their original secret. Since no solution has been found so far with respect of storing graphical password secrets, many studies normally store users' secret in the form of image reference (i.e. in the case of choice-based method) and coordinates (i.e. in the case of both click-based and draw-based methods). An example of effort studying this area is in [125] who studied the effect of assigning flexible square grid and John et al [126] who studied various acceptable tolerances. To reduce clicking error during secret entry, Birget et al. [127] introduced a mechanism known as robust discretization, with alternative improvements of the mechanism discussed in [128, 129].

The problem of getting and assigning suitable images for graphical schemes are another interesting area as humans perceive different images differently. Apart from the studies explained in the section 3.3, other studies with respect to this area include those from Abdullah et al. [130] who surveyed users' choices toward four image criteria, Suo et al. [131] analysed users click patterns with three image types and effect of users' involvement in the production of graphical secrets in [132].

Users' familiarity with the graphical methods is another vital area. It was observed that studies related to users' familiarity can be related to studies of usability. Study of GA in specific platforms or environments is also possible. Examples of attempts to study GA within the specific environments include those from Catugno and Galdi [133] who investigated a graphical pin for smart cards and low cost devices, a graphical password manager in the browser [134] and studies specific to the mobile phone platform can be found in [135-138]. Overall, it was found that many studies published so far relate to both click-based and choice-based methods, with less study reported for the draw-based approach. However, with the popularity of smart phones and touch-screen enabled technology, it is expected that the draw-based method should become increasingly popular due to the suitability of the method within such environments.

The final opportunity for further research is the predictability of the graphical schemes. Due to the nature of selecting images (i.e. choosing images, clicking on image and drawing), it is recognised that GA is easily observed by individuals (e.g. shoulder surfer) or devices (e.g. camera or screen capture software). As described in the preceding sections, a number of graphical schemes were introduced and evaluated to address this issue. In addition, analyses of users' secrets were also investigated, with the majority of the studies reporting that users' secret selections were often predictable and/or guessable.

As graphical methods are still relatively new and few studies are found to have investigated their suitability towards IT systems and applications, further research within this area is expected to increase. For reference, Table 3-3 shows the summary of criteria for comparing GA methods, mainly influenced by the work of Renaud [149] and personal experience of the author.

Factor	Criteria	Level	Graphical Methods			
			Click	Choice	Draw	Hybrid
Security	Info Harvesting		Yes	Yes	Maybe	No
	Guessable		No	Yes	No	No
	Breakable		Yes	Yes	Maybe	Maybe
Usability	Users' Perception		Yes	Yes	No	Maybe
	Memorability		Yes	Yes	Maybe	Maybe
	Repeatability		Maybe	Yes	No	Maybe
	Extra hardware		No	No	Maybe	Maybe
Applicability	Type of IT system	Online	Yes	Yes	No	Maybe
		Offline	Yes	Yes	Yes	Maybe
	IT system criticality	High	No	No	No	Yes
		Medium	Yes	No	Yes	Yes
		Low	Yes	Yes	Yes	Yes

Table 3-3: Graphical authentication comparison table

Three main factors for comparing graphical methods are security, usability and applicability. Security looks upon the safety of the graphical methods itself, usability is concerned with the ease of use and applicability deals with the viability of the method for IT applications/systems. Three criteria defined within the security factor are information harvesting, guessable and breakable. The term 'information harvesting' refers to the vulnerability or actions done by the observer or shoulder-surfer. 'Guessable' refers to the vulnerability or guessing actions perform by closed family or friends, while the term 'breakable' deals with the vulnerability to some sort of educated guess, dictionary attack and/or computer algorithms.

Four main criteria within the usability factor are users' perception, memorability, repeatability and the need for extra hardware. Users 'perception' refers to the users familiarity with and attitude towards the methods. 'Memorability' and 'repeatability' refer to the ability of users to remember their secrets (e.g.

both short and long term) and to reproduce them (i.e. during login) respectively, while ‘extra hardware’ considers whether the method requires any additional hardware in order to operate.

With respect to the applicability factor, the two main criteria are the criticality and type of IT system involved. In terms of criticality, three levels are defined; namely high, medium and low. The system could be defined as ‘high’ if the system itself deals with critical applications such as banking and medical, whereas the system could be defined as ‘low’ if it deals with normal applications such as student attendance and vehicle booking. Another criteria within this factor is the type of IT systems; either online or offline. Both are important to consider, given that most of the application systems can now be deployable within multiple platforms (e.g. mobile, desktop, etc.).

The aforementioned factors provide a useful usage for critically comparing graphical methods, as they collectively represent the ease of use, the safety and the viability of the method. Table 3-3 suggests that no single graphical methods are ideally matched with the given criteria. For instance, although click-based graphical methods are safe with the ‘guessable’ criteria, this is not the case with the ‘info harvesting’ and ‘breakable’ if users’ action are observed and they practice easy to guess secret creation. Similarly, although the method can be said as usable with respect to ‘users’ perception’, ‘remember’ and ‘extra hardware’, but not the case with the ‘reproduce’ especially to users with difficulty and if the acceptance tolerance is small. The ratings (i.e. Yes, No, Maybe) used in Table 3-3 are entirely based upon the collected literatures and experiences of the author of the thesis itself. Taken as a whole, to fully match with the suggested criteria, it is anticipated that more and more research need to conducted; either quantitatively or qualitatively.

3.6 Conclusions

This chapter discussed various approaches of authentication using images. Specifically, appropriate studies related to authentication using images were reviewed, and finally, six major issues and opportunities which need further actions were briefly highlighted.

It can be summarised that studies of graphical authentication are relative new (since 1991). It can be reported that many studies related to GA are focused upon usability (i.e. ease of use) and security. It has been found that studies related to the usability focus upon introducing the idea and concept of graphical schemes and improving existing GA methods; with studies related to the security focussing upon studying users' secrets, as well as creating new or novel attacks and vulnerabilities.

Based upon the preceding literatures, it can be rephrase that majority of the researchers come out with new ideas (i.e. various graphical schemes, various techniques for solving current problem in the GA, etc), and claim that their scheme was better than their predecessors. In addition to this, it was also found that most of researchers compared their scheme with the traditional password authentication (not with their predecessors), which limiting the usefulness of their introduced schemes.

Hence, motivated by the work of usable security and having identified the possibility and opportunity of further research, this thesis studied GA by comparing graphical schemes, developing an enhanced method and introducing guidelines or advice to users before they start selecting their secrets. Specifically, two comparative studies between graphical schemes were conducted with particular attention to investigate users' familiarity and perception towards usability and security issues within the GA schemes (i.e. explained in Chapter 4), and to assess the feasibility of graphical methods in web environment (i.e. explained in the Chapter 4). Graphical scheme known as the Enhanced Graphical

Authentication System (EGAS), combining the methods of click-based and choice-based was developed and tested in terms of users' familiarity (i.e. explain in Chapter 5 and Chapter 6), suitability of login mechanism (i.e. explained in Chapter 5), with ideal combination of secrets and effect of using smaller tolerance towards EGAS are explained in Chapter 6. Finally, the Graphical Password Guidelines (GPG) was introduced and deployed within the EGAS software prototype, with evaluation on its effectiveness for helping users to create safer and memorable secrets is explained in the Chapter 6.

4. Comparative Evaluations

4.1 Motivation

As far as the prior research is concerned, no study is reported to have investigated and compared image-based authentication techniques. Previous studies of graphical authentication normally introduce the idea and then compare against traditional methods (as described in Chapter Three). One missing criterion that needs further attention is prior exposure to the technology by the end-users themselves. Thereby, it is anticipated that prior exposure (i.e. user familiarity) is an essential part for ease of use of the method. This chapter discusses the study carried out to compare graphical schemes and further, to assess the usability performance of two graphical authentication methods when used in a web-based environment.

4.2 Comparative One: Users' familiarity and perceptions

This section reports the first comparative evaluation comparing three major graphical schemes; namely click-based, choice-based and draw-based methods (as explained in Chapter 3). The objectives of comparison were to investigate users' familiarity and perceptions towards three methods of graphical authentication.

4.2.1 Methodology

A survey was conducted in order to investigate the objectives. Participants were asked to use the prototype and then answer a related questionnaire. This activity took approximately 10 to 15 minutes to complete depending on the participants' experience of using computers. The following sections explain the prototype, questionnaire and outline the steps and procedures the participants had to follow.

4.2.1.1 Software prototype

A prototype of three graphical methods was developed using Microsoft Visual Basic 6.0. All three schemes were deployed and combined in one application in order to give participants a brief hands-on experience and to demonstrate how graphical authentications could work in the real world.

The designs of three schemes were basically similar to the original Passfaces [46], Passpoint [43] and DAS [69] but simplified in term of the number of passwords they need to register or use. This is due to the fact that the study only needed the participants to get an impression of using graphical approaches and did not want to burden them by remembering up to five click points and five to six images.

There were two main modules in the prototype - registration and login. In the registration module, participants needed to register their secrets by clicking four times on the image for the click-based method, choosing two images for choice-based and drawing freely for the draw-based. The drawing took into account the location of mouse *click-down* and *click-up*. The types, shapes and number of drawings were left to the participants' preference. In the login module, participants were asked to log into the prototype by using their secrets, with no enforcement were made towards the number of login they were allowed to. Figures 4-1 to 4-3 illustrate the screenshot for each method with an example of secrets created by one of the participants.

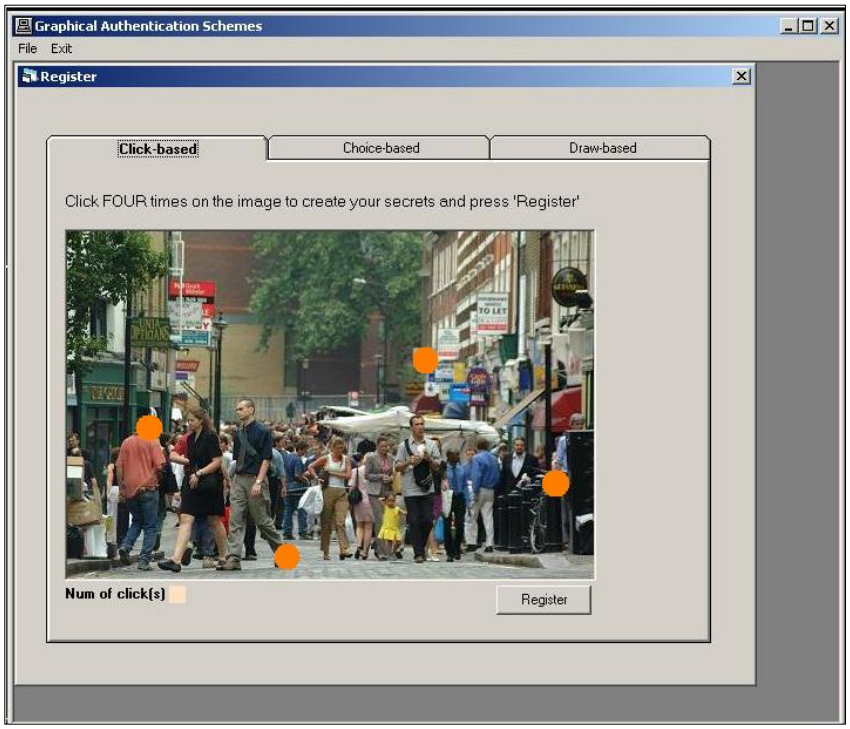

Figure 4-1: Example of secret from the click-based method

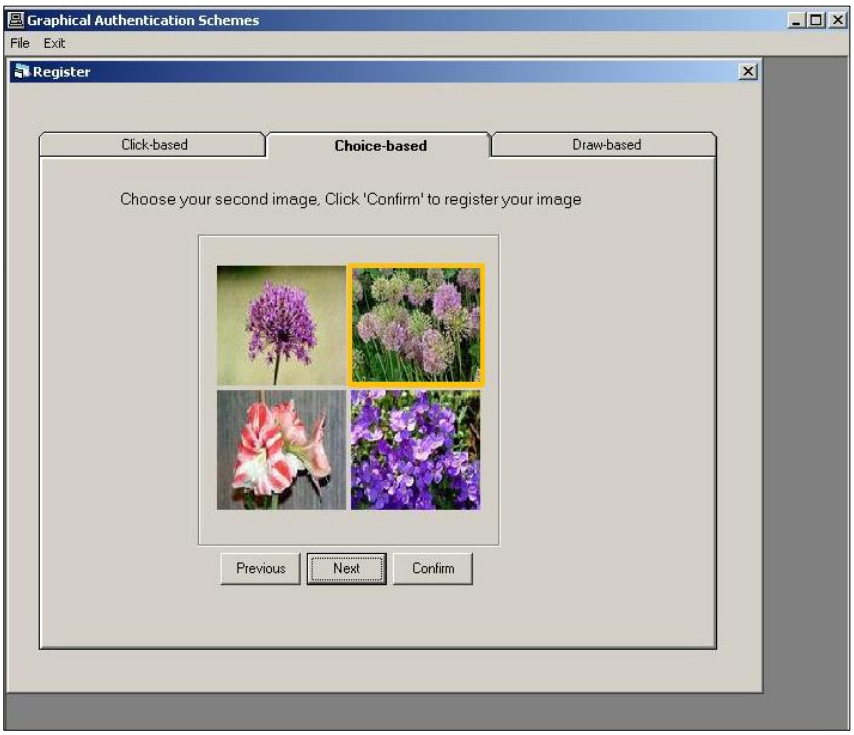

Figure 4-2: Example of secret from the choice-based method

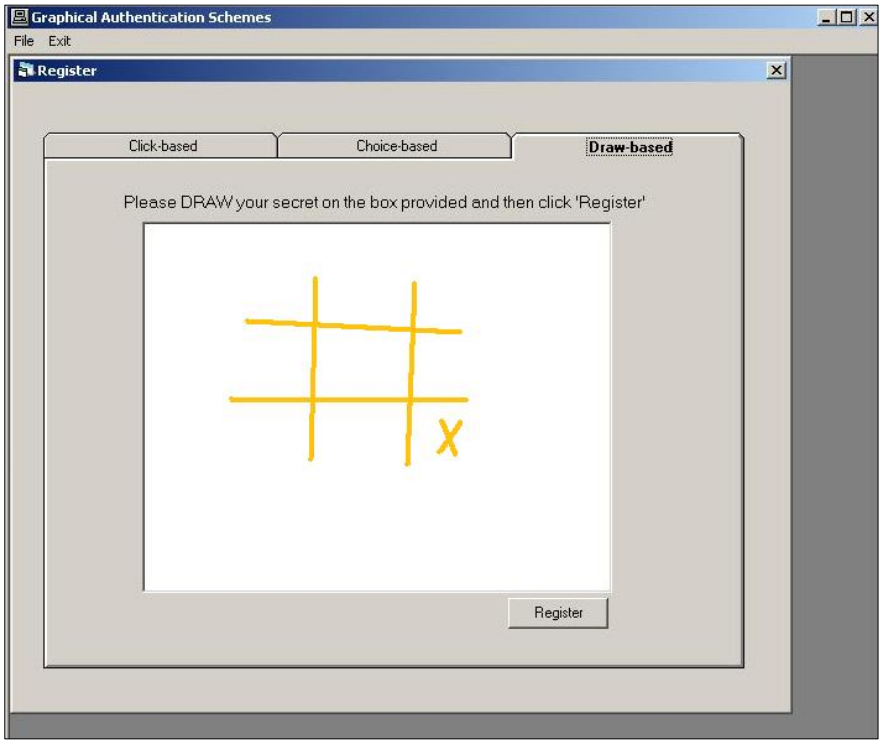

Figure 4-3: Example of secret from the draw-based method

4.2.1.2 Questionnaire

There were two sections in the questionnaire. Part A asked participants to provide information such as age, gender, nationality, highest level of education, current job, computer experience and asked their awareness and knowledge regarding the use of images/pictures as a means of alternative user authentication.

In part B, participants were asked to answer four questions. The first question was about their opinion on the ease of use of each method, how easily they remembered their secret, how easily they could reproduce their secrets and whether they felt that the methods could be used in a web-based environment, with 'Yes' or 'No' were used to obtain users answers. The second question asked participants to select the method they would most strongly prefer to use for web-based authentication. For the third question, participants were asked their opinion about whether they would consider each

method to be ‘safe’ or ‘unsafe’ against the following security threats: observer or shoulder-surfer, guessing by close family or friends and brute-force attack. The final question asked participants to give any comments and suggestions regarding image authentication. All of these questions were ‘close-ended’ type and a copy of questionnaire can be found in the Appendix A, No (1).

In order to validate users’ understanding and to reduce errors during the subsequent implementation, five participants took part in pilot testing where the prototype was evaluated. Appropriate changes and amendments were then made prior to the full run of the study.

4.2.1.3 Procedures and Steps

Participant in the study were obtained from an open call for volunteers within the university without any incentive. Participants were asked to use the methods in any order they wanted, without initial demo or briefing. The following list details the tasks each participant needed to complete.

1) Register and confirm their secret selections. Once succeed,
2) Re-authenticating by using their chosen secrets and
3) Answer feedback questionnaire on the paper provided.

Upon using the prototype, all of the participants’ actions and behaviour were observed for monitoring purposes. As this was an ‘uncontrolled’ type of survey, participants were allowed to use the prototype as many times as they wanted.

4.2.2 Results and Findings

A total of 25 participants took part in this study (12 males and 13 females). The minimum age of the participants was 30 years old. The majority of the participants were drawn from the university (e.g. students, researchers, administrators and lecturers) and all of them had more than 6 years experience using computers.

4.2.2.1 Users' preference and familiarity

All participants started their registration with the click-based method and finished with the draw-based. This was expected as the click-based method was located on the left-side, followed by the choice-based and finally the draw-based. Overall, only 12 participants managed to complete both registration and login tasks without any failed attempts. The remaining participants needed 2 to 5 attempts before completing their tasks. These suggest that for the authentication using images to be effective, appropriate training should be provided beforehand.

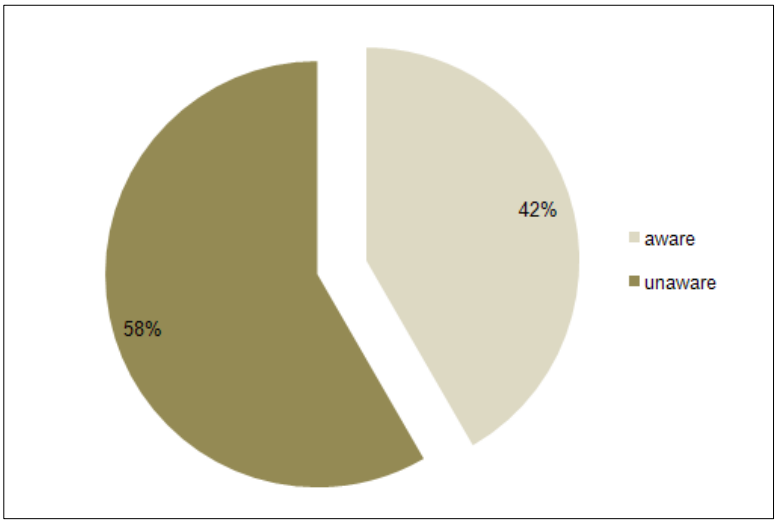

Figure 4-4: Participants' familiarity towards authentication using images

Figure 4-4 reports the result of the question about their familiarity with the use of images/pictures for authentication purposes. Only 11 participants indicated that they were familiar or aware of it, 6 of these participants were members of the research centre who were generally aware about the authentication technology through previous exposure.

From observation, it was found that participants were initially quite 'confused' with the 'state-of-the-art' of graphical authentication. For example in the click-based type, the majority of them had problems reproducing their secrets. This is possibly due to their misunderstanding of this approach because when they clicked on particular points (for example clicking on the person's hand); they were assuming the whole image (in this case, the whole body of the person) was chosen. Only the point or the area in which they clicked would be taken into account as their secret and not the whole object**.**

Users' preferences on the suitability of graphical scheme for web-based authentication showed that participants preferred click-based (13 participants) and choice-based (12 participants) with no participants indicating a preference for the draw-based method. From the results of voice feedback, the main reason why such schemes were preferable was because of their convenience and simplicity.

4.2.2.2 Perceived Usability

When using the prototype, it was found that all of the participants preferred using the choice-based method. They felt that the passwords were quite easy to remember and they had no problem reproducing their secrets during login. However, although the draw-based type was easy to use, participants had difficulty remembering and reproducing their drawings. It is likely that this was due to the usage of the mouse and if participants were to use some sort of special device such as a stylus, a drawing pad or

touch screen device, they would perform better due to the nature of the method itself. The results of usability perception towards ease of use, ease of memorising or recalling their secrets, ease of reproducing their secrets and suitability of the methods to be used for web-based authentication are shown in Figure 4-5.

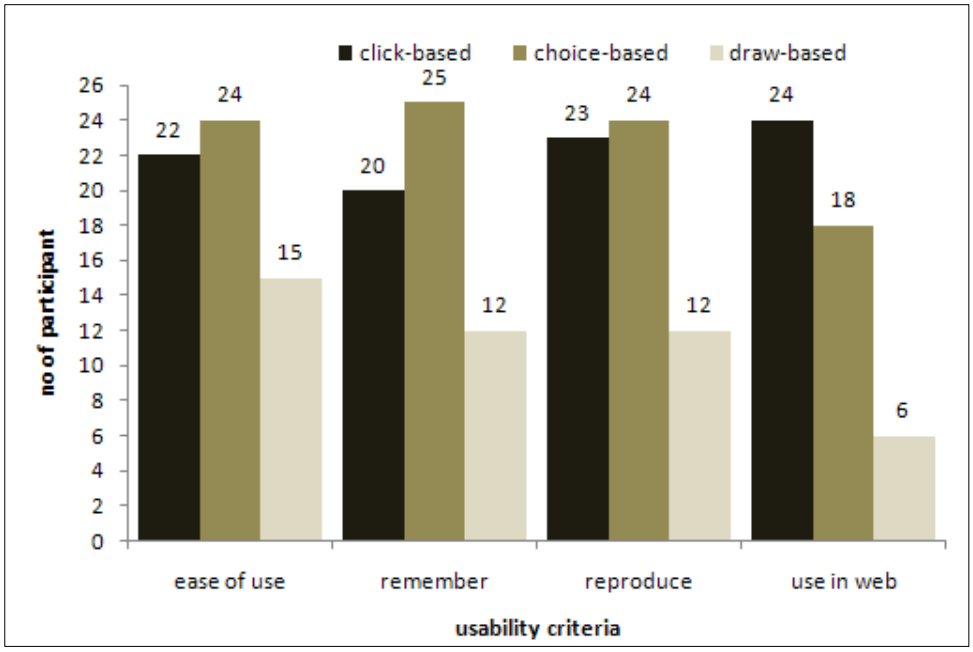

Figure 4-5: Users' perception towards ease of use, remembrance, reproduction and use in web

4.2.2.3 Perceived Security

With regard to the users' opinion of the level of security the methods might offer, the majority of the participants believed that the draw-based method offered better security. This is due to the fact that it is impossible for users to draw alike. Conversely, more than half of the participants felt that choice-based would be vulnerable to guessing, brute-force and information harvesting vulnerabilities and interestingly although they felt that the choice-based type was not secure enough; they still choose it as their preferred method for web-based authentication. The detailed results on users' opinions towards security issues are presented in Figure 4-6.

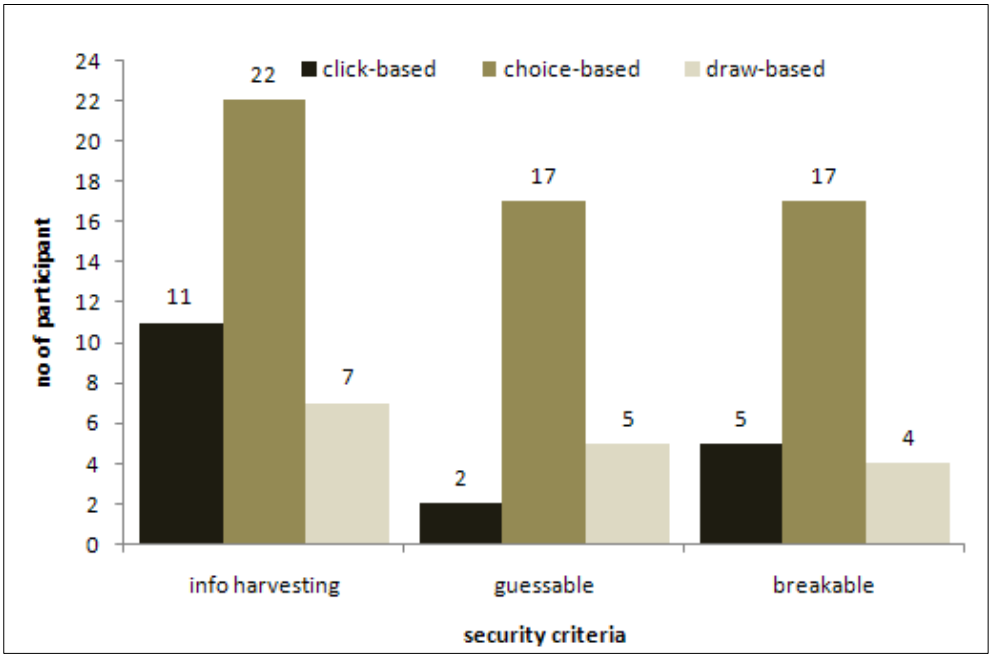

Figure 4-6: Users' perception of security like information harvesting, 'guessability' and 'breakability'

Here, the term 'information harvesting' refers to the vulnerability or actions done by the observer or shoulder-surfer. 'Guessable' refers to the vulnerability or guessing actions perform by closed family or friends, while the term 'breakable' deals with the vulnerability to some sort of educated guess, dictionary attack and/or computer algorithms.

Although users may not have been able to offer truly informed opinions about these aspects, their views were still a valid reflection of what they perceived the security to be (which would therefore influence their confidence in using the approaches).

4.2.3 Constraints

The contribution of this study when compared to other works is that it asked users to consider and compare all three types of graphical schemes (whereas others typically compared a single form of graphical authentication against traditional username/password methods).

As the nature of the software prototype was a stand-alone application and the chosen method was one to one, the number of participants was limited. To obtain more conclusive findings, it is suggested that participants from the various backgrounds, with a more varied range of computer skills needed to be recruited.

4.3 Comparative Two: Click versus Choice

This section compares two graphical methods and reports user studies with the objective of assessing the usability performance of two image-based authentication methods when used in a web-based environment. The comparative methods involve clicking secret points within a single image (click-based) and remembering a set of images in the correct sequence (choice-based). The key elements of usability performance in this study were users' accuracy while entering their secrets, the time taken to enter them, patterns of the chosen secrets and users' response towards the methods itself.

The click-based and choice-based methods were chosen since both were rated suitable to be used in a web context by participants (see Figure 4.5; use in web section), and it is anticipated that both methods are easily deployed in a web environment (using normal desktop and laptop) without the need for any additional hardware.

4.3.1 Methodology

A type of usability study was chosen as it was expected that the method could reveal participants' usability performance and problems. Participants had to experience using both methods and finally provide feedback. The following section details the development of the prototype, questionnaire and describes the procedure each participant needed to follow.

4.3.1.1 Web Prototype

Graphical authentication in the style of Passpoint and Passface was developed using PHP, JavaScript and MySQL. Before registering their details into the web prototype, they were asked to complete a short series of questions to record their age, gender and computer usage experience (see Figure 4-7).

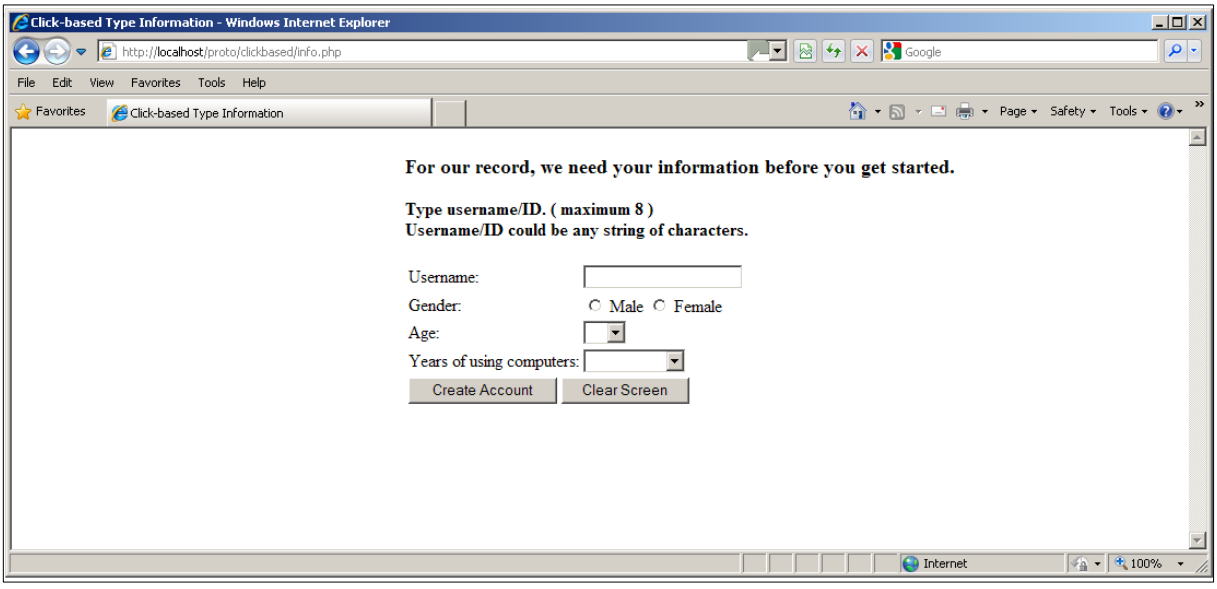

Figure 4-7: Participant information screen from the prototype

The development of the click-based method prototype was similar to the original scheme proposed in [43]. The display scale of the image was 450x330 pixels with acceptable tolerance (i.e. areas in which

the click is still valid) of 18x18 pixels. The small tolerance was used as Chiasson et al. [45] showed that the click-based method would still be usable even with the smaller tolerance. Participants were required to create their passwords by choosing and clicking upon five different points in the given image. They were told to remember their secrets in sequence order and to select their points from different areas of the image (see Figure 4-8).

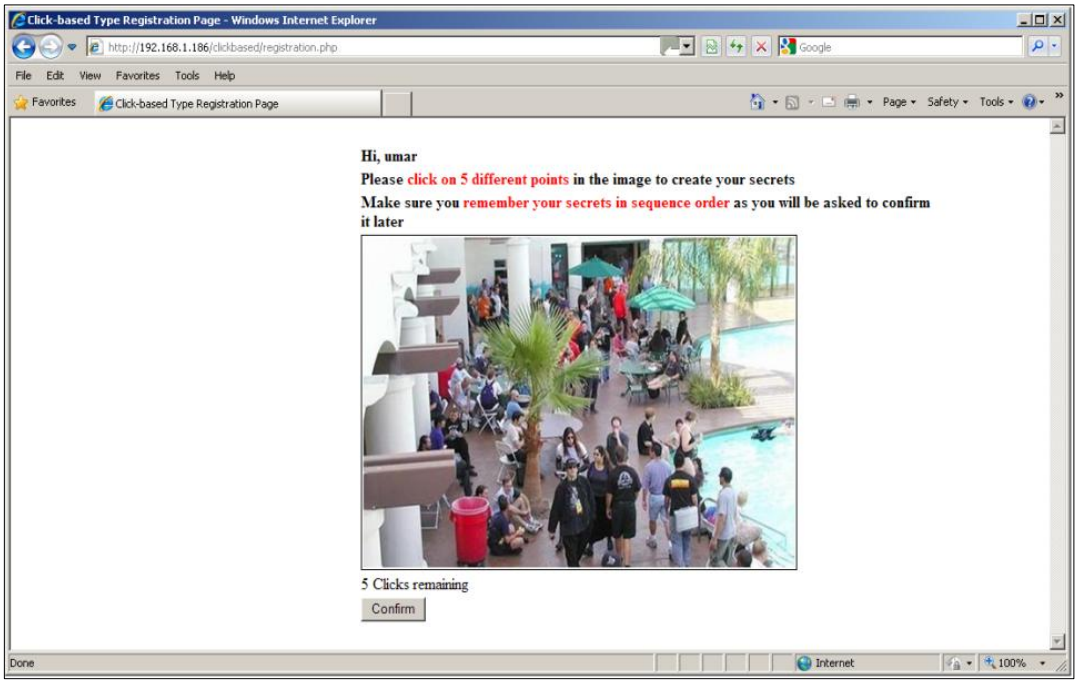

Figure 4-8: Registration screen from the click-based prototype

For the choice-based method, participants needed to remember five different images grouped within five different themes; namely ‘Animal’, ‘Transport’, ‘Nature’, ‘Food’ and ‘Other’. All of these images were manually chosen in order to prevent redundancy and taken from free image galleries available on the Internet[19].

During the registration, a total of 180 images (arranged in 5 separate 6x6 grids) were displayed to the participant, who then needed to choose one image from each theme. This process (displaying 36 images for each category) would continue until participants finished choosing their five images (see Figure 4-9).

[19] http://www.freeimages.co.uk/, http://www.freefoto.com/index.jsp, http://www.free-images.org.uk/index.htm

When it came to the confirmation of their images, only 16 images (arranged in 4x4 grids) were randomly displayed to them, one of which was their chosen images. This process continued for the other themes until they finished choosing all of their images within the themes (see Figure 4-10).

Figure 4-9: Registration screen from the choice-based prototype (showing the 'other' theme)

Figure 4-10: Confirmation screen from the choice-based prototype (showing the 'other' theme)

To login, participants were asked to authenticate in the web prototype by using their chosen username and secrets. The login process for the click-based method was pretty straight, while with the choice-based login, users' secrets were only displayed or allowed to proceed with the next steps if participants entered valid username. Examples of the login web pages for both methods are shown in Figures 4-11 and 4-12, with table 4-1 showing the entropy estimation of both schemes.

Figure 4-11: Login screen from the click-based prototype

Prototype	Entropy estimation
Click-based Number of secret = authentication rounds = 5 Total number of images per round = 16 (4x4 grid)	5 * ($\log_2$ 16) = 20 bits
Choice-based Number of secret = 5 Image size, i = 450x330 Tolerance, t = 18x18 Clickable areas = password space = (i/t) = ~458	5 * ($\log_2$ 458) = 44 bits

Table 4-1: Entropy estimation of the graphical prototype

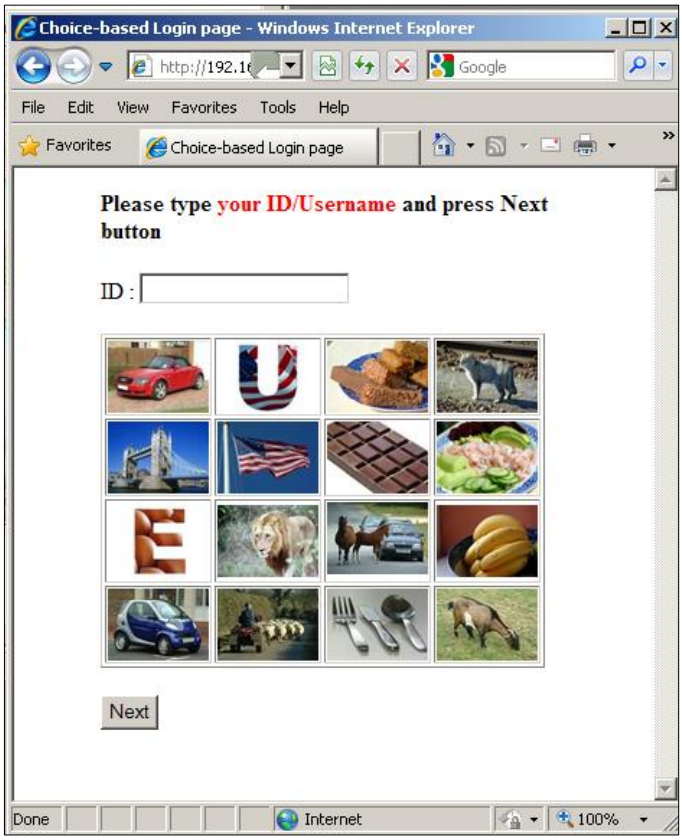

Figure 4-12: Login screen from the choice-based prototype

4.3.1.2 Questionnaire and Distraction Activity

The questionnaire was split into three parts; the first two were about the authentication methods, while the last one was about general opinions and the prototype itself. Among the questions asked were whether it was easy to remember the secrets, whether they had problems during login, whether they would use these methods, and whether they would prefer using their own images as their secrets. A copy of questionnaire can be found in the Appendix A, No (2).

Participants were asked to play a 'spot the difference' activity. The aim was to provide them with a mental distraction between the registration and login tasks, similar with the work in [45]. This gave them something to do other than focussing on remembering their chosen secrets. A copy of the 'spot the difference' images is attached in Appendix D, No (1).

4.3.1.3 Procedures and Steps

All participants were recruited via an open call for volunteer within the university without any incentive. The trial worked in two ways; participants came to the author's lab or the experimenter went to participants' workplace. In both cases, they were asked to complete the same tasks using the same materials (e.g. a laptop computer and software web prototypes). Due to the mobility issues, the web prototype was installed and the trial was undertaken on a laptop equipped with a wireless mouse. The following list details the tasks each participant needed to complete.

a) Register and confirm their secrets for both methods. Once succeed,
b) Playing a spot the difference activity. Once finished,
c) Authenticate using their chosen secrets for both methods (only once) and
d) Provide feedback by answering a questionnaire.

The questionnaire (d) and game activities (b) were done on paper, while tasks (a) and (c) were conducted online using Internet Explorer (IE8), with all of the materials (and the trial method itself) having received prior ethics approval. No longitudinal study was tested as the aim of this study was to obtain their short-term performances. However, it is suggested that long-term study need to be conducted in order to compare both short-term and long-term performances.

4.3.2 Results and Findings

A total of 40 participants (33 males and 7 females) agreed to participate, all of whom were university students and staff, with an average age of 27 (sample range from 21 to 44 years) and up to 7 years experience of using computers. Since the number of participants is small and the sample is biased, the results must be considered indicative rather than conclusive. However, with the idea of getting

participants to use and evaluate both techniques simultaneously, the results can still be used as an early indication for evaluating both methods empirically.

The discussion of the results is categorised into five areas, namely number of attempts, timing, accuracy, patterns and users' feedback.

4.3.2.1 Number of attempts

With the way the study was designed, all participants successfully completed all the authentication tasks (register, confirm and login).As the total number of attempts created by the participants was quite low (with only 40 participants); only general findings will be highlighted here. First, for the choice-based method, all participants were able to complete all of the authentication tasks with only one attempt. Second, for both methods the number of attempts starting from registration to login was reduced significantly. This could simply indicate that the interface made the process easy.

By contrast, it was found that the number of attempts for the click-based method was significantly higher, particularly during registration and confirmation. These results were predicted as participants had to carefully click on their secret areas, which sometimes they did not manage to do. When compared with the choice-based method, the above finding could be biased, as in the click-based method, participants needed to be accurate while entering their details and they had to remember the information in sequence, but for the choice-based method participants only needed to remember the images themselves.

4.3.2.2 Timing

Each participant's registration, confirmation (i.e. similar with confirming their passwords) and login duration was recorded to calculate their average time while entering their passwords. The time was measured from the first chosen click/image until the last. Table 4-2 gives the mean and standard deviation (SD) for each task.

N=40		Time (seconds)		
		Registration	Confirmation	Login
Choice-based	**mean**	34	17	17
	SD	21	6	6
Click-based	**mean**	12	8	8
	SD	7	4	5

Table 4-2: Mean and SD of time for entering secrets

For the choice-based method, it was clear that participants took longer during registration compared with the confirmation and login tasks. This is because during the registration, participants needed to familiarise (scanning 180 images) and carefully choose their images. As they became familiar with their chosen images, they took less time during confirmation and login (refer Table 4-2). For the click-based method, it was found that the mean time for confirmation and login task were similar. This is expected since participants just needed to click on their secret. Comparing both methods, it can be said that method based on clicking is superior with the method based upon selecting series of images, due to the aforementioned justification.

4.3.2.3 Accuracy

This section measures the correctness of the chosen images and the precision between clicks. For the choice-based method, since all of the participants managed to create their secrets during their first attempt, it could be suggested that the accuracy for both registration and login were very high.

For the click-based method, accuracy refers to how far the original click points during registration are from the click points during confirmation and login [45]. As explained in the previous section, the tolerance of 18x18 pixels was used. As long as participants clicked within their secret tolerance area, the click will be accepted. Figures 4-13 to 4-15 illustrate the distributions of click accuracy for all participants during both registration and login tasks (considering only the successful attempts), with Table 4-3 showing the mean and SD of accuracy for successful attempts during both tasks.

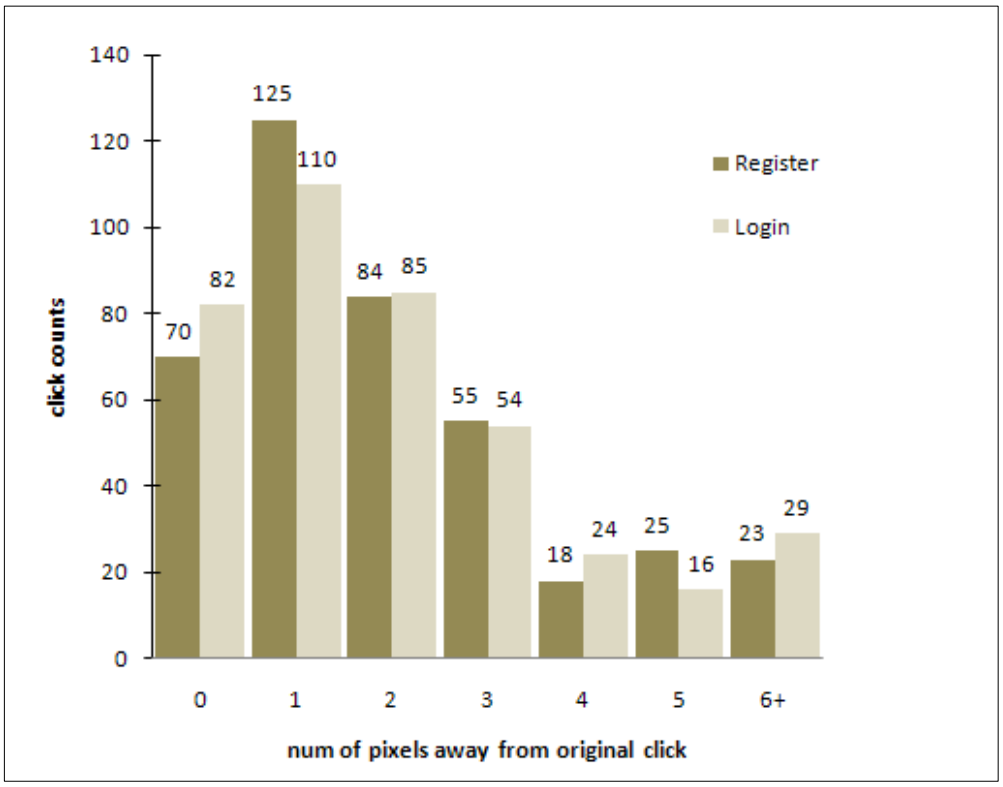

Figure 4-13: Accuracy during registration and login tasks

N=400	Accuracy (pixels away from original click)	
	Registration	Login
Mean	1.9	2.0
SD	1.7	1.8

Table 4-3: Mean and SD of accuracy for register and login tasks

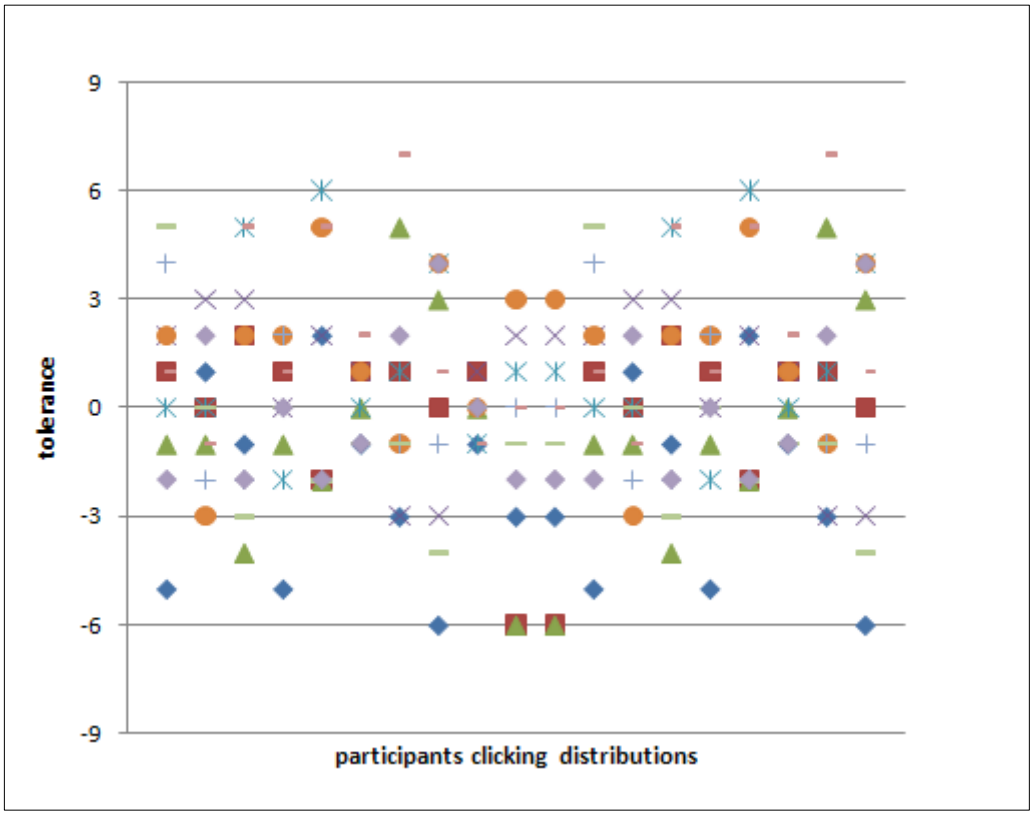

Figure 4-14: Participants' clicking distributions during confirmation task

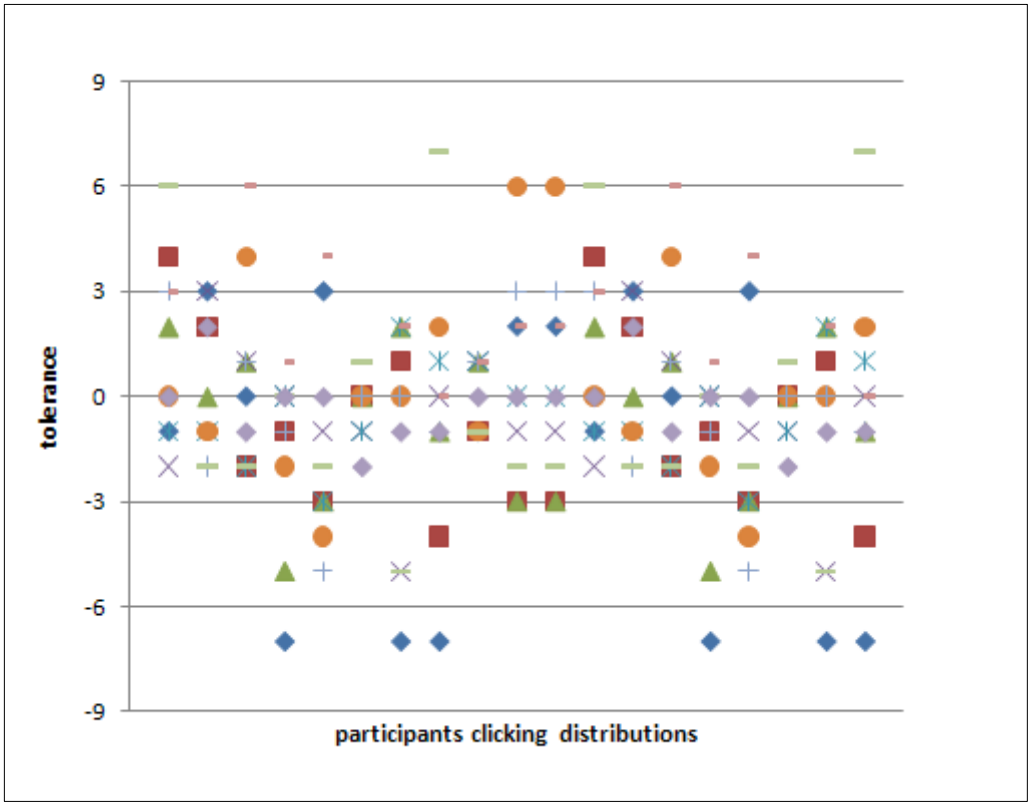

Figure 4-15: Participants' clicking distributions during login task

Based upon Figures 4-13 to 4-15, it is found that participants are relatively accurate in entering their secrets within 6x6 pixels of their original click point. Overall, the above result confirms and supports the research [45] and therefore, it is suggested that the click-based method would still be usable if it was designed with a tolerance as low as 6x6 pixels (note that the method would be more secure if a smaller tolerance is used, as it produces a larger secret space).

4.3.2.4 Pattern

This section highlights the types of images chosen and areas in the image clicked by the participants. The purposes are to investigate any relationships or patterns while creating the secrets, which might influence later predictability for an attacker.

For the choice-based method, the most commonly chosen images were 'sport cars', 'flags', 'eggs', 'burgers' and 'cats'. No relationship was found between the chosen images but it was found that a number of participants had chosen their images based on the sequences of a story (e.g. one participant chooses his favourite sport car (from the Transport theme) as their first secret image. In order for the car to be executed and moving, the participant chooses a key (from the Other theme) and highway (from the Nature theme) as their second and third secret image respectively. When driving and feels sleepy, he stops to take a break by having coffee (the participant fourth secret image from the Food theme) while watching butterflies (participant's fifth secret image from the Animal theme)).

With regard to patterns, it was found that nearly all of the participants had chosen the images that were significant to their name. For example, one participant used 'JP' as his username and chosen image letter 'J' as one of his secret images. On top of that, for the 'Transport' theme, it was found that male participants normally chose sport cars while female participants selected smaller, compact cars. Based on observation and informal chat during the trial, the chosen images can be grouped into two; their personal preferences and the recognisability of the image itself. Table 4-4 shows examples of secrets (images)

selected by a subset of users, with Table 4-5 highlighting the number of participants choosing popular images for each theme.

	Transport	Other	Nature	Food	Animal
User A	Helicopter	Cutlery	Clock	Eggs	Cow
User B	Mini Cooper	Letter	Bridge	Chocolate	Dog
User C	Sport car	Letter	London Eye	Chips	Penguin
User D	Sport car	Flag	Bridge	Carrot	Lion
User E	Sport car	Letter	Autumn	Cereal	Peacock
User F	Sport car	Letter	Bridge	Raspberry	Bird

Table 4-4: Example of images chosen by the participants

Theme	Image Description	Participant
Transport	Yellow mini car	6
	Red helicopter	6
	Red sports car	5
Other	UK flag	5
Nature	London Bridge	7
	Lighthouse	5
Food	Eggs	8
	Burger	6
Animal	Bird	7
	Peacock	7
	Lion	5

Table 4-5: Image popular for each theme

For the click-based method, the start/first click and the shape of the clicks are reported. For the start click, it was found that majority of the participants started their first click either in the bottom or top of the image areas (see Figure 4-16).

With regard to the image used, it could be anticipated that such chosen areas were obvious and recognisable (e.g. people wandering around, beams and umbrellas). After the first click, no interesting patterns were found since participants were likely to click anywhere but one noticeable finding was that participants chose to click on objects, as explained earlier. Example of clicks created by 6 of the participants is shown in Figure 4-17.

Figure 4-16: Participants' first click secret

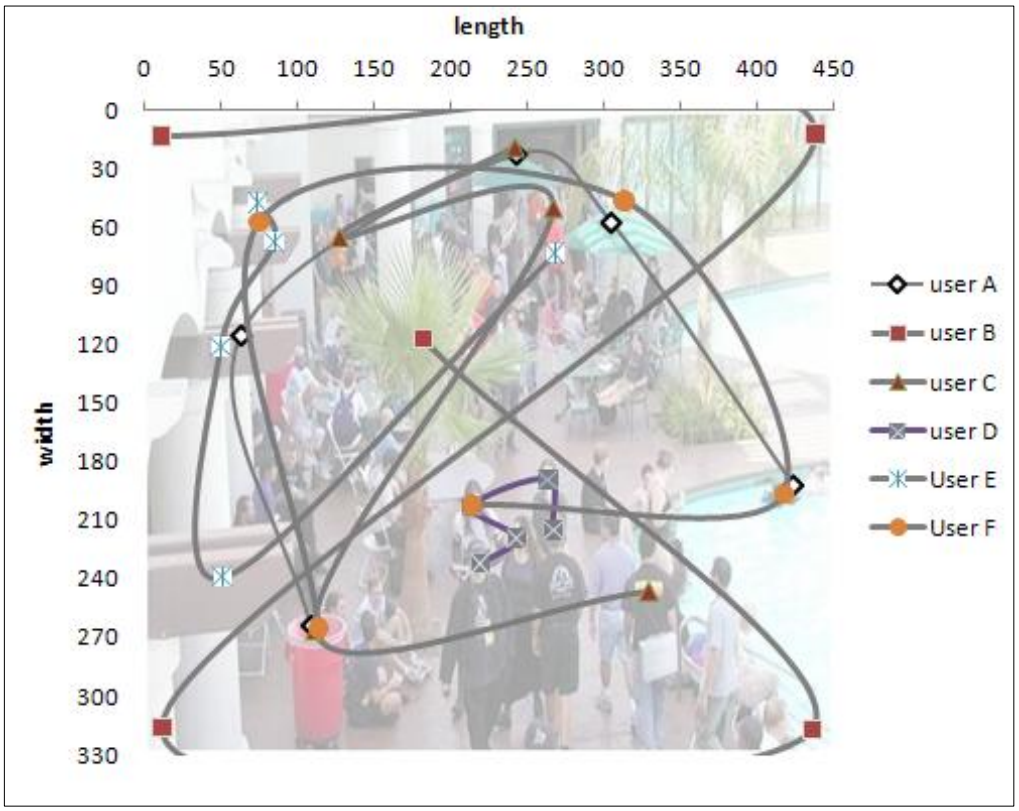

Figure 4-17: Example of secret clicks created by participants

From the distribution of the clicks drawn by the participants, it was found that the shapes of the click-pattern could be mapped into shapes like ‘U or V’, ‘Z or N’ and ‘L’. Here, it is obvious that the majority of them tended to click on recognisable objects (e.g. beams, bin, people faces, etc.) and the forms of shapes created were also straightforward and predictable. Although clicking on recognisable objects and forming straightforward shapes would make it easy to remember their secrets, if these habits continue it is possible to build more dictionaries based upon the users’ click points and click patterns and conduct an attack based on these. Overall, based upon the findings and referring to information entropy of the method, the aforementioned behaviours would make the entropy small and can be considered as less secure since their effective level of security is small.

4.3.2.5 Users’ feedback

For the choice-based method, 36 out of 40 participants agreed that they could remember their chosen images well and they did not have any major problems while carrying out the authentication tasks. Moreover, 27 of them would consider using the method on the web. However, 16 participants felt that the method would be vulnerable if they explained their secret images to others, and 21 of them preferred the themes to appear in a random order during the login (whereas in the trial themes had been presented in a fixed sequence) in order to tighten the security of the method.

For the click-based method, 30 participants agreed that they could easily remember their click points in sequence. During the registration and the login tasks, 23-27 participants rated the method as easy to use while the rest rated the method as difficult (note that no training was provided at the start of the trial; the participant briefing sheet simply presented a brief outline of how both methods worked). For other questions, 23 out of 40 participants would consider using this method on the web, and importantly, the vast majority of them (36 participants) agreed that it would be difficult for others to reproduce their login details if they just explained briefly what their secrets were (i.e. providing a perceived safeguard against social engineering attacks).

Participants agreed that the prototypes were suitable to be used for graphical authentication purposes, the usage of images and text were clear, and considered that the instructions during the trial were concise and understandable. The majority (38 participants) preferred using their own images rather than the images provided in the prototype, as they claimed it would be more memorable. Encouragingly, participants who did not manage to complete their authentication tasks on their first attempt, and rated the click-based method as difficult to use thought that they would perform better if enough training was provided beforehand. Finally, participants preferred using the choice-based method (21 participants) as opposed to the click-based method (14 participants) for replacing username and password authentication; while the remaining participants were 'unsure'. Overall, it could be summarised that all participants provided positive responses regarding the suitability of the prototype for use in web-based environments.

4.3.3 Constraints

This study enables a direct comparison of the usability of two alternative image-based techniques, using the same set of participants and the same set of environment settings.

The prototype used in the study was designed for the IE browser and might have compatibility issues when run in other browsers (e.g. Firefox, Chrome and Opera). In addition, the testing environment was running on the offline 'local host', not in an online web environment.

The recruited participants were those from the academic sector (students, lecturers, etc), had up to seven years IT experience and represented a biased gender balance. To obtain more conclusive results, participants should be recruited from various sectors, having a more varied IT experience and gender, in particular those with less experience such as old people, children and people with learning difficulties.

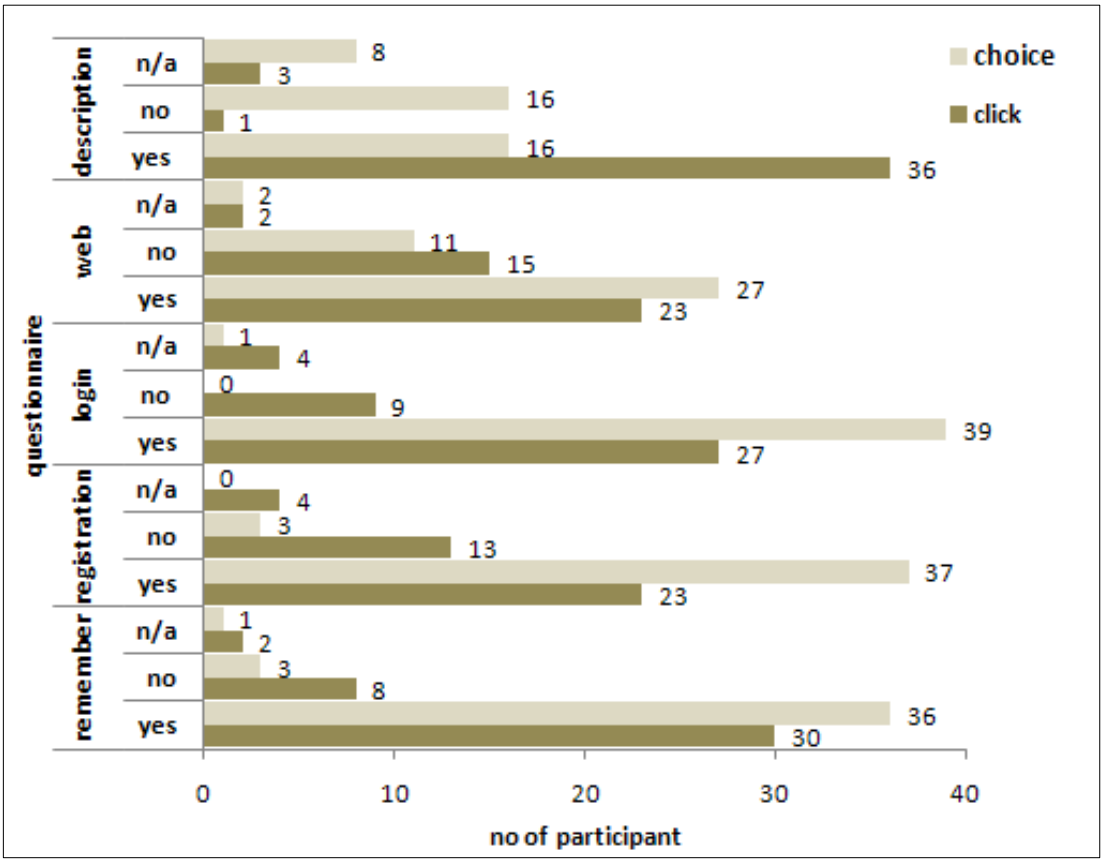

Figure 4-18: Participants' feedback

4.4 Conclusions

With the idea of providing a basis for comparing graphical methods between themselves, this chapter presented two comparative studies. The first comparative study obtained participants perception towards graphical authentication methods (as this technology is new), with the second comparative study empirically measured participants usability performances when they were deployed on the web environment.

From the results and findings based upon 25 participants, it can be suggested that the level of familiarity and awareness towards graphical authentication was balanced; participants preferred the click-based and choice-based methods and they provided contradictory opinions towards the issues of security and usability. The striking finding is that participants rated easy-to-use methods as unsecure and rated secure methods as difficult to use. Based on results and findings of this study, the research proceeded with a

second comparative evaluation to assess the performance of graphical methods within a web-based environment.

With the second comparative evaluation, there are a number of lessons to be learnt. First and foremost, the number of attempts for the click-based method was rather high compared to the choice-based method. This is perhaps due to the nature of the click-based method itself where participants needed to be accurate when clicking on their chosen areas (which they sometimes missed). Second for both methods, participants took longer during the registration (as they wanted to carefully look and choose their images) but then during the confirmation and login tasks, they performed significantly better. Third, participants had chosen/clicked on images or objects that were easy to recognise and formed shapes that were easy to recall, which directly could create hotspot (refers to the area in the image where the participant is most likely to click). Finally, although participants rated the choice-based method as weak, it was still their preferred alternative. This result suggests that participants preferred 'convenience', albeit with an awareness of the 'security' risks.

Although both studies did not found anything new, these studies confirmed that the problems identified were identical to other studies, regardless of the methods, prototypes used and environments itself. To further address or reduce the aforementioned problems, the study proceeded by introducing an enhanced method (explained in Chapter 5).

5. Enhanced Graphical Authentication System

5.1 Motivation

This chapter describes the study to explore the feasibility of combining both the click-based and choice-based methods which provides the novelty of the proposed method. In addition, specific evaluation has been conducted towards authentication strategies with the ultimate aim to find a suitable login mechanism based upon the proposed strategies.

Many GA schemes have been proposed with each of them claiming to be an improvement over their predecessors. However, it was found that to date, no single scheme has been successfully applied as a user authentication technique. This is due to the lack of performance (usability and security) and acceptance of the methods themselves. In an attempt to overcome these, the study proposes a novel scheme known as the Enhanced Graphical Authentication Scheme (EGAS), which combines the click and choice-based methods. The basis for combining both methods is to complement the strengths and weaknesses of both (refer Chapter 4), in order to make authentication using images more secure and usable.

There are two underlying novelties with the EGAS scheme. First, the EGAS scheme gives an opportunity for the user to choose their images (which each image totally independent of the preceding selection) and second, the user is free to choose their preference number of images and clicks as their secrets (i.e. ideal combination which balance between usability and security is reported in the chapter 6). In the EGAS method, the user is required to have two main secrets; comprising ‘images’ and ‘click points’. This means that each user will have to choose a number of images (their secret images) and later click on each image (the secret clicks). These actions (choosing images and selecting click points) are designed to enhance the usability and security of authentication using images.

In terms of similarity to prior research, Chiasson et al. [82] proposed Cued-click Points (CCP) to combine both choice and click techniques. In this approach the user only needs to memorise their secret clicks where the current click determines the next displayed images (all images are pre-assigned and determined within the system). Another variation of CCP is known as PCCP [83], where a method of persuasion (system proposes 'random' areas within the images) is used to enable and encourage stronger secret selection.

Early graphical authentication schemes used an authentication strategy where the user needs to correctly answer all of their secrets. For example, in the click-based method, the user needs to click on all of their secrets, while in the choice-based method the user needs to choose all of their secrets in order to be authenticated. This type of strategy suffers from various security problems such that a user's secrets could directly be observed or recorded by means of surveillance devices. This strategy could also be broken or easily guessed by means of brute-force; dictionary attack and even social engineering (refer to Chapter 3).

As the above approach is believed to be vulnerable, various strategies to remedy this have been proposed. It was found that the majority of these strategies are related to the choice-based method, some of which are described in the following paragraphs.

In the choice-based method, the user will be challenged with several rounds of authentication to identify their secrets. For example in the Passfaces login [139], users are challenged to find their secret at each authentication round. The number of authentication rounds depends on the number of secrets the user has to remember. For instance, if the user has memorised four secrets images, then they will be challenged via four rounds. Other examples of choice-based GA that apply similar ideas are VIP [52], Where-Is-Wildo [48], Passimages [51], ToonPassword [62] and DynaHand [63].

Another strategy for the choice-based method is where the user chooses their secret images but the form of the secrets is changed. Harada et al. [55] discussed a scheme where a user's secret images are transformed and made 'unclear' by means of alpha blending (combining the background image with the foreground) and random noise. During login, the user is presented with a set of 'unclear' images by which they need to choose their 'unclear' secrets, not the original secrets. Other graphical schemes that use a similar strategy are that from Hayashi et al., [94] and Yamamoto et al., [56].

For the click-based method, the user normally has to click on all of their secret click points in sequence order or the number of clicks the user has to click will depend upon system settings. There are a number of login/authentication strategies for both methods, which can be summarised as below:

a) Clicking or choosing images with or without several rounds of challenges.
b) Clicking or choosing a number of secrets out of total secrets.
c) Clicking or choosing the secrets that have been transformed into another form/shape/style.
d) Clicking on the object that is formed by their secret objects ([60] and [61]).
e) Combining with another technique, a 'multifactor' method ([108]).

With respect to the aforementioned strategies, it is anticipated that (a) would be the most unsecure strategy, with (e) would be the most secure. Although (c) and (d) would be considered as secure, however these strategies involve additional task, which sometimes could make the login session 'difficult' to use.

5.2 Methodology

To evaluate the proposed method, a user trial was conducted where participants were asked to use a software prototype and then provide feedback. As with the previous user studies (discussed in Chapter 4), the trial was conducted in one of two ways; participants either came to the experimenter's lab or the experimenter went to the participant's workplace. The software prototype was developed using Microsoft Visual Basic 2008, with Microsoft Access 2007 used for storage. In preparation for usage, participants were given the option of either reading a briefing sheet (see Appendix B, No 2) or listening to a demo. The briefing sheet and demo both highlighted GA in general, intention of the new method and finally what participants would be asked to do.

5.2.1 Software Prototype

At this stage, the EGAS method was purposely designed to suit with the requirement of the user trial itself (see Figure 5-1). Participants had to memorise six images; two of which were randomly assigned by the system (known as 'system-assigned') and four further images (known as 'user-chosen') selected from various sets of themed categories. Once selected the user clicks once on every image to create their secret clicks. Using system assigned images and enabling the user to select one image per category improves the security of the system as research has shown that users' own image selections were weak and predictable [50, 51].

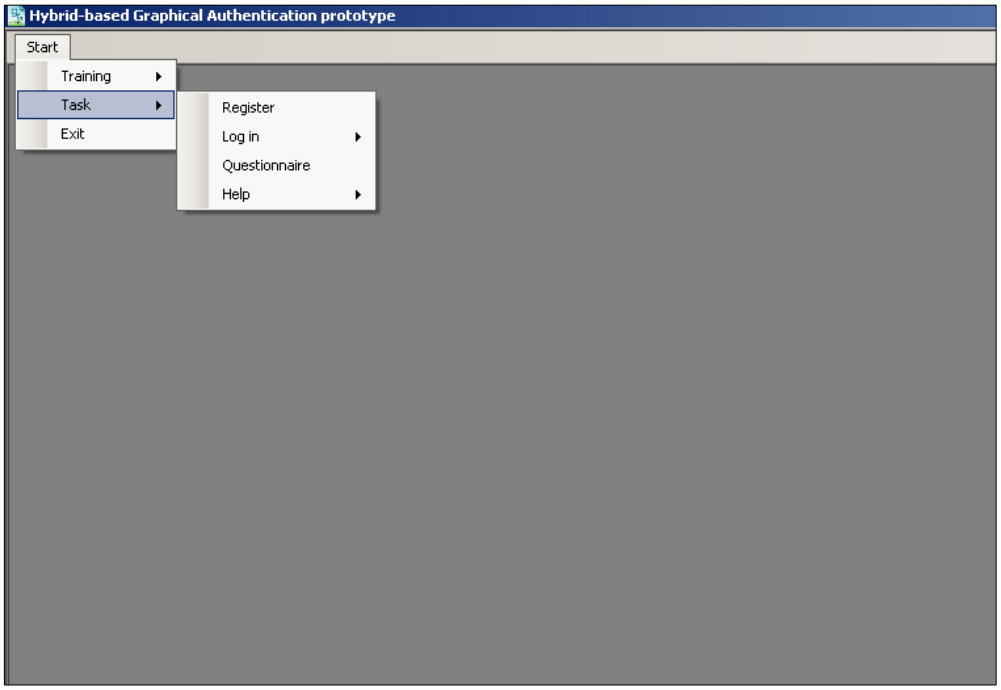

Figure 5-1: Main menu screen from the EGAS prototype

During account creation, participants were able to change their secret clicks or images by pressing the 'restart' button. Users could only change the user-chosen images as 'system-assigned' images were unique to each participant and are planned to be used as a control in the case of secret reset for future development/study. In total, there were thirteen different themed categories (e.g. Animal, Transport, Gadget, Building, Map, Flower, Food, Sport, Abstract, Sign, Children's Toys, People and Miscellaneous) with each category consisting of twelve distinct images (see Figure 5-3). These categories were chosen as they represented everyday seen images which were recognisable and memorable. As this was an initial prototype, system-assigned images were selected within these categories/themes. Each image was displayed at a 200x200 pixel resolution with an acceptable tolerance of 19x19 pixels around the click point. Although research has suggested that using a smaller tolerance is acceptable [45] and would enhance security, it was decided that larger tolerances should be used to enable further evaluation and justification of the clicking accuracy. Below are the steps each participant needed to follow when creating an account (registration and confirmation):

a) Insert memorable username.

b) Memorise system-assigned images and then click to create the secret clicks (see Figure 5-2). Participants were required to memorise two system-assigned images (as it believed could still be remembered/memorised by participants), which were randomly generated from the image pool within the software prototype.

Figure 5-2: System-assigned images screen from the prototype

c) Choose four images from the available themes/categories (user-chosen images, see Figure 5-3). To enable fair image selection, participants were only allowed to choose one image per category. This was done by disabling themes that they already choose.

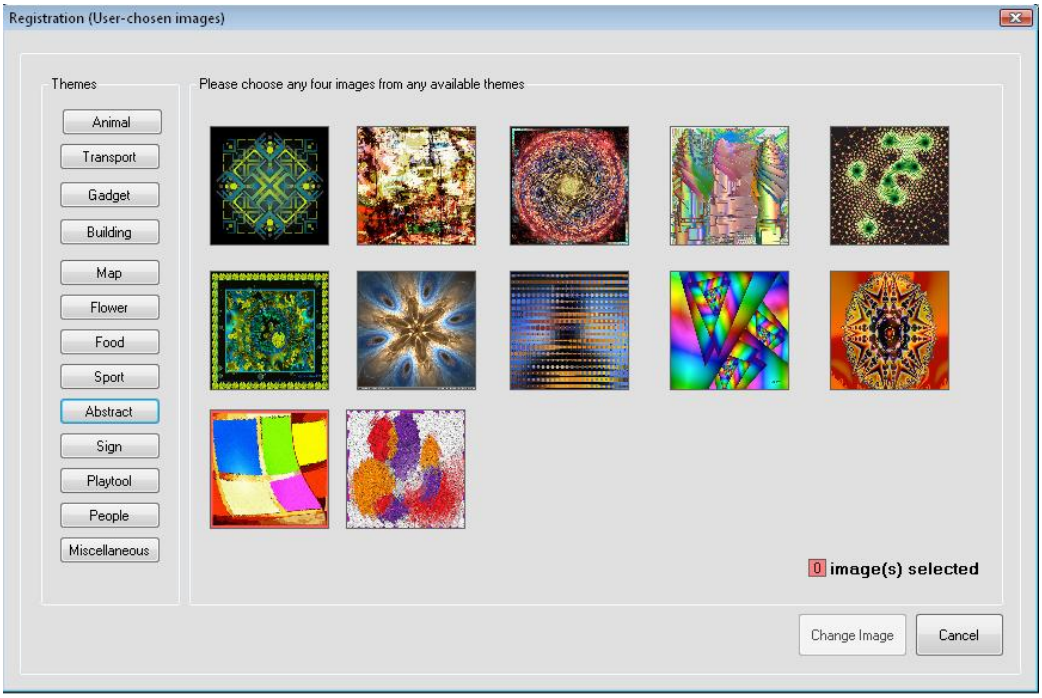

Figure 5-3: User-chosen images screen from the prototype (showing Abstract theme)

d) Create secret clicks for the user-chosen images (see Figure 5-4). Here, participants were asked to click once on each image.

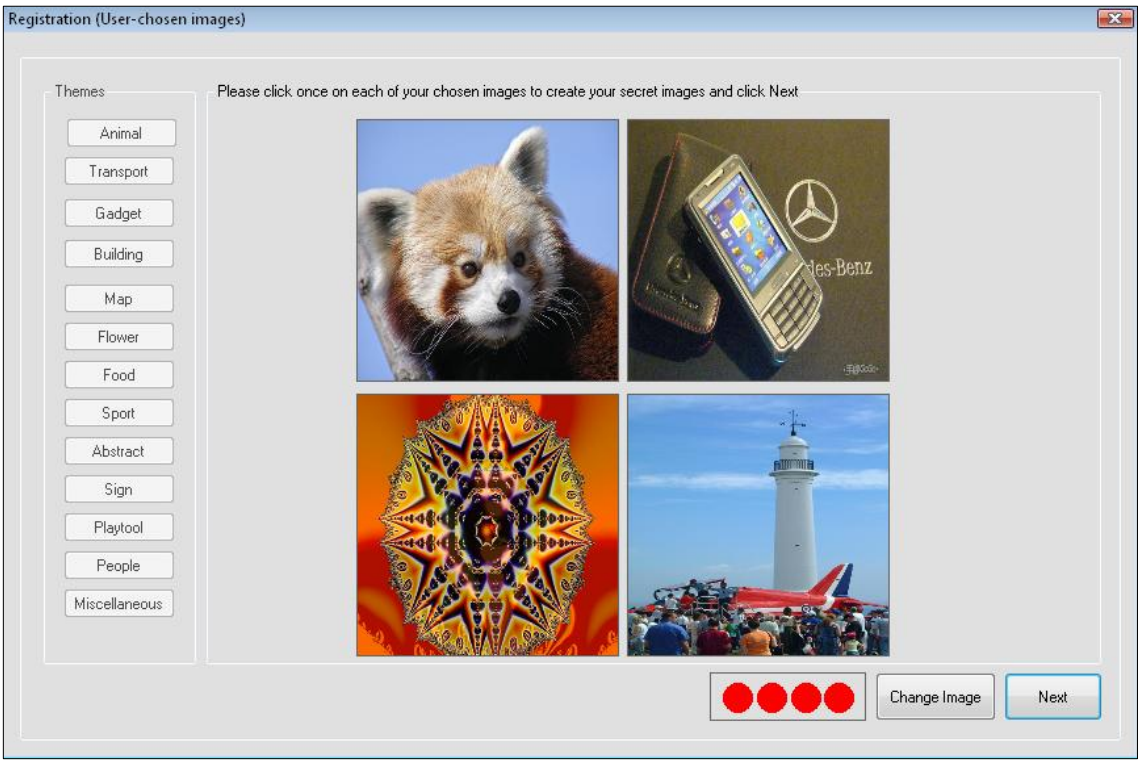

Figure 5-4: Example of images chosen by the participant

e) Confirm their registration by clicking on the same spot for their entire secret images (see Figure 5-5). In the case of participants failing to register, they were allowed to redo it by pressing the 'restart' button.

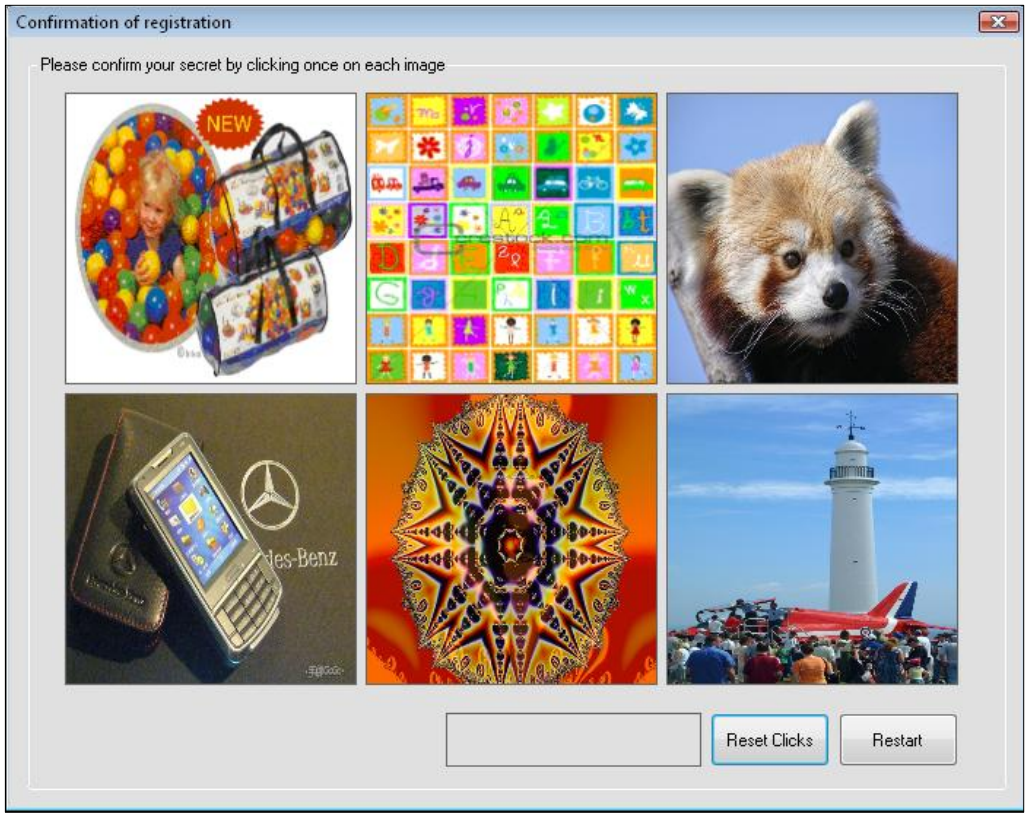

Figure 5-5: Confirmation screen (displaying both system-assigned and user-chosen images)

It was predicted that displaying all the users' secret images during login would make it less secure and adding extra measures like challenging the user to identify their secret images together with decoy images would take longer time. As EGAS combines both click and choice-based methods, it is assumed that any authentication strategy that suited either click or choice-based methods would be suitable for implementation. Based upon the reading on literatures (e.g. graphical passwords and password-based authentication), this study investigated the following login strategies.

a) User will be challenged to identify their secret images within decoy images.

b) User should be challenged for several rounds.

c) At any login session, the user will be challenged with a random number of secrets, never using all their secrets in a single session.

By applying the above strategies, it was anticipated that the login mechanism for EGAS should be more secure and at the same time metrics such as timing, accuracy and memorability should be similar or better than the existing login methods.

To simulate and test the above strategies, the study tested four scenarios. The differences between each scenario were the number of images displayed at each authentication round and the number of rounds presented to users (Table 5-1). In each scenario, participants were presented with both decoys and real secret images (each of which need to be clicked on). Clicking on all images (decoy and real) would make login/sign-in more secure since only the registered user knows the secret and accordingly, making it more difficult for an observer to guess a users' secrets. All decoy images were obtained or generated from a similar set of images during account creation.

Scenario	Number of images per round	Total rounds	Total images (decoy + secret)	Entropy estimation (bits)
One	1	8	8	Image size, i = 200x200, Tolerance, t = 19x19 Clickable areas, c = i/t = 110 Total secret image = 6 Image selection:- 6 * ($\log_2$ 8 or 9) = 18 or 27 Click selection:- 6 * ($\log_2$ 110) = 40.69 Total entropy (40.69+18 = 58)
Two	2	4	8	
Three	3	3	9	
Four	4	2	8	

Table 5-1: Proposed login scenarios used in the study

The authentication was considered successful when participants correctly click on all of their secret images. At each login session, a minimum of four user secret images (randomly generated) together with at least four decoy images were presented (see Figures 5-6 to 5-9 for examples of screenshots for each scenario). In Figures 5-6 to 5-9, the red circle indicates the number of images that participants needed to click, with the green circle indicating the number of images already clicked by the participants. Using only four of users secret image would lower the entropy, however it is anticipated that the strategies would still provide effective level of security as randomness of user secret images were used.

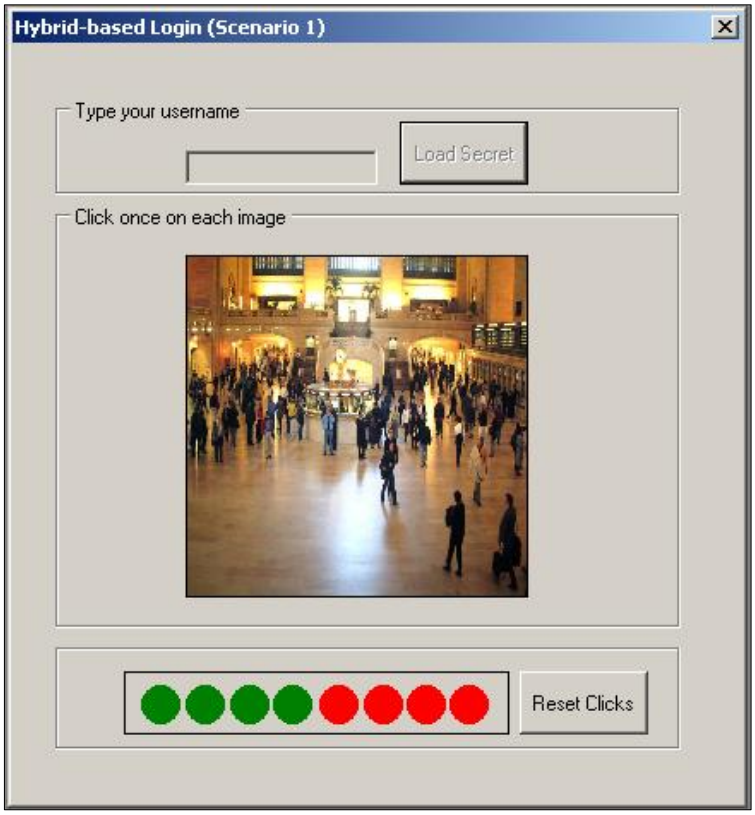

Figure 5-6: Interface of the Login Scenario One

Figure 5-7: Interface of the Login Scenario Two

Figure 5-8: Interface of the Login Scenario Three.

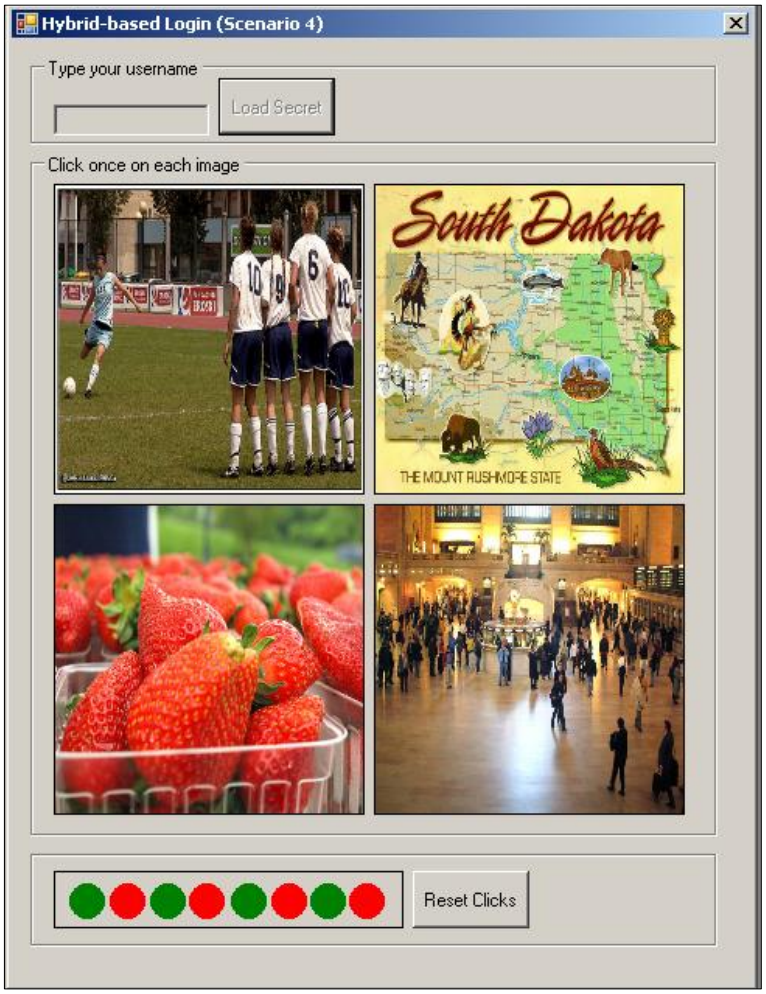

Figure 5-9: Interface of the Login Scenario Four

5.2.2 Questionnaire

After completing the scenarios, participants were asked a number of questions, which were divided into two sections. Firstly, four questions were asked covering demographic information (specifically gender, age, education level and experience using GA) and secondly, fourteen questions covering the ease of use during account creation, the ease of use for each of the scenarios, preference of sign in method and ease of use of the prototype itself. To further captured users experience, the 7-point scale was used by which all of the questions would need to be answered within the prototype. A copy of questionnaire can be found in the Appendix A, No (3).

5.2.3 Procedures and Steps

All participants were recruited via an open call for volunteers. The targeted participants were contacted via email and face-to-face conversation. The study gave an incentive of GBP10 each for five lucky participants who completed the tasks straightforwardly (i.e. those who can register their account without failed attempts). Below are the tasks each participant was asked to undertake:

a) Create an account by entering their username, choosing secret images and selecting secret click points. Both registration and confirmation tasks need to be successful in order for the account to be recorded into the system and move to the next task.
b) Log in to the system using four different proposed scenarios, with no restriction enforced on the number of login they were allowed to.
c) Answer questionnaire.

The software prototype recorded participant username, list of images and areas of click selected, timing, and answers from the questionnaire as well as details of login attempts for each scenario. All of these were used as the usability performance evaluation and are reported in the next section. This study only considers participants' short-term performances; therefore no longitudinal study was conducted. However, it is suggested that future study should consider long-term performances, in order to enable comparison of performances of both (i.e. short-term and long-term).

5.3 Results and Analysis

Thirty (30) participants from the University of Plymouth participated in the trial, all of whom were volunteered from different departments. There were 20 male and 10 female participants with an average age of 31 years. From the questionnaire, 21 out of 30 participants stated that they had no previous

experience using graphical authentication, with the remaining 9 previously involved in the user trial conducted in [124]. As the proportion of experienced participants was relatively high, their experiences (using other graphical schemes) are actually valuable to judge and evaluate the merit of the new approach.

It can be reported that 19 participants went through the trial within their workspace, with the remaining participants came to the experimenter's lab. It is expected that the obtained results will not give obvious implication as they used similar testing materials (i.e. laptop equipped with wireless mouse, etc.). The results and analysis section is divided into two; usability performance of the method itself and feasibility of the authentication strategies with different login scenarios.

5.3.1 Usability performance

This section discusses the number of attempts made by participants, time took to create their account, their level of accuracy during both registration and login, identified patterns as well as their feedback and suggestions.

5.3.1.1 Number of attempts

All 30 participants managed to create their account successfully. Overall, the system recorded 34 usernames of which 4 were incomplete. Investigation revealed that 3 participants had to change their usernames, with one participant needing two usernames before they were successful. This was due to their difficulty clicking consistently within the same spot precisely as they were unable to understand how the technique worked. Once they were more familiar with the technique, they managed to create their account without further problems.

During the confirmation phase, 19 participants managed to register their account in a single attempt and 5 participants managed to register with only two attempts. 2 participants needed three attempts and 3 participants needed four attempts to complete their registration. It was found that participants who needed more attempts registering their account were actually having difficulty clicking on the same spot rather than forgetting their click areas.

5.3.1.2 Timing

The time taken to login was recorded in order to calculate participants' performance when using the prototype. Image selection time was measured when participants started to click on their secret clicks for system-assigned images up to the last secret clicks for their user-chosen images. In addition the account creation time was recorded and the total time needed for each participant during account tasks. The confirmation time was recorded when participants clicked to confirm their registration details. Table 5-2 illustrates the time in minutes and seconds (shortest, longest, mean and median) for all participants during account creation (image selection + confirmation), image selection and confirmation.

From Table 5-2, it can be seen that one participant was able to create their account within 90 seconds. Further investigation found that this participant was actually quite familiar with graphical authentication methods. During account confirmation, participants were quite good when they recorded 12 seconds and 23 seconds for the fastest and median time respectively. On average, it was found that participants took 220 seconds (3 minutes 40 seconds) to create their accounts with 151 seconds (2 minutes 31 seconds) and 25 seconds needed for image selection and confirmation respectively.

It can be seen that different participants took different time to register themselves into the software prototype. Hence, it can be concluded that differentiation of registration time were due to their competency, which has direct relationship with their level/experience of using technology (i.e.

computer). It can also be concluded that the time is outperformed as compared with the traditional password authentication, however since participants needed to browse through images and then creating secret click on their secret images, it is anticipated that the registration time is still acceptable (i.e. based upon the informal voice feedback of the participants).

	Account creation	Image selection	Confirmation
Shortest	1m 22s	41s	12s
Longest	12m 45s	8m 16s	50s
Mean	3m 40s	2m 31s	25s
Median	2m 54s	2m 12s	23s

Table 5-2: Account creation Time

5.3.1.3 Clicking accuracy

Clicking accuracy looks at the users' ability to click within the allowable tolerance to identify possible weaknesses and suggest appropriate measures to solve the problem of clicking. Figure 5-10 shows the distribution of click areas for all participants during registration (image selection) and confirmation (considering only successful attempts, n=180).

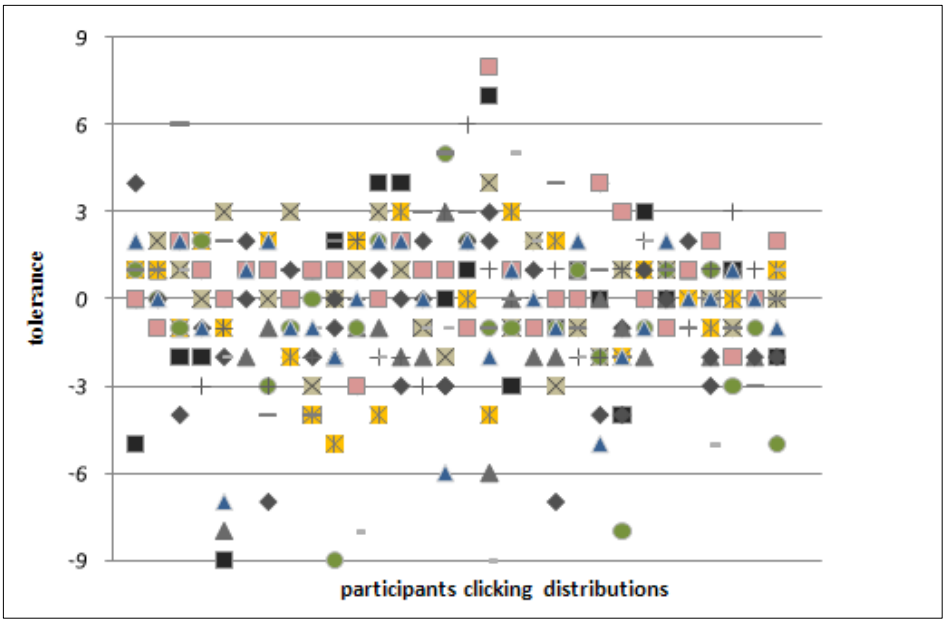

Figure 5-10: Participants' clicking distribution during account creation

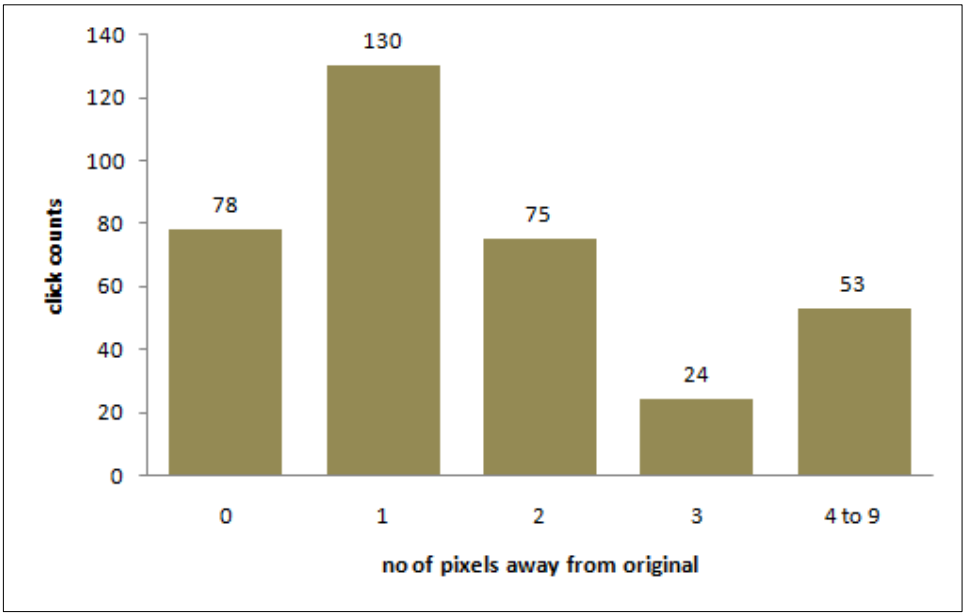

Figure 5-11: Frequency of accuracy

Figure 5-11 displays the accuracy (difference between the click during confirmation and the click during registration) based upon total clicks. 360 clicks were recorded (12 clicks x 30 participants) and it can be seen that more than half of the total clicks are within 0 to 3 pixels away from the original click.

From these two figures (5-10 and 5-11), it is found that the majority of the participants had clicked between the ranges of -3 to 3 or specifically within 3 pixels of the original click points. It can be concluded that participants were accurate within 7x7 pixels (note that the study used a tolerance of 19x19 pixels). These results are comparative with the data obtained in previous user trials in [124] and supports earlier research in [45].

5.3.1.4 Pattern

This section reports participants' image preferences and their click areas. The intention was to identify or look for possible patterns and suggest appropriate methods to eliminate or reduce the identified patterns. The steps used to investigate the users' image selection are:

a) Frequency of the most popular themes chosen by users is calculated.
b) For the most popular themes, the most popular image is determined.
c) Identify participants' click areas towards popular images.
d) Determine and investigate the click patterns and hotspot occurrences.

As the system only permitted participants to choose one image per theme, the possibility of choosing images within a similar theme was eliminated. Table 5-3 shows that the Animal and Flower themes were the most selected themes/categories, with themes such as Sports, Transport, Gadget and Building were also well-liked, whereas Abstract, Map and Misc themes were the least popular.

Theme	No of Participant	Male	Female
Animal	17	8	9
Flower	17	7	10
Gadget	15	13	2
Transport	14	11	3
Sport	13	8	5
Building	10	8	2
Food	9	4	5
Sign	6	3	3
Children's toys	6	5	1
People	5	3	2
Abstract	4	4	0
Map	3	0	3
Miscellaneous	1	1	0

Table 5-3: Participants' image selection

Further investigations were carried out to look at the relationship between participants' theme selections with gender. In general, it could be revealed that all 10 female participants chose the flower theme (which was relatively unpopular with males), whereas two-thirds of males chose gadgets (one of the least popular themes with females). Therefore, it could be deduced that there is some clear gender-bias in the choice of themes, which resulted in a level of predictability. As the themes like animal, sign, food and sports are well-liked among both genders, it is suggested that these themes can be used as they can help to reduce gender bias selection.

Given that participants had to create one click per image and each image is distinct, initial analysis found that participants tended to click across the entire image and not in any obvious 'hotspot'. 'Hotspot' in this case refers to the area in the image where the participant is most likely to click. To confirm this, an analysis of a number of popular images for each theme was conducted and the results (showing the four most popular themes) are shown in figures 5-12 to 5-15.

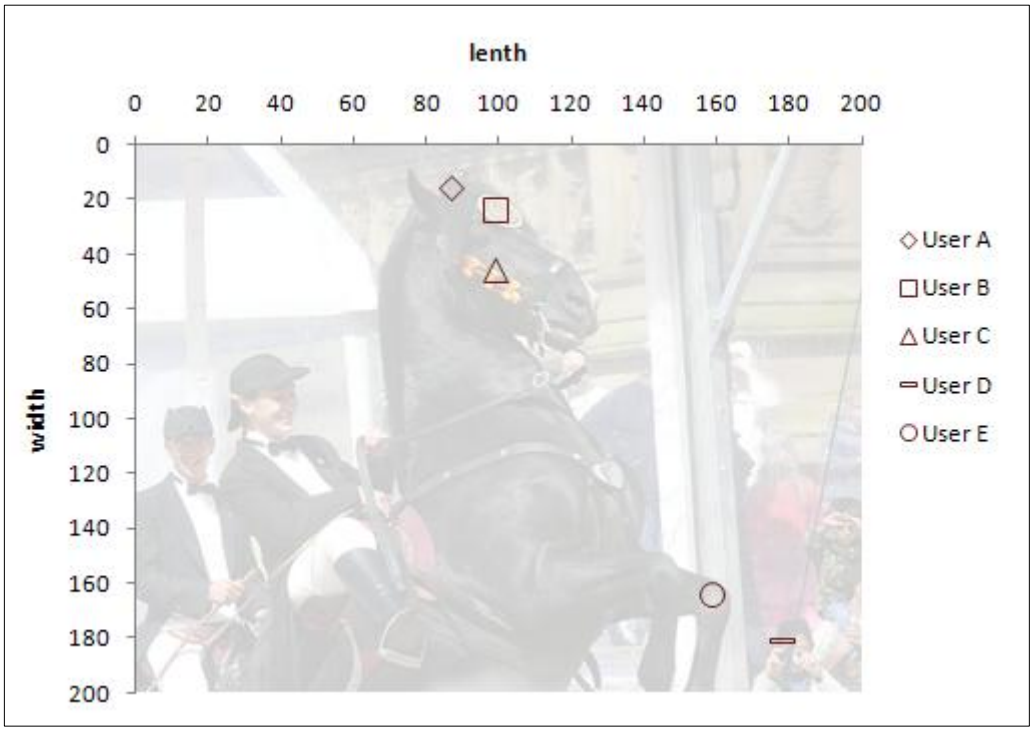

Figure 5-12: Image popular for animal theme

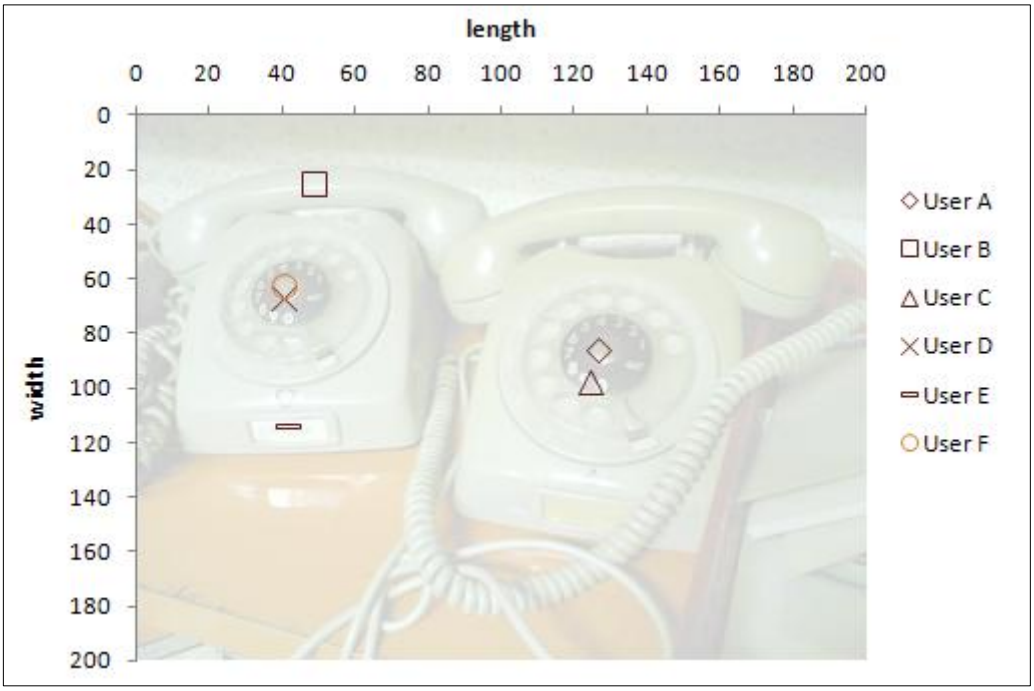

Figure 5-13: Image popular for gadget theme

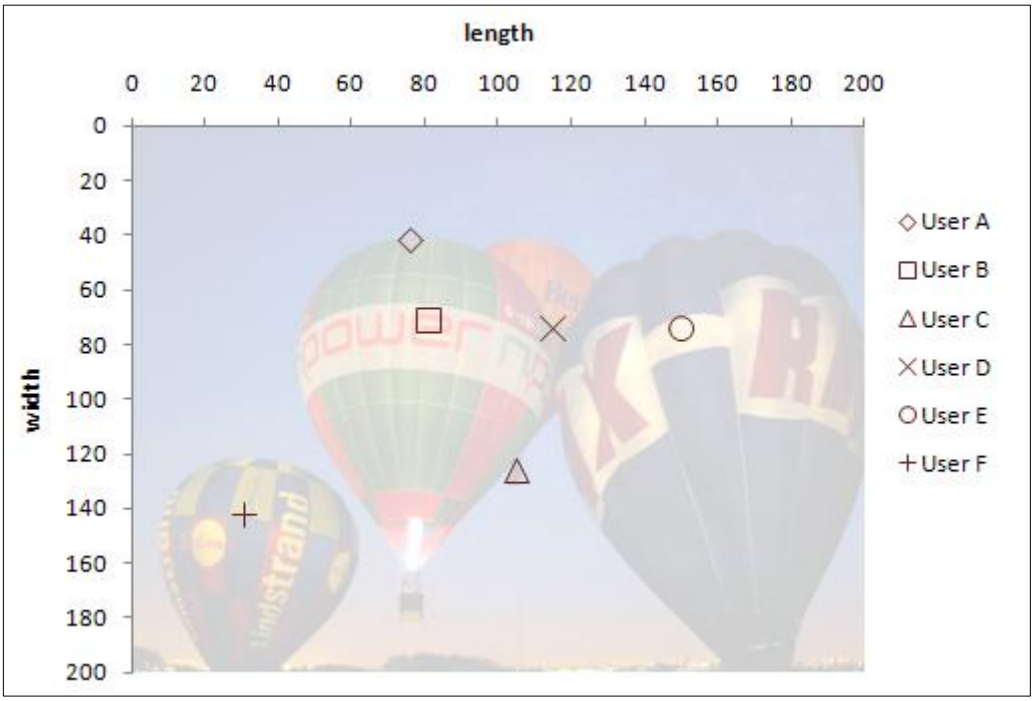

Figure 5-14: Image popular for sport theme

Figure 5-15: Image popular for transport theme

Regarding images assigned by the system (system-assigned) to each participant, it could be said that the prototype system did a good job of assigning random different images from different categories/themes. However analysis towards users' clicking areas has shown discouraging results where although it was

found that participants tended to click everywhere, their clicks were centralised or focused upon striking/identifiable objects which made them guessable and predictable. Specifically, they had created hotspots by clicking on the same spot (refers to figure 5-15) or clicking on the same area (refers to figure 5-12 and 5-13).

5.3.1.5 Users' feedback

This section reports general observations and experience while conducting user trials, user feedback, comments on the technique itself and finally results from the questionnaire.

a) General observations

I. Half of the participants opted not to read the briefing sheet as they found it too long. As an alternative, they watched the demo.
II. Only four participants went through the training phase – the majority of them felt that the demo was enough for them to start the trial.
III. It was found that inexperienced participants (those who did not have previous experience using graphical authentication) gave the impression of being confused at the beginning of the trial. Later, once they went through the trial and became familiar with the technique, their face changed dramatically, they enjoyed using the technique and gave positive feedback.
IV. Only three participants browsed all of the themes before deciding which secret images they wanted to pick. The majority of them were just choosing the first categories in the list such as Animal, Building, Gadget and Transport.
V. Two participants had user-chosen images similar to the system-assigned images. However, they did not create similar patterns for their secret clicks.

VI. During login task, majority of inexperienced participants spend longer time on their secret images as compared to decoy images.

b) User comments

I. "Initially, I'm worried but once done it, I enjoyed and like the approach" (User A).

II. "I think by giving user a chance to choose his own images could make the technique more useful and easy to remember his images" (User B).

III. "I believe clicking twice for each image could enhance security as people who wanted to steal my passwords would confuse the real one" (User C).

IV. "I do not like simple and bright images" (User D).

V. "I prefer clicking in the middle of each image as I find it easy to remember" (User E).

The above feedback ultimately gives an insight into the participants' perceptions during the trial. Feedback from User A directly suggests participant satisfaction when using the scheme and that improvement could be made (Users B to D). With respect to User E, it appears that their secret clicks could be guessed easily (as they created patterns) and therefore, in order to combat or eliminate this type of 'insecure user' practice, a level of system control is needed.

c) EGAS Scheme

Participants who had experience in the previous GA user trial felt that the new method could improve existing techniques, while inexperienced participants felt that the EGAS scheme was a viable approach. However, a number of participants expressed their uncertainty about how they were going to remember their secret images in the future if they had multiple graphical images.

To investigate this uncertainty, a further study was conducted two weeks later where 10 randomly chosen participants were invited to do the trial for the second time. The idea of asking participants to redo the trial was to look at their memory performance. The aim of this was to determine how many secret clicks each participant could remember and what types of images they were able to remember.

In the trial, the prototype system displayed the participants' secret images (provided they entered a valid username) and later, they needed to click on their secrets. The number of clicks for each secret image and times were captured and brief outcomes are described below.

With **system-assigned** images, 6 out of 10 participants managed to click correctly on both of their images without any problem. Three participants guessed their first image immediately and later, needed 4-7 attempts to correctly click on the right spot/area for their second image while the remaining participant had to guess twice and more than fifty times for their first and second images respectively.

For the **user-chosen** images, it can be revealed that only 2 participants managed to click correctly on all of their secret images, with the other 7 participants managed to recall their first three images easily while needing between two to five guesses before correctly click. It can also be reported that the participant who had difficulty guessing his system-assigned images performing significantly better. For the result about time, figure 5-16 shows participants' time in seconds (slowest, fastest and average) for the second trial.

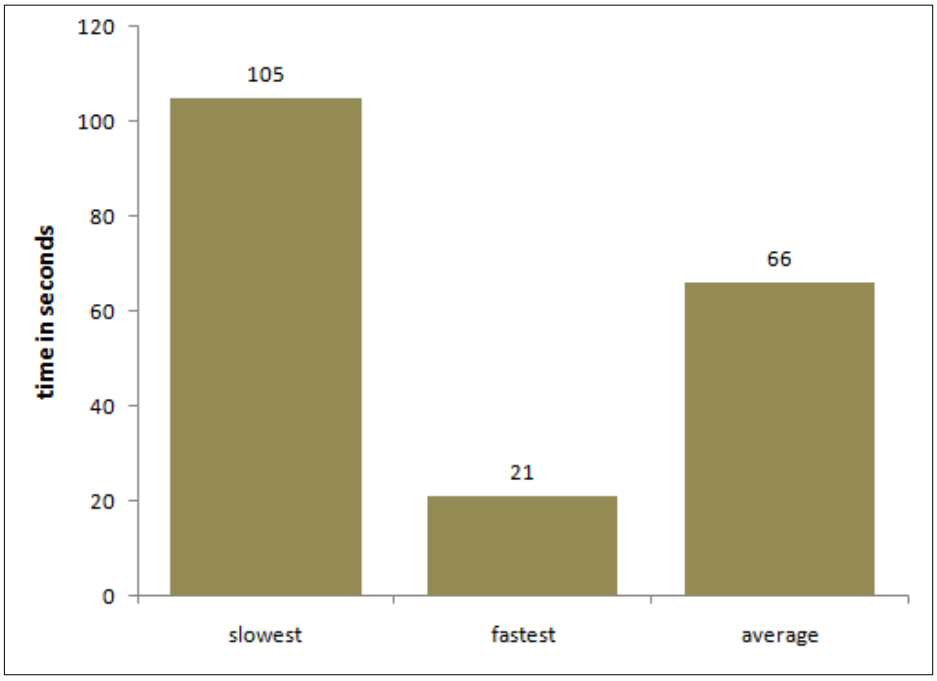

Figure 5-16: Timing for second trial

It was expected that system-assigned images would be less memorable when compared with the user-chosen images due to the nature of selection, however the trial showed that participants' had a greater ability to recall system-assigned images. It was also found that more attempts were needed due to the participants not clicking within the allowable tolerance and finally, with respect to duration, participants performed considerably well, considering the duration between first and second trials.

d) Questionnaire results

Statements	Mean Score
I believe I can remember my secrets (click and choice) well	2.3
Account creation tasks were easy and understandable	1.9
The level of 'ease of use' during account creation	2.2
The design of the interface and instruction were understandable	2.0
The size of images was appropriate/just right	2.6
The messages were helpful and clear	2.0

Table 5-4: Questionnaire results for account creation task

With respect to the 7-point scale, values ranged from 1 indicating strongly agree to 7 indicating strongly disagree. Table 5-4 shows questions/statements asked with their average scores.

5.3.2 Feasibility of the authentication strategies

This section discusses the results of evaluating authentication strategies towards the EGAS method, with specific focus upon the safety and viability of the method itself.

5.3.2.1 Guessability

Guessability is a measure of the probability of correctly predicting the correct responses/interactions required to successfully authenticate. The guessability is the equivalent of a traditional password's "key space" i.e. the number of characters in the password multiplied by the range of allowed password characters/symbols. For example in the 'Passfaces' scheme by Brostoff and Sasse [139]; guessability can be measured if information such as the number of authentication/login rounds, the number of target images (real secret images) need to be chosen at each round and the number of decoy images (non-real secret images) used are known beforehand. Table 5-5 highlights the guessability calculation for a number of graphical schemes including EGAS.

Graphical Scheme	Guessability prediction
Passfaces [139] Authentication round = 4 (9 images per round) Target = 1 image per round Decoy = 8 images per round	1/9 * 1/9 * 1/9 * 1/9 = 1 in 6561
VIP [52] Authentication round = 1 (10 images in total) Target = 4 images Decoy = 6 images	1/10 * 1/9 * 1/8 * 1/7 = 1 in 5040
Passimages [51] Authentication round = 4 (25 images per round) Target = 6 images Decoy = 94 images	1/100 * 1/99 * 1/98 * 1/97 * 1/96 * 1/95 = Approx 1 in $8.6x10^{11}$
Passpoint [43] Authentication round = 1 Target = 5 clicks Decoy = none Image size, I = 450x330 Tolerance, T = 20x20 Password space = (I / T) ~ 371	1/371 * 1/370 * 1/369 * 1/368 * 1/367 = 1 in $6.8x10^{12}$
EGAS scheme (choosing image) Authentication round = 8 Target = 4 images Decoy= 4 images EGAS scheme (clicking on image) Target = 4 clicks Decoy = 4 images Image size = 200x200 Tolerance = 19x19 Password space = ~110	1/8 * 1/7 * 1/6 * 1/5 = 1 in 1680 (assuming the user only needs to identify 4 secret images and secrets are random chosen) 1/110*1/110*1/110*1/110= Approx 1 in $1.5x10^{8}$ (assuming the user needs to click on both real and decoy images)

Table 5-5: Guessability predictions

5.3.2.2 Login attempts

It was found that in each scenario, 26-28 participants took only one attempt to login into their account. The highest number of attempts recorded for login scenario one, two, three and four were 3, 3, 5, and 9 respectively, with all of these for different participants. The results suggest that mixing participants' secret images together with decoy images and randomly challenging participants with their secret images and clicks seemed to make no difference towards their recall performance.

5.3.2.3 Timing

For each login scenario, the time was calculated when participants clicked on the first image until the last image. Figure 5-17 shows the time in seconds (shortest, longest and mean) needed to login for each scenario.

From Figure 5-17, it is found that one participant managed to login in less than 10 seconds. Overall, it could be summarised that login scenario four has the most 'suitable' login time with average time of 23 seconds. Increasing the number of challenge rounds did not have any effect on login scenarios two, three and four but slightly increased the time taken for scenario one.

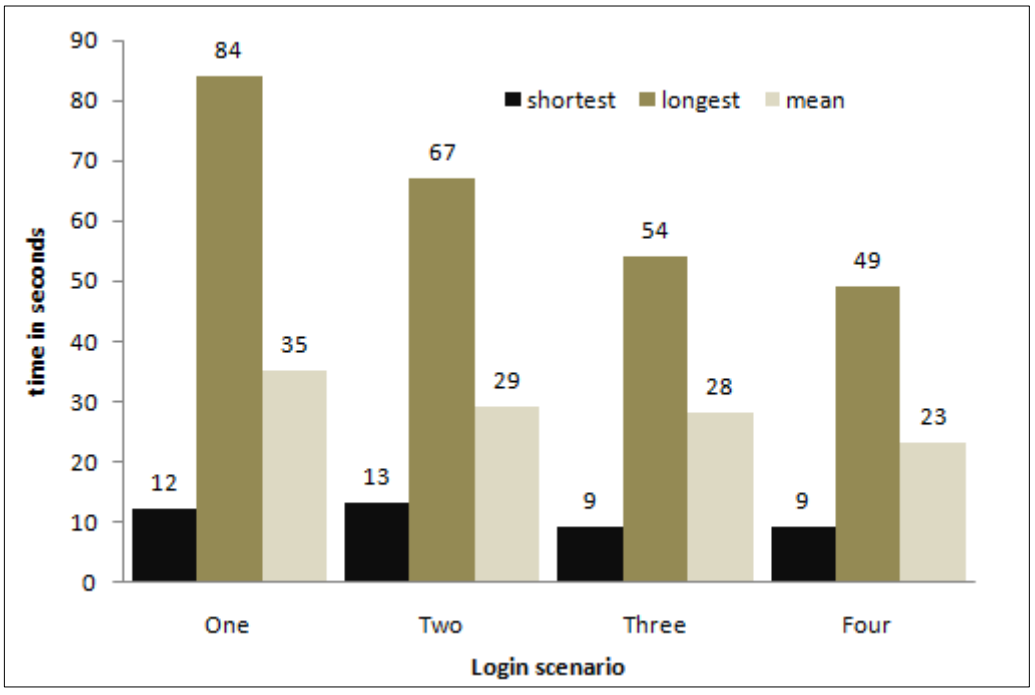

Figure 5-17: Login Time for each scenario

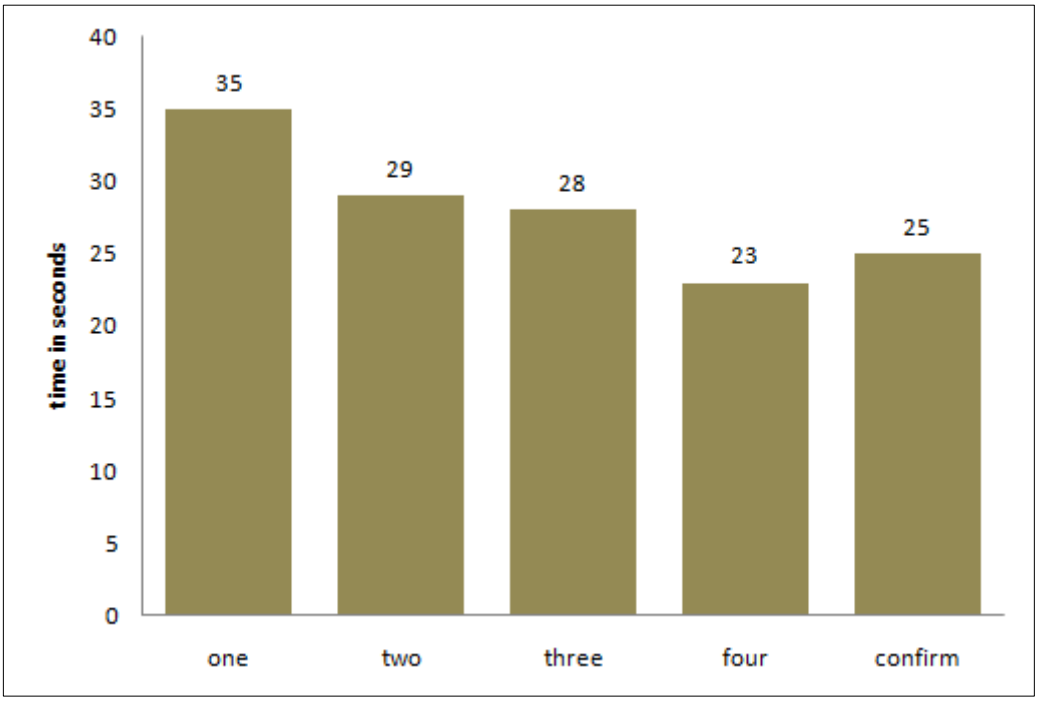

Figure 5-18: Comparison of the login time between scenarios with the confirmation task

As the study did not measure the exact time needed for participants to login using all of their secrets, it was decided to compare participants' login time with the confirmation time (as the confirmation task is similar). Figure 5-18 compares the average time (in seconds) of confirmation with the login times of the proposed scenarios. It can be concluded that the time-to-authenticate was very similar across all scenarios, but scenario four was slightly faster than the others. However, it could still be deduced that the time is far longer when compared with the traditional username/password-based authentication (which can take just a few seconds if the user is a competent typist and makes no mistakes).

5.3.2.4 Users' feedback

Statements	Mean score
Login tasks were easy and understandable	1.8
Ease of use for login Scenario One	1.8
Ease of use for login Scenario Two	2.0
Ease of use for login Scenario Three	2.0
Ease of use for login Scenario Four	2.1

Table 5-6: Questionnaire results for login task

When asked what their preferred login scenario was, 10 participants' preferred using scenario one, 8 participants' preferred scenario four and 5 participants each preferred using scenarios two and three during login. In contrast, only 2 participants indicated they were not going to use the proposed login scenario as they preferred to be challenged by all of their secret images.

With regard to clicking preference, 15 participants preferred to click once on an image while 12 of them preferred multiple clicks. When asked the maximum number of preferable multiple clicks, they answered between 2 to 3.

When asked which scenario was perceived as the most secure, half of the participants (17) rated scenario four as the most secure as they thought it was difficult for an observer to guess a users secret when many images were displayed at one time. Six participants rated scenario one as the most secure with scenario two having the lowest rating.

5.4 Constraints

This study assessed the feasibility of combining both the click-based and choice-based methods by introducing an enhanced method known as the Enhanced Graphical Authentication (EGAS).

The obvious constraint with this study was the number of recruited participants. In addition, a fully functional and deployable software prototype was not properly built, as the software was designed to suit with the testing environment. Therefore, to obtain convincing rather than indicative findings, it is recommended that the technique is used with a larger population and that modifications and

enhancement should be undertaken. Also with respect to combining graphical methods, it is believed that there are significant opportunities for future study and research.

5.5 Conclusions

This chapter presented a study to evaluate usability performance when two graphical authentication methods (clicking on image and selecting from a set of images) were combined. Elements such as the number of successes and failures during account creation, time taken, pattern of secret clicking and choosing secret images as well as user preference were investigated and reported. As a conclusion, it is suggested that the method of clicking on images and choosing a series of images can be combined effectively, without significant impediment to users. However, although the results have shown that memorability was maintained, users' clicking accuracy was high, timing was reasonable and users' preference were positive, the trial had also found serious problems. Specifically, participants tended to choose similar and predictable images, thus creating 'hot-images' and participants also tended to click on guessable objects and predictable areas, thus creating 'hotspots' (both are well-known weaknesses with the underlying techniques).

In addition, suitable authentication strategies were investigated, with the number of successes and failures during login, time taken and user preferences presented. Three authentication strategies were evaluated; identifying secret images together with decoy images, multiple rounds, and random numbers of secrets. To simulate these strategies, four scenarios were created with each scenario differing in terms of the number of images and rounds presented. It was found that the participants' level of recall of their secret images and their level of accuracy clicking within the allowable tolerance were still maintained. Based on a number of criteria (login time, security rating by participants, preference rating, ease of use and the balance between security and usability), it is suggested that scenario four is the best approach to be used as the main login mechanism for EGAS (in the case of using one click per image).

Factor	Criteria	Level	Graphical Methods		
			Click	Choice	EGAS
Security	Info Harvesting		Yes	Yes	Maybe
	Guessable		No	Yes	No
	Breakable		Yes	Yes	No
Usability	Users' Perception		Yes	Yes	Yes
	Memorability		Yes	Yes	Yes
	Repeatability		Maybe	Yes	Yes
	Extra hardware		No	No	No
Applicability	Type of IT system	Online	Yes	Yes	Yes
		Offline	Yes	Yes	Yes
	IT system criticality	High	No	No	Yes
		Medium	Yes	No	Yes
		Low	Yes	Yes	Yes

Table 5-7: Comparison of current graphical methods with the EGAS

Table 5-7 compares both click-based and choice-based methods with the EGAS. With respect to the comparison factors originally used in the Table 3-2, it can be said that the EGAS method would be better than both click-based and choice-based methods, and as comparable as with other hybrid-based methods.

In an attempt to reduce problems pertaining to the introduced graphical method, the study proceeded by improving the design of EGAS and introducing advice and guidance to the user before they started to choose their secret. This is the focus of the discussion in Chapter 6.

6. Enhanced Graphical Authentication System: Further Evaluation

6.1 Motivation

This chapter discusses further evaluations that were conducted to assess the ease of use of the proposed method. The evaluations cover ideal number of clicks and images, effect of using smaller tolerance as well as users' perception towards Graphical Password Guidelines (GPG) which could be introduced before they started to select their secrets during registration.

With respect to security, the main issue with the choice-based method can be referred to as the 'hot-image' problem, and the click-based method can be referred to as the 'hotspot' problem. A hot-image happens when a similar image is selected by many users. This problem could also occur when users choose similar categories/themes or through gender preferences (e.g. males choose cars and females choose flowers). The hotspot problem could occur in two conditions. Firstly, the user clicks within the same or similar point on the given image or clicks on the same point or area when two or more images are given. Secondly the user produces predictable shapes such as straight lines and clicks on obvious/predictable objects within the image

Reducing the aforementioned problems and at the same time maintaining memorability, many studies have been published with regards to the impact of using various types of images, as well as using persuasive techniques (refer Chapter 3) . Motivated and influenced by the persuasive technique, the study investigated the impact and viability of giving tips or advice to the user before they start choosing their graphical secrets. It was conjectured that users will choose so called 'safe' graphical secrets if they obtain enough information about the necessity of creating safe secrets (creating less predictable and guessable secrets). Before the study started, two preliminary investigations were carried out to survey the level of usage and practice of password-based authentication guidelines (i.e. as no graphical guidelines were found); with the following paragraphs reporting the findings.

The first investigation was to review and survey literature related to password guidelines. Password guidelines from a number of major organisations (e.g. Goggle [142], NIST [143] and Microsoft [144]) were reviewed, and their guidelines can be simplified as follows:

i) Minimum length for passwords is between six or eight characters. The longer, the better.
ii) Passwords should be changed regularly.
iii) Good and strong passwords should be random with a mix of letters and numbers. Do not use keyboard patterns, sequential numbers or repeating characters.
iv) Good password should not consist of words found in the dictionary. In addition, personal data such as identification numbers, date of birth, house number and address should not be used.
v) Passwords should not be written down in a discoverable or easy to guess places. Also, password should not be sent by email or told to anyone.
vi) Use different passwords for different sites/accounts ensuring that passwords do not relate to each other.

Furnell [145] investigated password guidelines for 10 popular websites and fully examined whether these guidelines were enforced during registration and reset. It was reported that many sites provided little or no guidance at all, and only provided guidelines during password reset, not during registration. It was also reported that several sites had imposed restrictions but the standard of restrictions varied from one to another.

Garrison [146] investigated password practices among a group of students. At the beginning of term, students were asked to complete an assignment to locate password guidelines and then compare these with their current passwords. As the results were varied, a further session was conducted during a lecture

to discuss the process of creating passwords which corresponded to the password guidelines. Overall, it was reported that the session had a positive outcome where 34% changed their passwords, and a further 32% planned to change. With regards to the password guidelines, it was reported that 91% who changed their passwords followed the guidelines.

The study then proceeded with an empirical evaluation. A number of websites such as eBay, Yahoo, Google, Hotmail/MSN, Facebook, Twitter and Amazon were surveyed on September 1, 2010. These websites were chosen as they were popular in their domain (e.g. EBay was a popular auction platform while Facebook was a popular social networking platform). An attempt was made to register on each of these websites by inputting username/email and attempting different passwords to verify the strength and process for registration approval.

It can be reported that the forms of password guidelines for each website were varied and could be further categorised into three, as indicates below.

a) Provide 'password checker' to users while they typed their passwords (**G1**).
b) Provide detailed guidelines on the good choice/selection of passwords (e.g. password should be more than six characters, password should be a mixture of letters, numbers and special characters) (**G2**).
c) Display 'meter strength' to indicate the strengths of users passwords (e.g. Weak, Good, Strong) (**G3**).

Website	G1	G2	G3
Google Mail (Gmail)	No	Yes	Yes
Yahoo! Mail (Y!Mail)	Yes	No	Yes
Hotmail (MSN)	Yes	No	Yes
Facebook (FB)	No	No	No
Twitter	Yes	No	No
eBay	Yes	Yes	Yes
Amazon	No	No	No

Table 6-1: Surveys results

Table 6-1 shows if the surveyed websites provide the guidelines indicated previously (G1-G3). eBay is the only website who offered all three features while Facebook and Amazon offered none of them. It was also found that not many websites offered feature G2 (only Gmail and eBay), while many of them offered G1 and G3.

Word	Gmail	Y!Mail	MSN	Twitter	eBay1[20]	FB	Amazon
Password	Weak	Invalid	Weak	Obvious	2 out of 4	Invalid	Allow[21]
password_	Good	Invalid	Medium	good	3 out of 4	Allow	Not tested
pass_wor	Strong	Strong	Medium	good	3 out of 4	Not tested	Not tested
pass_word	Good	Strong	Medium	good	3 out of 4	Not tested	Not tested
Pass_word	Good	Very strong	Strong	strong	3 out of 4	Not tested	Not tested
pass_wor1	Strong	Very Strong	Strong	Strong	4 out of 4	Not tested	Not tested

Table 6-2: 'Strength' displayed on the surveyed websites

Table 6-2 has given an insight of differentiation or less standardisation among websites to determine the strength of password entered by users. For instance, although the majority rejected or gave a low rating for the word 'password', this was not the case with Amazon. Likewise, by adding '_' at the end of the word (password_), Gmail, MSN, Twitter and eBay rated it as Good/Medium, and surprisingly Facebook approved the registration. Other than that, it was also found that 'pass_wor' was rated as strong by both Gmail and Y!Mail, but not with 'pass_word'.

[20] For eBay, to obtain 4 out of 4, users' passwords should be more than 6 characters, contain special characters, upper case and numbers.
[21] 'Allow' means the website approved the registration

Judging from these popular websites; the study summarises that password guidelines are available to assist the user during their account registration. However, the finding reveals a lack of standardisation where not many websites were able to offer the complete categorisation of guidelines (as explained earlier), not emphasising or forcing the user to view the guideline before they proceed with the password selection and not applying any method of password restriction before or after the registration process.

As far as the thesis is aware, no study was found to have investigated or introduced user guidelines as part of the enrolment process. Therefore, a set of guidelines were introduced for graphical authentication, referred to as the Graphical Password Guidelines (GPG) which were presented to the user before they began choosing their secrets. The development of GPG were mainly influenced by the empirical findings of the study on password guidance, results of the insecure users' behaviours during graphical user studies (see Chapters 4 and 5) and to combat the underlying problems within the graphical password itself (i.e. hotspot and hotimage), Table 6-3 details the graphical password guidelines (GPG) shown to the user.

6.2 Methodology

Two types of data collection were implemented; referred to as 'internal' and 'external'. Internal means the experimenter observed the participants during the trial (similar with the one-to-one usability testing) and they had to complete the current task before proceeding to the next (controlled by the software prototype). Participants within the external group had to install the software prototype on their personal computer and use it for three weeks, with all of their activities recorded into a database (no means of control was enforced by the software prototype). The trial was conducted over two months with the participants of the internal group recruited via an open call for volunteers within the university.

Participants of the external group were colleagues/friends (external to the University) and invited via email, IM chat and text message.

Task	Guideline	Explanation
Choosing images	Choose different themes and images	Users perceive images differently and previous studies have found gender bias in user image selections [50, 93, 124]. As a result, the user is advised to choose different images, the image itself should not relate to gender and more importantly, they are advised to choose images that they think could offer them memorable areas for placing their secret clicks.
	Try to avoid imagery that could be associated with your gender	
	Please choose images that offer you various memorable areas for placing your secret clicks	
Clicking on images	Try not to click within the same or adjacent areas	Oorchot et al. [114] showed that some users' secrets were predictable. To reduce this, the user is advised to create their secret randomly. Specifically, they are not permitted to click on or within the same area (also applied to many images), advised not to create an easy to guess pattern (e.g. straight line) and encouraged not to click on obvious objects (e.g. edge, centre of each image).
	Try to click on various areas, not only on an obvious object	
	Please avoid predictable patterns (e.g. straight line, edges, central of images, etc)	

Table 6-3: Graphical password guidelines

6.2.1 Software Prototype

The improved software prototype of the EGAS was developed, using Microsoft Visual Basic 2008 as the development platform and Microsoft Office Access 2007 as the database storage (database were password protected). In the improved EGAS software prototype, users were given freedom to choose their secret click, with the software later on assign the number of images they needed to choose. Table 6-4 gives a combination of the number of clicks, the allowable number of images assigned and their entropy estimation calculations; with figures 6-1 and 6-2 illustrating screenshots from the prototype for both external and internal group participants. In the external software prototype, no means of control was

enforced. Meanwhile, the control was enforced (i.e. participants needed to complete current task before proceeding to the next one) within the internal software prototype. Both software prototypes (i.e. for internal and external), were equipped with the training module; to enable participants to get familiar with the developed software (see Figure 6-3).

Click number	Images assigned	Image size/tolerance	Click Entropy, c	Choice Entropy, d	Entropy, c+d (in bits)
1	6	200x200 / 7x7 = 816	6 * ($\log_2$ 816) = 58	6* ($\log_2$ 6) = 15	58+15 = 73
2	5	200x200 / 7x7 = 816	10 * ($\log_2$ 816) = 97	5* ($\log_2$ 5) =12	97+12 = 109
3	4	200x200 / 7x7 = 816	12 * ($\log_2$ 816) = 116	4* ($\log_2$ 4) = 8	116+8 = 124
4	3	200x200 / 7x7 = 816	12 * ($\log_2$ 816) = 116	3* ($\log_2$ 3) = 5	116+5 = 121
5	2	200x200 / 7x7 = 816	10 * ($\log_2$ 816) = 97	2* ($\log_2$ 2) = 2	97+2 = 99

Table 6-4: No of clicks/images used in the software prototype

Figure 6-1: Main menu screen for the external group

Figure 6-2: Main menu screen from the internal group

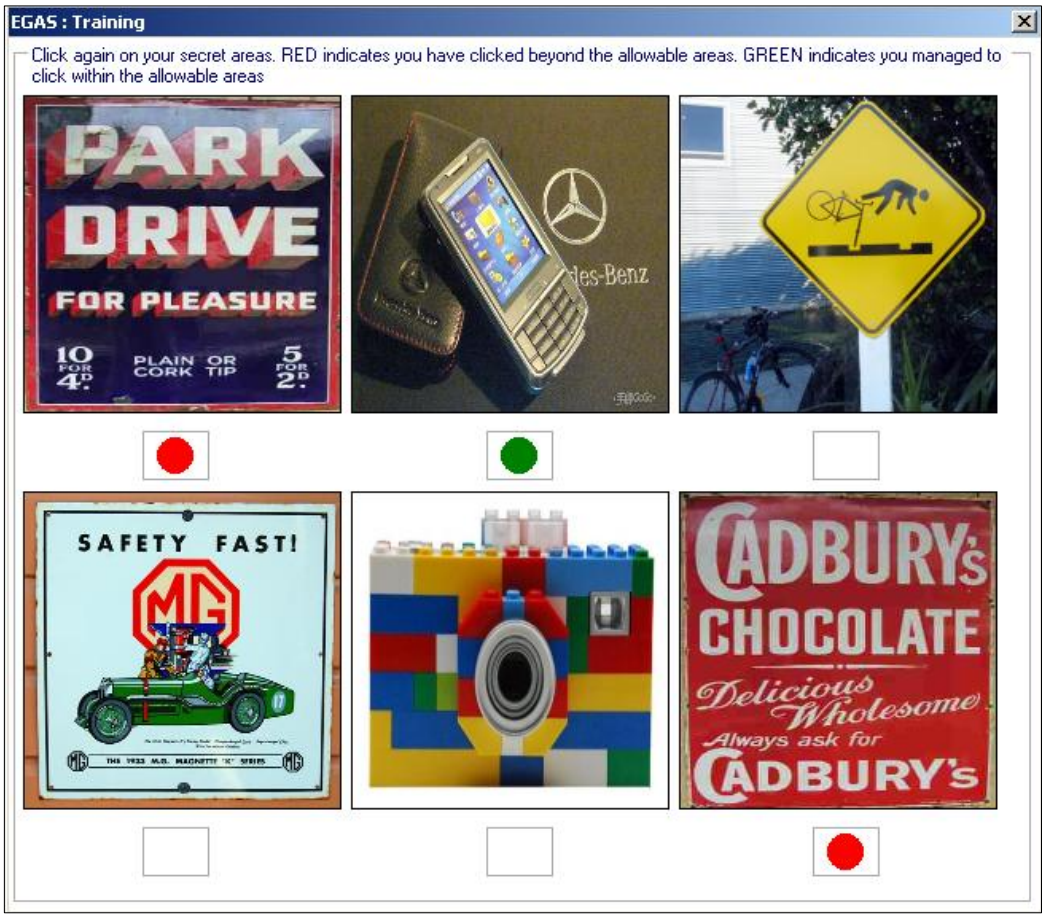

Figure 6-3: Training screen from the prototype

During the secret registration (enrolment), the GPG were first displayed (by which they had to acknowledge the GPG) before they chose their secret. During image selection, participants were able to choose images from ten different themes (buildings, abstract, food, animals, flowers, view, people, sport, transport and fruits), with each of them consisting of nine distinct images (arranged in 3x3 grids). The following list highlights the enrolment process in the EGAS software prototype.

a) Participants enter username, choose preferable click secret. The software then displayed to participants the number of images they were allowed to choose (see Figure 6-4).

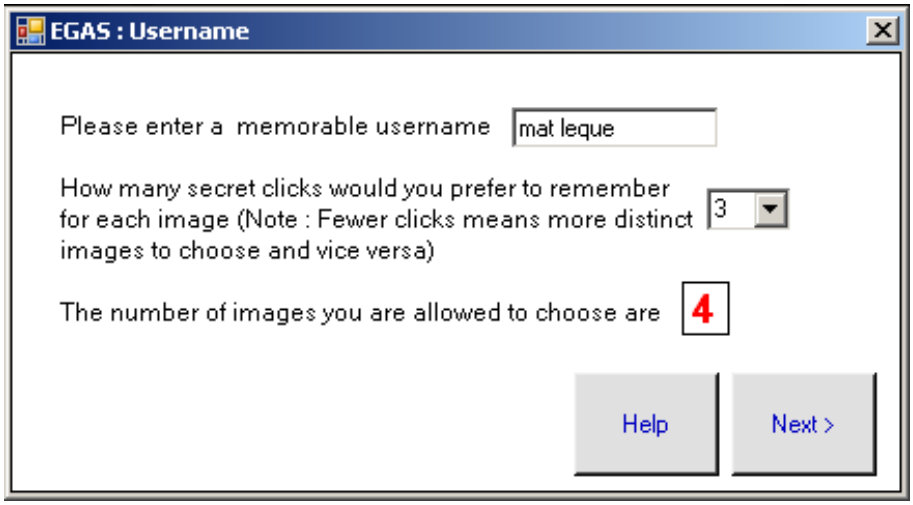

Figure 6-4: Account registration screen from the prototype

b) The guidelines for selecting secret images were displayed to participants. They needed to acknowledge the guidelines before moving to the next task (see Figure 6-5).

Figure 6-5: Guidelines displayed to participants before they started to select secret images

c) Screen for selecting secret images displayed. Participants needed to choose their secret images. In this case, only one image per category is permitted to enable fair selection of image themes. To enforce this, the theme that already chosen by the participant will be disabled. (Note that the button for displaying the guidelines (i.e. image of padlock) was also provided within the screen; see Figure 6-6).

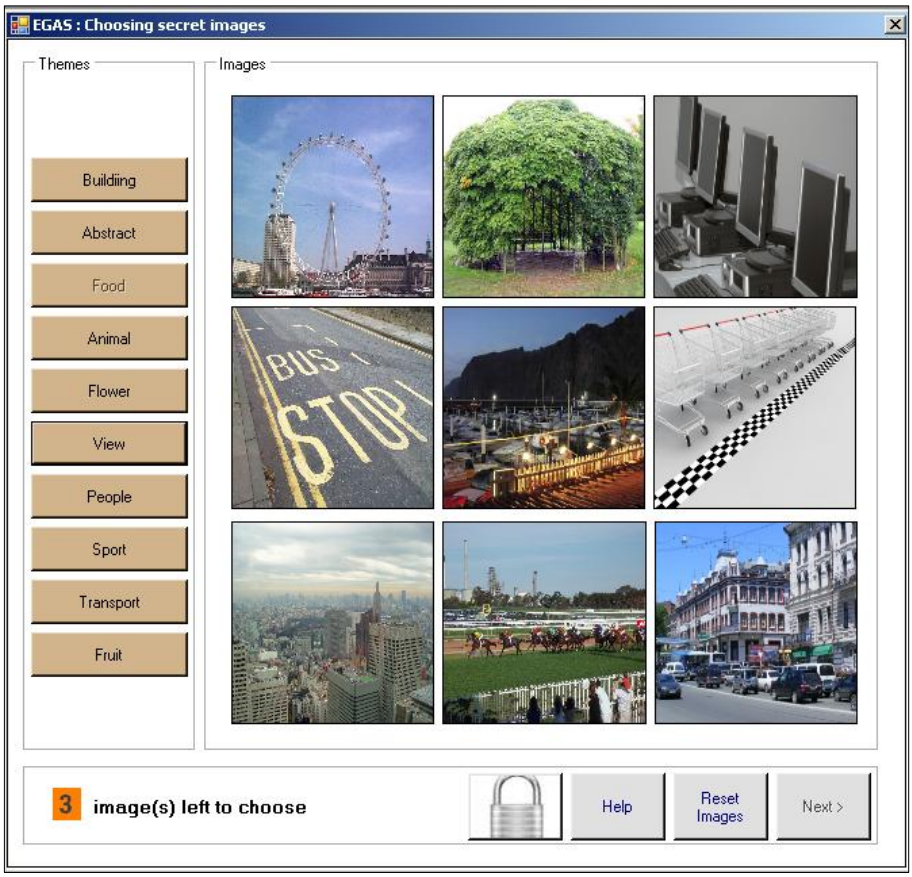

Figure 6-6: User selection images screen from the prototype

d) Screen of guidelines for selecting secret clicks was displayed to participants. Again, they needed to acknowledge before proceeding to select their secret clicks. Participants were able to see examples by hover the mouse over Example 1 and Example 2 (see Figure 6-7).

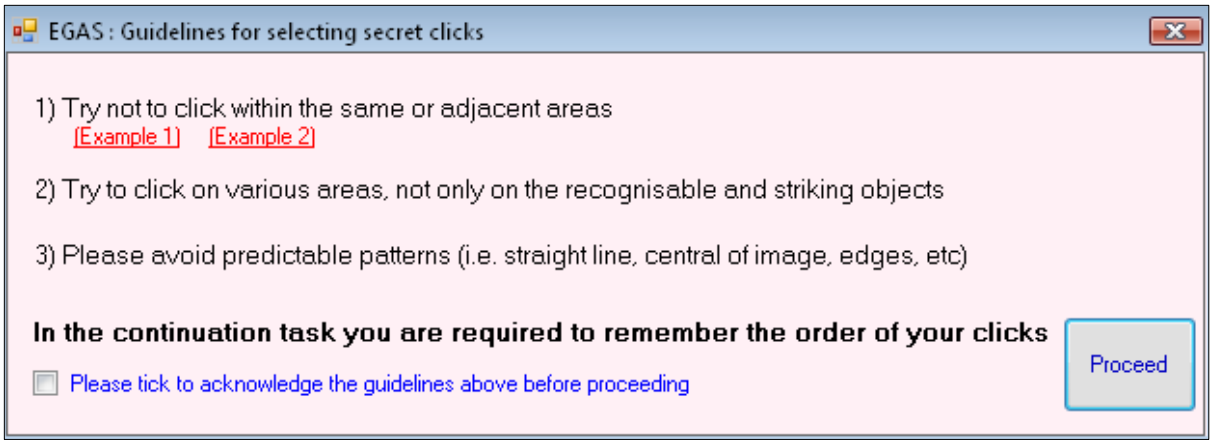

Figure 6-7: Guidelines displayed to participants before they started to select secret clicks

e) Screen for choosing secret clicks was displayed. Participants needed to create their secret clicks. Figure 6-8 shows an example of the screen for selecting secret clicks. The white circles illustrate an example of secret clicks chosen by the participant. Note that participants should click on different areas/points on each image. If the software prototype detected that the participant clicked on a similar area/point (on their other secret images), an appropriate message will be displayed (see Figure 6-9).

Figure 6-8: Screenshot for selecting secret clicks

f) The screen for confirmation was displayed and participants needed to click on their secret areas again (see Figure 6-10, blank images indicate that the participant had finished clicking on their secret clicks). Later, a result of success or failure is displayed. In the case of failure after three attempts, the system offered participants the opportunity to choose different images and clicks, restart their registration from the beginning and to view their secret clicks.

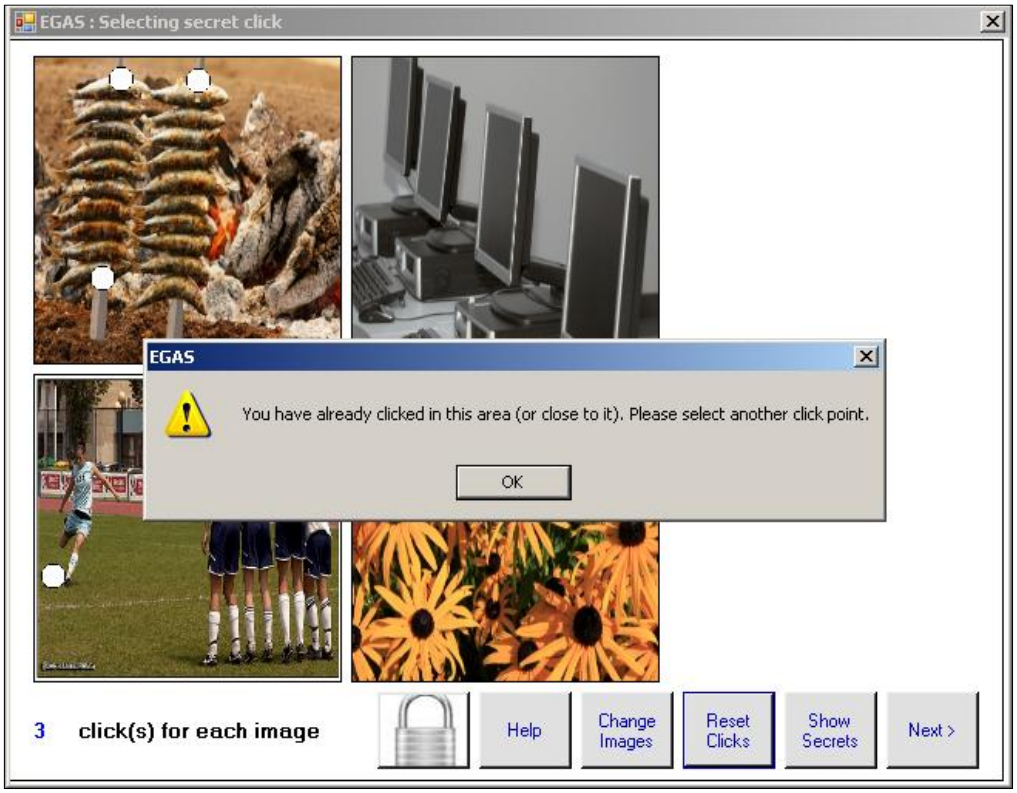

Figure 6-9: Example of restriction during selecting click

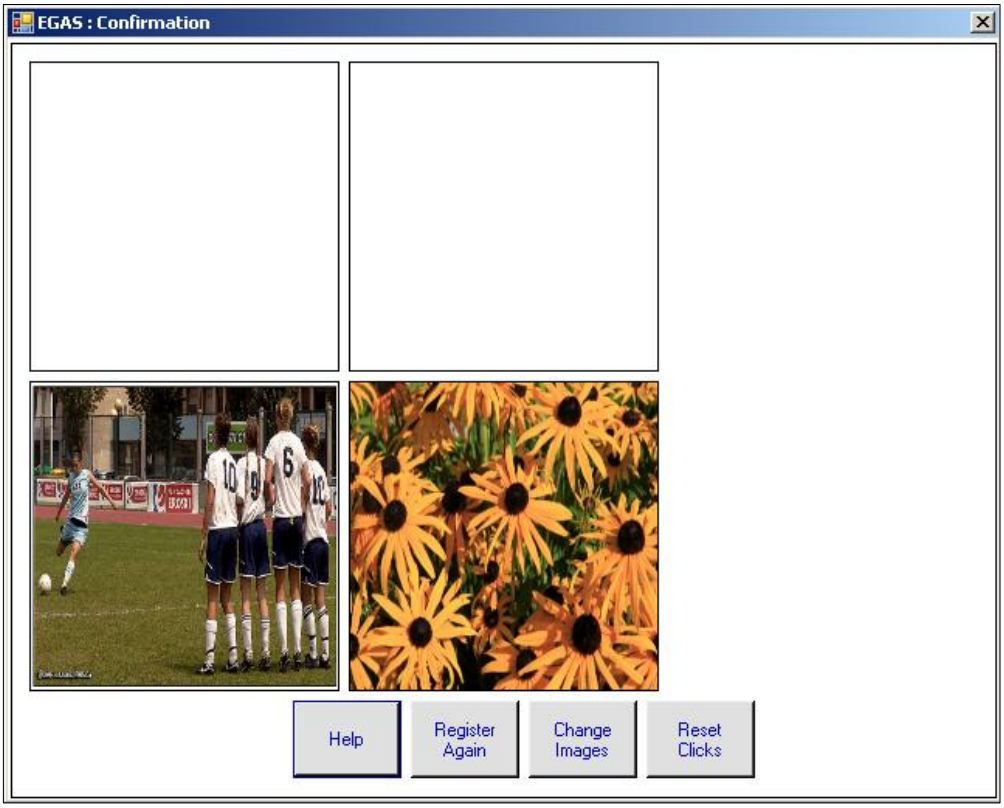

Figure 6-10: Example of confirmation screen from the prototype

To login into the software prototype, participants had to click on the padlock icon on the main screen of the prototype. Once clicked, an input box is displayed (see Figure 6-11) by which participants needed to insert their username and if the username is valid, they are allowed to proceed with the next process of login. Otherwise, their login session will be terminated. In the case of forgetting their secret details, participants were able to retrieve their secret by clicking on the key and padlock icon within the main screen (i.e. provided they supplied the valid username). Example of secrets (i.e. both images and click areas) shown to the participant as in the Figure 6-12.

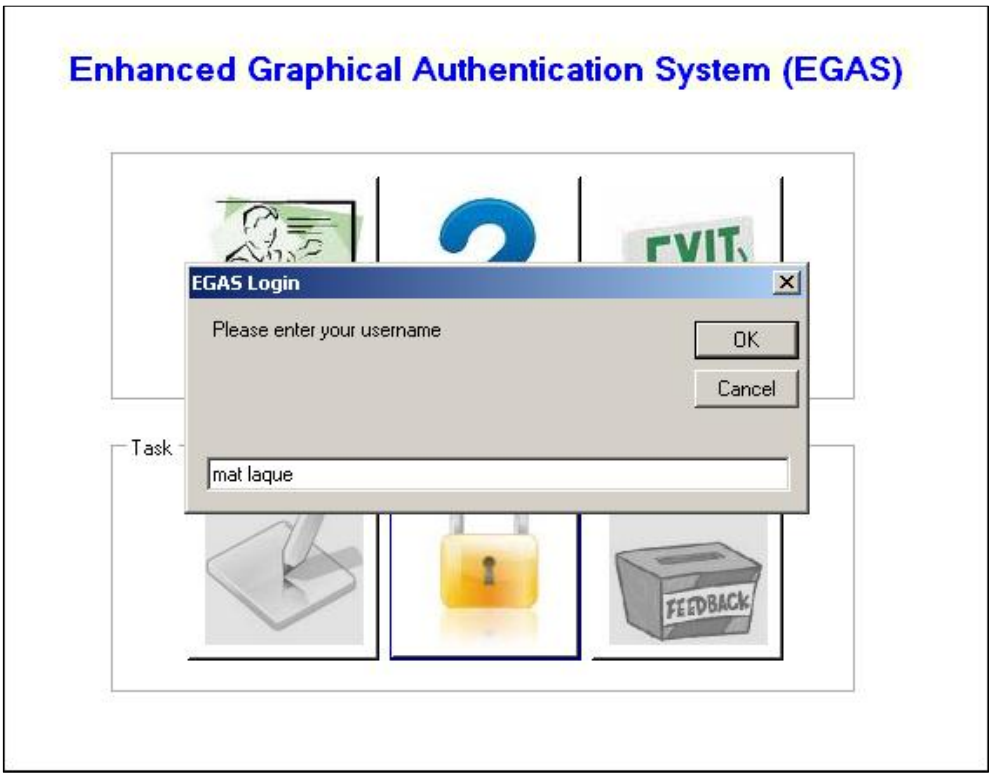

Figure 6-11: Main Login screen from the prototype

Figure 6-12: 'Show my secret' screen from the external prototype

6.2.2 Questionnaire

There were two sections in the feedback questionnaire. Section one obtained participants' demographic information such as age range, gender, highest qualification, experience with graphical authentication and source of experience if they had one. Section two of the questionnaire obtained participants' perceptions towards GPG, restrictions, login and registration times, preferable click and image combinations and finally their suggestion for future enhancements. The questionnaire should be completed once the trial tasks (i.e. register and login) have finished and a copy of questionnaire can be found in Appendix A, No (4).

6.2.3 Procedures and steps

All participants were voluntary and they were not offered any incentive at any point. The testing platform for the internal group was held on a laptop equipped with a wireless mouse, with all of them requested to come to the experimenter's lab or the experimenter went to their workplace.

Participants of both groups had to register their details (username and secrets) into the software prototype, logged into the software and finally answered the feedback questionnaire. Specifically, participants within the internal group had to login three times, with the external group needed to login four different days in week 1, two different days in week 2 and finally login once in week 3. This aimed to examine their familiarity and competency (e.g. login time, clicking accuracy, total attempts).

6.3 Results and Discussion

A total of 48 participants volunteered to participate in the trial. Table 6-5 gives information for both groups highlighting the gender mix, the minimum and maximum age range and number of participants who had previously participated in graphical password studies [89].

Demographic	Internal group	External group
Male participant	12	10
Female participant	18	8
Minimum age range	18-24	Below 18
Maximum age range	Above 60	35-39
Experienced using GA	10	2

Table 6-5: Participants' information

6.3.1 Number of Attempts

This section discusses the number of attempts made by both internal and external group participants.

6.3.1.1 Internal group

Overall, all participants within this group managed to register their secrets within the software prototype. They undertook a total of 356 authentication attempts. Of these, 94 logins were successful and 47 failed, 156 failed during registration and 66 were able to register successfully (note that the software recorded two trials for each participant if they managed to register). It is predicted that the large failed attempts was due to the small tolerance used (i.e. which made the login task quite difficult to achieve because of the accuracy required of the users).

Participants who changed their click decided to choose the lowest click. Of the total seven participants who initially chose three clicks on each image, five of them went to one click, while the remaining chose two clicks. Moreover, all five participants who initially chose two clicks and one participant who initially chose four clicks also decided to choose one click.

Table 6-6 reports the fail and successful usernames within the group. Examination on the failed usernames found four usernames actually succeeded during registration but failed during the login task. With respect to the successful usernames, sixteen participants managed to register without failure attempts, with another twelve participants recording failed attempts. Specifically, two participants who chose five clicks managed to register their details without failed attempts, with only one participant in the three clicks group managed to register with ease and two others needing three attempts each. Two participants within the two clicks group managed to register without a failed attempt, with three others

needing seven, five and one respectively. Of all the eighteen participants whose chose one click, only seven participants were unable to register straight away. Six of them needed less than three attempts while one participant needed a total of twenty four attempts before succeeding (i.e. note that this participant was an elderly member of staff who had less experience using a computer).

Fail username		Successful username	
Click group	**Participant**	**Click group**	**Participant**
1	4	1	18
2	9	2	5
3	7	3	3
4	1	4	0
5	2	5	2
Total	**23**	**Total**	**28**

Table 6-6: Fail and successful usernames within the internal group

During login, all participants within all click groups performed well where they managed to login, these results improved with experience. Only ten participants recorded a complete failure to login. There were six occurrences of failed attempts for login one, four occurrences for login two and only three occurrences for login three. The ability of participants to login with fewer failed attempts suggests participants performance improved with experience.

6.3.1.2 External group

With eighteen participants within this group, the software recorded a total of 283 login attempts in week one, 61 for week two and finally 30 for week three. Of these, there were 92 successful logins for week one, 51 for week two and 20 for week three (note that there were participants who logged into the software more than was asked for).

Investigation of successful usernames who continued with the login tasks found mixed results. It was found that only 12 participants followed the login interval task, with the remaining 6 participants using the software occasionally. For those who logged into the software according to the specified tasks, 9 participants had chosen one click, 1 participant chose two clicks and 2 participants chose five clicks. Analysis has also found that 6 participants (who did not complete the login tasks) infrequently login during week one, with three of them logged twice for week two and finally all of them logged into the software in the third week. Five of them had chosen one click, while the remaining participant went for five clicks.

Only eight of the external group participants managed to register by using their first username. Of the remaining 10 participants who used a second username, six of them changed their secret click to the least click. Unless otherwise stated, most of the analysis for this group was based upon 18 participants who completed the specified tasks.

Similar with the Table 6-6, Table 6-7 displays the number of fail and successful usernames for the external group, arranged according to click group.

Fail username		**Successful username**	
Click group	**Participant**	**Click group**	**Participant**
1	10	1	17
2	8	2	4
3	2	3	0
4	1	4	0
5	5	5	3
Total	**26**	**Total**	**24**

Table 6-7: Fail and successful usernames within the external group

6.3.2 Timing

This section discusses the time taken for both groups during registration and login.

6.3.2.1 Internal group

The time for participants to register and then log into the software prototype was recorded with the time during registration calculated from the point when they pressed the 'register account' button until the result for registration is displayed. The time for login was calculated from when the participant started to enter their username until the last click for their secret images. Table 6-8 shows participants' time (average, shortest, longest and standard deviation) during registration and three logins, in minutes, (m) and seconds, (s), with Figure 6-13 graphically showing the average login time for each click group.

Click	Participant	Time	Registration	Login One	Login Two	Login Three
1	18	Average	5m 23s	24	20	18
		Shortest	1m 43s	15	11	9
		Longest	21m 58s	42	42	4
		SD	4m 43s	8	8	6
2	5	Average	10m 29s	40	35	27
		Shortest	2m 23s	28	25	18
		Longest	23m 33s	71	69	40
		SD	7m 56s	17	18	8
3	3	Average	9m 56s	39	33	33
		Shortest	5m 47s	36	23	22
		Longest	16m 46s	43	39	42
		SD	5m 58s	4	9	10
5	2	Average	2m 56s	26	20	23
		Shortest	1m 12s	24	19	21
		Longest	4m 40s	28	21	24
		SD	2m 27s	3	1	2

Table 6-8: Timing for the internal group

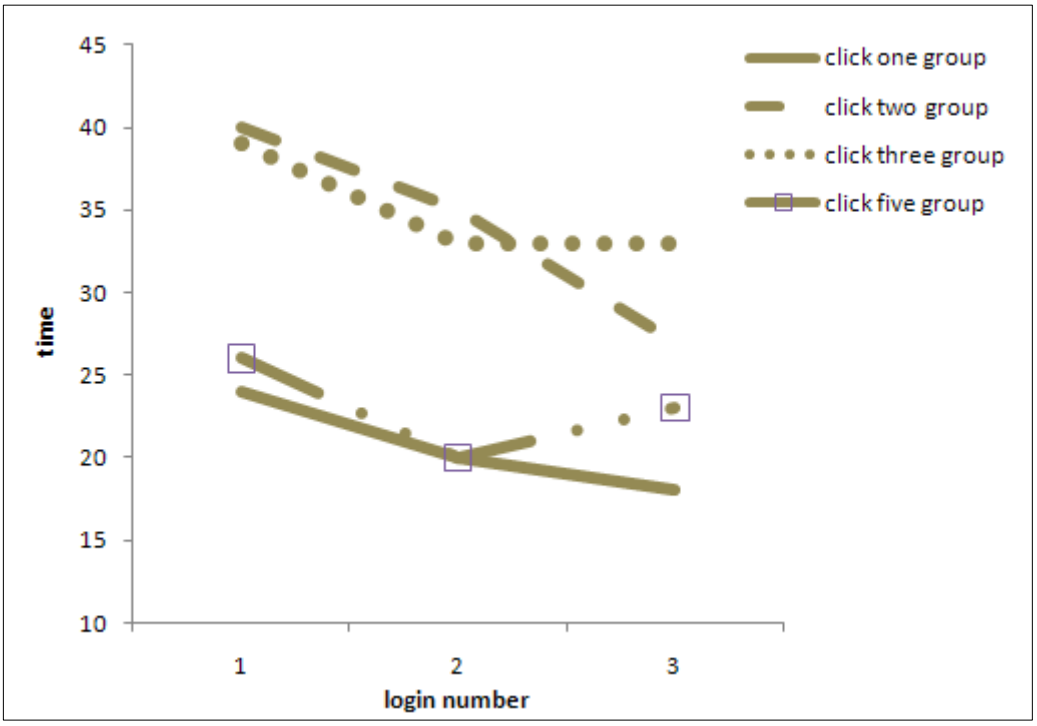

Figure 6-13: Average login time for internal group

For all click groups, the registration time can be considered long due to the action of selecting images and then clicking on the chosen images. It can be reported that for all click groups, the time to login during login attempts one to three are significantly better. The study also found that participants do not immediately select their click area, often taking several seconds before they start clicking on it. This action is believed to be due to the small tolerances used, which suggests it could directly affect login time and security if the users were observed.

6.3.2.2 External Group

Table 6-9 shows the time for 12 participants as they managed to login according to the specified login intervals. L1 to L5 refers to the login times, measured in seconds (s), for week one, L6 and L7 are login times for week two and finally L8 refers to the login time for the third week. It was found that the login time across the three weeks varied, although with one click, participants showed little change. Figure 6-

14 then displays average login time of participants for each login task. Similar with the participants who login occasionally, it was found the login time across three weeks time were up and down, with one click participants shown marginal movement.

Click	Participant	Time	Register	L1	L2	L3	L4	L5	L6	L7	L8
1	9	Average	11m 17s	17	20	17	20	14	17	17	14
		Shortest	2m 15s	14	14	13	11	12	10	10	9
		Longest	47m 23s	23	39	28	37	22	31	43	21
		SD	14m 2s	4	8	7	10	3	6	11	3
2	1	Average	3m 22s	19	26	21	31	16	15	18	24
		Shortest	3m 22s	19	26	21	31	16	15	18	24
		Longest	3m 22s	19	26	21	31	16	15	18	24
		SD	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
5	2	Average	10m 2s	33	29	23	35	25	28	20	27
		Shortest	2m 39s	29	24	22	22	23	23	19	26
		Longest	17m 25s	37	34	23	48	27	32	20	28
		SD	10m 26s	6	7	1	18	3	6	1	1

Table 6-9: Timing for the external group

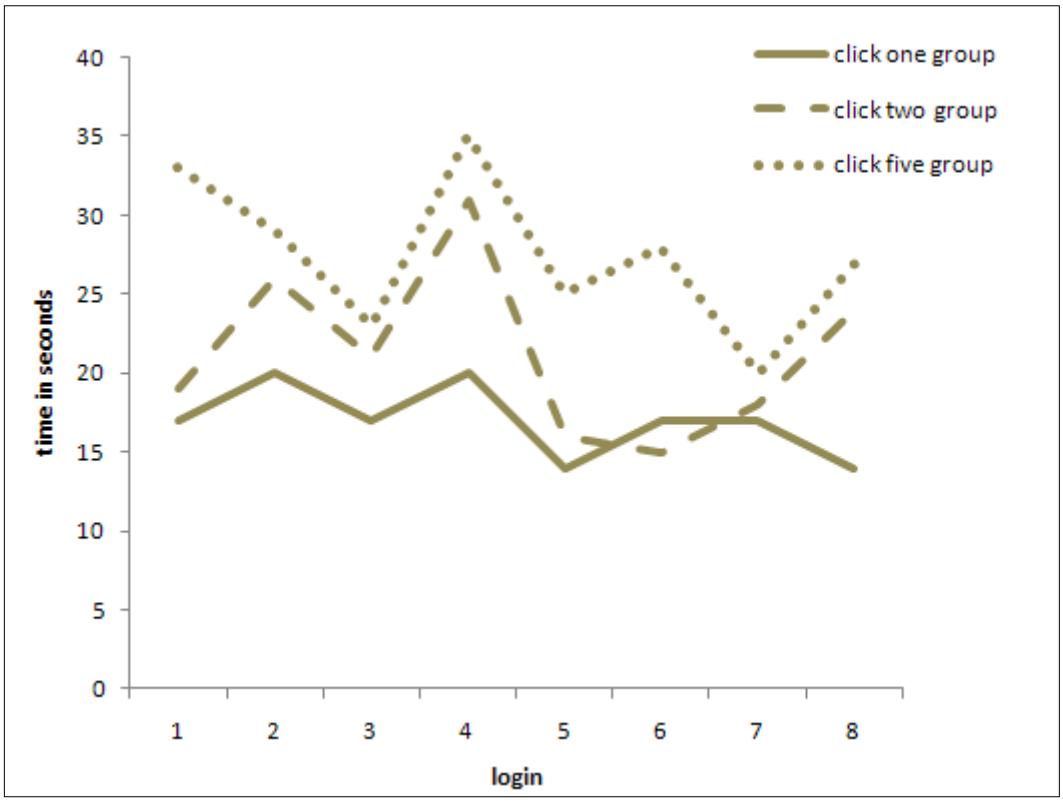

Figure 6-14: Average time for the external group participants

6.3.3 Accuracy

This section discusses the level of accuracy during secret entry for both internal and external groups.

6.3.3.1 Internal group

During login, participants were only challenged to click on their secret clicks. Unless otherwise stated, most results within this section are discussing the accuracy of the click, both during registration and login. The study discovered two main errors as indicated below.

a) Participant unable to click within the allowable tolerance.
b) Participant did not click in sequence order, as the result of forgetting their secret order or areas.

Table 6-10 reports the number of participants who made such errors during both registration and login, considering both fail and success usernames. From Table 6-10, all errors during both registration and login were associated with the participants who selected more clicks. However, once participants knew they needed to click in the sequence order, all of them made no mistake. For both tasks, participants who made tolerance errors were moderately higher than participants who made order errors. This finding is expected as the software prototype used a small allowable click tolerance. It could be said that although previous studies reported a positive outcome with respect to clicking accuracy, data within this trial indicates using a smaller tolerance is not viable, especially for a scheme that requires more clicks within a single image.

Username	Task	Participant who made order error	Participant who made tolerance error	Total
Fail	Registration	8	11	19
	Login	1	3	4
Success	Registration	2	10	12
	Login	0	10	10

Table 6-10: Internal group participants who made order error or tolerance errors

As already outlined in the methodology section, the software prototype used an allowable tolerance of 3 pixels (7x7 pixel block). Therefore, the study measured how accurately participants clicked on their original secrets by calculating the difference of participant's current click with their original click. For each participant, the difference of each secret click was calculated and later on their mode (frequency of occurrences in the data) is taken. Figure 6-15 reports the mode of accuracy for all participants during confirmation of registration and all three logins (mode for all logins were calculated together), with Table 6-11 reporting their accuracy arranged in click groups.

Although it was reported that participants struggled to click on their secret correctly, Figure 6-15 showed contradictory results where the majority of participants clicked within 1 pixel of their original secret. Overall, it can be said that participants were able to click accurately as they became familiar using the software and understand what they needed to accomplish.

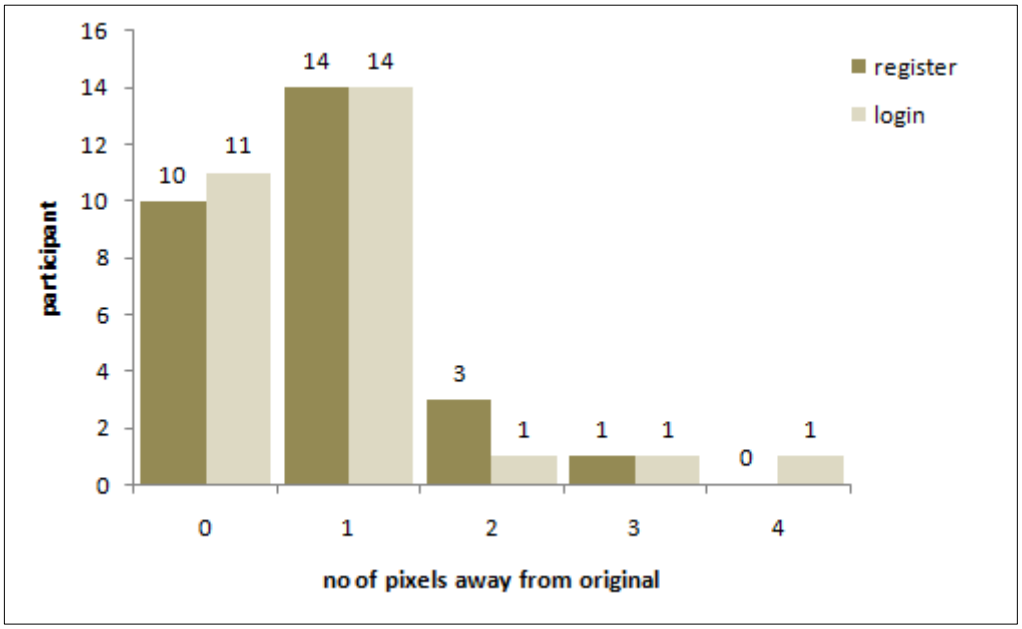

Figure 6-15: Mode of accuracy within the internal group participants

Click Group	Participant	Pixel	Register	Login
1	18	0	6	6
		1	9	10
		2 and above	3	2
2	5	0	2	2
		1	2	2
		2 and above	1	1
3	3	0	1	3
		1	2	0
		2 and above	0	0
5	2	0	1	0
		1	1	2
		2 and above	0	0

Table 6-11: Mode of accuracy for internal group participants (arranged in click groups)

6.3.3.2 External group

With respect to successful usernames, only seven recorded failed attempts during registration. It was found that the highest number of attempts before successful registration for one click group was three, with one participant of the five clicks group needing eight attempts. During week one, only ten participants recorded failed occurrences (highest number of recorded failed attempts was seven). Weeks

two and three recorded even better results as only two participants recorded failed occurrences for week two (highest number of failed attempts was five) and three participants recorded failed occurrences for week three (highest number of failed attempts was three). Table 6-12 presents the major errors with their associated number of participants who made such errors during both registration and login.

Username	Task	Participant who made order error	Participant who made tolerance error	Total
Fail	Registration	12	14	26
Success	Registration	1	6	7
	All Login	2	13	15

Table 6-12: External group participants who made order error or tolerance errors

As with the previous section, accuracy during both registration and login were investigated by measuring their accuracy. Figure 6-16 illustrates participants clicking accuracy for both registration and login. It was found that the majority managed to click their secrets exactly or within one pixel of their original. This finding is similar to the results obtained from the internal group participants.

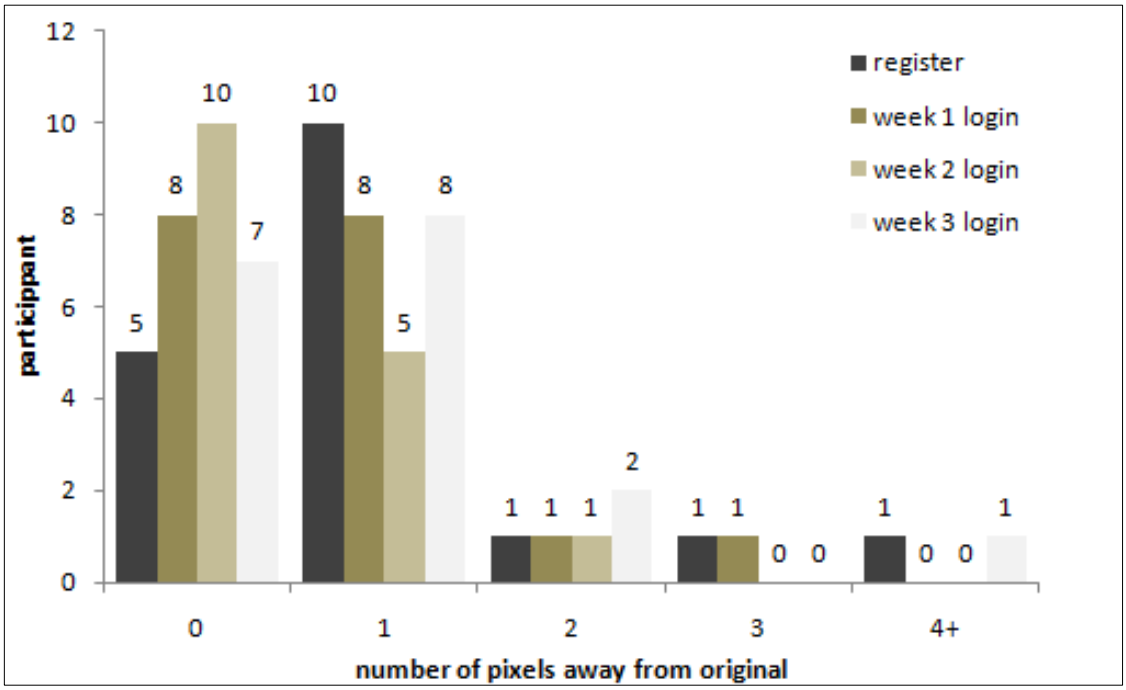

Figure 6-16: Mode of accuracy within the external group participants

6.3.4 Pattern

Patterns are created during image selection when participants choose the same images (in the case of changing username of click), gender skew selection (e.g. men choosing sports car while women chose flowers) and following image order (e.g. participants choosing the first image in each theme). Moreover, patterns during the click selection are created when participants clicked on the same area across all images, producing obvious shapes or clicking their secrets in a straight line (e.g. top, bottom and left side of image area), and clicked on the image that appeared to be offering a pattern. Results for both groups are reported together within this section as they used a similar software prototype.

With the internal group, the study found the majority of participants who changed their username or secrets (click or image) used their previously chosen images. One participant from the five clicks group used both of his previous images while two participants from the two clicks group used three and one of

their previous images respectively. Of all the participants from the one click group who changed their username or clicks, only one did not use their previous image. Specifically for the one click group, two participants used four of their previous images while the others were ranging from one to three. In addition, it was also found one of these participants selected the first image for each theme as their secret images.

The external group also used their previous secret images with one participant using all of their previous images, with six other participants using up to two of their previous chosen images .It was also found that two participants of the one click group chose their images in sequence (choose the first six themes); however their chosen images were different with each other. Taken as a whole, it can be suggested that such behaviours should not be allowed as it is susceptible to guessability.

Table 6-13 reports the total number of images recorded for each click group, with Table 6-14 presenting the number of participants who chose the most popular images within each theme. It was found that the view and sport themes are the most popular, with the transport and people themes as the least popular selection.

Although it was found that a number of participants clicked within similar areas when creating their secret clicks, such action was eliminated due to the software prototype preventing participants from clicking on the same area within multiple images. Analysis was carried out to examine the area of clicking for participants who chose more clicks and although it can be reported that participants with two or three click groups create less obvious patterns, participants of the five clicks group clearly create patterns. It can be deduced that such scenarios are related to the images themselves, which clearly offer the opportunity for a pattern to be created (see Figures 6-17 to 6-19).

Click	Image	Participant	Total Image
1	6	32	192
2	5	6	30
3	4	3	12
4	3	0	0
5	2	5	10
Total		46	244

Table 6-13: Number of images recorded for all participants

Theme	Total Images recorded	No of participants choosing popular image	Male	Female
Building	32	11	3	8
Abstract	28	12	6	6
Food	28	8	4	4
Animal	27	7	3	4
Flower	21	10	4	6
View	28	14	7	7
People	19	5	2	3
Sport	21	13	8	5
Transport	20	4	1	3
Fruit	20	7	2	5

Table 6-14: Popular images with their associated number of male and female

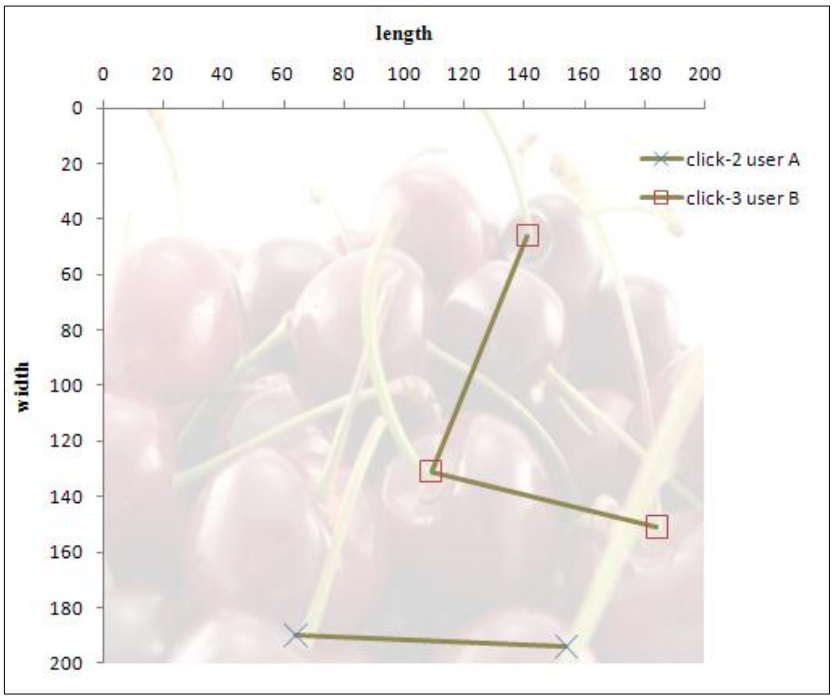

Figure 6-17: Two examples of secret clicks created by participants for the fruit theme

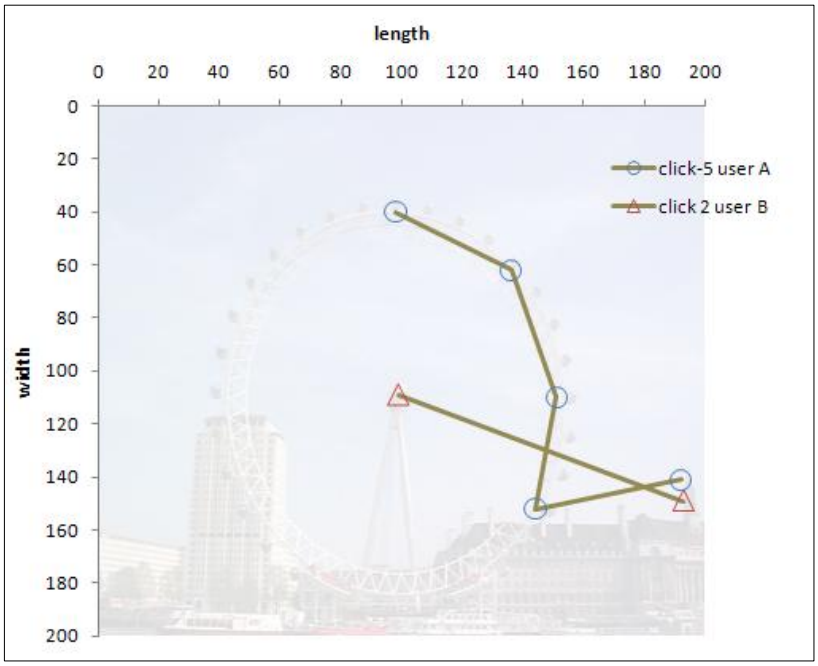

Figure 6-18: Two examples of secret clicks created by participants for the view theme

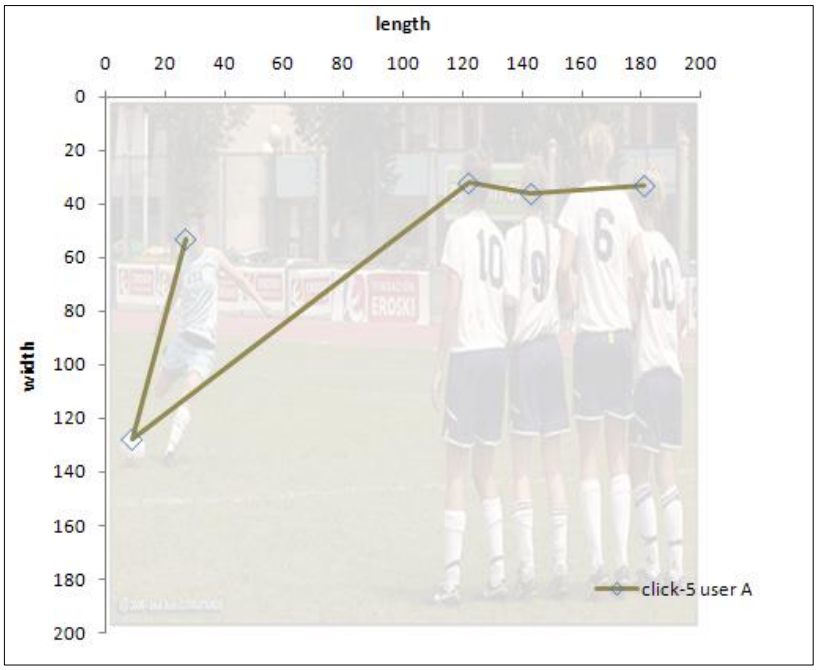

Figure 6-19: Example of the secret clicks created by participant for the sport theme

Analysis was also done to examine the location (see Table 6-15) and click areas in popular images for each theme. Analysis on the one-click group who chose the most popular image revealed that ten of the

twelve participants who chose popular images in the sports theme clicked on the three most popular areas (see Figure 6-20), four of the nine participants who chose popular images for the building theme clicked on similar areas (see Figure 6-21), with seven out of twelve participants who chose the most popular image for the 'view' theme clicking on the same area (see Figure 6-22). Equally, all other popular images have shown a pattern where participants clicked on similar spots.

Theme	Popular image location
Building	First
Abstract	Seventh
Food	Ninth
Animal	First
Flower	First
View	First
People	Second
Sport	Seventh
Transport	Second
Fruit	Eighth

Table 6-15: Commonly selected images and their location within the software prototype

Figure 6-20: Participants' click areas for the popular image of the sport theme

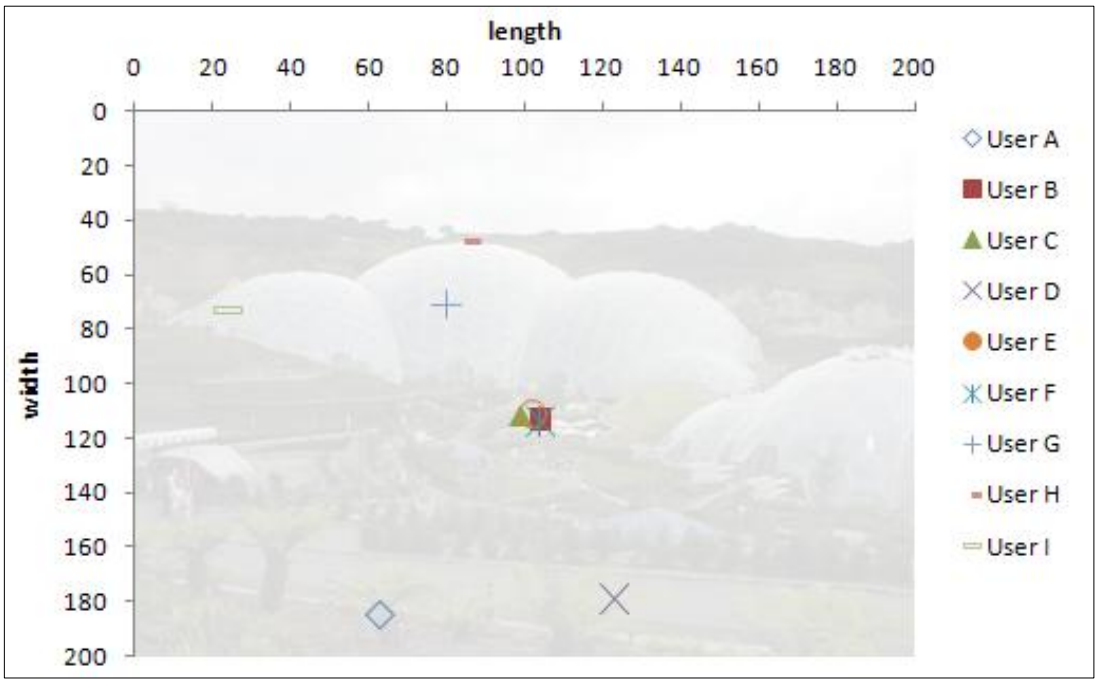

Figure 6-21: Participants' click areas for the popular image of the building theme

Figure 6-22: Participants' click areas for the popular image of the view theme

Theme	No of participants clicked on hotspot	Hotspot managed to guess
Building	4 out of 9	None
Abstract	6 out of 11	6
Food	2 out of 8	5
Animal	2 out of 5	4
Flower	4 out of 8	7
View	7 out of 12	7
People	none	No hotspot were correctly guessed
Sport	6 out of 12	7
Transport	None	No hotspot were correctly guessed
Fruit	2 out of 4	8

Table 6-16: Hotspot survey results

To further confirm the above finding, a quick study was carried out. All popular images were printed in black and white, and participants were asked to guess the potential area or spot on each image that they thought participants of the trial had clicked (see Appendix D, No (2) for the images). Table 6-16 demonstrates the number of participants (ten in total) who managed to guess hotspots created by one-click group participants. Overall, it is obvious that half of the participants managed to guess the hotspot for each popular image created by one-click group participants. To address this issue, it can be suggested that control towards image popular need to be enforced (refer to section 7.3.1.3 for further details).

From the collected data, it can be summarised that participants who chose more clicks tended to create patterns during their clicking task, while the existence of patterns during image selection was unidentified. Participants who chose more images (fewer clicks) tended to create patterns during both image and click selection. Patterns where users chose the first or last image for each theme were also reported. It can, however, also be said that the restrictions together with the guidelines during secret click selection played a minor role during the click selection task. Although not representative, participants with a higher number of clicks created more patterns (possibly as it is easier for them to remember), with analysis towards one click participants revealing the existence of hotspot.

6.3.5 Users' Feedback

A five point scale rating was used to obtain participant feedback with the lowest score indicating participants' agreement with the statements while the highest score indicating disagreement. Table 6-17 reports the mean score of feedbacks for the first three questions within the internal group.

When asked about their average login time (the software prototype displaying their average login time), it can be revealed that twenty participants found their login times were acceptable, with eight unacceptable. Seventeen participants agreed that their total registration time was acceptable while the remaining eleven disagreed. With the statement on the optimum combination of image and click, twenty two of the participants felt that having more images was more memorable than having more clicks, while five participants felt that the balance between both click and images were still memorable.

Participants who were new to the graphical method felt the method could be very useful and provided excellent protection. However, the majority of the participants who were involved in the previous trial felt that having larger clickable areas was more usable. In addition, they felt that having more clicks could be troublesome as they had to memorise too many spots and finally all participants agreed that in order for them to perform better, they needed to become more familiar with the method

Question	Mean score
1) Opinion towards graphical password guidelines (GPG)	1.6
2) Opinion towards restrictions	1.8
3) Opinion towards combining GPG with the restrictions	1.8

Table 6-17: Questionnaire results

No specific question was asked to the participants within the external group. However during the three week trial, emails and text messages were sent to them asking about their experience using the software. Although not representative, below are selected responses.

a) "I wish the software ask me the number of images I prefer, not the number of click"
b) "I found we need to click exactly on the spot. To be honest, it is frustrating as the area was small"
c) "I have to write down my secrets as I believe I cannot remember it"
d) "I captured the screen, clicked on the right area according to the captured/printed screen, but still having trouble to register"
e) "For me, week one was difficult but week two and three were easy"

The responses yield mixed opinions as they used the software without any means of control. While it takes effort to ask them to use the software prototype for three weeks, overall informal feedbacks suggested that they would consider the method as an alternative to authentication using password.

6.4 Constraints

The study evaluated practicality of giving guideline to the user before they started to choose their secrets. In addition, the study also investigated users' familiarity when they were asked to use the software prototype for a period of time.

Although the study was able to obtain participants from a variety of backgrounds, it is anticipated that the recruited participants were not widely representative. Therefore to obtain conclusive rather than

indicative results, participants who have different backgrounds and more varied computing skills should be recruited.

6.5 Conclusions

The initial EGAS software was improved and later investigated in terms of practicality of giving guidelines to a user before they chose their secrets for a graphical authentication system as well as evaluating user attitudes and opinions to the enhanced techniques. The following paragraphs summarise the findings from the conduct of this study.

During the registration task, participants struggled to click accurately within the allowable click tolerance and those who chose more clicks often failed to click in the correct order. To address this they had to create new accounts or change to fewer clicks. The login task had shown improvement as they managed to login with fewer failed attempts, and the time to login to the software prototype was reduced marginally across login attempts. The above findings reflect participants' familiarity with the software prototype as they used the software regularly.

Introducing guidelines to the participants before they start selecting their secrets had obtained positive feedback from the majority of participants. However, this study has shown that guidelines on their own cannot guarantee the security of the method itself. This is because participants used their previous images and created secret clicks using easy to remember spots, which resulted in predictable click-areas. By combining the introduction of guidelines with restrictions, user behaviour can be controlled to safeguard the method. This was proven where cases such as clicking on similar areas within the same or multiple images and where creating predictable patterns were reduced.

Finally, this study has shown that the click patterns created by users who chose more clicks had a direct relationship with the nature of the image itself. It could be said that the introduction of guidelines gave no effect on participants' usability performance, but might have positive or negative impact on security. The study also suggests that using one click per image is an ideal combination. This is because using one click per image requires less memorisation (i.e. it is more suitable for users with multiple accounts), less time to authenticate, convenience and significantly more resistant to predictability. The study also suggests that using a small tolerance without giving sufficient opportunity for familiarity to the user could result in a lack of usability of the proposed method.

As less study has found to have investigated or come out with the guidelines for both users and implementers, it is expected that opportunities for further research is widely open. This chapter has provided an initial effort by giving guidelines to users (i.e. embedding the guidelines within the software prototype) before they began choosing their secrets. To further evaluate the viability and user acceptance towards graphical password guidelines, it is proposed that more studies need to be conducted.

Although the thesis has shown that comparing graphical methods by using the same set of participants and within similar environment are possible (refer to chapter 4), it is identified that criteria or measurements for further comparison is still lacking, thus making system implementer's job rather difficult to choose the best methods. Therefore, a set of characteristics (especially for the use of system implementers) to choose and use the graphical methods to best effect are presented in the Table 6-18. These guidelines are mainly influenced by the criteria and characteristics discussed in both Furnell [145] and Renaud [149].

Factor	Criteria	Characteristic	Description
External	Applicability	Various Platform	Suitability to be used in different environments such as normal desktop, kiosks and mobile phones.
		Application Type	The importance of that application is ranked either low, medium and high
		Extra Hardware	Extra hardware needed or not. Examples are the 'reader', doodle, etc.
		Different User	Suitability to be used by different types of users like the elderly, peoples who had difficulty (learning and reading)
		Cost	The cost of that application itself. The higher the cost, the important the application itself.
	Security	Guessable	Easily guessed by means of peoples such as family/friends or shoulder surfer(s)
		Breakable/Crack able	Secret could be found by using certain algorithms or special software like dictionary, etc.
		Encryption/Hardening	Any ways of making the scheme secure such as the encryption used, make password space larger and others
		Information Harvesting	How easy the secret or information being manipulated by others.
Internal	Learnability	Training	How easy to learn and use it during training?
		Login	How easy to enter the secret during real login?
		Reset	How easy to reset the forgettable secret and what sort of guidance offered?
	Memorability	Retrieval	Is it easy for the secret to be recalled? (during login)
		Memorising	Is it easy for the secret to be memorised? (after long time)
	Satisfaction	Ease of use	The overall opinion on the level of ease of use
		Frustration	Any frustration experience when using the scheme
		Login length	The appropriateness of login length
	Interface	Use of image	The types of images used in the method
		Screen size	Appropriateness of the screen size
		Help	Any guidance offered before and after authentication
		Text and Font	The use of texts and fonts
		Error Type	The type of error messages used in the method

Table 6-18 : Guideline for choosing graphical methods

As the guidelines cover different characteristics and settings, it is anticipated that system implementers could use it as an initial step for choosing the best graphical method within their application systems. For instance, if the system implementer has a web application that running on both normal computers and mobiles (e.g. phone, tablet PCs, etc), he could find the suitable graphical method to be used by properly and critically follow the above guidelines. However, the guideline within Table 6-18 cannot be said as mutual or perfect as their effectiveness and appropriateness are not fully tested and examined.

7. Conclusions

7.1 Achievements

Based upon claims that images are easier to remember than words/phrases and the ease of use, the thesis presented a series of studies related to user authentication using images as a possible solution for the established problems with password-based authentication. Having reviewed the literature relating to graphical passwords from the past twenty years, the thesis presented attempts to complement and address the missing studies so far. These attempts conducted comparative evaluations, developed a novel method based upon the existing and introducing guidelines for secret selection.

In an attempt to provide the initial idea of comparing graphical methods, two comparative studies were conducted and tested. Specifically, the first comparative study evaluated three main schemes; namely click-based, choice-based and draw-based. The objectives of this evaluation were investigating users' familiarity of these methods, and at the same time obtaining their perception towards security and usability issues. Overall, it was found that participants preferred the choice-based and click-based methods more than the draw-based. Participants in the study rated the method with the highest level of ease of use as insecure, with the most secure method rated 'difficult to use'.

The second comparative study proceeded by comparing the effectiveness of click-based and choice-based methods when both are used for web authentication. From the total participants of 40, it was found that the number of attempts for the click-based method was rather high compared to the choice-based method. This is perhaps due to the nature of the click-based method itself where participants needed to be accurate when clicking on their chosen areas (which they sometimes missed). It was also found that for both methods, participants took longer during the registration (as they wanted to carefully look and choose their images) but then during the confirmation and login tasks, they performed significantly better. With respect to pattern analysis, participants had chosen/clicked on images or objects that were

easy to recognise and formed shapes that were easy to recall, with the most striking finding that, although participants rated the choice-based method as weak, it was still their preferred alternative.

Hoping to answer the question of why no single graphical scheme had been successfully implemented and successive claims by developers/researchers that their schemes were better than their predecessors, the thesis introduced a novel method known as the Enhanced Graphical Authentication Scheme (EGAS); combining both click-based and choice-based methods. A number of evaluation of EGAS were conducted; looking at users' familiarity using the method, the ideal combination of click and image, suitable login strategy based upon proposed scenario and the effect of using a small tolerance. Combining the findings from Chapters 5 and 6, it can be said that the method of clicking on images and choosing a series of images can be combined effectively, without significant impediment to users. Although the results have shown that memorability was maintained, users' clicking accuracy was high, timing was reasonable and users' preference were positive, participants tended to choose similar and predictable images and also tended to click on guessable objects and predictable areas. In addition, it was also found that using one click per image is an ideal combination as opposed to other combinations. This was due to the fact that using one click per image involves less memory (i.e. suitable in the case of having more accounts), less time to authenticate, convenience and significantly secure. The study also suggested that using a small tolerance without giving proper familiarity to the user could result in a lack of usability for the proposed method.

Finally in an attempt to reduce users' insecure behaviour (i.e. choosing predictable and guessable graphical secrets), the thesis introduced Graphical Password Guidelines (GPG). Basically, GPG is a set of advice for selecting secrets and is displayed to users before they start choosing their secrets. Evaluation had been made to assess its effectiveness in helping users during password creation and with a total of 48 participants; it was found that introducing guidelines to the participants before they start selecting their secrets had obtained positive feedback from the majority of participants. However,

experimental data has proven that the guidelines on their own cannot guarantee the security of the method itself. This is because participants used their previous images and created secret clicks on easy to remember spots, which resulted in a high level of predictability. By combining the introduced guidelines with restrictions, users' behaviour can be controlled to safeguard the method. This was proven where cases such as clicking on similar areas within the same or multiple images and creating predictable patterns were reduced.

7.2 Limitations

The thesis classified limitations from the conduct of studies into two, as described below.

7.2.1 Software prototypes

The software prototypes were developed and designed purposely to obtain the aims and objectives of each study; but were not aimed to be fully-functional, deployable applications. In addition to this, only local (e.g. desktop) and offline web environments were tested. To enable representative results and the ease of use of the novel method itself, testing on different platforms (e.g. mobile, different operating systems, etc) should be conducted.

7.2.2 General practice of research methodology

The majority of the participants worked or studied in the university. This was due to the fact that they were easy to recruit and there were minimal incidental costs involved. In addition, the numbers of male and female participants were also uneven, with no statistical analysis undertaken to evaluate sample

significance. Therefore, it could be said that the results and findings within the thesis are indicative rather than definitive. However, these results and findings are fairly important as they represent the group of participants who work/study within the academic sector and more importantly, they are the future generation of end-users who would actually use the proposed method.

In addition to the above, the thesis only used five criteria to evaluate the usability of the proposed method. These criteria were the number of attempts, users' clicks and image patterns, timing, accuracy during secret entries and finally the users' feedback. While there are other options for evaluating effectiveness and efficiency of the proposed method, it is anticipated that the aforementioned criteria are fitting to be used within the scope of knowledge-based authentication.

7.3 Final thought: The Future

This section highlights the future of authentication using images as well as the proposed novel method itself.

7.3.1 EGAS Method

As the thesis has shown that combining two graphical methods is possible without significant impediment to users, it is anticipated that opportunities for future research and combination between other methods are also possible (refer to Chapter 3, on the hybrid-based method). The following list highlights possible improvements that could be done to the EGAS method.

7.3.1.1 System-assigned images versus user chosen images

Although assigning six images to each user was successful in terms of both memorability and recall (refer Chapter 5), the specific number of system-assigned and user-chosen images that need to be assigned is still questionable. Assigning system-assigned images as a control (i.e. to facilitate password reset) and as a preventive measure (i.e. to limit the ability of an observer guessing a user's secrets) have not been thoroughly tested. Detailed studies need to be conducted to enable direct comparison and effectiveness of the image assignment.

7.3.1.2 Larger set of images/ different set of images

Using a larger set of images and separating images between account creation and authentication could address or reduce the problem of intersection attacks (as explained in [47]). The problem of popular (or hot) images could also be reduced as the user has many options and choices for selection. However, using a larger set of images could result in larger storage capacity, copyright issues and speed of access (if deployed on the web); all of which directly relate to cost.

7.3.1.3 Controlling user chosen images

Enabling the EGAS scheme to be implemented by using a limited set of images, it is proposed that the system could apply the concept of 'first come, first served'. Each image that is chosen or selected by the user needs to be assigned a value or counter. If that image has achieved the threshold value (assigned manually depending upon criticality of the system), that image should not be available to another user.

Alternatively, to reduce the problem of a user choosing the popular categories during registration, the system could generate random image themes/categories for the user to choose from (i.e. not all categories will be displayed to the user at each registration session).

Both enhancements could limit the number of categories/themes displayed to each user, eliminate the hot image problem and at the same time provide an opportunity for other image/categories to be chosen. However, these enhancements would also limit the range of images available for selection.

7.3.1.4 Controlling user click patterns

It is proposed that the EGAS scheme could use an approach similar to [82]. If the system detected that the same image has been selected, the system would examine the click area of previous users and could suggest that the current user click on other less common areas. This method should be properly done to prevent from revealing other users' click patterns. More importantly, the system should not permit predictable patterns (e.g. clicking on straight, horizontal, vertical; centre of every images, edges, etc).

7.3.1.5 Adjustable/flexible tolerance

From the results in Chapter 5, it is suggested that a smaller tolerance could be used as this would make the secret-space larger, thus increasing security. However, the study from Chapter 6 has shown that there were participants who were unable to click accurately within the allowable tolerance setting. Therefore, it is suggested that flexible tolerances could be implemented to reduce this (on a per-user basis).

7.3.2 Authentication using images

The main benefit of authentication using images compared to other solutions is that it enables direct implementation without any additional hardware and software requirements. With respect to the finding of the thesis, it has shown that comparing graphical schemes between themselves and specifically combining multiple methods are possible and thus could be the basis for future research or directions for better security.

The thesis identified six issues that provide opportunities for future works (refer Chapter 3). Studying the effect of using authentication using images within a longer period time, having multiple graphical passwords and an effective method for password reset should be considered. In addition, various techniques (e.g. algorithm, encryption, etc.) during image selection, entry of secret and storage of the secret should also be the focus for future research. Attention should also be given to users' familiarity and training. Examples could include integrating the training module with the developed graphical scheme (i.e. as already shown in EGAS), and using HCI principles during development of a graphical scheme to enable higher user acceptance.

Although significant studies have been reported, reducing predictability in the method by conducting more studies covering various aspects (e.g. users' behaviour, vulnerabilities, graphical dictionaries, graphical representation, etc.) needs to be properly tested. The final issues that the author of the thesis thought suitable for future research include testing graphical methods within multiple usage scenario or environments and designing the graphical scheme for flexibility (e.g. different click tolerance, system criticality, etc.) as the result of differences in human knowledge, skills, cultures, interests, perceptions as well as advances with the technology itself.

8. References

[1] Bevan, N.: ‘International standards for HCI and usability’. International Journal of Human Computer Studies, 55(4) pp. 533-552 (2001)

[2] Abran, A., Khelifi, A. & Suryn, W.: ‘Usability meanings and interpretations in ISO standards'. Software Quality Journal, 11 pp 325-338 (2003)

[3] Karat, C.-M., Karat, J. & Brodie, C.: 'Why HCI research in privacy and security is critical now'. International Journal of Human-Computer Studies, 63 pp. 1-4 (2005)

[4] Cranor, L.F. & Garfinkel, S.: ‘Security and Usability: Designing Secure Systems That People Can Use’. O'Reilly, ISBN: 9780596008277 (2005)

[5] Morris, R. & Thompson, K.: 'Password security: a case history'. Communications of the ACM, 22 (11) pp. 594-597(1979)

[6] Klein, D. V.: 'Foiling the Cracker: A survey of, and improvement to, password security', Proceedings of the second (USENIX) Workshop on Security. pp. 5-14 (1990)

[7] Bishop, M. & Klein, D.V.: 'Improving system security via protective password checking'. Computer & Security, 14 (3) pp. 233-249 (1995)

[8] Spafford, E.: 'Observing reusable password choices'. Purdue University Technical Report [CSD–TR 92–049]. Available at: http://ftp.cerias.purdue.edu/pub/papers/gene-spafford/spaf-OPUS-observe.pdf (Accessed: 12 November 2010) (1992)

[9] Adams, A., Sasse, M. A. & Lunt, P.: 'Making passwords secure and usable', Proceedings of HCI on People and Computers XII. Springer-Verlag pp. 1-19 (1997)

[10] Carstens, D. S., McCauley-Bell, P. R., Malone, L. C. & DeMara, R. F.: 'Evaluation of human impact of password authentication practices on information security'. Informing Science Journal, 7 (1) pp. 67-85 (2004)

[11] Schneier, B.: 'MySpace passwords aren't so dumb'. [Online]. Available at: http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300?currentPage=all (Accessed: 12 November 2010) (2006)

[12] Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. & Furlong, M.: 'Password sharing: Implications for security design based on social practice', CHI 2007 Proceedings of the SIGCHI conference on Human factors in computing systems. San Jose, USA April 28-May 3, 2007. ACM pp. 895-904 (2007)

[13] Florencio, D. & Herley, C.: 'A large-scale study of web password habits', Proceedings of the 16th International Conference on World Wide Web. Banff, Alberta, Canada ACM New York, USA, pp. 657-666 (2007)

[14] Zhang, J., Luo, X., Akkaladevi, S. & Ziegelmayer, J.: 'Improving multiple-password recall: an empirical study'. European Journal of Information System, 18(2), pp. 165-176 (2009)

[15] Hoonakker, P., Bornoe, N. & Carayon, P.: 'Password authentication from a human factors perspective: results of a survey among end-users', Proceedings of the Human Factors and Ergonomics Society 53rd Annual Meeting. Grand Hyatt San Antonio, Texas, USA Human Factors and Ergonomics Society, pp. 459-463 (2009)

[16] Bonneau, J. & Preibusch, S.: 'The password thicket: technical and market failures in human authentication on the web'. The 9th Workshop on the Economics of Information Security (WEIS 2010). Harvard University, USA: June 7-8. (2010)

[17] Inglesant, P. G. & Sasse, M. A.: 'The true cost of unusable password policies: password use in the wild', Proceedings of the 28th international conference on Human factors in computing systems. Atlanta, Georgia, USA ACM, pp. 383-392 (2010)

[18] Yan, J., Blackwell, A., Anderson, R., & Grant, A.: 'The memorability and security of passwords' In L. F. Cranor & S. Garfinkel (eds.), Security and Usability: Designing secure systems that people can use pp. 129-142, O'reilly, ISBN: 9780596008277. (2005)

[19] Kuo, C., Romanosky, S. & Cranor, L. F.: 'Human selection of mnemonic phrase-based passwords', In Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS). Pittsburgh, Pennsylvania ACM, pp. 67-78 (2006)

[20] Keith, M., Shao, B. & Steinbart, P. J.: 'The usability of passphrases for authentication: An empirical field study'. International Journal of Human Computer Studies, 65 pp 17-28 (2007)

[21] Burnell, J., Podd, J., Henderson, R., Napier, R. & Kennedy-Moffat, J.: 'Cognitive, associative and conventional passwords: Recall and guessing rates'. Computers and Security, 16 (7) pp. 645-657 (1997)

[22] Zhivan, M. & Haga, W. J.: 'A comparison of password techniques for multilevel authentication mechanism'. Journal of Computing, 36 pp. 723-736 (1993)

[23] Jakobsson, M., Yang, L. & Wetzel, S.: 'Quantifying the security of preference-based authentication', Proceedings of the 4th ACM workshop on Digital identity management. Alexandria, Virginia, USA ACM, pp. 61-70 (2008)

[24] Conlan, R. M. & Tarasewich, P.: 'Improving interface designs to help users choose better passwords', CHI '06 extended abstracts on Human factors in computing systems. Montreal, Quebec, Canada ACM, pp. 652-657 (2006)

[25] Schechter, S. & Herley, C.: 'Popularity Is Everything: A New Approach to Protecting Passwords from Statistical-Guessing Attacks'. 5th USENIX Workshop on Hot Topics in Security. Washington, DC: 10th August, 2010. USENIX (2010)

[26] Weirich, D. & Sasse, M. A.: 'Pretty good persuasion: a first step towards effective password security in the real world', Proceedings of the 2001 workshop on New security paradigms. Cloudcroft, New Mexico ACM, pp. 137-143 (2001)

[27] Forget, A., Chiasson, S., Oorschot, P.C.V. & Biddle, R.: 'Improving text passwords through persuasion', Proceedings of the 4th symposium on Usable Privacy and Security. Pittsburgh, Pennsylvania ACM, pp. 1-12 (2008)

[28] Shepard, R. N.: 'Recognition memory for words, sentences and pictures'. Journal of Verbal Learning and Verbal Behavior, 6 pp. 156-163 (1967)

[29] Nickerson, R. S.: 'A note on long-term recognition memory for pictorial material'. Psychonomic Science, 11 (2) pp. 58 (1968)

[30] Paivio, A., Rogers, T. & Smythe, P. C.: 'Why are pictures easier to recall than words?' Psychonomic Science, 11 (4) pp. 137-138 (1968)

[31] Standing, L., Conezio, J. & Baher, R. N.: 'Perception and memory for pictures: Single-trial learning of 2500 visual stimuli'. Psychonomic Science, 19 (2) pp. 73-74 (1970)

[32] Standing, L.: 'Learning 10,000 pictures'. Quarterly Journal of Experimental Psychology, 25 pp. 207-222 (1973)

[33] Mandler, J. M. & Johnson, N. S.: 'Some of the thousand words a picture is worth'. Journal of Experimental Psychology: Human Learning and Memory, 2 (5) pp. 529-540 (1976)

[34] Luck, S. J. & Vogel, E. K.: 'The capacity of visual working memory for features and conjunctions'. Nature, 390 pp. 279-281 (1997)

[35] Weldon, M. S., Roediger, H. L. & Challis, B. H.: 'The properties of retrieval cues constrain the picture superiority effect'. Memory and Cognition, 17 (1) pp. 95-105 (1989)

[36] King, M. M.: 'Rebus Passwords', Computer Security Applications Conference. San Antonio, TX, USA IEEE, pp. 239-243 (1991)

[37] Suo, X.: ‘A design and analysis of graphical password’. MSc., Georgia State University. Available at: http://digitalarchive.gsu.edu/cs_theses/27/ (Accessed: 8 December 2010) (2006)

[38] Tao, H.: ‘Pass-Go: A new graphical password scheme’. MSc., University of Ottawa, Canada. Available at: http://www.site.uottawa.ca/~cadams/papers/HaiTaoThesis.pdf (Accessed: 8 December 2010) (2006)

[39] Komanduri, S.: ‘Improving password usability with visual techniques’. MSc, Bowling Green State University. Available at: http://etd.ohiolink.edu/send-pdf.cgi/Komanduri%20Saranga.pdf?bgsu1194297698 (Accessed: 8 December 2010) (2007)

[40] Chiasson, S.: ‘Usable Authentication and Click-based Graphical Password’. PhD. Carleton University. Available at: http://hotsoft.carleton.ca/~sonia/content/Chiasson_PhDThesis2008_UsableAuthentication.pdf (Accessed: 8 December 2010) (2008)

[41] Blonder, G.: ’Graphical password’. US Patent 5559961 (1996)

[42] Renaud, K. & De Angeli, A.: 'My passport is here! An investigation into visuo-spatial authentication mechanisms’'. Interacting with Computers, 16 pp. 1017 – 1041 (2004)

[43] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. & Memon, N.: 'PassPoints: design and longitudinal evaluation of a graphical password system'. International Journal of Human Computer Studies, 63 pp. 102-127 (2005)

[44] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. & Memon, N.: 'Authentication using graphical passwords: effects on tolerance and image choice'. Proceedings of the 2005 Symposium on Usable Privacy and Security. Pittsburgh, Pennsylvania, ACM pp. 1-12 (2005)

[45] Chiasson, S., Biddle, R. & Oorschot, P.C.V.: 'A second look at the usability of click-based graphical passwords', Proceedings of the 3rd Symposium on Usable Privacy and Security. Pittsburgh, Pennsylvania ACM, pp. 1-12 (2007)

[46] Passfaces: 'Next generation graphical authentication'. [Online]. Available at: http://www.realuser.com/personal/index.htm (Accessed: 5 May 2011) (2003)

[47] Djamila, R. & Perrig, A.: 'Deja Vu: A user study using images for authentication', Proceedings of the 9th USENIX Security Symposium. Denver, Colorado, USA August 14-17, 2000. USENIX Association, pp. 45-58 (2000)

[48] Man, S., Hong, D. & Matthews, M.: 'A shoulder-surfing resistant graphical password scheme - WIW'. Proceedings of 2003's International Conference on Security and Management, Las Vegas, USA, pp. 105-111 (2003)

[49] Hong, D., Man, S., Hawes, B. & Matthews, M.: 'A password scheme strongly resistant to spyware', Proceedings of 2004's International Conference on Security and Management. Las Vegas, USA, pp. 94-100 (2004)

[50] Davis, D., Monrose, F. & Reiter, M. K.: 'On user choice in graphical password schemes', Proceedings of the 13th USENIX security symposium. California, USA August 9-13, 2004. USENIX Association, pp. 1-11 (2004)

[51] Charruau, D., Furnell, S. & Dowland, P.: 'PassImages: An alternative method of user authentication', ISOneWorld. Las Vegas, USA March 30, 2005 - April 1, 2005 (2005)

[52] De Angeli, A., Coventry, L., Johnson, G. & Coutts, M.: 'Usability and user authentication: Pictorial passwords vs. pin': in McCabe, P.T. (ed.) Contemporary Ergonomics 2003. Taylor & Francis, pp 253–258 (2003)

[53] De Angeli, A., Coventry, L., Johnson, G. & Renaud, K.: 'Is a picture really worth a thousand words? Reflecting on the usability of graphical authentication systems'. International Journal of Human Computer Studies, 63 (1-2) pp. 128-152 (2005)

[54] Dunphy, P. & Yan, J.: 'Is FacePIN secure and usable'. Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania ACM, pp. 165-166 (2007)

[55] Harada, A., Isarida, T., Mizuno, T. & Nishigaki, M.: 'A User Authentication System Using Schema of Visual Memory'. LNCS: Biologically Inspired Approaches to Advanced Information Technology. Springer Berlin / Heidelberg, pp. 338-345 (2006)

[56] Yamamoto, T., Harada, A., Isarida, T. & Nishigaki, M.: 'Improvement of User Authentication Using Schema of Visual Memory: Exploitation of "Schema of Story"', Proceedings of the 22nd International Conference on Advanced Information Networking and Applications. IEEE Computer Society, pp. 40-47 (2008)

[57] Hasegawa, M., Miyachi, T., Tanaka, Y. & Kato, S.: 'A graphical password using discrete wavelet transform and its evaluation'. IIEEJ Image Electronics and Visual Computing Workshop 2010. Le Meridien Hotel, Nice, France: 5-7 March 2010 (2010)

[58] Weinshall, D.: 'Cognitive authentication schemes safe against spyware', 2006 IEEE Symposium on Security and Privacy. 21-24 May 2006. IEEE Computer Society, pp. 295-300 (2006)

[59] Golle, P. & Wagner, D.: 'Cryptanalysis of a cognitive authentication scheme (extended abstract)'. Proceedings of the 2007 IEEE Symposium on Security and Privacy, IEEE Computer Society pp. 66-70 (2007)

[60] Wiedenbeck, S., Waters, J., Sobrado, L. & Birget, J.C.: 'Design and evaluation of shoulder-surfing resistant graphical password scheme', Proceedings of the working conference on advanced visual interfaces. Venezia, Italy May 23-26, 2006. ACM New York, USA, pp. 177 – 184 (2006)

[61] Sobrado, L. & Birget, J.C.: 'Graphical passwords'. [Online]. Available at: http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm (Accessed: 8 December 2010) (2002)

[62] Hinds, C. & Ekwueme, C.: 'Increasing security and usability of computer systems with graphical password', ACM Southeast Regional Conference. Winston-Salem, North Carolina, USA ACM New York, USA, pp. 529-530 (2007)

[63] Renaud, K. & Olsen, E. S.: 'DynaHand: Observation-resistant recognition-based web authentication'. IEEE Technology and Society, Special Issue on Usable Security and Privacy, 26 (2) pp. 22-31 (2007)

[64] Bandyopadhyay, S. K., Bhattachrayya, D. & Das, P.: 'User authentication by secured graphical password implementation', 7th Asia-Pacific Symposium on Information and Telecommunication Technologies, APSITT. IEEE, pp. 7-12 (2008)

[65] Eljetlawi, A. M. & Ithnin, N.: 'Graphical password: prototype usability survey', International Conference on Advanced Computer Theory and Engineering, 2008. ICACTE '08. . 20-22 Dec, 2008. IEEE Computer Society, pp. 351-355 (2008)

[66] Komanduri, S. & Hutchings, D. R.: 'Order and entropy in picture passwords', Proceedings of graphics interface 2008. Windsor, Ontario, Canada. Canadian Information Processing Society, pp. 115-122 (2008)

[67] Lin, P. L., Weng, L. T. & Huang, P. W.: 'Graphical password using images with random tracks of geometric shapes', Proceedings of the 2008 Congress on Image and Signal Processing. IEEE Computer Society, pp. 27-31 (2008)

[68] Gao, H., Liu, X., Dai, R., Wang, S. & Chang, X.: 'Analysis and Evaluation of the ColorLogin Graphical Password Scheme', Fifth International Conference on Image and Graphics. IEEE Computer Society, pp. 722-727 (2009)

[69] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K. & Rubin, A. D.: 'The design and analysis of graphical password', Proceedings of the 8th USENIX Security Symposium. Washington DC, USA August 23-26, 1999. The USENIX Association, pp. 1-14(1999)

[70] Nali, D. & Thorpe, J.: 'Analysing user choice in graphical password'. School of Information Technology and Engineering, University of Ottawa, US. May 27, 2004. [Online]. Available at: http://www.cs.carleton.ca/research/tech_reports/2004/TR-04-01.pdf (Accessed: 20 March 2009) (2004)

[71] Malek, B., Orozco, M. & Saddik, A. E.: 'Novel shoulder-surfing resistant haptic-based graphical password'. Proceedings of Eurohaptics 2006. Paris, France: July 3-6, 2006 (2006)

[72] Por, L. Y., Lim, X. T., Su, M. T. & Kianoush, F.: 'The design and implementation of background Pass-Go scheme towards security threats'. WSEAS Transaction of Information Science and Applications, 5 (6) pp. 943-952 (2008)

[73] Por, L. Y. & Lin, X. T.: 'Multi-grid background Pass-Go'. WSEAS Transaction of Information Science and Applications, 5 (7) pp. 1137-1148 (2008)

[74] Dunphy, P. & Yan, J.: 'Do background images improve "Draw A Secret" graphical passwords?' Proceedings of the 14th ACM Conference on Computer and Communications Security. Virginia, USA ACM New York, USA, pp. 36-47 (2007)

[75] Lin, D., Dunphy, P., Yan, J. & Olivier, P.: 'Graphical passwords and qualitative spatial relations'. Symposium On Usable Privacy and Security. Pittsburgh, USA: July 18-20, 2007 (2007)

[76] Gao, H., Guo, X., Chen, X., Wang, L. & Liu, X.: 'YAGP: Yet Another Graphical Password Strategy', Computer Security Applications Conference, Annual. IEEE Computer Society, pp. 121-129 (2008)

[77] Li, Z., Sun, Q., Lian, Y. & Giusto, D. D.: 'An association-based graphical password design resistant to shoulder-surfing attack'. IEEE International Conference on Multimedia and Expo 2005. July 6-8, 2005(2005)

[78] Zhao, H. & Li, X.: 'S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme', 21st International Conference on Advance Information Networking and Application Workshops. IEEE Computer Society, pp. 467-472 (2007)

[79] Minne, P., Wells, J., Hutchinson, D. & Pierce, J.: 'An investigation into the usability of graphical authentication using AuthentiGraph': In Valli, G. and Woodward, A. (eds.) Proceedings of the 5th Australian Information Security Management Conference. Edith Cowan University, Australia. pp. 175-185 (2007)

[80] Pierce, J. D., Wells, J. G., Warren, M. J. & Mackay, D. R.: 'A conceptual model for graphical authentication'. First Australian Information Security Management Conference. Perth, Australia: November 24, 2008 (2003)

[81] Chiasson, S., Oorschot, P. C.V. & Biddle, R.: 'Graphical password authentication using cued click-points': in Biskup, J. and Lopez, J. (eds.). ESORICS 2007, 12th European Symposium on Research in Computer Security. Dresden, Germany September 24-26, 2007. Springer, pp. 359-374 (2007)

[82] Chiasson, S., Forget, A., Biddle, R. & Oorschot, P.C.V.: 'Influencing users towards better passwords: persuasive cued click-points', Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1. Liverpool, United Kingdom British Computer Society, pp. 121-130 (2008)

[83] Parc, S. L.: 'InkClick: A new authentication method using graphical password'. MSc, University of Edinburgh, UK (2009)

[84] Gao, H., Ren, Z., Chang, X., Liu, X. & Aickelin, U.: 'A New Graphical Password Scheme Resistant to Shoulder-Surfing', International Conference on CYBERWORLDS, 20-22 Oct, Singapore (2010)

[85] Forget, A., Chiasson, S. & Biddle, R.: 'Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords', Proceedings of the 28th international conference on Human factors in computing systems. Atlanta, Georgia, USA ACM, pp. 1107-1110 (2010)

[86] Suo, X., Zhu, Y. & Owen, G. S.: 'Graphical password: a survey', Proceedings of the 21st Annual Computer Security Applications Conference. Washington, US IEEE Computer Society, pp. 463-472 (2005)

[87] Eljetlawi, A. M. & Ithnin, N.: 'Graphical Password: comprehensive study of the usability features of the recognition-base graphical password methods', 3rd International Conference of Convergence and Hybrid Information Technology, ICCIT '08. 11-13 Nov. 2008. IEEE Computer Society, pp. 1137-1143 (2008)

[88] Abdullah, M. D. H., Abdullah, A. H., Ithnin, N. & Mammi, H. K.: 'Towards identifying usability and security features of graphical password in knowledge based authentication technique', Asia International Conference on Modelling and Simulation. IEEE Computer Society, pp. 396-403 (2008)

[89] Jali, M. Z., Furnell, S., Dowland, P. & Reid, F.: 'A survey of user opinions and preference towards graphical authentications': In Bleimann, U.G., Dowland, P., Furnell, S. and Grout, V. (eds.) Proceedings of the Fourth Collaborative Research Symposium on Security, E-Learning, Internet and Networking (SEIN 2008). Wrexham, UK 5-8 November 2008. University of Plymouth, pp. 11-20 (2008)

[90] Lashkari, A. H., Farmand, S., Zakaria, O. & Salleh, R.: 'Shoulder-surfing attack in graphical password authentication'. International Journal of Computer Science and Information Security, 6 (2) pp. 145-154 (2009)

[91] Towhidi, F. & Masrom, M.: 'A survey on recognition-based graphical user authentication algorithms'. International Journal of Computer Science and Information Security, 6 (2) pp. 119-127 (2009)

[92] Biddle, R., Chiasson, S. & Oorschot, P.C.V.: 'Graphical Passwords: learning from the first generation'. Technical Report. School of Computer Science, Carleton University, Ottawa, Canada. TR-09-09 (Version October 2, 2009). Available at: http://hotsoft.carleton.ca/~sonia/content/Chiasson_gp_survey_techreport.pdf (Accessed: 6 October 2010) (2009)

[93] Tullis, T. S. & Tedesco, D. P.: 'Using personal photos as pictorial passwords', CHI 05 extended abstracts on Human factors in computing systems. Portland, Oregon, USA ACM New York, pp. 1841-1844 (2005)

[94] Hayashi, E., Dhamija, R., Christin, N. & Perrig, A.: 'Use Your Illusion: secure authentication usable anywhere', Proceedings of the 4th symposium on Usable privacy and security. Pittsburgh, Pennsylvania ACM, pp. 35-45 (2008)

[95] Chiasson, S., Forget, A. & Biddle, R.: 'Accessibility and graphical passwords'. Symposium on Usable Privacy and Security (SOUPS). July 2008 ACM (2008)

[96] Renaud, K.: 'Guidelines for designing graphical authentication mechanism interfaces'. International Journal of Information and Computer Security, 3 (1) pp. 60-85 (2009)

[97] Poet, R. & Renaud, K.: 'A mechanism for filtering distractors for doddle passwords'. International Journal of Pattern Recognition and Artificial Intelligence, 23 (5) pp. 1005-1029 (2009)

[98] Gao, H. & Liu, X.: 'A new graphical password scheme against spyware by using CAPTCHA', Proceedings of the 5th Symposium on Usable Privacy and Security. Mountain View, California ACM, pp. 1-1 (2009)

[99] Moncur, W. & Leplatre, G.: 'Pictures at the ATM: Exploring the usability of multiple graphical password', CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems. San Jose, USA, ACM, pp. 887-894 (2007)

[100] Everitt, K. M., Bragin, T., Fogarty, J. & Kohno, T.: 'A comprehensive study of frequency, interference, and training of multiple graphical passwords', Proceedings of the 27th international conference on Human factors in computing systems. Boston, MA, USA ACM, pp. 889-898 (2009)

[101] Chiasson, S., Forget, A., Stobert, E., Oorschot, P. C.V. & Biddle, R.: 'Multiple password interference in text passwords and click-based graphical passwords', Proceedings of the 16th ACM Conference on Computer and Communications Security. Chicago, Illinois, USA ACM, pp. 500-511 (2009)

[102] Magalaes, S.T.D., Revett, K. & Santos, H.M.: 'Generation of authentication strings from graphics keys'. International Journal of Computer Science and Network Security, 6 (3B) pp. 240-246 (2006)

[103] Rass, S., Schuller, D. & Kollmitzer, C.: 'Entropy of Graphical Passwords: Towards an Information-Theoretic Analysis of Face-Recognition Based Authentication'. Communications and Multimedia Security. Springer Berlin / Heidelberg, pp. 166-177 (2010)

[104] Stobert, E. 'Usability and strength in Click-based graphical passwords'. CHI 2010. Atlanta, Georgia, USA: 10-15 April 2010 ACM (2010)

[105] Brostoff, S., Inglesant, P. & Sasse, M. A.: 'Evaluating the usability and security of a graphical one-time PIN system'. 24th BCS Conference on Human Computer Interaction (HCI2010). Dundee, Scotland: 6-10 September 2010. Available at: http://hornbeam.cs.ucl.ac.uk/hcs/publications/Brostoff+Inglesant+Sasse_Evaluating%20the%20usability%20and%20security%20of%20a%20graphical%20one-time%20PIN%20system%20-%20HCI2010.pdf (Accessed: 23 September 2010) (2010)

[106] Renaud, K. & Just, M.: 'Examining User Responses to Association-Based Authentication'. HCI 2010: The 24th BCS Conference on Human Computer Interaction. University of Abertay, Dundee: 6-10 Sept, 2010 (2010)

[107] Alsulaiman, F. A. & Saddik, A. E.: 'Three-Dimensional password for more secure authentication'. IEEE Transactions on Instrumentation and Measurement, 57 (9) pp. 1929-1938 (2008)

[108] Sabzevar, A. P. & Stavrou, A.: 'Universal Multi-Factor Authentication Using Graphical Passwords', IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008. SITIS '08, IEEE pp. 625-632 (2008)

[109] Oorschot, P. C. V. & Wan, T.: 'TwoStep: An authentication method combining Text and Graphical Passwords', E-Technologies: Innovation in an Open World, Lecture Notes in Business Information Processing. 4-6 May 2009. Springer Berlin Heidelberg, pp. 233-239 (2009)

[110] Zheng, Z., Liu, X., Yin, L. & Liu, Z.: 'A hybrid password authentication scheme based on shape and text'. Journal of Computers, 5 (5) pp. 765-772 (2010)

[111] Hayashi, E., Hong, J. & Christin, N.: 'Educated guess on graphical authentication schemes: vulnerabilities and countermeasures', ACM International Conference Proceeding Series Proceedings of the 5th Symposium on Usable Privacy and Security (Poster Session). Mountain View, California ACM New York, USA, pp. Article no 25. (2009)

[112] Peach, S., Voster, J. & Heerden, R. V.: 'Heuristic Attacks against graphical password generators': In Clarke, N., Furnell, S. and Solms, R.V. (eds.). Proceedings of the South African Information Security Multi Conference (SAISMC 2010). Port Elizabeth, South Africa May 17-19, 2010. University of Plymouth, pp. 272-284 (2010)

[113] Salehi-Abari, A., Thorpe, J. & Oorschot, P. C.V.: 'On purely automated attacks and click-based graphical passwords', ACSAC '08: Proceedings of the 2008 Annual Computer Security Applications Conference. IEEE Computer Society, pp. 111-120 (2008)

[114] Oorschot, P. C.V., Salehi-Abari, A. & Thorpe, J.: 'Purely automated attacks on Passpoints-style graphical passwords'. Transactions on Information Forensics and Security, 5 (3) pp. 393-405 (2010)

[115] LeBlanc D., Alain, F. & Robert, B.: 'Guessing click-based graphical passwords by eye tracking', Eighth Annual International Conference on Privacy Security and Trust (PST), IEEE, pp. 197-204 (2010)

[116] Thorpe, J. & Oorschot, P.C.V.: 'Human-seeded attacks and exploiting hot-spot in graphical passwords', 16th USENIX Security Symposium. Boston, MA USENIX.org, pp. 102-118 (2007)

[117] Dunphy, P., Nicholson, J. & Olivier, P.: 'Securing Passfaces for description', Proceedings of the 4th symposium on Usable privacy and security (SOUPS 2008). Pittsburgh, Pennsylvania, USA July 23-25, 2008. ACM, pp. 24-35 (2008)

[118] Tari, F., Ozok, A. A. & Holden, S. H.: 'A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords'. Proceedings of the second symposium on Usable privacy and security, Pittsburgh, Pennsylvania, ACM pp. 56-66 (2006)

[119] Dirik, A. E., Memon, N. & Birget, J.C.: 'Modeling user choice in the Passpoints graphical password scheme'. Proceedings of the 3rd symposium on Usable Privacy and Security. Pittsburgh, PA ACM, pp. 20-28 (2007)

[120] Golofit, K.: 'Picture passwords superiority and picture passwords dictionary attacks'. Journal of Information Assurance and Security, 2 pp. 179-183 (2007)

[121] Golofit, K.: 'Click passwords under investigation': In Biskup, J. and Lopez, J. (eds.) Computer Security - ESORICS 2007, 11th European Symposium on Research in Computer Security. Springer Berlin/Heidelberg, pp. 343-358 (2007)

[122] Oorschot, P. C. v. & Thorpe, J.: 'On predictive models and user-drawn graphical passwords'. ACM Transactions on Information and System Security (TISSEC), 10 (4) pp. 1-33 (2008)

[123] Chiasson, S., Forget, A., Biddle, R. & Oorschot, P.C.V.: 'User interface design affects security: Patterns in click-based graphical passwords'. International Journal of Information Security, 8 (6) pp. 387-398 (2009)

[124] Jali, M. Z., Furnell, S. M. & Dowland, P. S.: 'Assessing image-based authentication techniques in a web-based environment'. Information Management & Computer Security, 18 (1) pp. 43-53 (2010)

[125] Doja, M. N. & Kumar, N.: 'Image authentication schemes against key-logger spyware', ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. IEEE Computer Society, pp. 574-579 (2008)

[126] John, M. S., Parvathi, V. S., Sekhar, M. R. & Babu, P. R.: 'Enhancing security of Passpoints system using variable tolerance'. International Journal of Advanced Networking and Applications, 1 (4) pp. 270-274 (2010)

[127] Birget, J. C., Hong, D. & Memon, N.: 'Graphical passwords based on robust discretization'. IEEE Transactions on Information Forensics and Security, IEEE Xplore, 1 (3) pp. 395-399 (2006)

[128] Chiasson, S., Srinivasan, J., Biddle, R. & Oorschot, P.C.V.: 'Centered discretization with application to graphical password'. Proceedings of the 1st Conference on Usability, Psychology, and Security, San Francisco, California, USENIX Association, pp. 1-9 (2008)

[129] Bicakci, K.: 'Optimal discretization for high-entropy graphical passwords'. 23rd International Symposium on Computer and Information Sciences, IEEE ISCIS. Istanbul, Turkey: October 27-29. IEEE, pp. 1-6 (2008)

[130] Abdulah, M. D. H., Abdullah, A. H., Ithnin, N. & Mammi, H. K.: 'Graphical password: User's affinity of choice-An analysis of picture attributes selection', International Symposium on Information Technology, 2008. ITSim 2008. IEEE Computer Society, pp. 1-6 (2008)

[131] Suo, X., Zhu, Y. & Owen, G. S.: 'The Impact of Image Choices on the Usability and Security of Click Based Graphical Passwords', Proceedings of the 5th International Symposium on Advances in Visual Computing: Part II. Las Vegas, Nevada Springer-Verlag, pp. 889-898 (2009)

[132] Renaud, K.: 'On user involvement in production of images used in visual authentication'. Journal of Visual Languages and Computing, 20 (1). pp 1-15 (2009)

[133] Catuogno, L. & Galdi, C.: 'A graphical pin authentication mechanism for smart cards and low-cost devices'. 2nd Italian Workshop on Privacy and Security (Prise2007). Rome, Italy (2007)

[134] Bicakci, K., Yuceel, M., Erdeniz, B., Gurbaslar, H. & Atalay, N. B.: 'Graphical passwords as browser extension: implementation and usability study'. Trust Management III: IFIP Advances in Information and Communication Technology. Springer Boston, pp 15-29 (2009)

[135] Jansen, W.: 'Authenticating mobile device users through image selection'. The Internet Society: Advances in Learning Commerce and Security, 1 pp 183-194 (2004)

[136] Takada, T., Onuki, T. & Koike, H.: 'Awase-E: Recognition-based Image Authentication Scheme Using Users' Personal Photographs'. Innovation in Information Technology (IIT2006). Dubai, UAE: 19-21 November 2006 IEEE (2006)

[137] Onali, T. & Ginesu, G.: 'Transmission-efficient image-based authentication for mobile devices'. Visual Content Processing and Representation. Springer Berlin / Heidelberg, pp. 22-28 (2006)

[138] Dunphy, P., Heiner, A.P. & Asokan, N.: 'A closer look at recognition-based graphical passwords on mobile devices', Proceedings of the Sixth Symposium on Usable Privacy and Security. Redmond, Washington ACM, pp. 1-12 (2010)

[139] Brostoff, S. & Sasse, A.: 'Are Passfaces more usable than passwords? A field trial investigation': in McDonald, S. et al., (ed.) Proceedings of HCI 2000. Sunderland, UK Springer, pp. 405-424 (2000)

[140] Valentine, T.: 'An evaluation of the Passfaces personal authentiation'. Technical Report. Goldsmiths College, University of London (1998)

[141] Valentine, T.: 'Memory for Passfaces after a long delay'. Technical Report. Goldsmiths College, University of London (1999)

[142] Google: 'Google password guidelines'. [Online]. Available at: https://www.google.com/accounts/PasswordHelp (Accessed: 24 May 2010) (2010)

[143] NIST: 'NIST password guidelines'. [Online]. Available at: http://www.itl.nist.gov/fipspubs/fip112.htm (Accessed: 24 May 2010) (2010)

[144] Microsoft: 'Microsoft password guidelines'. [Online]. Available at: http://www.microsoft.com/protect/fraud/passwords/create.aspx (Accessed: 24 May 2010) (2010)

[145] Furnell, S.: 'An assessment of website password practices'. Computers and Security, 26 pp. 445-451 (2007)

[146] Garrison, C. P.: 'Encouraging good passwords', Proceedings of the 3rd Annual Conference on Information Security Curriculum Development. Kennesaw, Georgia ACM, pp. 109-112 (2006)

[147] Gao, H., Chang, X., Ren, Z., Aickelin, U. & Wang, L.: 'Can Background Baroque Music Help to Improve the Memorability of Graphical Passwords?': In Campilho, A. and Kamel, M. (eds.) 'Image Analysis and Recognition'. Springer Berlin / Heidelberg, pp 378-387 (2010)

[148] O'Gorman, L.: 'Comparing passwords, tokens, and biometrics for user authentication': Proceedings of the IEEE, 91(12), pp 2019 - 2040 (2003)

[149] Renaud, K.: 'Quantifying the quality of web authentication mechanism: A usability perspective'. Journal of Web Engineering 3(2), pp. 95-123 (2003)

[150] Smith, R.E.: 'Authentication: from passwords to public keys'. Addison-Wesley Professional. ISBN 978-0201615999. (2001)

[151] Shepard, R. N.: 'Recognition memory for words, sentences and pictures'. Journal of Verbal Learning and Verbal Behaviour, 6, pp. 156-163. (1967)

[152] Nickerson, R. S.: 'A note on long-term recognition memory for pictorial material'. Psychonomic Science, 11 (2). pp. 58. (1968)

[153] Standing, L., Conezio, J. and Baher, R. N.: 'Perception and memory for pictures: Single-trial learning of 2500 visual stimuli'. Psychonomic Science, 19 (2), pp. 73-74. (1970)

[154] Standing, L.: 'Learning 10,000 pictures'. Quarterly Journal of Experimental Psychology, 25, pp. 207-222. (1973)

APPENDIX A:

List of Questionnaires

(1)Users’ familiarity and perception
(2)Click versus Choice comparisons
(3)EGAS
(4)EGAS : Further evaluations

Appendix A, No 1

The purpose of this questionnaire is to obtain your opinion on the use of images/pictures as one alternative for user authentication.

Part 1: Your details (Please circle you answer)

a) Your age is _____ years old in 2008.
b) Your sex : (Male / Female)
c) Your nationality : _____
d) Your highest education : (Bachelor / Master / PhD / Other: _____)
e) Your job : (Student / Researcher / Lecturer / Other: _____)
f) Years of using computer : (1 - 5 / 6 - 10 / 11 - 15 / 16+)
g) Have you ever heard or know images/pictures could be used as one of the user authentication methods (Yes / No)

Part 2: Your Opinion (Please answer the questions after using the prototype)

Briefly, there are three well-known approaches of images/pictures authentication,

a) **click-based** - you need to click on a set of secret regions or points within an image
b) **choice-based -** you need to select a sequence of secret images from a larger set
c) **draw-based -** you need to draw something that only you know it (e.g. using mouse or a touchpad)

Now, please use the prototype and later answer the following questions. The purpose of this prototype is to give you an idea on the existing methods for authentication using images/pictures as explained before.

1) Please circle on **Yes** or **No** for each statement.

Click-based	1) It is easy and fun to use.	Yes / No
	2) I don't have problem to remember my passwords/secrets.	Yes / No
	3) It is easy for me to re-produce my passwords.	Yes / No
	4) I think it can be used for web authentication	Yes / No
Choice-based	1) It is easy and fun to use.	Yes / No
	2) I don't have problem to remember my passwords/secrets.	Yes / No
	3) It is easy for me to re-produce my passwords.	Yes / No
	4) I think it can be used for web authentication.	Yes / No
Draw-based	1) It is easy and fun to use.	Yes / No
	2) I don't have problem to remember my passwords/secrets.	Yes / No
	3) It is easy for me to re-produce my passwords.	Yes / No
	4) I think it can be used for web authentication.	Yes / No

2) If given an option, which type do you prefer to be used for the **web authentication?**
(Click-based / Choose-based / Draw-based / None of them)

Why?_____
_____

3) What do you think images/pictures authentication towards potential 'threats' as below? (Please mark/circle **Safe** or **Unsafe** for each statement)

Click-based	1) Observer / shoulder-surfer, etc	Safe / Unsafe
	2) Close family / friend, etc	Safe / Unsafe
	3) Dictionary attacks, algorithms, etc	Safe / Unsafe
Chose-based	1) Observer / shoulder-surfer, etc	Safe / Unsafe
	2) Close family / friend, etc	Safe / Unsafe
	3) Dictionary attacks, algorithms, etc	Safe / Unsafe
Draw-based	1) Observer / shoulder-surfer, etc	Safe / Unsafe
	2) Close family / friend, etc	Safe / Unsafe
	3) Dictionary attacks, algorithms, etc	Safe / Unsafe

4) Do you have anything to comment/suggest regarding the image/picture authentication?
_____
_____

End of questions

Thank you very much for your cooperation. If you have any questions regarding this research, do not hesitate to contact me via email mohd.jali@plymouth.ac.uk

Appendix A, No 2

This questionnaire is to obtain your opinion. Please answer all questions.

a) Click-based as web authentication

Rating Scales

(1 – Strongly Don't Agree**) (2 –** Don't Agree**) (3 –** Neutral**) (4 –** Agree**) (5 –** Strongly Agree**)**

Statements	1	2	3	4	5
a) I think I can easily remember my secrets (passwords). If (1) or (2), please explain why? _____					
b) During confirmation of my secret, I can easily provide the information (my chosen secrets) required. If (1) or (2), please explain why? _____					
c) I can login with my secrets without any major problem. If (1) or (2), please explain why? _____					
d) I would consider using this method in the web If No, please explain why? _____	(Yes / No / Don't Know)				
e) If you answered 'Yes' for (d), what types of web application do you think this method could be beneficial for? (**you may choose more than one**)	[ ] – Banking [ ]–Intranet (internal) [ ] – Email [ ] – Others: _____ _____ _____				
f) I think my partner/close friends will have difficulty to reproduce my secrets if I just briefly explain to them what my secrets are. If (1) or (2), please explain why? _____					
g) Suggestions _____					

Appendix A, No 2

b) Choice-based as web authentication

Rating Scales

(1 – Strongly Don't Agree**) (2 –** Don't Agree**) (3 –** Neutral**) (4 –** Agree**) (5 –** Strongly Agree**)**

Statements	1	2	3	4	5
a) I think I can easily remember my secrets (passwords). If (1) or (2), please explain why? _____					
b) During confirmation of my secret, I can easily provide the information (my chosen secrets) required. If (1) or (2), please explain why? _____					
c) I can login with my secrets without any major problem. If (1) or (2), please explain why? _____					
d) I would consider using this method in the web If No, please explain why? _____	(Yes / No / Don't Know)				
e) If you answer is 'Yes' for (d), what types of web application do you think this method could be benefit for? (**you may choose more than one**)	[ ] – Banking [ ] – Intranet (internal) [ ] – Email [ ] – Others: _____ _____ _____				
f) I think my partner/close friends will have difficulty to reproduce my passwords if I just briefly explain to them what my secrets are. If (1) or (2), please explain why? _____					
g) Would you be happy if your secrets arranged/grouped in categorical order? If No, please explain why? _____	(Yes / No / Don't Know)				
h) If you answered 'Yes' for (g), in what order you prefer it to be arranged (**please number from 1 to 5 to indicate the preferred sequence if you choose Fixed order**) (1) Fixed order - Transport [ ] - Other [ ] - Nature [ ] - Food [ ] - Animal [ ] (2) I prefer random order [ ]					

Appendix A, No 2

i) Suggestions _____	

c) Web Prototype

Rating Scales

(1 – Strongly Don't Agree**) (2 –** Don't Agree**) (3 –** Neutral**) (4 –** Agree**) (5 –** Strongly Agree**)**

General	**1**	**2**	**3**	**4**	**5**
a) The design of this prototype was appropriate for graphical authentication If (1) or (2), please explain why? _____					
b) The images and texts displayed in the prototype were clear and reasonable If (1) or (2), please explain why? _____					
c) The instructions for registration, confirmation and login steps were clear and understandable. If (1) or (2), please explain why? _____					
d) To ensure I do not forget my secrets, I would prefer using my own images rather than those provided by the system. If (1) or (2), please explain why and state what types of image? _____					
e) If enough training provided, I could do better for both methods. If (1) or (2), please explain why? _____					
f) I prefer using username/password authentication as compared to these both methods. If (1) or (2), please explain why? _____					
g) Suggestions _____ _____					

End of questions

Thank you very much for your cooperation. If you have any questions regarding this research, do not hesitate to contact me via email mohd.jali@plymouth.ac.uk

Appendix A, No 3

The questionnaire aims to give opportunity for you to provide comments, feedbacks and suggestions. Briefly, the questionnaire is grouped into five categories and you are requested to answer all.

Section A: Demographic

1) Gender : (Male / Female)
2) Age : _____ years old.
3) Education : (Certificate / Degree / Masters / PhD / Others)
4) Computer experience(s) : (Beginner, Intermediate, Advanced)

Section B: Registration and Confirmation

1) I believe I can easily remember all my secrets (images and clicks) well.

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

2) Overall, the registration process was easy and understandable.

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

3) Please indicate the **level of 'ease of use'** during registration and confirmation.

1 Really difficult	2	3	4 Neutral	5	6	7 Really easy

4) I prefer clicking all my 'secret clicks' onto **one image only** instead of **one click per image**.

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

Section C: Various Login Strategies

1) Overall, the Login processes were easy and understandable.

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

2) Please indicate the **level of 'ease of use'** for **scenario One**

1 Really difficult	2	3	4 Neutral	5	6	7 Really easy

Appendix A, No 3

3) Please indicate the **level of 'ease of use'** for **scenario Two**

1 Really difficult	2	3	4 Neutral	5	6	7 Really easy

4) Please indicate the **level of 'ease of use'** for **scenario Three**

1 Really difficult	2	3	4 Neutral	5	6	7 Really easy

5) Please indicate the **level of 'ease of use'** for **scenario Four**

1 Really difficult	2	3	4 Neutral	5	6	7 Really easy

6) Which scenario you most likely prefer to use during Login.

One	Two	Three	Four	None of them

7) Please rate your chosen scenario above in term of 'preference'

1 Really dislike	2	3	4 Neutral	5	6	7 Really prefer

8) Which scenario do you think could **offer the most security** and could **protect your secrets**

One	Two	Three	Four	None of them

9) Please rate **the level of security** of your preferred scenario

1 Really unsecure	2	3	4 Neutral	5	6	7 Really secure

Section D: Interface Design

1) Overall, I found the interface designs and instructions were understandable.

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

Appendix A, No 3

2) The **size of each image during user-chosen images** was appropriate

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

3) The **size of images during Login** was appropriate/just right

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

4) The 'error' messages were helpful and clear

1 Strongly disagree	2	3	4 Neutral	5	6	7 Strongly agree

Section E: Recommendations/Suggestions/Comments

_____
_____
_____

End of question. Thank you for your time participating in this study

Appendix A, No 4

The questionnaire aims to give opportunity for participant to provide comments, feedbacks and suggestions. There are three sections. Please answer all.

Section A: Demographic

1) Gender : _____
2) Age : __ years
3) Highest Education : _____
4) Have you heard about authentication using images/graphical passwords before this trial? (Yes / No)
5) If 'yes', where did you hear about it? _____

Section B: Perceived Usability

1) Please indicate your opinion on the Graphical Password Guidelines (GPG).
   a. Very useful
   b. Useful
   c. Neither useful nor useless
   d. Useless
   e. Very useless

2) Please indicate your opinion towards the Graphical Password Restrictions (GPR).
   a. Very useful
   b. Useful
   c. Neither useful nor useless
   d. Useless
   e. Very useless

3) I found that both GPG and GPR during the account registration stage were helpful and informative.
   a. Strongly agree
   b. Agree
   c. Neither agree nor disagree
   d. Disagree
   e. Strongly disagree

4) The average time for your login was _____ seconds. How do you rate your login time?
   a. Acceptable
   b. Unacceptable

5) The time for account creation was ____ minutes and ____ seconds. How do you rate your account creation time?
   a. Acceptable
   b. Unacceptable

6) With regards to the image and click preferences, please choose one of the statements below.
   a. I think having **more clicks** is more memorable than having **more images** (e.g. 2 images with 5 clicks on each image)
   b. I think having **more images** is more memorable than having **more clicks** (e.g. 6 images with 1 click on each image)
   c. I think the **balance between clicks and image** are memorable (e.g. 3 images with 3 clicks on each image)

Appendix A, No 4

7) Do you think you can recall all your secrets if you not using it for a while? Please indicate one of the statements.
   a. Yes, both images and clicks
   b. Yes, only images
   c. Yes, only clicks
   d. No, neither clicks nor images

Section C: Feedback

1) Did you use any specific techniques/methods when selecting your secret images and the click locations?

_____

_____

2) Any other recommendations/suggestions/comments you would like to add?

_____

_____

End of questionnaire. Thank you for your time participating in this study.

APPENDIX B:

Participant Briefing Sheets

(1)Click versus Choice comparisons
(2)EGAS
(3)EGAS : Further evaluations

Appendix B, No 1

Enhancing the Usability of User Authentication

Briefing document for potential participants in user trial

Mohd Zalisham Jali
mohd.jali@plymouth.ac.uk
Centre for Information Security & Network Research (CISNR)
School of Computing, Communications and Electronics
University of Plymouth

About the research:

The main objective of this research is to investigate usability and security of graphical authentication methods, which provide possible alternatives to traditional username/password authentication.

What you are required to do?

In this trial, you are required to use two different types of graphical authentication method; one that involves clicking upon areas within a given image (hereafter called **click-based** type) and another that involves selecting a series of images from within a set of larger images (hereafter called **choice-based** type). In the first case the authentication task will involve remembering the points that you chose within the image, whereas in the second case it will be recalling the series of images. Below is the series of tasks you need to perform:

1) Register and confirm your areas for **click-based** method (online)
2) Register and confirm your images for **choice-based** method (online)
3) Do the 'spot the difference' activity (on paper)
4) Login by using your **click-based** method (online)
5) Login by using your **choice-based** method (online)
6) Answer the questionnaire (on paper)

Before registering to your secrets, you are required to type username and provide information such as gender, age and years of using a computer. Please be informed that the maximum length of your username is **8** characters and it can be made up of any characters (i.e. alphabetic, numeric, etc).

For the **click-based** method, you are required to register your secret by **clicking on five different points** in the given image. You must remember **not to** click your secrets in the same place or within the same click areas. For **choice-based** method, you are required to create your secret by **selecting five images.** As the images are grouped within themed categories, all you need to do is choose one image for each category. For both click-based and choice-based approaches, you must remember your secrets in sequence without writing them down.

Before proceeding to the Login task, you need to do the **'spot the difference'** activity. The purpose of doing this activity is to provide you with a spare time between the registering and the login task. Here, you will be provided with three set of images and what you need to do is to **identify the difference or missing objects** between the original and the edited one. **Each set of image contains at least 8 differences or more**.

During the Login task, no restriction applied to the number of authentication rounds. It means that if you do not manage to login for the first time, you may allow to do it until successful. In addition to that, if by any reasons you totally forgot your secrets and wish not to continue the tasks, you are allowed to do it as well.

Appendix B, No 1

All of the data will be captured and stored into the database. Among of the stored data are the username, time of registration, confirmation and login, number of attempts and the secrets itself. All of these will be analysed and investigated further.

In this trial, you will have the right to withdraw at any time, and to withhold any data collected from you up to the point of your withdrawal. In addition to that, the researcher will be available to provide any necessary assistance and answer any questions that you may have regarding the progress of the tasks

How long will it take?

The time required to complete all the tasks will typically be between 30 to 40 minutes and no more than an hour.

What will the results of the study are used for?

The result of this trial will contribute towards PhD research that is assessing the usability and security of different authentication methods, with the ultimate aim of devising new (or enhanced) methods that address any current problems.

All results from this trial will be used and reported anonymously in the ongoing research. You will be given an opportunity to find out the results of this trial by asking for a copy of the findings to be emailed to you after the full study has been conducted and analysed.

Finally, any further enquiries about how this user trial should be conducted, please do not hesitate to contact the Faculty of Technology Business Manager, Sarah Tilley at +44 (0)1752 233311 or email sarah.tilley@plymouth.ac.uk.

Thank you very much indeed for your time and kind participation.

Participant's Informed Consent

I hereby confirm that I have read the briefing sheet, I am clear on what needs to be done and I am happy to participate in this trial.

_____

Name :
Email :

Appendix B, No 2

Enhancing User Authentication with Graphical Approach

Briefing document for participant participating in the study

Mohd Zalisham Jali
(mohd.jali@plymouth.ac.uk)
Centre for Security, Communications & Network Research (CSCAN)
School of Computing and Mathematics, Faculty of Science and Technology
University of Plymouth

About the study

The main objectives of this study are to identify and investigate the usability of new graphical method for user authentication, which provide possible alternatives to traditional username/password approaches. The trial attempts to evaluate a number of alternative scenarios, in order to determine which one(s) work most effectively and are most acceptable to participants.

What you are required to do

In this trial, you are required to use the software prototype and later on provide feedback. The study involves two (2) phases and is explained as below:-

Phase One: User trial

- This phase requires you to create an account and then sign back into the system later using a number of alternative scenarios. The details of each process are as follow:

  a) Register and confirm to the secret (Account creation)
  - You need to **remember six images** (4 images that will be chosen by you and 2 that are randomly assigned to you by the system), and **clicking once on any area for each of your remembered images**. The combination of images and clicks within images will form your secrets (passwords), which you will need to use it later during login.

  b) Signing back into the system
  - You are required to sign back into the system by using four (4) different login scenarios.
  - There will be no limitation on the number of attempts; therefore you could try as many as you wish to try.

- You are recommended to go through the training (provided in the software prototype) before starting your trial as it will provide a clearer idea on how the new methods work.

Phase Two: Answering a questionnaire

- The purpose of the questionnaire is to give opportunity to you to express feedbacks and suggestions about the new method. The questionnaire can be found and will be carried out within the software prototype.

All of your details such as username, registration details (time, secret images and secret clicks) and login details (time, number of attempts, secret clicks) will be recorded into the database. None of these will be used for any purpose other than evaluating the authentication approaches under trial.

The detail instructions on the tasks you need to carry out is attached in the separate sheet

Appendix B, No 2

How long will it take?

The total amount of time will depend upon your experiences with the new methods, but on average the trial requires **no more than 40 minutes**.

What will the results of the study are used for?

The result of this trial will contribute towards PhD research that is assessing the usability and security of different authentication methods, with the ultimate aim of devising new (or enhanced) methods that address any current problems.

All results from this trial will be used and reported anonymously in the ongoing research. You will be given an opportunity to find out the results of this trial by asking for a copy of the findings to be emailed to you after the full study has been conducted and analysed.

Any further enquiries about how the study has been conducted, do not hesitate to contact the Secretary, Faculty of Science and Technology Human Research Ethics Committee, **Mrs Paula Simson** at **paula.simson@plymouth.ac.uk**

Thank you very much indeed for your time and kind participation.

Participant's Informed Consent

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

Under these circumstances, I agree to participate in the research.

_____

Name :
Date :
Email :

Appendix B, No 3

Enhancing User Authentication with a Graphical Approach

Briefing document for participants in the study

Mohd Zalisham Jali
(mohd.jali@plymouth.ac.uk)
Centre for Security, Communications & Network Research (CSCAN)
School of Computing and Mathematics, University of Plymouth

About the user trial

This user trial investigates the usefulness and effect of introducing 'graphical password guidelines' and 'graphical password restrictions' during account registration using an Enhanced Graphical Authentication Scheme (EGAS), one possible alternative for traditional username and password authentication.

Briefly, a Graphical Password Guideline (GPG) is a course of actions for supporting the user when creating passwords; choosing better images and creating 'safer and secure' clicks towards chosen images. In addition, a Graphical Password Restriction (GPR) is a course of rules for restrict users' actions in order to eliminate and control the problem of insecure user behaviour which resulted in graphical password vulnerabilities.

The study hypothesises that combining graphical password guidelines with the graphical password restrictions may perhaps encourage the user to create better and safer passwords (both images and clicks).

What you are required to do

In this trial, you are required to use the software prototype and later on provide feedback. The trial involves two phases and is explained below:-

Phase One: User trial

- This phase requires you to create an account and then login with your secrets.
  - ***c) Register and confirm the secret (Account creation)***
    - The tasks involve selecting a series of images (as your secret) from the image pool and then clicking on chosen points within the selected images (as your secret clicks). The number of images you are allowed to choose will depend on the number of click points you are willing to choose within each one (i.e. more click points means fewer images and vice versa).
    - Further details on what you are required to do as provided at each stage within the software prototype.
  - ***d) Logging back into the system***
    - This task assesses your ability to login using your chosen images and click points. You are required to login three times. There is no restriction of the number of attempts, hence you are allowed to continue trying to login until you are successful.

- You are recommended to go through the training (provided in the software prototype) before starting your trial as it will provide a clearer idea on how the new method works.

Appendix B, No 3

Phase Two: Answering a questionnaire

- The purpose of the questionnaire is to give an opportunity for you to express feedback and suggestions.

All of your details such as username, registration details (time, secret images and secret clicks) and login details (time, number of attempts, secret clicks) will be recorded into the database. None of these will be used for any purpose other than evaluating the authentication approaches under trial.

How long will it take?

The total amount of time will depend upon your ability to use the new methods consistently, but on average the trial requires **no more than 20 minutes**.

What will the results of this study be used for?

The result of this trial will contribute towards PhD research that is assessing the usability and security of different authentication methods, with the ultimate aim of devising new (or enhanced) methods that address current problems.

All results from this trial will be used and reported anonymously in the ongoing research. You will be given an opportunity to find out the results of this trial by asking for a copy of the findings to be emailed to you after the full study has been conducted and analysed.

If you have any queries about how the study has been conducted, please contact the researcher in the first place. Alternatively, please contact the Secretary, Faculty of Science and Technology Human Research Ethics Committee, **Mrs Paula Simson** at **paula.simson@plymouth.ac.uk**

Thank you very much indeed for your time and kind participation.

Participant's Informed Consent

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

Under these circumstances, I agree to participate in the research.

_____

Name :
Date :
Email :

APPENDIX C: Copy of Ethical Approval Letters

Appendix C, No 1

Faculty of Science and Technology

Smeaton 009, Plymouth

To:	Mohd Zalisham Jali	From:	Paula Simson
cc:	Prof Steven Furnell		Secretary to Human Ethics Committee
Your Ref:		Our Ref:	scitech:\d:\human ethics:
Date:	09 September 2010	Phone Ext:	84503

Application for Ethical Approval

Thank you for submitting the ethical approval form and details or the amendments concerning your project:

'Enhancing user authentication with graphical techniques'

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson

Faculty of Science and Technology

Portland Square A106, Plymouth

To:	Mohd Jali	From:	Paula Simson
cc:	Prof Steven Furnell, Dr Paul Dowland		Secretary to Human Ethics Committee
Your Ref:		Our Ref:	scitech:\d:\human ethics:
Date:	02 February 2010	Phone Ext:	84503

Application for Ethical Approval

Thank you for submitting the ethical approval form and details or the amendments concerning your project:

'Enhancing the usability of user authentication by using graphical techniques'

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson

APPENDIX D:

(1) Spot the different Image

(2) Can you spot the hotspot?

Appendix D, No 1

Source: http://www.santaspostbag.co.uk/spot-the-difference-christmas-quiz.shtml (Date accessed: 22 Dec. 2010)

Total differences for each pair of images are eight(8)

Appendix D, No 2










Assuming you are a hacker, can you guess one area that you think normal user will choose for each image. Thank you very much for your time

APPENDIX E: Copy of Published Papers

A survey of user opinions and preference towards graphical authentication

Abstract

User authentication is a process of proving a user's identity to the services or systems that they wish to use. The traditional way of using authentication is the combination of username and password. This paper presents a study carried out to investigate users' opinions and preferences towards the use of images/pictures as an alternative method of authentication. A survey was carried out within a university environment and participants were asked to use a standalone graphical authentication prototype and provide feedback. Overall, preliminary results of the study showed that although participants initially had problem using the prototype, they enjoyed using it after a few attempts. This indication and other positive results suggested that user authentication using pictures/images could be used as one of the alternatives for balancing the weaknesses in traditional username/passwords.

Keywords

Graphical password, Authentication, Usability

1. Introduction

User authentication is the first layer of interaction between human and machines. Generally, the purposes of user authentication are to confirm or validate the person and as the next steps from him/her to use the services offered. Today, the use of passwords, or other secret or knowledge-based methods (e.g. what is your mother's maiden name, what is the name of your pet) are still the most widely used. Despite of this widespread use, traditional user authentication has many issues and problems. Adams & Sasse (2005) summarised that people normally had problems remembering long and complex passwords, that passwords chosen were vulnerable to various types of attacks and problems with the usability of passwords themselves.

As a result of these problems, among the solutions that have been developed so far are using Single-Sign-On, Multi-factor authentication and the use of biometric-based approaches such as retina, hand, iris, voice, thumbprint and the patterns of mouse and keyboard movements (O'Gorman, 2003), with each of these solutions having their own strengths and weaknesses.

The objective of this paper is to report an initial study evaluating users' opinions and preferences on the use of images/pictures as an alternatives means for user authentication. The paper begins with an explanation of the background areas of the study and is followed by an explanation of how the study was approached together

with the results and findings. The paper ends by highlighting the conclusions and future work that the authors are planning to conduct.

2. Background

This section briefly discusses the issues of authentication and graphical password.

2.1 Authentication

Authentication can be defined as a process of proving who you are or claim to be. There are two main types of authentication; user authentication and machine authentication. User authentication deals with the interaction of a human (as the user) with the computer while machine authentication deals with the interaction between computers. This paper only discusses user-based authentication.

Users often confuse the concept of authentication with other services or processes such as access control, auditing and administration. Generally, auditing is a process of recording all of the activities conducted by users (as either legitimate or not), access control is to limit or restrict the actions and operations the legitimate users should perform; and administration is the process of managing the system services (Sandhu, 1997).

There are many approaches for user authentication. O'Gorman (2003) categorised user authentication into three; something you have or object-based (e.g. tokens), something you know or knowledge-based (e.g. password or other secret) and something you are in terms of psychology and/or behaviour (e.g. biometrics).

Even though many authentication methods have emerged, no single method is applicable for all applications. For instance, the use of biometrics is not practical when used with the current ATM machines and the use of long and complex passwords could pose difficulties to certain members of the community (e.g. the elderly or people with learning difficulties). That is why research into user authentication is still important and has gained much interest from the psychology and security domains.

2.2 Graphical Authentication

The idea of using graphics to aid with remembering passwords is not new, however the idea of using graphics as a replacement for passwords has emerged with the work patented by Blonder (1996), to offer better usability and security as opposed to the traditional username/password approach, claiming that using pictures/images could offer a larger password space and thus offer greater security. It was also suggested that the problem of remembering long and complex passwords could be

addressed by recognising images/pictures, as humans are very good at recognising and recalling images as opposed to words, sentences or phrases (Shepard, 1967).

In this paper, graphical authentication methods are grouped into three categories, based on the type of user interaction required: Choice-based, Click-based and Draw-based. The idea of each type is as follows:

- Choice-based requires users to select their chosen images from a set of decoy images. The image selection can be continued for several rounds depending on the system settings.

- Click-based requires users to click anywhere they prefer in the image. These clicks are actually their password. There are two further variations in this type; users click all locations in one image or users click once for each image.

- Draw-based requires users to draw their secret/password on the provided grid/screen. In this case, the drawing is interpreted as the password in order to be authenticated.

The Choice-based type taking place with the product known as Passfaces (Passfaces, 2003) in which, users needed to choose the image of faces in order to be authenticated. Later, Dejavu was introduced by Djamija and Perrig (2000). This used abstract images deployed from the Andrej Bauer's Random Art algorithm, an algorithm where bit of strings converted into the form of interesting abstract images. Overall, the Choice-based type is the most well-known because of its ease and simplicity while still maintaining the level of security. Other work within this group include ToonPasswords (Hinds & Ekwueme, 2007), VIP (De Angeli et al., 2003) and PassImages (Charruau et al., 2005).

The Click-based type was first developed and patented by Blonder (1996). In this scheme, users clicked on the predetermined areas of the image. As the password of this approach is easy to guess, Wiedenbeck et al. (2005) introduced an enhanced scheme known as Passpoints. In this approach, users are required to click on anywhere they prefer on the image. From all the usability studies carried out by the authors, they concluded that participants satisfied with the approach and it could be one of the alternatives for future user authentication. Recently, Chiasson et al. (2007) introduced the Cued Click Point (CCP) in which users are required to click once per image on a sequence of images. The next image is based on the previous click-point. The authors claimed that the approach could reduce the burden of memorising a sequence of click points as in Passpoints while at the same time enhancing the usability and security.

The first Draw-based scheme was Draw-A-Secret (DAS), developed by Jermyn et al., (1999). Another scheme in this group is Pass-Go (Tao, 2006). Recently, Yan & Dunply (2007) introduced the Background-DAS, claiming that this could eliminate

the problem of accuracy of user drawings and also offered larger password space and enhanced usability. Most of the schemes within this type were developed to be used in restricted environments such as phones and handheld devices.

In addition to the above schemes, graphical authentication is also being introduced to tackle the problem of shoulder-surfing and spyware (Li et al, 2005; Malek et al, 2006; Man et al, 2003). Overall, it was found that only a small number of approaches were actually tested for their usability, the others simply explain their idea and describe how their schemes would be able to prevent shoulder-surfing and spyware.

3. Methodology

The objectives of this study were to investigate users' opinions and preferences towards three types of graphical authentication, as explained in the earlier section. The study made an assumption that users would choose Click-based and Choice-based methods as their preferences for web authentication. This is based on the point of view where both are easy to use, memorable, offer an appropriate level of security and more importantly, can be used directly on the web without needing any additional hardware/software.

A survey was conducted in order to investigate the objectives. In this survey, participants were asked to use the prototype and then answer a related questionnaire. This activity took approximately 10 to 15 minutes to complete depending on the participants' experiences using computers. The following sections explain the prototype, questionnaire and outline the steps and procedures the participants had to follow.

3.1 Prototype

The prototype of three graphical authentication techniques was developed using Microsoft Visual Studio. All three schemes were developed and bundled in one application. The developed prototype was analogous in context with the Passpoints, Passfaces and DAS approaches. The purpose of this prototype was to give participants a brief hands-on experience and to demonstrate how graphical authentications could work in the real world.

Initially, the main intention of this study was to get participants opinions on web authentication using a graphical approach; however after considering many factors like accessibility, mobility and time, it was decided not to develop the prototype in a web environment but simply to have a small standalone application. The designs of three schemes were basically similar to the original Passfaces, Passpoint and DAS but simplified in terms of the number of passwords they need to register or use. This is due to the fact that the study only needed the participants to get an impression of

using graphical approaches and did not want to burden them by remembering up to five click points and five to six images.

There were two main modules in the prototype; Register and Login. In the register module, participants needed to register their passwords by clicking four times on the image for the click-based type, choosing two images for the Choice-based type and drawing freely for the draw-based type. Here, the drawing will take into account the location of mouse *click-down* and the location of mouse *click-up*. The types, shapes and number of drawings were left to the participants' preferences. Example screenshots for the prototype are shown in Figures 1, 2 and 3.

Figure 1: Screen shot of the click-based type

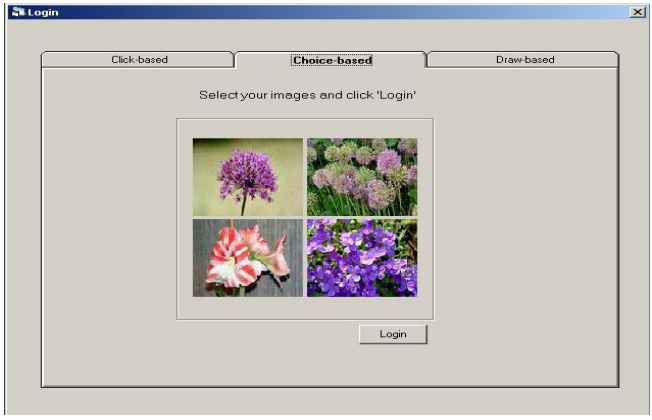

Figure 2: Screen shot of the choice-based type

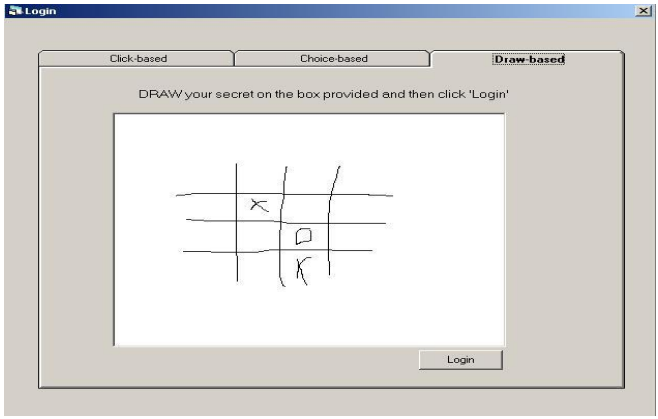

Figure 3: Screen shot of the draw-based type with an example of a secret drawn by one of the participants

3.2 Questionnaire

There were two sections in the questionnaire. Part A asked the participants to give their demographic information such as their age, gender, nationality, highest level of education, current job, years of using computers and asked their awareness and knowledge regarding the use of images/pictures as a means of alternative user authentication.

In part B, participants were asked to answer four questions after they finished using the prototype. The first question was about their opinion on the ease of use of each method, how easily they remembered their secret, how easily they could reproduce their password and whether they felt that the methods could be used in a web-based environment. The second question asked participants to select the method they would most strongly prefer to use for web-based authentication. For the third question, participants were asked their opinion about whether they would consider each method to be 'Safe' or 'Unsafe' against the following security threats: observer or shoulder-surfer, guessing by close family or friends and brute-force attack. The final question asked participants to give any comments and suggestions regarding image authentication.

In order to validate users' understanding and to reduce errors during the subsequent implementation, five participants took part in pilot testing where the prototype was evaluated. Appropriate changes and amendments were then made prior to the full run of the study.

3.3 Procedures and Steps

Participants were asked to use the prototype displayed on a 14-inch laptop screen with a wireless mouse as their input device. They were first to register their password and later, reproduce it or login by using the same password/secret they had chosen earlier. During the registration and login, appropriate messages were displayed in order to alert and give them information. After using the prototype, they were asked to answer the provided questionnaire. Upon using the prototype, all of the participants' actions and behaviour were observed for monitoring purposes. As this was an 'uncontrolled' type of survey, participants were allowed to use the prototype as many times as they wanted.

4. Results and Findings

A total of 25 volunteers took part in this initial study (12 males and 13 females). The minimum age of the participants was 30 years old. The majority of the participants were university staff (e.g. students, researchers, administrators and lecturers) and all of them had more than 6 years experience using computers.

When asked about their familiarity with the use of images/pictures for authentication purposes, only 11 participants indicated that they were aware of it. Accordingly, from the observation, it was found that participants were initially quite 'confused' with the 'state-of-the-art' of graphical authentication. For example in the Click-based type, the majority of them had problems reproducing their passwords. This is possibly due to their misunderstanding of this approach because when they clicked on particular points (for example clicking on the person's hand); they were assuming the whole image (in this case, the whole body of the person) was chosen. Only the point or the area in which they clicked would be taken into account as their password and not the whole object**.** Overall, only 12 participants managed to complete all the tasks successfully. This demonstrates that for the graphical password to be effective, appropriate training should be provided beforehand.

Users' preferences on the suitability of graphical scheme towards web authentication showed that participants preferred click-based (13 participants) and choice-based (12 participants) with no participants indicating a preference for the draw-based method. From the informal interview, the main reason why such schemes were preferable was because of their convenience and simplicity. However, the majority of the participants pointed 'unsure' or 'doubt' for the level of security of the choice-based method.

When using the prototype, it was found that all of the participants preferred using the choice-based method. They felt that the passwords were quite easy to remember and they had no problem reproducing their passwords during login. However, although the draw-based type was easy to use, participants had difficulty remembering and reproducing their drawings. It is likely that this was due to the

usage of the mouse and if participants were to use some sort of special device such as a stylus or a drawing pad, they would perform better. The results of ease of use, ease of recollection, ease of reproduction and suitability to be used in web environments were shown in Figure 4.

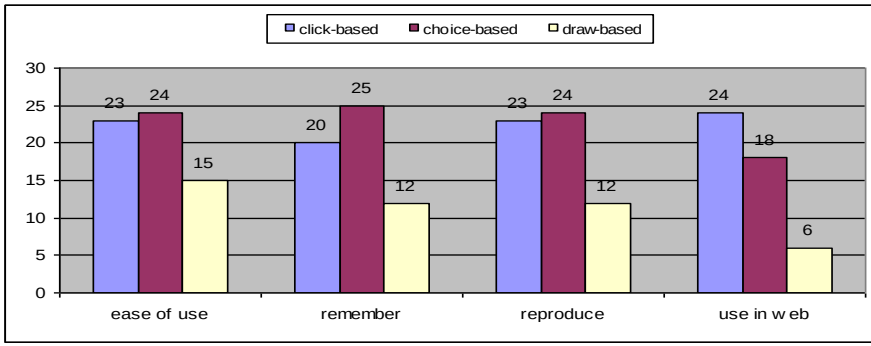

Figure 4: Users' opinion towards ease of use, remembrance, reproduction and use in web

The users' opinion towards the level of security the methods might offer, the majority of the participants believed that the draw-based method offered better security. This is due to the fact that it is impossible for users to draw alike. Conversely, more than half of the participants felt that choice-based would be vulnerable to guessing, brute-force and information harvesting vulnerabilities and interestingly although they felt that the choice-based type was not secure enough; they still choose it as their preferred method for web authentication. The detailed results on users' opinions towards security issues are presented in Figure 5.

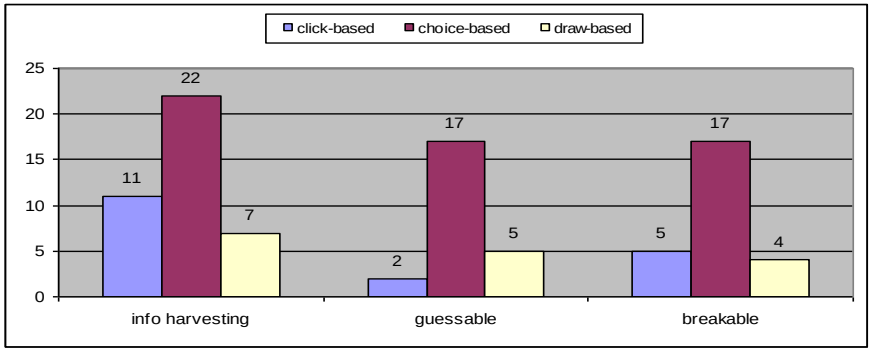

Figure 5: Users' opinion towards security issues like information harvesting, 'guessability' and 'breakability'

Here, the term ‘information harvesting’ refers to the vulnerability or actions done by the observer or shoulder-surfer. ‘Guessable’ refers to the vulnerability or guessing actions perform by closed family or friends, while the term ‘breakable’ deals with the vulnerability to some sort of educated guess, dictionary attack and/or computer algorithms. Although users may not have been able to offer truly informed opinions about these aspects, their views were still a valid reflection of what they perceived the security to be (which would therefore influence their confidence in using the approaches).

In summary, the assumption that participants would prefer choice-based and click-based types for web authentication was confirmed in this study. The contribution of this study when compared to earlier works is that it asked users to consider and compare all three types of graphical schemes (whereas others typically compared a single form of graphical authentication against traditional username/password methods).

5. Conclusion and the future

This paper presented an initial study on user opinions and preferences towards authentication using images/pictures. From the results and findings from 25 participants, it has shown that the level of familiarity and awareness towards graphical authentications were balanced; participants preferred the click-based and choice-based methods for web usage and they provided mixed opinions towards the issues of security and usability. Overall, the study concludes and suggests that using images and pictures could by some means be one of the alternatives for user authentication, especially in the web-environment.

However with the current state of graphical authentication, the authors feel that it is still too immature to be implemented on a large-scale and thus more work needs to be done in the areas of security and usability. The authors plan to extend this study with additional participants in order to obtain more conclusive and representative findings. In addition, a fully working prototype of graphical web authentication will be developed, enabling a series of experiments (both in-lab and field trial) to be carried out in order to more comprehensively assess user experiences in practice.

6. References

Adams, A. and Sasse, M.A. (2005), 'Users are not the enemy', in Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability: Designing secure systems that people can use*, O'Reilly Media Inc, CA, pp619-630, ISBN: 0-596-00827-9.

Blonder, G. (1996), *Graphical password*, 5.559.961, available at: http://www.patentstorm.us/patents/5559961.html, (accessed: 10 March 2008).

Charruau, D., Furnell, S. and Dowland, P. (2005), 'PassImages: an alternatives method of user authentication', *Proceedings of the ISOneWorld 2005 Conference*. Las Vegas, USA March 30 - April 1.

Chiasson, S., Oorschot, P.C.V. and Biddle, R. (2007), 'Graphical password authentication using Cued Click-points', In Biskup, J. and Lopez, J. (eds.) *ESORICS 2007, 12th European Symposium On Research In Computer Security*. Dresden, Germany September 24-26. Springer, pp359-374.

De Angeli, A., Coventry, L., Johnson, G. and Coutts, M. (2003), 'Usability and user authentication: Pictorial passwords vs. pin'. In McCabe, P.T. (ed.) *Contemporary Ergonomics 2003*. Taylor & Francis, pp253–258.

Djamila, R. and Perrig, A. (2000) 'Deja Vu: A user study using images for authentication', *Proceedings of the 9th USENIX Security Symposium*. Denver, Colorado, USA August 14-17, pp45-58.

Hinds, C. and Ekwueme, C. (2007), 'Increasing security and usability of computer systems with graphical password', *ACM Southeast Regional Conference*. Winston-Salem, North Carolina, USA ACM New York, USA, pp529-530.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.D. (1999), 'The design and analysis of graphical password', *Proceedings of the 8th USENIX Security Symposium*. Washington DC, USA, August 23-26, pp1-14.

Li, Z., Sun, Q., Lian, Y. and Giusto, D.D. (2005), 'An association-based graphical password design resistant to shoulder-surfing attack', *IEEE International Conference on Multimedia and Expo 2005*. July 6-8, pp245-248.

Malek, B., Orozco, M. and Saddik, A.E. (2006), 'Novel shoulder-surfing resistant haptic-based graphical password', *Proceedings of Eurohaptics 2006*, Paris, France, July 3-6.

Man, S., Hong, D. and Matthews, M. (2003), 'A shoulder-surfing resistant graphical password scheme - WIW', *Proceedings of the International Conference on Security and Management 2003*. Las Vegas, USA, pp105-111.

O'Gorman, L. (2003), 'Comparing passwords, tokens, and biometrics for user authentication', *Proceedings of the IEEE*, 91 (12), pp2019 - 2040.

Passfaces (2003), 'Next generation graphical authentication', available at: http://www.realuser.com/personal/index.htm (accessed: 15 March 2008).

Sandhu, R.S. and Samarati, P. (1997), 'Authentication, access control, and intrusion detection', in Tucker, A.B. (ed.) *The Computer Science and Engineering Handbook*, CRC Press, pp1929-1948.

Shepard, R.N. (1967), 'Recogition memory for words, sentences and pictures', *Journal of Verbal Learning and Verbal Behavior*, 6(0), pp156-163.

Tao, H. (2006), *Pass-Go: A new graphical password scheme*. MSc. University of Ottawa, Canada, available at: http://www.site.uottawa.ca/~cadams/papers/HaiTaoThesis.pdf (accessed: 8 May 2008).

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N. (2005), 'PassPoints: design and longitudinal evaluation of a graphical password system', *International Journal of Human Computer Studies*, 63(0), pp102-127.

Yan, J. and Dunply, P. (2007), 'Background Draw A Secret', available at: http://homepages.cs.ncl.ac.uk/jeff.yan/bdas.htm, (accessed: 10 March 2008).

Evaluating Web-Based User Authentication using Graphical Techniques

M.Z.Jali[1], S.M.Furnell[1,2] and P.S.Dowland[1]

[1]Centre for Information Security & Network Research,
University of Plymouth, Plymouth, UK
[2]School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia
e-mail: info@cisnr.org

Abstract

Graphical techniques are one of the many alternatives proposed to address the weaknesses in the conventional authentication based upon username and passwords. In this paper, two methods of graphical technique, namely 'click-based' and 'choice-based' are studied in term of their usability for web-based authentication. A total of 21 participants were asked to use prototype implementations and provide feedback. From the data analysed in terms of number of attempts, accuracy, time, pattern and user feedback, it was found that the choice-based method performed better. However, with regard to security, participants rated the choice-based method as weak. Overall, it was found that although both methods have advantages and could be used for authentication, more work needs to be done to balance the issues of security and usability.

Keywords

Graphical Technique, Usability, Security, Web Authentication

1. Introduction

There are many forms of user authentication, but the username/password combination is still the most widely used and accepted method by end-users. This is because the username/password authentication is simple and easy to deploy, involves less cost, and requires no additional hardware. However, this method of authentication is potentially vulnerable to compromise through a variety of means, including dictionary attacks, shoulder surfing, spyware, phishing and even social engineering. In addition to above, there are also problems with users forgetting their passwords, using the same ones for different applications, writing them down in discoverable locations, and generally facing usability issues when required to remember long and complex strings (Brostoff, 2004; Yan *et al.* 2005).

The aim of this study was to investigate the usability of graphical techniques for user authentication in a web-based environment. A user trial was conducted in which participants were asked to use the prototype implementations and provide feedback. The key elements of usability in this study were in terms of users' accuracy while entering their secrets, the time taken to enter them, patterns of the chosen secrets and users' feedback about the methods.

The paper is arranged as follows. The next section outlines the current state of the art in graphical technique. It highlights the psychological studies about the 'picture superiority effect' and then continues to explain the current research trends for both types used in the study. Section three discusses methodologies used in the study, with section four presenting the results from practical evaluation. Finally, the conclusion and thoughts towards future work are described in section 5.

2. Graphical Technique

The fundamental idea of graphical technique is using images or pictures rather than strings of characters as the basis for the user's secret. From the literature, it was found that among an early attempt to use pictures during authentication was described in the paper by King (1991), entitled 'Rebus Password'. Rebus is a method of association using images or graphics in order to aid remembering sequences of nonsense passwords. In this paper, graphical techniques were grouped into two categories; namely 'click-based' and 'choice-based'. These categories were solely based on the users' actions while carrying out authentication tasks. Briefly, click-based refers to the users' action clicking on areas within a given image, whereas choice-based refers to the action of selecting a series of images from among a larger set of images. Another variation of these graphical techniques is the 'draw-based' method, in which users draw their secret in order to be authenticated.

From various psychological studies, it was found that participants are better at recognising and recalling images compared with recognising and recalling words, phrases or even sentences (Shepard, 1967; Nickerson, 1968; Standing, 1970). It was also claimed that graphical techniques are more secure than conventional passwords since they offer larger secret spaces (Blonder, 1996).

In the click-based method, Blonder (1996) patented his graphical scheme where users' click or tap on the predetermined areas of the given image which is already defined within the system. Following this the 'Passpoints' systems (Wiedenbeck *et al.* 2005a) was developed, which enhanced the original scheme from Blonder by giving users the opportunity to choose their own images and the system itself does not need any predefined click-region or well-marked boundaries. Chiasson *et al.* (2007a) evaluated 'Passpoints' and determined that the scheme was less effective as users had problems while entering their passwords. As a result, Chiasson *et al.* (2007b) introduced the 'Cued Click Point' (CCP). CCP addresses the 'Passpoints' problem by letting users to click once on a series of images with the current click determines the next images. Another variation of CCP was the Persuasive CCP (Chiasson *et al.* 2008a), where a method of persuasion is used in order to advise users to choose more secure passwords. Among the usability studies carried out for click-based method were investigating the level of memorisation (Wiedenbeck *et al.* 2005a; Chiasson *et al.* 2007a), assessing the effect of having multiple passwords (Chiasson *et al.* 2008b), investigating the use of different images (Wiedenbeck *et al.* 2005b; Chiasson *et al.* 2007a), and predicting the click points chosen by users (Golofit, 2007; Thorpe and Oorchot, 2007).

The most familiar choice-based method was the scheme known as 'Passfaces' (Passfaces, 2003). Users have to select images of peoples' faces in order to

authenticate. Djamila and Perrig (2000) introduced 'Dejavu', which uses images deployed from the Andrej Bauer's Random Art algorithm, an algorithm where bits of strings are converted into interesting abstract images. Users of this scheme have to remember a number of images and the authentication rounds are dependent on the total number of images chosen by users. De Angeli *et al.* (2003) introduced 'Visual Identification Protocol' (VIP), an ATM-based pictorial password and conducted a usability study to compare it with the conventional ATM-style. Other schemes that could be considered to be in this category are 'Story' by Davis *et al.* (2004), 'PassImages' by Charruau *et al.* (2005) and 'ToonPasswords' by Hinds and Ekwueme (2007). Among the usability studies carried out for this method were the level of memorisation and recall (Djamija and Perrig, 2000; De Angeli *et al.* 2003), image types and effect on screen size (De Angeli *et al.* 2005; Davis *et al.* 2004; Renaud, 2009), the effect of having multiple passwords (Moncur and Lepatre, 2007), and the security against 'description' attack (Dunphy *et al.* 2008).

3. Methodology

As far as the prior research is concerned, no study is reported to have investigated the alternative graphical techniques by using the same user sample. With this in mind, a study was undertaken with 21 participants evaluating both the click-based and choice-based methods in terms of performance and user acceptance. Participants needed to complete five main tasks. These started with registering and confirming their 'passwords' for both methods, playing a spot the difference activity (explained below), then re-authenticating using their chosen passwords for both methods, and finally providing feedback by answering a questionnaire. The questionnaire and game activities were done on paper, while the remaining tasks were conducted online using the Internet Explorer (IE 7) browser, with all of the materials (and the trial method itself) having received prior ethics approval.

The development of the click-based method prototype was similar to the original scheme proposed by Wiedenbeck *et al.* (2005), while the choice-based method prototype was developed with consideration and references from 'Passfaces' (2003), Djamila and Perrig, (2000) and De Angeli *et al.* (2003). Both prototypes were developed using a combination of PHP and JavaScript as the interface and MySQL as the platform for storing data.

In the click-based method, the type of image used was similar to those used in Wiedenbeck *et al.* (2005a). The display scale of the image was 450x330 pixels with a selection tolerance (areas in which the click is still valid) of 18x18 pixels. The small tolerance was used as Chiasson *et al.* (2007a) proved that the click-based method would still be usable even with the smaller tolerance. Participants were required to create their passwords by choosing and clicking upon five different points in the given image. They were told not to click their passwords in the same place or within the same tolerance areas and remember their secret in sequences order.

For the choice-based method, the majority of images were taken from FreeFoto (2008) and personal collections. Similar to the click-based method, participants needed to remember five different images grouped within five different themes; namely 'Animal', 'Transport', 'Nature', 'Food' and 'Other'. These categories were

chosen because they were common everyday images, easy to recognise and remember. All of these images were manually chosen in order to prevent redundancy. During the registration, a total of 180 images (arranged in 5 separate 6x6 grids) were displayed to the participant, who then needed to choose one image from each theme. This process (displaying 36 images for each category) would continue until participants finished choosing their five images. When it came to the confirmation of their images, only 16 images (arranged in 4x4 grids) were randomly displayed to them, one of which their chosen images. This process continued for the other themes until they finished choosing all of their images within all the themes. The screen shots of both methods are shown in Figure 1.

Figure 1: Screen shot from the click-based (left) and the choice-based (right) methods

The purpose of the 'spot the difference' activity was to provide participants with a mental distraction between the registration and login tasks. This gave them something to do other than to focus on remembering their chosen secrets. It was anticipated that it could take between 3 to 5 minutes to find all 28 differences (eight for each image). After completing the authentication tasks, the participants were asked to complete a three-part questionnaire. The first two parts were about the authentication methods, while the last one was about general opinions and the prototype itself. Among the questions asked were whether it was easy to remember the secrets, whether they had problems during login, whether they would use these methods, and whether they would prefer using their own images as their secrets.

4. Results and Findings

A total of 21 participants (16 males and 5 females) volunteered to participate, all of whom were university students doing various courses, with an average age of 26 years old (Standard Deviation (SD) = 3.9, sample range from 21 to 36 years) and up to 7 years experience of using computers. Since the number of participants is small, the results might not be conclusive. However, with the idea of getting participants to use and evaluate the both methods simultaneously, the results can still be used as an early indication for evaluating the both methods empirically.

The discussion of the results is categorised into five areas, namely number of attempts, timing, accuracy, patterns and user feedback.

4.1 Number of attempts

With the way the study was designed, all participants successfully completed all the authentication tasks (register, confirm and login) and they did not have any major problems creating their secrets. Moreover, as the total number of attempts created by the participants was quite low (with only 21 participants), only general findings will be highlighted here. First, for the choice-based method, all participants were able to complete all of the authentication tasks with only one attempt. Second, for both methods the number of attempts starting from the registration to the login was reduced significantly. This suggested the participants' level of familiarity as high.

By contrast, it was found that the number of recorded attempts for the click-based method was significantly higher, particularly during registration and confirmation. These results were predicted as participants had to carefully click on their secret areas, which sometimes they did not manage to do. When compared with the choice-based method, the above finding could be biased as in the click-based method, participants needed to be accurate while entering their details and they had to remember the information in sequence, but for the choice-based method participants only needed to remember the images themselves.

4.2 Timing

Each participant's registration, confirmation and login duration was recorded to calculate their average time while entering their passwords. The time was measured from the first chosen click/image until the last. Table 1 gives the mean and the SD for each task.

N=21		**Register**	**Confirm**	**Login**
Choice-based	**mean**	38.4	16.4	15.1
	SD	19.5	4.9	4.7
Click-based	**mean**	12.9	8.6	7.7
	SD	6.7	3.9	2.5

Table 1: Mean and SD of time for entering secrets

For the choice-based method, it was clear that participants took longer during registration compared with the confirmation and login tasks. This is because during the registration, participants needed to familiarise (scanning 180 images) and carefully choose their images. As they became familiar with their chosen images, the time for confirmation and login was reduced considerably. For the click-based method, it was found that the mean time for each task was marginal to each other. To summarise, although these times are greater than the time for username/passwords method, they are still likely to be within bounds that are acceptable to users.

4.3 Accuracy

This section measures the correctness of the chosen images and the precision between clicks. For the choice-based method, since all of the participants managed to create their secrets during their first attempt, it could be summarised that the accuracy for both registration and login were very high.

For the click-based method, accuracy refers to how far the original click points during registration are from the click points during confirmation and login (Chiasson *et al.* 2007a). As explained in previous section, the tolerance of 18x18 pixels was used. As long as participants clicked within their secret tolerance area, the click will be accepted. Figure 2 illustrates the distribution of accuracy for all participants during both registration and login tasks (considering only the successful attempts), followed by Table 2 showing the mean and SD of accuracy for successful attempts during both tasks.

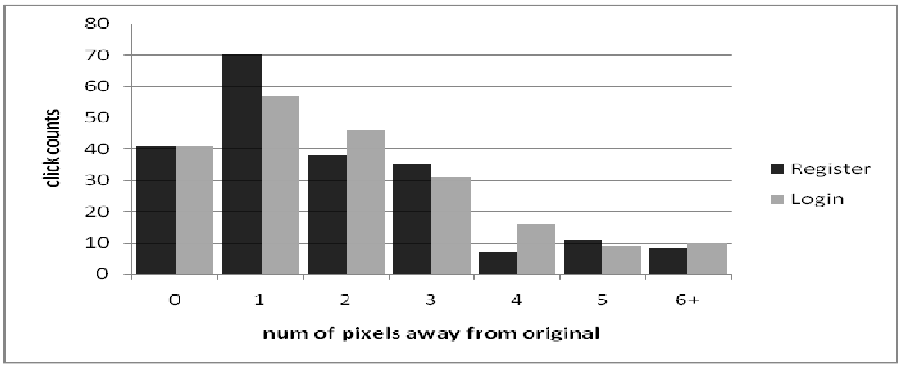

Figure 2: Accuracy during Registration and Login tasks

N=210	**Register**	**Login**
Mean	1.8	2.1
SD	1.7	1.9

Table 2: Mean and SD of Accuracy for Register and Login Tasks

Based upon Figure 2, it was found that participants were good and relatively accurate in entering their secrets within 3 pixels of their original click point. Taking the results of both into consideration, it could be suggested that the click-based method is still usable if it is designed with a tolerance as low as 6x6 pixels (note that the method would be more secure if the smaller tolerance is used, as it produces a larger secret space).

4.4 Patterns

This section highlights the types of images chosen and areas in the image clicked by the participants. The purposes are to investigate and further finding any relationships or patterns while creating the secrets.

For the choice-based method, among of the chosen images were sport cars, flags, eggs, burgers, lion and cat. No relationship was found between the chosen images

but it was found that one participant had chosen his images based on the sequences of a story (**car – key – road – coffee - bird**). With regard to patterns, it was found that nearly all of the participants had chosen the images that related to their name. For example, one participant used 'JP' as his username and chosen image letter 'J' as one of his secret images. On top of that, it was found the male participants normally chosen sport cars while the female participants chosen mini cars. Based on observation and informal interviews, it could be summarised that the chosen images were based on two main things; their personal preferences and the recognisability of the image itself. The table below shows the example of secrets (list of images) chosen by them.

Theme	Transport	Other	Nature	Food	Animal
User A	Helicopter	Cutlery	Clock	Eggs	Cow
User B	Mini	Letter	Bridge	Chocolate	Dog
User C	Sport car	Letter	London	Chips	Penguin
User D	Sport car	Flag	Bridge	Carrot	Lion
User E	Sport car	Letter	Autumn	Cereal	Peacock
User F	Sport car	Letter	Bridge	Raspberry	Bird

Table 3: Example of images chosen by the participants

For the click-based method, the start point of the click and the shape of the clicks are reported. For the start click point, it was found that majority of the participants started their first click in the bottom area of the image where 6 participants clicked on the 'bottom left' area, 4 participants clicked on the 'bottom middle' area and 3 participants clicked on 'bottom right' area. Other preferences for starting the first click were the 'top left' (3 participants) and the 'top middle' (2 participants) of the image, whereas others clicked randomly. With regard to the image used, it could be anticipated that such chosen areas were obvious and recognisable (e.g. people wandering around, beams, umbrellas and etc.). After the first click, no interesting patterns were found since participants likely to click everywhere but one noticeable finding was that participants chosen to click on the objects, as explained earlier. Examples of clicks created by 6 of the participants are shown in Figure 3.

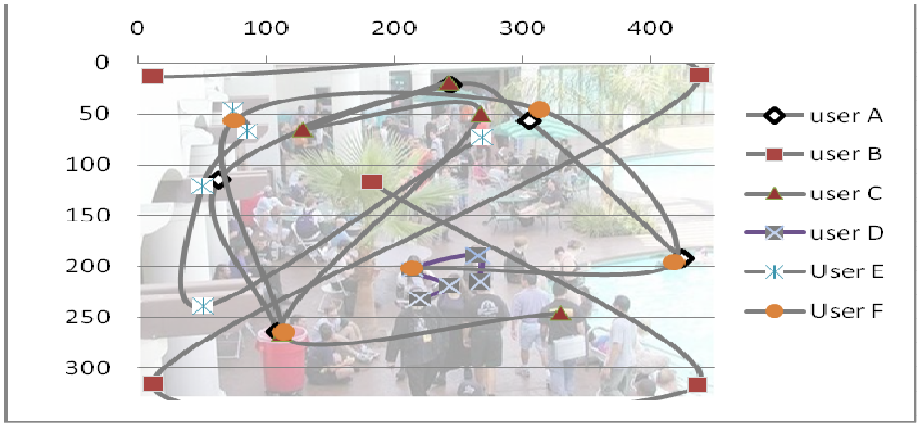

Figure 3: Example of the clicks created by participants

From the distribution of the clicks drawn by the participants, it was found that the shapes of click could be mapped into shapes like ‘U or V’, ‘Z or N’ and ‘L’. Here, it is obvious that the majority of them tended to click on recognisable objects (e.g. beams, bin, people faces, etc.) and the forms of shapes created were also straightforward and predictable. Although clicking on recognisable objects and forming straightforward shapes would make it easy to remember their secrets, if these habits continue it is not possible to build more dictionaries based upon the users’ click points and click patterns and conduct an attack based on these; as already discussed in Thorpe and van Oorschot (2007).

4.5 User Feedback

For the choice-based method, 19 out of 21 participants agreed that they could remember their chosen images well, with all of them did not have any major problems while carrying out the authentication tasks and 16 of them would consider using the method on the web. On the other question, 12 participants think that the method would be vulnerable if they explained their secret images to others and 15 of them preferred the themes to appear in a random order during the login (whereas in the trial themes had been presented in a fixed order) in order to tighten the security of the method.

For the click-based method, 16 participants agreed that they could easily remember their click points in sequence. During the registration and the login tasks, between 11 to 13 participants rated the method was easy to use while the rest rated the method as difficult (note that no training was provided at the start of trial; only description on how both methods work was outlined in the participant briefing sheet). For other questions, 13 out of 21 participants would consider using this method on the web and importantly, the vast majority of them (17 participants) agreed that it is difficult for others to reproduce their login details if they just explain briefly what their secrets were.

Participants agreed the prototypes as suitable to be used for graphical authentication purposes, the usage of images and text as clear, and considered that the instructions during the trial were concise and understandable. The majority of them (20 participants) preferred using their own images rather than the images provided in the prototype, as they claimed it would be more memorable. Encouragingly, participants who did not manage to complete their authentication tasks on their first attempt and rated the click-based method as difficult to use agreed that they would perform better if enough training was provided beforehand. Finally, participants preferred using the click-based method (11 participants) as opposed to the choice-based method (6 participants) for replacing username and password authentication; whereas the remaining rated ‘unsure’ about it. Overall, it could be summarised that all participants provided positive response with regard to the suitability of the prototype to be used in the web-based environment.

5. Conclusions

There are numbers of lessons to be learnt from the conduct of this study. First and foremost, the number of attempts for the click-based method was rather high

compared to the choice-based method. This is perhaps due to the nature of the click-based method itself whereby participants needed to be accurate when clicking on their chosen areas (which they sometimes missed). Second for both methods, participants took longer during the registration (as they want to carefully look and choose their images) but then during the confirmation and login tasks, they performed significantly better. Third, participants had chosen/clicked images or objects that were easy to recognise and formed shapes that were easy to predict. Here, it could be summarised that participants preferred convenience rather than security. Last but not least, participants always gave positive feedback, as well as suggestions on how to improve the methods for future use.

This study confirmed that the problems identified were identical to other studies, regardless of the methods and prototypes used. However, the contribution of this paper is the comparison of both methods within a single study, using a common population of test subjects. With regards to the results and findings, it seems that both are complementary to each other and there is potential for both methods should be combined in order to create a graphical password that is not only usable but also secure. Combining the nature of the click-based method, which can be summarised as ‘secure but unusable’, and the choice-based method, which can be summarised as ‘usable but unsecure’, will be the main focus of ongoing research. Appropriate evaluation in terms of usability and security will then be conducted in order to validate the enhanced scheme.

6. References

Blonder, G. (1996) *Graphical password.* 5.559.961. [online]. Available at: http://www.patentstorm.us/patents/5559961.html (Accessed: 10 March 2008).

Brostoff, A. (2004) *Improving password system effectiveness*. PhD. University College London.

Chiasson, S., Biddle, R. and Oorschot, P.C.v. (2007a) 'A second look at the usability of click-based graphical password'. *Symposium On Usable Privacy and Security 2007*. Pittsburgh, USA: July 18-20, 2007.

Chiasson, S., Oorschot, P.C.v. and Biddle, R. (2007b) 'Graphical password authentication using Cued Click-points', Biskup, J. and Lopez, J. (Eds.). *ESORICS 2007, 12th European Symposium On Research In Computer Security*. Dresden, Germany September 24-26, 2007. Springer, pp. 359-374.

Chiasson, S., Forget, A., Biddle, R. and Oorschot, P.C.v. (2008a) 'Influencing users towards better passwords: Persuasive cued click-point'. *HCI 2008*, September 1-5, Liverpool, UK.

Chiasson, S., Forget, A., Stobert, E., Oorschot, P.C.v. and Biddle, R. (2008b) 'Multiple password inteference in text and click-based graphical passwords'. [Technical Report TR-08-20] School of Computer Science, Carleton University.

Charruau, D., Furnell, S. & Dowland, P. (2005) 'PassImages: an alternatives method of user authentication', *ISOneWorld 2005*. Las Vegas, USA March 30 - April 1, 2005.

Davis, D., Monrose, F. and Reiter, M.K. (2004) 'On user choice in graphical password schemes'. *Proceedings of the 13th USENIX security symposium*. California, USA: August 9-13, 2004 USENIX Association, pp. 1-11.

Djamila, R. and Perrig, A. (2000) 'Deja Vu: A user study using images for authentication', *Proceedings of the 9th USENIX Security Symposium*. Denver, Colorado, USA August 14-17, 2000. USENIX Association, pp. 45-58.

De Angeli, A., Coventry, L., Johnson, G. and Coutts, M. (2003) 'Usability and user authentication: Pictorial passwords vs. pin'. in McCabe, P.T. (ed.) *Contemporary Ergonomics 2003*. Taylor & Francis, pp. 253–258.

De Angeli, A., Coventry, L., Johnson, G. and 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 pp. 128-152.

Dunphy, P., Nicholson, J. and Olivier, P. (2008) 'Securing Passfaces for description', *Proceedings of the 4th symposium on Usable privacy and security (SOUPS 2008)*. Pittsburgh, Pennsylvania, USA July 23-25, 2008. ACM, pp. 24-35.

FreeFoto (2008) 'Free Pictures'. [Online]. Available at: http://www.freefoto.com/index.jsp (Accessed: 10 March 2008).

Golofit, K. (2007) 'Click passwords under investigation'. in Biskup, J. and Lopez, J. (eds.) *Computer Security - ESORICS 2007*. Springer Berlin/Heidelberg, pp 343-358.

Hinds, C. and Ekwueme, C. (2007) 'Increasing security and usability of computer systems with graphical password', *ACM Southeast Regional Conference*. Winston-Salem, North Carolina, USA ACM New York, USA, pp 529-530.

King, M. M. (1991) 'Rebus Passwords', *Computer Security Applications Conference*. San Antonio, TX, USA IEEE, pp 239-243.

Moncur, W. and Leplatre, G. (2007) 'Pictures at the ATM: Exploring the usability of multiple graphical password', *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*. San Jose, USA April 28- May 3, 2007. ACM, pp. 887-894.

Nickerson, R.S. (1968) 'A note on long-term recognition memory for pictorial material'. *Psychonomic Science*, 11 (2) pp. 58.

Passfaces (2003) 'Next generation graphical authentication'. [Online]. Available at: http://www.realuser.com/personal/index.htm (Accessed: 15 March 2008).

Renaud, K. (2009) 'On user involvement in production of images used in visual authentication'. *Journal of Visual Languages and Computing*, 20 (1) pp. 1-15.

Shepard, R.N. (1967) 'Recogition memory for words, sentences and pictures'. *Journal of Verbal Learning and Verbal Behavior*, 6 pp. 156-163.

Standing, L., Conezio, J. and Baher, R. N. (1970) 'Perception and memory for pictures: Single-trial learning of 2500 visual stimuli'. *Psychonomic Science*, 19 (2) pp. 73-74.

Thorpe, J. and Oorschot, P.C.v. (2007) 'Human-seeded attacks and exploiting hot-spot in graphical passwords', *16th USENIX Security Symposium*. Boston, USA. USENIX, pp. 102-118.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005a) 'PassPoints: design and longitudinal evaluation of a graphical password system'. *International Journal of Human Computer Studies*, 63 pp. 102-127.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005b) 'Authentication using graphical passwords: effects on tolerance and image choice'. *Symposium On Privacy and Security*. Pittsburgh, USA: July 6-8, 2005.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2005) 'The memorability and security of passwords'. in Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability: Designing secure systems that people can use.* O'Reilly, pp. 129-142.

The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Assessing image-based authentication techniques in a web-based environment

M.Z. Jali
Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK

S.M. Furnell
Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK and School of Computer and Security Science, Edith Cowan University, Perth, Western Australia, and

P.S. Dowland
Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK

Received 30 September 2009
Accepted 1 October 2009

Abstract

Purpose – The purpose of this paper is to assess the usability of two image-based authentication methods when used in the web-based environment. The evaluated approaches involve clicking secret points within a single image (click-based) and remembering a set of images in the correct sequence (choice-based).

Design/methodology/approach – A "one-to-one" usability study was conducted in which participants had to complete three main tasks; namely authentication tasks (register, confirm and login), spot the difference activity and provide feedback.

Findings – From analysing the results in terms of timing, number of attempts, user feedback, accuracy and predictability, it is found that the choice-based approach is better in terms of usability, whereas the click-based method performed better in terms of timing and is rated more secure against social engineering.

Research limitations/implications – The majority of participants are from the academic sector (students, lecturers, etc.) and had up to seven years' IT experience. To obtain more statistically significant results, it is proposed that participants should be obtained from various sectors, having a more varied IT experience.

Practical implications – The results suggest that in order for image-based authentication to be used in the web environment, more work is needed to increase the usability, while at the same time maintaining the security of both techniques.

Originality/value – This paper enables a direct comparison of the usability of two alternative image-based techniques, with the studies using the same set of participants and the same set of environment settings.

Keywords Message authentication, Graphical user interfaces, Data security

Paper type Research paper

1. Introduction

User authentication is the first layer of interaction between human and machine. Generally, the purpose of user authentication is to confirm or validate the identity of an

Information Management & Computer Security
Vol. 18 No. 1, 2010
pp. 43-53

0968-5227
DOI 10.1108/09685221011035250

individual prior to allowing them access to systems, data and services. There are many forms of user authentication, but the username/password combination is still the most widely used and accepted by end-users. This is because such authentication is simple and easy to deploy, involves less upfront cost and requires no additional hardware. However, this method of authentication is potentially vulnerable to compromise through a variety of means, including dictionary attacks, shoulder surfing, spyware, phishing and even social engineering. In addition to these vulnerabilities, there are also problems with users forgetting their passwords, using the same ones for different applications, writing them down in discoverable locations, and generally facing usability issues when required to remember long and complex strings (Adams and Sasse, 2005; Yan *et al.*, 2005).

The idea of using graphics/images/pictures to aid memorability is not new. For example, an early attempt to use pictures during authentication was described by King (1991), entitled "Rebus password". Rebus is a method of association using images or graphics in order to aid the recollection of sequences of nonsensical passwords. Later, the idea of using graphics as a replacement for passwords emerged with the work patented by Blonder (1996), aiming to offer better usability and claiming that using pictures/images could offer a larger password space and thus offer greater security than the traditional username/password approach. It was also suggested that the problem of remembering long and complex passwords could be addressed, as humans are very good at recognising and recalling images as opposed to words, sentences or phrases (Shepard, 1967; Nickerson, 1968; Standing *et al.*, 1970).

The purpose of this paper is to assess the usability of user authentication using images in a web-based environment. A user trial was conducted in which participants were asked to use the prototype implementations and provide feedback. The key elements of usability in this study were in terms of users' accuracy while entering their secrets, the time taken to enter them, patterns of the chosen secrets, and users' feedback about the methods.

2. Image-based authentication

In this paper, image-based authentication approaches were grouped into two categories; namely "click-based" and "choice-based". These categories were solely based on the users' actions while carrying out authentication tasks. Briefly, click-based refers to the users' action when clicking on areas within a given image, whereas choice-based refers to the action of selecting a series of images from among a larger set of images. Another variation is the "draw-based" method, in which users draw their secret on the provided space/area/grid in order to be authenticated.

In the click-based method, Blonder (1996) patented his graphical scheme where users click or tap on the predetermined areas of the given image which is already defined within the system. Following this, the "Passpoints" system (Wiedenbeck *et al.*, 2005b) was developed, which enhanced the original scheme from Blonder by giving users the opportunity to choose their own images. Chiasson *et al.* (2007a) evaluated "Passpoints" and determined that the scheme was less effective. As a result, Chiasson *et al.* (2007b) introduced the "cued click point" (CCP). CCP addresses the "passpoints" problem by letting users click once on a series of images with each click determining the next image. Another variation of CCP was the persuasive CCP (Chiasson *et al.*, 2008a), where a method of persuasion is used in order to advise users to choose more

secure passwords. Among the usability studies carried out for the click-based method were investigating the level of memorisation (Wiedenbeck *et al.*, 2005b; Chiasson *et al.*, 2007a), assessing the effect of having multiple passwords (Chiasson *et al.*, 2008b), investigating the use of different images (Wiedenbeck *et al.*, 2005a; Chiasson *et al.*, 2007a), and predicting the click points chosen by users (Golofit, 2007; Thorpe and van Oorschot, 2007).

The most familiar choice-based method was the scheme known as Passfaces (2003). Users have to select images of peoples' faces in order to authenticate. Djamila and Perrig (2000) introduced "Dejavu", which uses images deployed from the Andrej Bauer's Random Art algorithm, an algorithm where strings are converted into abstract images. De Angeli *et al.* (2003) introduced the "visual identification protocol", an ATM style pictorial password and conducted a usability study to compare it with the conventional ATM-style. Other schemes that could be considered to be in this category are "Story" by Davis *et al.* (2004), "PassImages" by Charruau *et al.* (2005) and "ToonPasswords" by Hinds and Ekwueme (2007). Among the usability studies carried out for this method were the level of memorisation and recall (Djamila and Perrig, 2000; De Angeli *et al.*, 2003), image types and effect on screen size (De Angeli *et al.*, 2005; Davis *et al.*, 2004; Renaud, 2009), the effect of having multiple passwords (Moncur and Leplatre, 2007) and the security against social engineering (Dunphy *et al.*, 2008).

3. Methodology

As far as the prior research is concerned, no study is reported to have investigated and compared the image-based authentication techniques. With this in mind, a study was undertaken with a total of 40 participants evaluating both the click- and choice-based methods in terms of performance and user acceptance. Participants needed to complete the following tasks:

(1) registering and confirming their "passwords" for both methods;

(2) playing a spot the difference activity (for reasons explained later);

(3) re-authenticating using their chosen passwords for both methods; and

(4) providing feedback by answering a questionnaire.

The questionnaire (4) and game activities (2) were done on paper, while tasks (1) and (3) were conducted online using the internet explorer browser, with all of the materials (and the trial method itself) having received prior ethics approval.

The development of the click-based method prototype was comparatively similar to the original scheme proposed by Wiedenbeck *et al.* (2005b). The display scale of the image was 450×330 pixels with a selection tolerance (areas in which the click is still valid) of 19×19 pixels. Participants were required to create their passwords by choosing and clicking upon five different points in the given image. They were told to remember their secret in sequence order and to select their points from different areas of the image.

For the choice-based method, participants needed to remember five different images grouped within five different themes; namely "Animal", "Transport", "Nature", "Food", and "Other". All of these images were manually chosen in order to prevent redundancy. During the registration, a total of 180 images (arranged in five separate 6×6 grids) were displayed to the participant, who then needed to choose one image

from each theme. This process (displaying 36 images for each category) would continue until participants finished choosing their five images. When it came to the confirmation of their images, only 16 images (arranged in 4 × 4 grids) were randomly displayed to them, one of which was their chosen images. This process continued for the other themes until they finished choosing all of their images within the themes. The screen shots of both methods are shown in Figures 1-3.

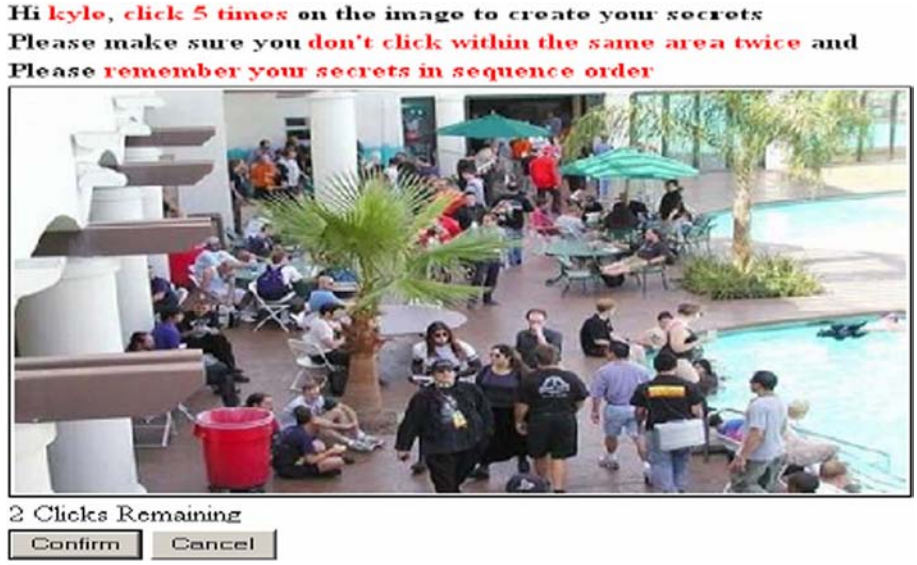

Figure 1.
Screen shot example from the click-based prototype

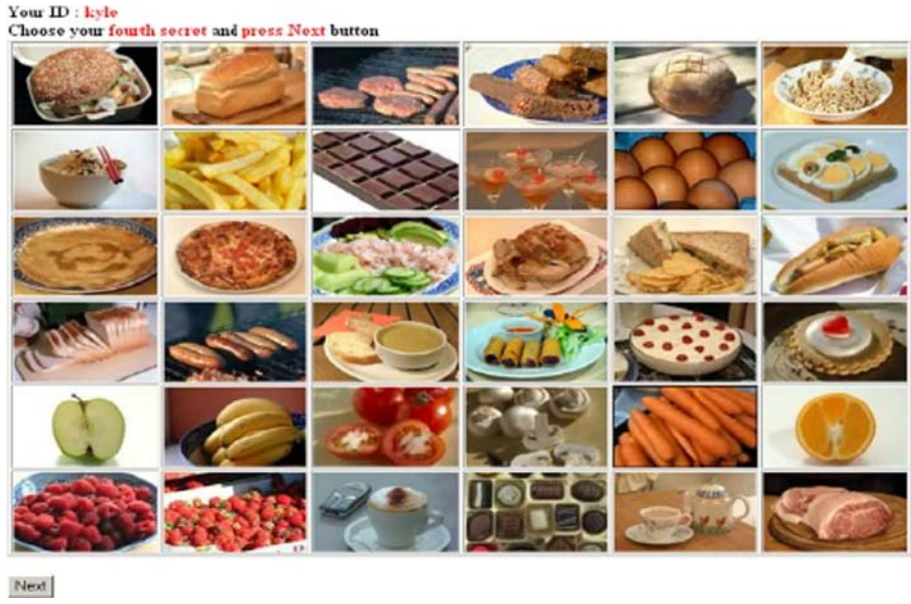

Figure 2.
Screen shot example from the choice-based prototype (registration)

Figure 3.
Screen shot example from the choice-based prototype (confirmation)

The purpose of the "spot the difference" activity was to provide participants with a mental distraction between the registration and login tasks. This gave them something to do other than focussing on remembering their chosen secrets. The questionnaire was split into three parts, the first two were about the authentication methods, while the last one was about general opinions and the prototype itself. Among the questions asked were whether it was easy to remember the secrets, whether they had problems during login, whether they would use these methods, and whether they would prefer using their own images as their secrets.

4. Results

A total of 40 participants (33 males and seven females) chosen randomly agreed to participate, all of whom were in the field of academia (university students and staffs), with an average age of 27 years old (sample range from 21 to 44 years) and up to seven years experience of using computers. Since the number of participants is small and the sample is imbalanced, the results must be considered indicative rather than conclusive. However, with the idea of getting participants to use and evaluate both techniques simultaneously, the results can still be used as an early indication for evaluating both methods empirically.

The discussion of the results is categorised into five areas, namely number of attempts, timing, accuracy, patterns and user feedback.

4.1 Number of attempts

With the way the study was designed, all participants successfully completed all the authentication tasks (register, confirm and login). Briefly, as the total number of attempts created by the participants was quite low (with only 40 participants), only general findings will be highlighted here. First, for the choice-based method, all participants were able to

complete all of the authentication tasks with only one attempt. Second, for both methods the number of attempts starting from the registration to the login was reduced significantly. This suggested the participants' level of familiarity as high.

By contrast, it was found that the number of attempts for the click-based method was significantly higher, particularly during registration and confirmation. These results were predicted as participants had to carefully click on their secret areas, which sometimes they did not manage to do. When compared with the choice-based method, the above finding could be biased, as in the click-based method, participants needed to be accurate while entering their details and they had to remember the information in sequence, but for the choice-based method participants only needed to remember the images themselves.

4.2 Timing

Each participant's registration, confirmation and login duration was recorded to calculate their average time while entering their passwords. The time was measured from the first chosen click/image until the last. Table I gives the mean and SD for each task.

For the choice-based method, it was clear that participants took longer during registration compared with the confirmation and login tasks. This is because during the registration, participants needed to familiarise (scanning 180 images) and carefully choose their images. As they became familiar with their chosen images, they took less time during confirmation and even comparatively equal with the time taken during the login (Table I). For the click-based method, it was found that the mean time for each task was marginal to each other. To summarise, although these times are greater than the time for traditional username/password login methods, they are still likely to be within the bounds of acceptability to users.

4.3 Accuracy

This section measures the correctness of the chosen images and the precision between clicks. For the choice-based method, since all of the participants managed to create their secrets during their first attempt, it could be summarised that the accuracy for both registration and login were very high.

For the click-based method, accuracy refers to how far the original click points during registration are from the click points during confirmation and login (Chiasson *et al.*, 2007a). As explained in the previous section, the tolerance of 19 × 19 pixels was used. As long as participants clicked within their secret tolerance area, the click will be accepted. Figure 4 shows the distribution of accuracy for all participants during both registration and login tasks (considering only the successful attempts), followed by Table II showing the mean and SD of accuracy for successful attempts during both tasks.

Table I.
Mean and SD of time for entering secrets

	Time (seconds)		
$n = 40$	Register	Confirm	Login
Choice-based			
Mean	34	17	17
SD	21	6	6
Click-based			
Mean	12	8	8
SD	7	4	5

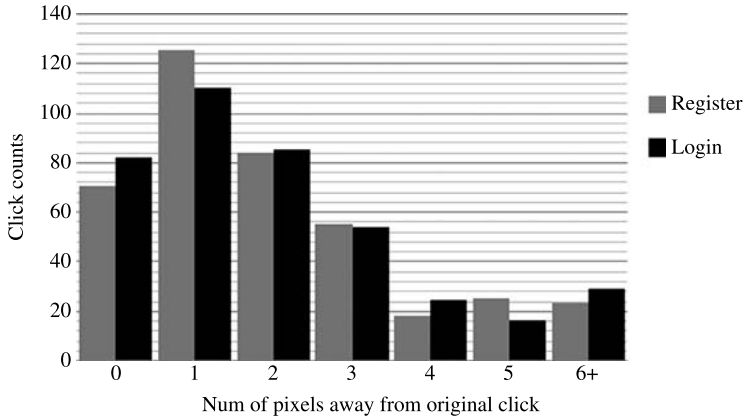

Figure 4.
Accuracy during registration and login tasks

$n = 400$	Accuracy (pixels away from original click) Register	Login
Mean	1.9	2.0
SD	1.7	1.8

Table II.
Mean and SD of accuracy for register and login tasks

Based upon the Figure 4, it is found that participants are relatively accurate in entering their secrets within 7×7 pixels of their original click point. Overall, the above result supports the research by Chiasson *et al.* (2007a) and therefore, it is suggested that the click-based method would still usable if it was designed with a tolerance as low as three pixels (note that the method would be more secure if the smaller tolerance is used, as it produces a larger secret space).

4.4 Pattern

This section highlights the types of images chosen and areas in the image clicked by the participants. The purposes are to investigate any relationships or patterns while creating the secrets, which might influence later predictability for an attacker.

For the choice-based method, among the favourite chosen images were sport cars, flags, eggs, burgers and cats. No relationship was found between the chosen images but it was found that a number of participants had chosen their images based on the sequences of a story. With regard to patterns, it was found that nearly all of the participants had chosen the images that were significant to their name. For example, one participant used "JP" as his username and chosen image letter "J" as one of his secret images. On top of that, for the image "Transport" theme, it was found that male participants normally chose sport cars while female participants selected smaller, compact cars. Based on observation and informal interviews, the chosen images were based on two main things; their personal preferences and the recognisability of the image itself. Table III shows examples of secrets (images) selected by a subset of users.

For the click-based method, the start/first click and the shape of the clicks are reported. For the start click, it was found that majority of the participants started their first click either in the bottom or top of the image areas (Figure 5).

With regard to the image used, it could be anticipated that such chosen areas were obvious and recognisable (e.g. people wandering around, beams, umbrellas, etc.). After the first click, no interesting patterns were found since participants were likely to click everywhere but one noticeable finding was that participants chose to click on objects, as explained earlier. Examples of clicks created by six of the participants are shown in Figure 6.

Table III.
Example of images chosen by the participants

	Transport	Other	Nature	Food	Animal
User A	Helicopter	Cutlery	Clock	Eggs	Cow
User B	Mini cooper	Letter	Bridge	Chocolate	Dog
User C	Sport car	Letter	London eye	Chips	Penguin
User D	Sport car	Flag	Bridge	Carrot	Lion
User E	Sport car	Letter	Autumn	Cereal	Peacock
User F	Sport car	Letter	Bridge	Raspberry	Bird

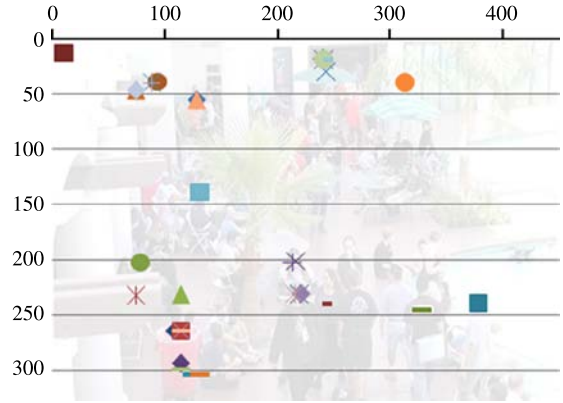

Figure 5.
Participants' first click point

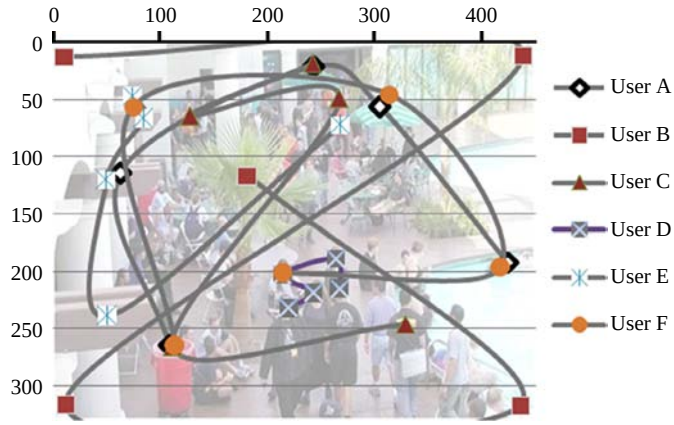

Figure 6.
Example of the clicks created by participants

From the distribution of the clicks drawn by the participants, it was found that the shapes of the click-pattern could be mapped into shapes like "U or V", "Z or N" and "L". Here, it is obvious that the majority of them tended to click on recognisable objects (e.g. beams, bin, people faces, etc.) and the forms of shapes created were also straightforward and predictable. Although clicking on recognisable objects and forming straightforward shapes would make it easy to remember their secrets, if these habits continue it is not possible to build more dictionaries based upon the users' click points and click patterns and conduct an attack based on these; as already discussed in Thorpe and van Oorschot (2007).

4.5 User feedback

For the choice-based method, 36 out of 40 participants agreed that they could remember their chosen images well and they did not have any major problems while carrying out the authentication tasks. Moreover, 27 of them would consider using the method on the web. Other than that, 16 participants felt that the method would be vulnerable if they explained their secret images to others, and 21 of them preferred the themes to appear in a random order during the login (whereas in the trial themes had been presented in a fixed sequence) in order to tighten the security of the method.

For the click-based method, 30 participants agreed that they could easily remember their click points in sequence. During the registration and the login tasks, between 23 and 27 participants rated the method as easy to use while the rest rated the method as difficult (note that no training was provided at the start of trial; the participant briefing sheet simply presented a brief outline of how both methods worked). For other questions, 23 out of 40 participants would consider using this method on the web, and importantly, the vast majority of them (36 participants) agreed that it would be difficult for others to reproduce their login details if they just explained briefly what their secrets were (i.e. providing a perceived safeguard against social engineering attacks).

Participants agreed the prototypes as suitable to be used for graphical authentication purposes, the usage of images and text as clear, and considered that the instructions during the trial were concise and understandable. The majority (38 participants) preferred using their own images rather than the images provided in the prototype, as they claimed it would be more memorable. Encouragingly, participants who did not manage to complete their authentication tasks on their first attempt, and rated the click-based method as difficult to use, agreed that they would perform better if enough training was provided beforehand. Finally, participants preferred using the choice-based method (21 participants) as opposed to the click-based method (14 participants) for replacing username and password authentication; whereas the balances were "unsure". Overall, it could be summarised that all participants provided positive responses regarding the suitability of the prototype for use in web-based environments.

5. Conclusion

There are a number of lessons to be learnt from this study. First and foremost, the number of attempts for the click-based method was rather high compared to the choice-based method. This is perhaps due to the nature of the click-based method itself where participants needed to be accurate when clicking on their chosen areas (which they sometimes missed). Second for both methods, participants took longer during the registration (as they wanted to carefully look and choose their images) but then during

the confirmation and login tasks, they performed significantly better. Third, participants had chosen/clicked on images or objects that were easy to recognise and formed shapes that were easy to recall. Finally, the most striking lesson is that, although participants rated the choice-based method as weak, it was still their preferred alternative for replacing passwords. This result suggests that participants preferred "convenience", albeit with an awareness of the "security" risks.

This study confirmed that the problems identified were identical to other studies, regardless of the methods, prototypes used and environments itself. However, the contribution of this paper is the comparison of both methods within a single study, using a common population of test subjects. With regards to the results and findings, it seems that both are complementary to each other and there is potential for both methods should be combined in order to create a graphical password that is not only usable but also secure. Combining the nature of the click-based method, which can be summarised as "secure but unusable", and the choice-based method, which can be summarised as "usable but insecure", will be the main focus of ongoing research. Appropriate evaluation in terms of usability and security will then be conducted in order to validate the enhanced scheme.

References

Adams, A. and Sasse, M.A. (2005), "Users are not the enemy", in Cranor, L.F. and Garfinkel, S. (Eds), *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly Media, Sebastopol, CA, pp. 619-30.

Blonder, G. (1996), "Graphical password", US Patent No. 5.559.961, available at: www.patentstorm.us/patents/5559961.html (accessed 10 March, 2008).

Charruau, D., Furnell, S. and Dowland, P. (2005), "PassImages: an alternatives method of user authentication", *Proceedings of the ISOneWorld 2005, Las Vegas, NV, USA, 30 March-1 April*.

Chiasson, S., Biddle, R. and van Oorschot, P.C. (2007a), "A second look at the usability of click-based graphical password", *Proceedings of the 3rd Symposium on Usable Privacy and Security 2007 (SOUPS), Pittsburgh, PA, USA, 18-20 July*.

Chiasson, S., van Oorschot, P.C. and Biddle, R. (2007b), "Graphical password authentication using cued click-points", in Biskup, J. and Lopez, J. (Eds), *ESORICS 2007, 12th European Symposium on Research in Computer Security, Dresden, Germany, 24-26 September*, Springer, Berlin, pp. 359-74.

Chiasson, S., Forget, A., Biddle, R. and van Oorschot, P.C. (2008a), "Influencing users towards better passwords: persuasive cued click-point", paper presented at the HCI 2008, Liverpool, 1-5 September.

Chiasson, S., Forget, A., Stobert, E., Oorschot, P.C.V. and Biddle, R. (2008b), "Multiple password inteference in text and click-based graphical passwords", Technical Report No. TR-08-20, School of Computer Science, Carleton University, Ottawa.

Davis, D., Monrose, F. and Reiter, M.K. (2004), "On user choice in graphical password schemes", *Proceedings of the 13th USENIX Security Symposium, California, CA, USA, 9-13 August*, USENIX Association, Berkeley, CA, pp. 1-11.

De Angeli, A., Coventry, L., Johnson, G. and Coutts, M. (2003), "Usability and user authentication: pictorial passwords vs. pin", in McCabe, P.T. (Ed.), *Contemporary Ergonomics 2003*, Taylor & Francis, London, pp. 253-8.

De Angeli, A., Coventry, L., Johnson, G. and Renaud, K. (2005), "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", *International Journal of Human Computer Studies*, Vol. 63, pp. 128-52.

Djamila, R. and Perrig, A. (2000), "Deja Vu: a user study using images for authentication", *Proceedings of the 9th USENIX Security Symposium, Denver, CO, USA, 14-17 August*, USENIX Association, Berkeley, CA, pp. 45-58.

Dunphy, P., Nicholson, J. and Olivier, P. (2008), "Securing passfaces for description", *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS 2008). Pittsburgh, PA, USA, 23-25 July*, ACM, New York, NY, pp. 24-35.

Golofit, K. (2007), "Click passwords under investigation", in Biskup, J. and Lopez, J. (Eds), *Computer Security – ESORICS 2007*, Springer, Berlin, pp. 343-58.

Hinds, C. and Ekwueme, C. (2007), "Increasing security and usability of computer systems with graphical password", *ACM Southeast Regional Conference, Winston-Salem, NC, USA*, ACM, New York, NY, pp. 529-30.

King, M.M. (1991), "Rebus passwords", *Computer Security Applications Conference, San Antonio, TX, USA,* IEEE, New York, NY, pp. 239-43.

Moncur, W. and Leplatre, G. (2007), "Pictures at the ATM: exploring the usability of multiple graphical password", *CHI '07: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, 28 April-3 May*, ACM, New York, NY, pp. 887-94.

Nickerson, R.S. (1968), "A note on long-term recognition memory for pictorial material", *Psychonomic Science*, Vol. 11 No. 2, p. 58.

Passfaces (2003), "Next generation graphical authentication", available at: www.realuser.com/personal/index.htm (accessed 15 March 2008).

Renaud, K. (2009), "On user involvement in production of images used in visual authentication", *Journal of Visual Languages and Computing*, Vol. 20 No. 1, pp. 1-15.

Shepard, R.N. (1967), "Recogition memory for words, sentences and pictures", *Journal of Verbal Learning and Verbal Behavior*, Vol. 6, pp. 156-63.

Standing, L., Conezio, J. and Baher, R.N. (1970), "Perception and memory for pictures: single-trial learning of 2500 visual stimuli", *Psychonomic Science*, Vol. 19 No. 2, pp. 73-4.

Thorpe, J. and van Oorschot, P.C. (2007), "Human-seeded attacks and exploiting hot-spot in graphical passwords", *16th USENIX Security Symposium. Boston, MA, USA,* USENIX, Berkeley, CA, pp. 102-18.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005a), "Authentication using graphical passwords: effects on tolerance and image choice", paper presented at the Symposium on Privacy and Security (SOUPS), Pittsburgh, PA, 6-8 July.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005b), "PassPoints: design and longitudinal evaluation of a graphical password system", *International Journal of Human Computer Studies*, Vol. 63, pp. 102-27.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2005), "The memorability and security of passwords", in Cranor, L.F. and Garfinkel, S. (Eds), *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly, Sebastopol, CA, pp. 129-42.

Corresponding author
M.Z. Jali can be contacted at: mohd.jali@plymouth.ac.uk

Quantifying the Effect of Graphical Password Guidelines for Better Security

MZ Jali[1,3], SM Furnell[1,2] and PS Dowland[1]

[1]Centre for Security, Communications and Network Research (CSCAN), Room A304, Portland Square, University of Plymouth, Plymouth PL4 8AA, UK.

[2]School of Computer & Security Science, Edith Cowan University, Perth, Western Australia

[3]Faculty of Science & Technology, Universiti Sains Islam Malaysia, Nilai, 71800, Negeri Sembilan, Malaysia.

Email: zalisham@usim.edu.my

Abstract. Authentication using images or graphical passwords is one of the possible alternatives for traditional authentication based upon passwords. This study aims to investigate the practicality of giving guidelines or advice to users before they start choosing their image passwords, the effectiveness of using a smaller tolerance (clickable areas) and the optimum combination of click and image passwords. An alternative graphical prototype known as the Enhanced Graphical Authentication Scheme (EGAS) was developed in order to achieve these aims which implemented two different types of data collection (internal and external). From the findings, both internal and external groups indicated that the implementation of guidelines alone cannot guarantee the security of image passwords created by participants; but, in combination with other usability measurements this study has shown positive outcomes.

Keywords: Graphical passwords, Authentication, Usability, Security, HCI

1 Motivation

Using images to authenticate users is one possible alternative for password-based authentication. Previous work has divided image-based authentication into three categories; namely 'click-based', 'choice-based' and 'draw-based'. The click-based approach refers to the action of clicking on the provided/chosen image(s) (i.e. selecting an element of the image), choice-based refers to the action of selecting a series of images (i.e. choosing images from a selection on screen) and draw-based refers to the action of drawing/sketching in order to be authenticated.

Regardless of the methodologies, previous studies have reported positive results, especially in the aspects of recall and memorability (i.e. participants were able to remember their secrets (i.e. image passwords) accurately after long periods of time) and usability (i.e. using images is user friendly) [1], [2] and [3]. Conversely, studies have also reported the disadvantages. Davis et al. [7] and Tullis and Tedesco [8]

found that users chosen secrets were influenced by gender. Chiasson et al. [4] reported that the concept of clicking on images (e.g. Passpoint [5]) was not secure as users tended to create hotspots (i.e. focussing upon one area in an image) and generating similar patterns (e.g. a straight line from top-bottom or left-right). Oorchot et al. [6] claimed that it was possible to crack users' secrets regardless of the background image, with the study by Everitt et al. [9] reporting that having multiple secrets resulted in more errors when compared with password-based authentication.

With respect to security, the main problem with the click-based method can be referred to as 'hotspot' while the problem with the choice-based method can be referred to as 'hot-image'. The problem of hot-image happens when a similar image is selected by many users. This problem could also be associated when users choose similar categories/themes or through gender preferences (e.g. males choose cars and females choose flowers). The hotspot problem could occur in two conditions. Firstly, the user clicks within the same or similar point on the given image or clicks on the same point or area when two or more images are given. Secondly the user produces predictable shapes such as straight lines and clicks on obvious/predictable objects within the image. Studies related to security in graphical passwords can be found in [10], [11], [12] and [13].

In an attempt to address or reduce the aforementioned problems and at the same time maintain users' memorability, many studies have been published with regards to the effect of using various types of images. Examples include using images of cartoon characters [3], images of geometric shapes [14] and using images that were later transformed into unclear or distorted forms during login [15] and [16]. With respect to the click-based method, a technique known as persuasion has been proposed [17] where the software recommends to the user possible 'safe' areas in which to create their secrets.

As far as the authors are aware, no study was found to have investigated or introduce user guidelines as part of the enrolment process. Therefore, the authors introduced a set of guidelines for graphical authentication, referred to as the Graphical Password Guidelines (GPG) which was presented to the user before they began choosing their secrets.

The authors also conjectured that GPGs on their own (Table 1) would not be a universal solution due to inherent human behaviour (i.e. certain users, although aware of the guidelines, sometimes violate the rules). To address this, restrictions were applied during registration. Two restrictions implemented in this study are as follows:

1. Users were only permitted to choose one image per category.
2. Users were not permitted to click on the same areas within an image. If they choose more images, they were also not permitted to click on the same area within the images.

The above restrictions together with the GPG were integrated into a software prototype. The software applied these restrictions by displaying warning messages if the software identified the user attempting to breach the rules.

The study was conducted in order to examine the impact on usability as well as user perception towards the introduction of the GPGs and image selection restrictions. Each participant had two types of secret; namely click-secrets (based upon the action of clicking on an image) and image-secrets (based upon the action of choosing a sequence of images). In addition to this, the study aimed to find ideal (usable and secure) combinations of click and image-secrets. A third investigation was undertaken to evaluate the impact of reducing the tolerance of the click positions. Tolerance can be explained as the extent of the area surrounding the users' secret clicks which are still accepted as legitimate. Prior research has indicated that participants were quite good when entering their secrets, both during registration and login [19]. Thus, the authors believed that using a smaller tolerance is possible and for this reason, users' performance when using smaller tolerance was investigated.

Table 1: Graphical password guidelines.

Task	Guideline	Explanation
Choosing images	Choose different themes and images	Users perceives image differently and previous studies have found gender bias in user image selections [7], [8] and [18]. As a result, the user is advised to choose different images, the image itself should not related to gender and more importantly, they are advised to choose images that they think could offer them memorable areas for placing their secret clicks.
	Try to avoid imagery that could be associated with your gender	
	Please choose images that offer you various memorable areas for placing your secret clicks	
Clicking on images	Try not to click within the same or adjacent areas	Oorchot et al., [6] showed that some users' secret were predictable. To reduce this, the user is advised to create their secret randomly. Specifically, they are not permitted to click on or within the same area (also applied to many images), advised not to create an easy to guess pattern (e.g. straight line) and encouraged not to click on obvious objects (e.g. edge, centre of each image).
	Try to click on various areas, not only on an obvious object	
	Please avoid predictable patterns (e.g. straight line, edges, central of images, etc)	

The next section of this paper highlights the methodology, followed by the results, discussion and conclusions.

2 Methodology

A graphical software prototype known as the Enhanced Graphical Authentication System (EGAS) was developed using Microsoft Visual Basic 2008. EGAS is an alternative graphical authentication employing a combination of both click and choice-based methods. In the EGAS software prototype, users are given the freedom

to choose their preferred number of clicks (secret clicks), with the software assigning the number of images (secret images) they need to choose. Table 2 shows the combination of secret clicks and secret images.

Table 2: Click and Image details used in the software prototype.

Secret click chosen	Secret image assigned	Image size/Tolerance
1	6	200x200 / 7x7
2	5	200x200 / 7x7
3	4	200x200 / 7x7
4	3	200x200 / 7x7
5	2	200x200 / 7x7

Two types of data collection were implemented; named as 'internal' and 'external'. Internal means the experimenter observed participants during trial (similar with the one to one usability testing) and they had to complete current task before proceeding to the next (controlled by the software prototype). Participants within the external group had to install the software prototype into their personal computer and use it for three weeks, with all of their activities recorded into a database (no means of control was enforced by the software prototype).

Participants for both groups (internal and external) had to register their details (username and secrets) in the software prototype, were then required to log into the software using their chosen secrets and finally provide feedback via a questionnaire. All tasks were done within the software prototype.

During the secret registration (enrolment), the GPG were first displayed to them (by which they had to acknowledge the GPG) before they chose their secret. During image selection, participants were able to choose images from 10 different themes (buildings, abstract, food, animals, flowers, view, people, sport, transport and fruits), with each of them consisting of 9 distinct images (arranged in 3x3 grids).

Participants within the internal group were asked to login three times, while the external group needed to login on four different days in week 1, two different days in week 2 and finally login once in week 3. This aimed to examine their familiarity and competency (e.g. login time, clicking accuracy, total attempts).

The trial was conducted over two months with the participants of the internal group recruited via an open call for volunteers within the authors' university. Participants of the external group were colleagues/friends of the author (external to the University) and invited via email, chat messengers and text messages.

The data were interpreted and reported into five main categories; namely number of attempt, timing, pattern, accuracy and finally users' feedback. The number of attempt looks upon participants' failure and success trials during both registration and login tasks while timing reports the time needed for these tasks. Pattern discusses the occurrences of 'hotspot' and 'hot-image', with accuracy mainly focuses upon the participants' ability to click on their secret clicks and finally users' feedback reports participants' perception on the questionnaire.

3 Results and Discussion

In total, there were 48 participants participated. Table 3 gives information for both groups highlighting the gender split and number of participants who had previously participated in graphical password studies [18].

Table 3: Participants' information.

Demographic	Internal group	External group
Male participant	12	10
Female participant	18	8
Experienced using GA	10	2

3.1 Number of Attempt

3.1.1 Internal group

Members of this group undertook 356 of authentication attempts. Of these, 94 logins were successful and 47 failed, 156 failed during registration and 66 were able to register successfully (note that software recorded two trials for each participant if they managed to register).

Participants who changed their click decided to choose the lowest click. Of the total seven participants who initially chosen three clicks on each image, five of them went to one click, while the remaining chosen two clicks. Moreover, all five participants who initially chosen two clicks and one participant who initially chosen four clicks also decided to choose one click.

During login, all participants within all click groups performed well where they managed to login, these results improved with experience. Only ten participants recorded a complete failure to login. There were six occurrences of failed attempts for login one, four occurrences for login two and only three occurrences for login three. The ability of participants to login with fewer failed attempts suggests participants performance improved with experience.

3.1.2 External group

With eighteen participants within this group, the software recorded a total of 283 login attempts in week one, 61 trials for week two and finally 30 for week three. Of these, there were 92 successful logins for week one, 51 for week two and 20 for week three (note that there were participants who logged into the software more than was asked for).

Investigation of successful usernames who continued with the login tasks found mixed results. It was found only 12 participants followed the login interval task, with the remaining 6 participants using the software occasionally. For those who logged

into the software according to specified tasks, 9 participants had chosen one click, 1 participant chose two clicks and 2 participants chose five clicks. Analysis has also found that 6 participants (who did not complete the login tasks) infrequently login during week one, with three of them logged twice for week two and finally all of them logged into the software in the third week. Five of them had chosen one click, while the remaining participant went for five clicks.

Only eight of the external group participants managed to register by using their first username. Of the remaining 10 participants who used a second username, six of them changed their secret click to the least click. Unless otherwise stated, most of the analysis for this group was based upon 18 participants who completed the specified tasks.

3.2 Timing

3.2.1 Internal group

The time for participants to register and then log into the software prototype was recorded with the time during registration calculated from the point when they pressed the 'register account' button until to the result for registration is displayed. The time for login was calculated from when the participant started to enter their username until the last click for their secret images.

Table 4 shows participants' time (average, shortest, longest and standard deviation) during registration and three logins, in minutes, (m) and seconds, (s).

Table 4: Timing for the internal group.

Click	Participant	Time	Registration	Login One	Login Two	Login Three
1	18	Average	5m 23s	24	20	18
		Shortest	1m 43s	15	11	9
		Longest	21m 58s	42	42	4
		SD	4m 43s	8	8	6
2	5	Average	10m 29s	40	35	27
		Shortest	2m 23s	28	25	18
		Longest	23m 33s	71	69	40
		SD	7m 56s	17	18	8
3	3	Average	9m 56s	39	33	33
		Shortest	5m 47s	36	23	22
		Longest	16m 46s	43	39	42
		SD	5m 58s	4	9	10
5	2	Average	2m 56s	26	20	23
		Shortest	1m 12s	24	19	21
		Longest	4m 40s	28	21	24
		SD	2m 27s	3	1	2

For all click groups, the registration time can be considered long due to the action of selecting images and then clicking on the chosen images. It can be reported that for all click groups, the time to login during login attempts one to three are significantly

shorter. The study also found that participants do not immediately select their click area, often taking several seconds before they start clicking on it. This action is believed to be due to the small tolerances used, which suggests it could directly affect login time and security if the users were observed.

3.2.2 External Group

Table 5 shows the time for 12 participants as they managed to login according to the specified login intervals. L1 to L5 refers to the login times (measured in seconds, (s)) for week one, L6 and L7 are login times for week two and finally L8 refers to the login time for the third week. It was found that the login time across the three weeks varied, although with one click, participants showed little change.

Table 5: Timing for the external group.

Click	Participant	Time	Register	L1	L2	L3	L4	L5	L6	L7	L8
1	9	Average	11m 17s	17	20	17	20	14	17	17	14
		Shortest	2m 15s	14	14	13	11	12	10	10	9
		Longest	47m 23s	23	39	28	37	22	31	43	21
		SD	14m 2s	4	8	7	10	3	6	11	3
2	1	Average	3m 22s	19	26	21	31	16	15	18	24
		Shortest	3m 22s	19	26	21	31	16	15	18	24
		Longest	3m 22s	19	26	21	31	16	15	18	24
		SD	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
5	2	Average	10m 2s	33	29	23	35	25	28	20	27
		Shortest	2m 39s	29	24	22	22	23	23	19	26
		Longest	17m 25s	37	34	23	48	27	32	20	28
		SD	10m 26s	6	7	1	18	3	6	1	1

3.3 Accuracy

As reported earlier, the numbers of failed attempts during registration were high. As a result, participants had to use other usernames and changed their preference secret click or image. The authors discovered two main errors associated with such scenario, as indicates below.

a) Participant was unable to click within the allowable tolerance.
b) Participant did not click in sequence order, as the result of forgetting their secret order or areas.

From the data for both internal and external groups, it can be revealed that errors during both registration and login were correlated with participants who selected more clicks. In specific, there were slightly more participants who made tolerance errors than order errors. This is probably due to the software prototype using a small click tolerance.

Particularly within the external group, participants were unable to click accurately when they first started using the prototype. However, they managed to click within

the clickable areas as they became familiar with using the software and understood what they needed to accomplish.

3.4 Pattern

Patterns are created during image selection when participants chose the same images (in the case of changing username of click), gender skew selection (e.g. men choosing sports car while women chose flowers) and following image order (e.g. participants choosing the first image in each theme). Moreover, patterns during the click selection are created when participants clicked on the same area across all images, producing obvious shapes or clicking their secrets in a straight line (e.g. top, bottom and left side of image area), and clicked on the image that appeared to be offering a pattern. Results for both groups are reported together within this section as they used similar software prototype.

With the internal group, the study found the majority of participants who changed their username or secrets (click or image) used their previously chosen images. One participant from the five clicks group used both of his previous images while two participants from the two clicks group used three and one of their previous images respectively. Of all the participants from the one click group who changed their username or clicks, only one did not used their previous image. Specifically for the one click group, two participants used four of their previous images while the others were ranging from one to three. In addition, it was also found one of these participants selected the first image for each theme as their secret images.

The external group also used their previous secret images with one participant using all of their previous images, with six other participants using between one to two of their previous chosen images .It was also found that two participants of the one click group chose their images in sequence (choose the first six themes); however their chosen images were different with each other.

Table 6: Image popular with their associated number of male and female.

Theme	Number of participants choosing popular image	Male	Female
Buildings	11	3	8
Abstract	12	6	6
Food	8	4	4
Animals	7	3	4
Flower	10	4	6
View	14	7	7
People	5	2	3
Sport	13	8	5
Transport	4	1	3
Fruits	7	2	5

Table 6 presents the number of participants who chose popular images for each theme. It was found that the view and sport themes are the most popular, with the transport and people themes as the least popular selection.

Although it was found that a number of participants clicked within similar areas when creating their secret clicks, such action was eliminated due to the software prototype preventing participants from clicking on the same area within multiple images. Analysis was carried out to examine the area of clicking for participants who chose more clicks and although it can be reported that participants with two or three click groups create less obvious pattern, participants of the five clicks group clearly create patterns. The authors deduced that such scenarios are related to the images themselves, which clearly offer a pattern to be created.

Analysis was also done to examine the click areas in popular images for each theme. Analysis on the one-click group who chose the most popular image revealed that ten of the twelve participants who chose popular images in the sports theme clicked on the three most popular areas (see left side of the fig. 1), with seven out of twelve participants who chose the most popular image for the 'view' theme clicked on the same area (see right side of the fig. 1). Equally, all other popular images have shown a pattern where participants clicked on similar spots.

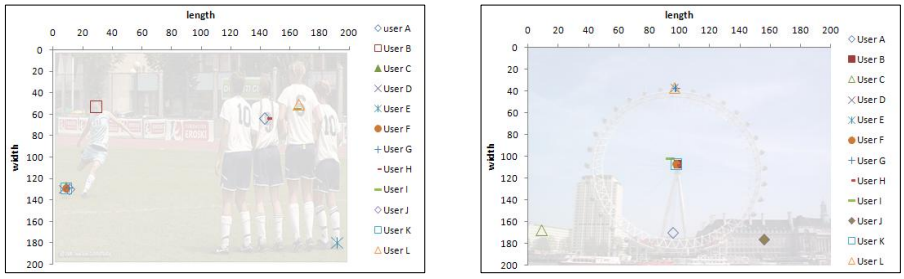

Fig. 1. Participants click areas for the popular image of the 'sport' (left) and 'view' (right) themes.

From the collected data, the authors summarised that participants who chose more clicks tended to create patterns during their clicking task, while the existence of pattern during image selection was unidentified. Meanwhile, participants who chose more images (fewer clicks) tended to create patterns during both image and click selection. Patterns where users chose the first or last image for each theme was also reported. Although the authors' approach of not implementing restrictions for image selections and depending solely upon the guidelines is less effective then the introduction of guidelines. The GPG itself has resulted in the reduction of gender bias image selection and image order patterns.

It can, however, also be said that the restrictions together with the guideline during secret click selection played a minor role during the click selection task. Although not representative, participants with a higher number of clicks created more patterns

(possibly as it is easier for them to remember), with analysis towards one click participants revealing the existence of hotspot.

3.5 Users' Feedback

A Likert five points scale rating was used to obtain participant feedback with the lowest score indicating participants' agreement with the statements while the highest score indicating disagreement. Table 7 reports the mean score of feedbacks for the first three questions within the internal group.

Table 7: Questionnaire results.

Question	Mean score
Perception towards graphical password guidelines (GPG)	1.6
Perception towards restrictions	1.8
Perception towards combining GPG with the restrictions	1.8

When asked about participants average login time (with the software prototype displaying their average login time), it can be revealed that twenty participants found their login time were acceptable, with eight unacceptable. Seventeen participants agreed that their total registration time was acceptable while the remaining eleven disagreed. With the statement on the optimum combination of image and click, twenty two of the participants felt that having more images was more memorable than having more clicks, while five participants felt that the balance between both click and images were still memorable.

Participants who were new to the graphical method felt the method could be very useful and provided excellent protection. However, the majority of the participants who were involved in the previous trial felt that having larger clickable areas was more usable. In addition, they felt that having more clicks could be troublesome as they had to memorise too many spots and finally all participants agreed that in order for them to perform better, they needed to become more familiar with the method.

4 Conclusions and future work

This paper presented an investigation of the practicability of giving guidelines to a user before they chose their secrets for a graphical authentication system as well as evaluating user attitudes and opinions to the enhanced techniques.

During the registration task, participants struggled to click accurately within the allowable click tolerance and those who chose more clicks often failed to click in the correct order. As the result, they had to change to create new accounts or change to fewer clicks. The login task had shown improvement as they managed to login with fewer failed attempts, and the time to login to the software prototype was reduced marginally across login interval. The above findings reflect participants' familiarity with the software prototype as they used the software regularly.

Introducing guidelines to the participants before they start selecting their secrets had obtained positive perception from the majority of participants. However, this study has shown that guidelines on their own cannot guarantee the security and safety of the method itself. This is because participants used their previous images and created secret clicks using easy to remember spots, which resulted in predictable click-areas. By combining the introduction of guidelines with restrictions, user behaviour can be controlled to safeguard the method. This was proven where cases such as clicking on similar areas within the same or multiple images and where creating predictable pattern were reduced.

Finally, this paper has shown that the click patterns created by users who chose more clicks had a direct relationship with the nature of the image itself. It could be said that the introduction of guidelines gave no effect on participants' usability performance, but might give positive or negative effects on the security. The study also suggests that using one click per image is an ideal combination. This is because using one click per image requires less memorisation (i.e. it is more suitable for users with multiple accounts), less time to authenticate, convenience and significantly safer from predictability. The study also suggests that using a small tolerance without giving sufficient opportunity for familiarity to the user could result in a lack of usability of the proposed method.

It is suggested that future work could include a larger and more varied participant based for conducting significance testing to validate the collected data, testing different restrictions with the GPG, further evaluation of the claim that 'one click per image is better' and evaluating the technique known as the 'graphical-passwords-strength-meter', for safer secret creation based upon feedback from the system itself.

5 References

1. De Angeli, A., Coventry, L., Johnson, G., Renaud, K.: Is a picture really worth a thousand words? Reflecting on the usability of graphical authentication systems. International Journal of Human Computer Studies 63(2), 128-152 (2005)
2. Chiasson, S., Oorschot, P.C.V., Biddle, R.: Graphical password authentication using Cued Click-points. In: Biskup, J., Lopez, J. (eds.) ESORICS 2007, 12th European Symposium On Research In Computer Security, Dresden, Germany, September 24-26, 2007, 359-374. Springer (2007)
3. Hinds, C., Ekwueme, C.: Increasing security and usability of computer systems with graphical password. In: ACM Southeast Regional Conference, Winston-Salem, North Carolina, USA, 529-530. ACM New York (2007)
4. Chiasson, S., Forget, A., Biddle, R., Oorschot, P.C.V.: User interface design affects security: Patterns in click-based graphical passwords. International Journal of Information Security 8(6), 387-398 (2009)
5. Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A., Memon, N.: PassPoints: design and longitudinal evaluation of a graphical password system. International Journal of Human Computer Studies 63, 102-127 (2005)
6. Oorschot, P.C.V., Salehi-Abari, A., Thorpe, J.: Purely automated attacks on Passpoints-style graphical passwords. Transactions on Information Forensics and Security 5(3), 393-405 (2010)

7. Davis, D., Monrose, F., Reiter, M.K.: On user choice in graphical password schemes. In: Proceedings of the 13th USENIX security symposium, California, USA, August 9-13, pp. 1-11. USENIX Association (2004)
8. Tullis, T.S., Tedesco, D.P.: Using personal photos as pictorial passwords. In: CHI 05 extended abstracts on Human factors in computing systems, Portland, Oregon, USA, 1841-1844. ACM (2005)
9. Everitt, K.M., Bragin, T., Fogarty, J., Kohno, T.: A comprehensive study of frequency, interference, and training of multiple graphical passwords. In: Proceedings of the 27th international conference on Human factors in computing systems, Boston, MA, USA, pp. 889-898. ACM (2009)
10. Dirik, A.E., Memon, N., Birget, J.-C.: Modelling user choice in the Passpoints graphical password scheme. Paper presented at the Symposium On Usable Privacy and Security, Pittsburgh, PA, USA, July 18-20 (2007)
11. Golofit, K.: Click passwords under investigation. In: Biskup, J., Lopez, J. (eds.) Computer Security - ESORICS 2007, vol. 4734/2007. Lecture Notes in Computer Science, pp. 343-358. Springer Berlin/Heidelberg, (2007)
12. Golofit, K.: Picture passwords superiority and picture passwords dictionary attacks. Journal of Information Assurance and Security, 2, 179-183 (2007).
13. Peach, S., Voster, J., Heerden, R.V.: Heuristic Attacks against graphical password generators. In: Clarke, N., Furnell, S., Solms, R.V. (eds.) Proceedings of the South African Information Security Multi-Conference (SAISMC 2010), Port Elizabeth, South Africa, pp. 272-284. University of Plymouth (2010)
14. Lin, P.L., Weng, L.T., Huang, P.W.: Graphical password using images with random tracks of geometric shapes. In: Proceedings of the 2008 Congress on Image and Signal Processing, pp. 27-31. IEEE Computer Society (2008)
15. Harada, A., Isarida, T., Mizuno, T., Nishigaki, M.: A User Authentication System Using Schema of Visual Memory. In: LNCS: Biologically Inspired Approaches to Advanced Information Technology, vol. 3853/2006. 338-345. Springer (2006)
16. Hayashi, E., Dhamija, R., Christin, N., Perrig, A.: Use Your Illusion: secure authentication usable anywhere. In: Proceedings of the 4th symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 35-45. ACM (2008)
17. Chiasson, S., Forget, A., Biddle, R., Oorschot, P.C.V.: Influencing users towards better passwords: persuasive cued click-points. In: Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1, Liverpool, United Kingdom, 121-130. British Computer Society (2008)
18. Jali, M.Z., Furnell, S.M., Dowland, P.S.: Assessing image-based authentication techniques in a web-based environment. Information Management & Computer Security 18(1), 43-53 (2010)
19. Chiasson, S., Biddle, R., Oorschot, P.C.V.: A second look at the usability of click-based graphical passwords. In: Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 1-12. ACM (2007)