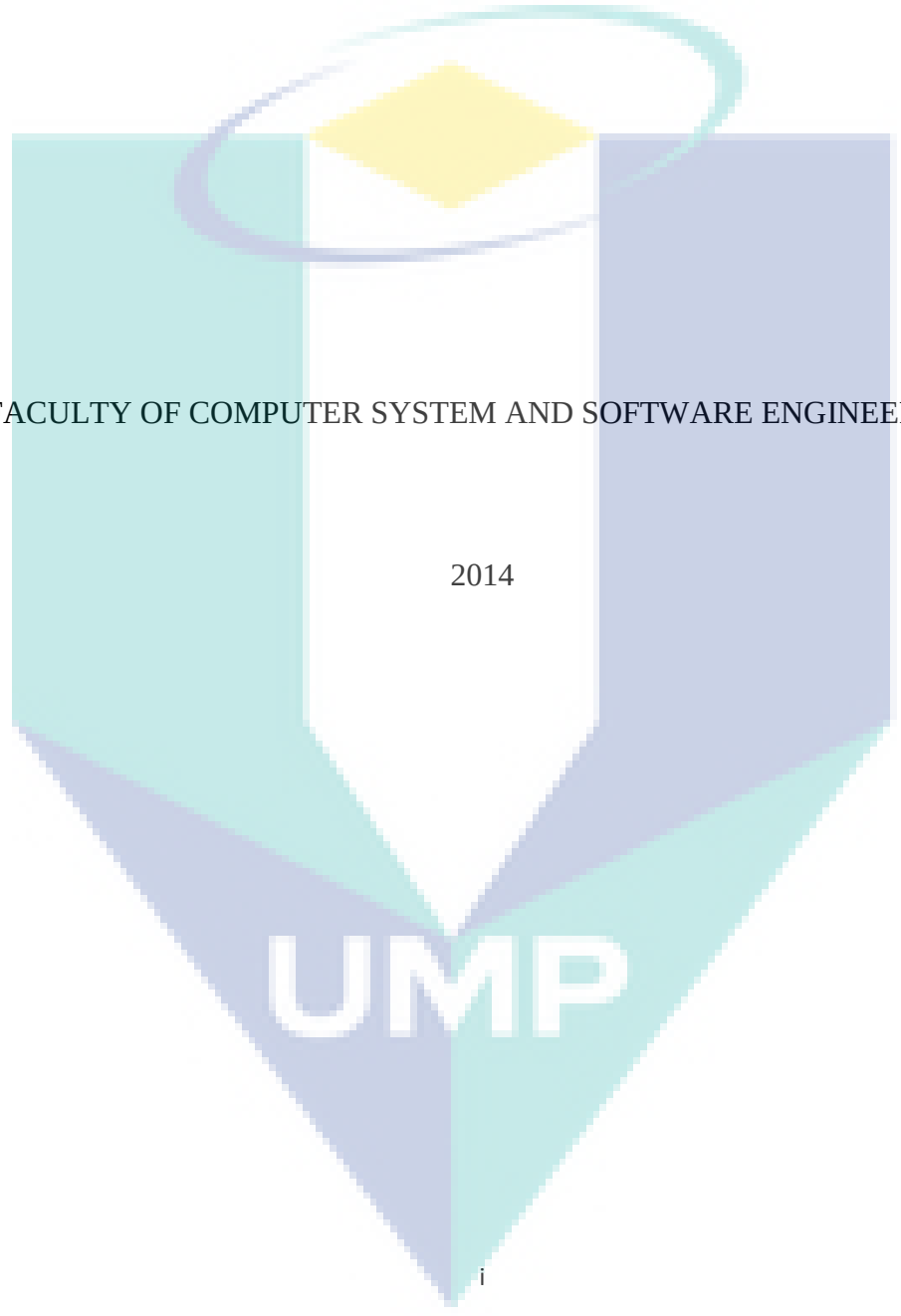
STUDY OF GRAPHICAL AUTHENTICATION SYSTEM BASED ON PERSUASIVE ROTATION, RESIZING AND CUED CLICK POINT (GUAS)



FACULTY OF COMPUTER SYSTEM AND SOFTWARE ENGINEERING

2014

UMP

Abstract

Nowadays, the most accepted computer authentication technique is to use alphanumerical usernames with text-based password. This method has been proven to have significant multiple weaknesses. For example, users tend to choose the passwords that can be easily cracked. On the other hand, if a password is difficult to guess, then it is often hard to memorize. To address those issues, some researchers have developed graphical-based authentication algorithm that implement pictures as passwords. In this project, I had conduct an in-depth comprehensive review regarding the existing graphical password scheme. Furthermore, I classify these existing Graphical User Authentication System (GUAS) into two kinds of mechanism, which are: recognition-based and recall-based approaches. Besides that, I will examine the strengths and limitations of each technique and identify the future research directions. I also developed an improved version of GUAS algorithm address the common limitation exists in the current graphical password techniques. Overall, in this thesis, the scheme of the new technique will be proposed, the advantages of technique will be outlined and lastly, the future work will be anticipated as well.

ABSTRAK

Pada masa kini, teknik pengesahan pengguna komputer yang paling diterima oleh masyarakat adalah menggunakan kata laluan berasaskan teks. Kaedah ini telah dibuktikan mempunyai pelbagai kelemahan yang ketara. Sebagai contoh, pengguna cenderung untuk memilih kata laluan yang mudah diteka. Sebaliknya , jika kata laluan yang sukar untuk diteka , maka ia sering sukar untuk dihafal oleh pengguna. Bagi menangani isu-isu ini, beberapa penyelidik telah berlahirkan teknik pengesahan dengan berdasarkan bantuan grafikal seperti, mengguna gambar sebagai kata laluan. Dalam projek ini , saya akan menjalankan kajian semula yang mendalam dan komprehensif mengenai skim kata laluan grafik yang sedia ada. Tambahan pula, saya telah mengelaskan teknik pengesahan grafikal kepada dua jenis mekanism. Selain itu, saya akan mengkaji kekuatan dan batasan setiap teknik serta mengenal pasti arah penyelidikan masa depan. Saya juga membangunkan satu teknik pengesahan grafikal yang lebih baik dan dapat menyelesaikan isu-isu wujud dalam teknik kata laluan grafik semasa ini. Dalam tesis ini, skim teknik baru akan dicadangkan, kelebihan teknik akan dibincang, akhir sekali, kerja masa depan akan dijangka juga.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

1.1 Project Overview

Indeed, the internet and the usage of computer are rising up rapidly.

More and more aspects of human life are moving to online nowadays. The internet is a global network connecting of billions computer to exchanges of data, news and opinions. Obviously, vast range of human activities is depending on internet, including online banking transaction, online merchandize/shopping and online research.

Furthermore, peoples also using the Internet as their main social tools as well. Undoubtedly, in the last few years there is been an impressive growth in the number of social networking sites such as Facebook. Peoples often tend to share many kinds of their personal information on the social networking website as well as their name, recent status, their current location and etc. Hence, It is essential for us both as internet users and as educated man to continually think about the issues had been arise from internet technology.

With the amount of online identify theft and hackers currently prowling on the internet, it is very crucial to fully protect our computer from online dangers. This is important for every one of us, not just the overly security conscious. Foremost, the very first line of defense on the web is using the password. Passwords able to ensure the confidentiality and security of data which are stored on various workstations and prevent our online account exposed to the identity theft easily. Ultimately, the usage of password will decrease the risk of internet user to become a victim of cybercrime

The most usual computer authentication method is to implement the alphanumerical password for account or system login session. But, this method has been proven to have some significant drawbacks. For example, users tend to choose the passwords which can

be easily hacked or guessed. On the other hand, if a password is strong enough, then it is always difficult to memorize it. To address this problem, some IT researchers have developed many kind of alternative authentication methods that based on the usage of image as passwords or the combination of picture and alphanumerical method.

Even though the graphical user authentication system (GUAS) is able to counter some of the drawback of the alphanumerical method, yet the strengths and limitations of each graphical method are still remain disputable such as implementation issues and major design weakness for the graphical password. Thus, this project will aim to discuss the usability of the current available GUAS and propose an improved version of graphical user authentication techniques against the commonly seeing problems in the graphical password area nowadays.

1.2 Problem Statement

Current available authentication systems are suffered from many kinds of weaknesses and limitation. The vulnerabilities of the text-based password scheme have been well known. Users always tend to choose short-length passwords or passwords which are easy to memorize, hence, this situation makes the passwords susceptible to password crackers or hackers. Furthermore, text-based password in alphanumerical scheme is vulnerable to dictionary attack, brutal guessing, social engineering, key-loggers, hidden-camera,spyware attacks, shoulder surfing and etc.

To address the limitations of text-based password, techniques such graphical-based password have been put in use. Other than that, additional input devices such as mouse, stylus and touch-screen that permit have raised the usability of the graphical user authentication techniques. The primary objective of enhancing the current user authentication scheme is to strengthen the method in the aspect of security and usability. Graphical password schemes have been proposed as a possible alternative to text-based schemes which motivated by the fact that humans can recognize graphical images better than text. In additional, psychological studies have shown that pictures are generally easier to be memorized or recognized than text. However, they are still mostly vulnerable to shoulder-surfing as well.

Shoulder-surfing attack is a direct observation technique, such as peeking over someone's shoulder (casual eavesdropping) to sneak their sensitive personal information. For instance, when a user enters information or password using a mouse, keyboard, touch screen or any conventional input device, a malicious observer may be able to acquire the user's password easily by watching in the user's vicinity. This is a problem that has been difficult to overcome even for the current GUAS scheme.

Previous research has proven that a graphical password is more memorable than a strong (non-dictionary term) alphanumeric passwords. On the others hand, participants in a prior study expressed concerns that the improvement of memorability necessarily leads

to higher risks of shoulder-surfing. Another potential drawback with graphical passwords is that it takes longer to input graphical passwords than textual passwords. The login process is slow and it may frustrate the impatient users. These entire limitations appear to be yet another classic example of the common trade-off between security and usability for a user authentication system.

For this project, I will first conduct a comprehensive outline of the existing graphical user authentication systems. Furthermore, a deeper discusses of the strengths and limitations of each method will be carrying out. Ultimately, this project will proposed an improved version of graphical password scheme which has desirable usability and better security feature by combination of the current available GUAS (hybrid of GUAS).

1.3 Background

One of the primary functions of any security system is to manage the movement of people to the protected areas, such as physical buildings, national borders or even our information systems. In fact, the systems data and the information those commit to computer memory or store on internet mostly are valuable resources which need to be protected. The first line of defense to repel the cybercriminal from ours crucial information is creating a password to authenticate the identity of user.

Typically, conventional password is composing of a string of letters and digits, i.e. alphanumeric. Passwords are simply secrets that shared by the verifier and the system user. Besides that, the passwords are in an encrypted form when stored on a server so that an invasion of the file system does not necessary will expose the password lists. Yet, such passwords have the drawback of being hard to remember. While weak passwords are often susceptible to dictionary attacks and brute force attacks where as strong passwords are difficult to memorize.

To resolve the problems associated with text-based authentication systems, the researchers have proposed the concept of GUAS and constructed alternative authentication mechanisms. GUAS is the most promising alternative to the conventional text-based password authentication systems. GUAS utilize the usage of images instead of textual passwords and are particularly motivated by the reality that humans can memorize graphical object more efficient than a string of characters. Thus, GUAS provide a measure for a more user-friendly password authentication session while able to enhance the level of security.

Just like humans, there is no perfect technology existed, hence, there will be type of flaw or limitation for the GUAS scheme as well. But, as an organism could using own minds in autonomous and creative manners, we should explore our limits and ask for what is not obvious. Ultimately, we are able propose and evaluate a new GUAS scheme which has a desirable usability with ideal security level.

1.4 Aim of the Project

The objectives of this project are:-

1. To discuss and analyze the current existing GUAS in term of security, usability and reliability features.
2. To propose an improved version of GUAS method that able to achieve balance between the aspect of security, usability and reliability.

1.5 Project Scope

1. Develop a user authentication system based on graphical scheme.
2. Proposing an improved GUAS algorithm while balance the trade-off between level of security, usability and reliability.

1.6 Thesis Organizations

This thesis consists of six main chapters. Chapter 1 will provide some brief overview on the introduction of the project. In this chapter, we can identify the need of a reliable alternative user authentication system is crucial due to the rampant cybercriminal and information security issues nowadays. Chapter 1 will expose the fact that GUAS had facing some limitation and drawback as well. Lastly, this chapter will cover the main objectives, scope of project and the overall thesis organizations.

In Chapter 2, it will contain the literature review of the project. We will first conduct a discussion of the several well-known and frequently used GUASs. Furthermore, the analysis of the strengths and limitations of each method will be undergone, hence, point out the future research directions in this area. Recommendations and opinion will be given based on the GUAS scheme as well on this chapter.

Chapter 3 will describes about the detail of methodology use for this project. Thus, we are able to explore on selected methodology and the steps used to establish this project. Furthermore, we will also be defining the requirement on which technique or tools are utilized when conducting the project. In addition, we will be discussing on which software and hardware is applied for carry out the development of this project. The Gantt chart is available to be review on this chapter as well.

Hence, in chapter 4 we propose the development of the framework and model through flow work. It will reveal the process and data gathering for research purposes, thus, sketching the work flow and model. We will also suggest on how the data or model has been implemented into the selected algorithm. Furthermore, we will be approach to the process that involved during the development of this project. The test and result will presented using the statistical tools accordingly.

Chapter 5 generalized the explanations about the findings and the results from data analysis. We also evaluated on the analysis result that related with the project aims and objectives. Through the chapter, the statement of constraint met and trade-off between

security and efficiency during development of project will be exposed. Discussion about the suggestion and space of improvement in order to secure utilization for the future development of this project will be provided on this chapter as well.

For the last chapter, chapter 6 will summarize the findings throughout of the project. Finally, the implication of the future enhancement and project constraint will be discussed to conclude the project.

1.7 Summary

As a conclusion, for this chapter we have explored the overview on the introduction of the project. Besides that, we also identified the need of a reliable alternative user authentication system is crucial due to the rampant cybercriminal and information security issues nowadays. Furthermore, we had point out the aim of the project as our future research directions. Lastly, this chapter has outlined the scope of project and the overall thesis organizations as well.

CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

For the security sensitive environments, it is crucial to safeguard the resources against unauthorized access at all cost such as enforcing the access control mechanisms. Hence, authentication session plays an important part in protecting resources against unauthorized malicious use. Tons of authentication methods exist in our environment nowadays, from simple password text-based authentication system to the costly and computation profound biometric authentication systems. Basically, current existing user authentication scheme can be branches into three fundamental fields:

- Token based authentication
- Biometric based authentication
- Knowledge based authentication
  - ✓ Text based
  - ✓ Graphic based

Token based techniques, such as tag cards, ATM cards and key cards are broadly used. Several token-based authentication systems also applied with knowledge based techniques to amplify the security level. For instance, ATM cards are usually used together with the PIN number.

For the biometric based authentication techniques, it consists of a few methods, such as, iris scanning, fingerprints authentication or facial recognition, but they are not yet widely adopted by the society. The major drawback of the biometric approach is that such systems can be over-costly, and the identification procedure can be time-consuming and often unreliable. Nevertheless, this sort of method presents the uppermost level of security.

Knowledge based techniques are the most popular authentication techniques in this century and it include of text-based and graphic-based authentication method. The most common knowledge text-based authentication approach is for a user to comply a user name and a text-based password. The vulnerabilities of this technique have been well known. One of the main worriment is the difficulty of memorizing the passwords. On the others hand, the graphic-based scheme can be further divided into two groups: recognition-based and recall-based graphical techniques. Implement the recognition-based techniques, firstly, a user will be presented with a set of images and the user must get through the authentication by identifying and recognizing the images he or she pre-selected during the registration phase. However, recall-based techniques require a user to regenerate something that he or she created or previously chosen during the registration phase. For this chapter, we will have a depth analysis on the existing current GUAS and discuss in term of their limitation as well as the advantages respectively.

2.2 Recognition-based Techniques

The basic idea of this method is a user will be presented with a set of images and the user must get through the authentication by identifying and recognizing the images he or she pre-selected during the registration phase.

2.2.1 D´ej`a Vu

Dhamija and Perrig developed a graphical authentication scheme based on hash visualization technique.

"We develop a prototype of D´ej`a Vu and conduct a user study that compares it to traditional password and PIN authentication. Our user study shows that 90% of all participants succeeded in the authentication tests using D´ej`a Vu while only about 70% succeeded using passwords and PINS. Our findings indicate that D´ej`a Vu has potential applications, especially where text input is hard (e.g., PDAs or ATMs), or in situations where passwords are infrequently used (e.g., web site passwords). (R. Dhamija and A.

Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.)"

In the Deja Vu system, user will be asked to choose particular number of picture from a set of random images provided by a program. Later, user will be required to recognize the pre-selected pass-images in order to be authenticated. The results showed that almost 90% of all participants succeeded in the authentication session while using their technique, while only 70% successful accomplish using text-based passwords and Pins. However, the average time to complete the process is longer than the conventional approach, but has a much lesser failure rate. A drawback is that the server is required to store a huge amount of graphical material which may have to be transferred over the network, hence, delaying the authentication procedure. Another limitation of this system is that the server also needs to store the seeds of the portfolio images of each user in plain text. In term of interface, the process of selecting a picture from picture database can be time consuming and tedious for the user.

Figure 1: Example of random art images.

In Akula and Devisetty's algorithm, the system displays batch of images to the user and the user would then choose their pass-image to authenticate themselves to the server. Generally, the basic scheme of this method is identical to the technique proposed by Dhamija and Perrig.

"The system does not store the images. The images are read byte wise and hashed using a secure hashing function SHA-1. Images are large files. But SHA-1 algorithm produces a 20 byte output which is very secure and requires less memory. This system was implemented in Java. Java is platform independent, portable and most suitable for Internet applications. (S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.)"

On the contrary, the difference is that this technique implements the hash function SHA-1, which produces a 20 byte output. This ensures the authentication to be more secure and requires less memory. However, image files still tempt to occupy more space than normal text file even after hashing. For this reason, Akula and Devisetty had suggested a possible future enhancement by providing the persistent storage and this could be integrated on the Internet, cell phones or PDA's.

2.2.2 Sobrado and Birget Algorithm

Sobrado and Birget proposed a graphical password technique that able to deal with shoulder-surfing limitation. At first, the system will show a few of pass objects (pre-selected by user) among many other decoy objects. The user is required to recognize pass-objects and clicking inside the area of convex hull which formed by the pass objects.

"The system randomly scatters a set of N objects on the screen. In practice, the number N could be a few hundred or a few thousand, and the objects should be different enough so that the user can distinguish them. In addition, there is a subset of K pass-objects (e.g., K = 10) previously chosen and memorized by the user. At login the system will randomly choose a placement of the N objects. However, the system first randomly chooses

a patch that covers half the screen, and randomly places the K chosen objects in that patch. To login, the user must find 3 of the pass-objects and click inside the invisible triangle created by those 3 objects. This is equivalent to saying that the user must click inside the convex hull of the pass-objects that are displayed. In addition, for each login this challenge is repeated a few (e.g., 10) times using a different display of some of the N objects. Therefore, the probability of randomly clicking in the correct region in each challenge is very low.(L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.)"

In order to strengthen the password and make it hard to predict, Sobrado and Birget recommended using 1000 objects, which making the display very complicated and the objects almost indistinguishable. Besides that, using fewer decoy objects may lead to a smaller password space due to the resulting convex hull can be huge. In their second algorithm, a user is order to move a frame (contain the one of the pass objects within it) until the pass object on the frame lines up and meet with the other pass-objects. In additional, the authors advise the authentication session should repeat the process for a few more times to diminish the likelihood of logging in by randomly rotating or clicking. The main limitation of these algorithms is that the procedure can be very time consuming and frustrated the user.

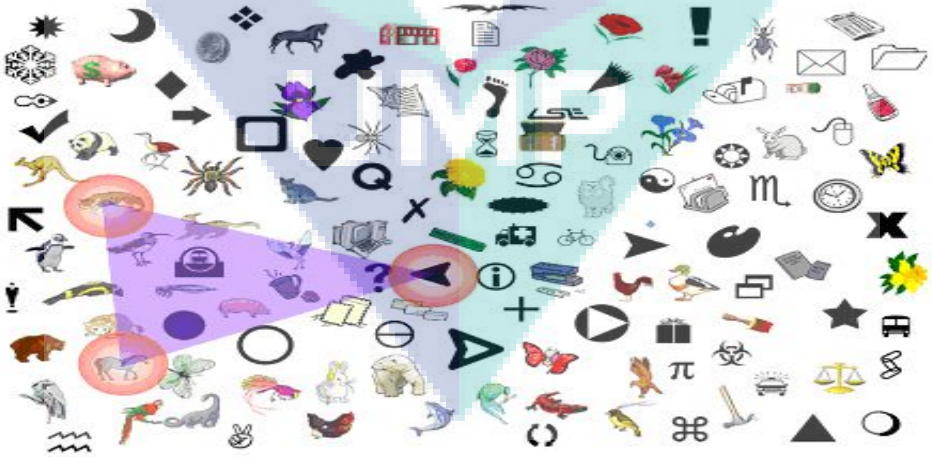


Figure 2: Sobrado and Birget first algorithm.

Figure 3: Sobrado and Birget second algorithm.

2.2.3 Man,et al Algorithm

Man, et al. had proposed another shoulder-surfing resistant algorithm.

"We propose a password scheme. This scheme is obtained by adding light graphic layer to the traditional text-based password scheme. In this graphic layer, we randomly generate patterns of icons which are easy for user who owns the password to recognize and difficult for a shoulder-surfing attacker to find out.(S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.)"

In this algorithm, a user asked to choose a few of image as pass-objects. Each pass-object consist several variants and each variation is designated a unique text-based code. During the authentication, user is confronted with several scenes. Each scene consists of several pass-objects (each in the form of a randomly picked variant) and many decoy objects. The user has to insert a string contain the unique codes matching to the pass-object variants introduce in the scene as well as a code expressing the relative location of the pass-objects. The argument is that it is very difficult to crack or guess this kind of password

even if the whole authentication procedure is sneaking by shoulder surfer or recorded on video. However, this technique demands users to memorize the alphanumeric password for each pass-object variant. For instance, if there are 3 images each with 4 variants, then each user has to memorize 12 unique codes. Despite the pass-objects provide some hints to help the users for recalling the codes, it is still consider very tiresome and inconvenient to memorize all those code.

"Formally, in our scheme a set of strings is used as a password. A part of this idea appeared in one of our early work. In this paper, we much further develop the idea in a practical way. Also, we programed this new scheme and run experiment. The result is promising. (D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.)"

In the next year, Hong, et al. extended this method (Man's algorithm) by approve user to attach their own unique codes to the pass-object variants. However, this mechanism still demand user to memorize large number of text strings and therefore suffer from some significant drawbacks of text-based passwords.

Figure 4: Sample of variants, 8 pictures with 4 variants

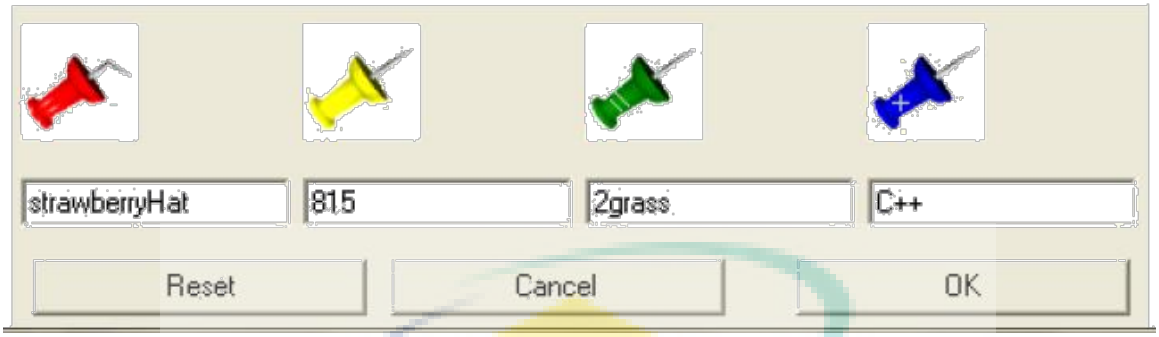


Figure 5: Register 4 variants with different code.

2.2.4 Passface

"Passface" is a authentication technique developed by Real User Corporation.

"Passfaces are graphical passwords that use faces as a unique verification technology for secure logon. Offering two factor authentication to provide a high level of authentication assurance, Passfaces supports a wide range of operating environments in which strong authentication is required. Passfaces Web Access easily integrates with existing security systems in financial, government, healthcare, and corporate networks. Passfaces is completely intuitive to use and combines two way authentication – user-to-site and site-to-user – in a single, reliable process.(RealUser, www.realuser.com, last accessed in October 2013)"

The basic idea is as follows. The user will be required to choose a certain number of images of human faces from the face database server as their future pass-image. In the authentication phase, the user is presented with a grid (3 x 3) of nine faces, containing of one face previously selected by the user and the others are decoy faces. The user should recognize it and clicks on the known face. This process is repeated for a few rounds. The users will consider as authenticated once he or she correctly identify the four faces. This method is based on the assumption that people can memorize human faces easier than other pictures and able to recall it back even after years.

Figure 6: Example of Passface system.

"Passfaces showed a third the login failure rate of passwords, despite having users with a third the frequency of use (less frequent means the memory task was more difficult). This performance difference was partly due to the password confusions of participants who had recently changed from Passfaces to passwords. While Passfaces' low error rate may be due to their superiority over passwords, there are other explanations that need to be ruled out. (S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.)"

User studies conduct by Brostoff and Sasse showed that Passfaces had only about 30% of the login failure rate compare with text-based passwords, despite with a third the frequency of usage. Additionally, their study stated that Passface login session took much longer than text passwords and therefore were used less commonly by users. Although the exploratory user studies have proven some favorable results for the Passface technique, yet, the effectiveness of this scheme is still questionable.

Davis, et al. had studied the graphical passwords based on the Passface technique and found an obvious trend among these passwords. In particular, mostly users will tend to select the faces of people which are the same race with them. Besides that, female faces were preferred by both female and male users. Moreover, a better looking faces were more

favored to be chosen. Above all, it actually makes the Passface password relatively predictable. This problem may be able to mitigate by randomly assigning Passface image to users, but it would be difficult for people to memorize the password since they are force to recognize the face but not following their please.

2.2.5 Picture Password

Jansen et al. developed a graphical password mechanism for the mobile devices named as Picture Password.

"The method described in this paper authenticates a user to a device using a visual login technique called Picture Password. Its aim is to give users a simple and intuitive means of authentication through image selection that avoids the pitfalls of alphanumeric passwords, yet is as effective a mechanism. (W. Jansen, "Authenticating Mobile Device Users through Image Selection," in Data Security, 2004.)"

During registration phase, users required to select a theme which consists of thumbnail photos and then register the image in an order of sequence as a password. Meanwhile the authentication stage, the user must reenter the registered images in the appropriate sequence. After the successful authentication, user may alter the password, register a new sequence, or possibly switch the theme. One weakness of this method is that the number of thumbnail image (5 x 6) is finite to 30, the password space is limited. Each thumbnail image is attached with a numerical value, and the order of selection will virtually produce a numerical password. Particularly, the result stated that the image sequence length was basically shorter than the alphanumerical password length. To address this problem, two pictures can be combined or united to generate a new alphabet element, thus, enlarge the image alphabet size.

"This paper proposes a novel authentication method called "Awase-E". The system uses image passwords. It, moreover, integrates image registration and notification interfaces. Image registration enables users to use their favorite image instread of a text password. Notification gives users a trigger to take action against a threat when it happens. Awase-E is implemented so that it has a higher usability even when it is used through a mobile phone.(T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images",2006.)"

Takada and Koike discussed a similar authentication technique for mobile devices as propose by Jansen. Conversely, this mechanism allows users to implement their favorite image for authentication. Firstly, the users register their favorite images to the server. When authentication stage, user needed to go through a certain rounds of verification. At each round, the user either chooses the pass-image among several decoy images or selects nothing if the pass-image is absent. The system will authenticate a user once all of the verifications are successful. The advantage of permitting users to register their own images is this scenario will make memorization the pass-image easier. But, this method does not necessarily consider as a more secure authentication scheme than text-based method. As proven in the studies by Davis, the users' choices of image passwords are usually predictable. Moreover, allowing users to apply their own pictures would make the password even more foreseeable, especially if the attacker or password cracker is familiar with the user.

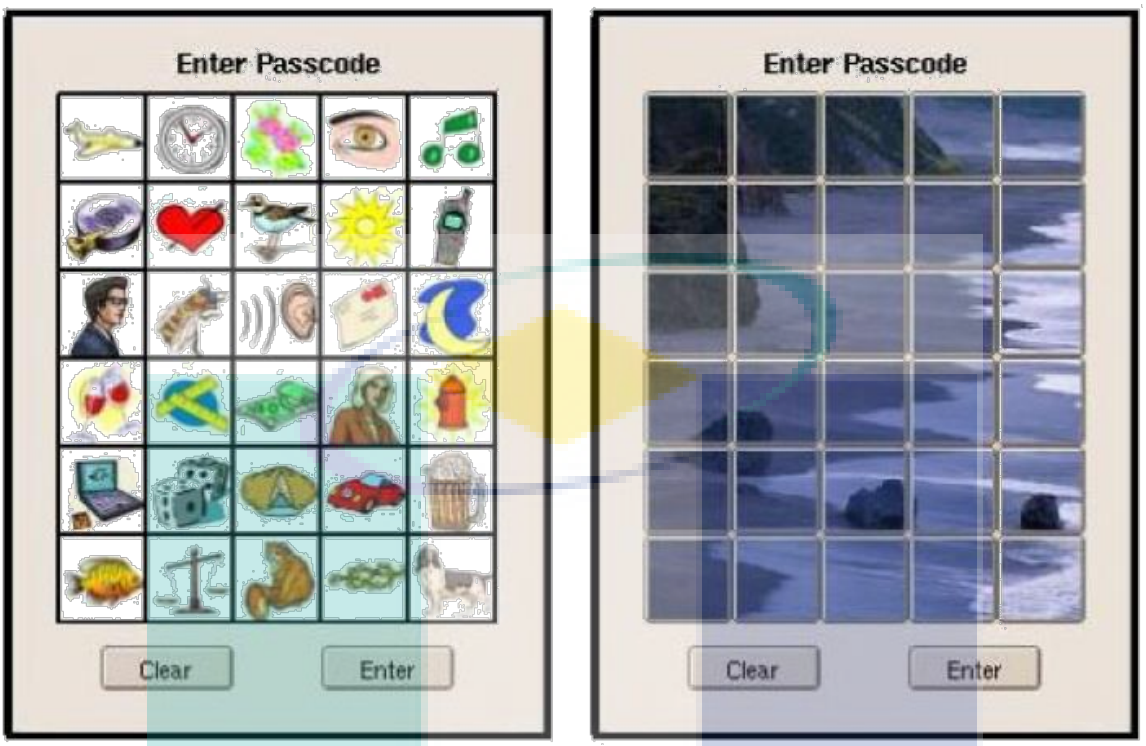


Figure 7: Example of Jansen Picture Password.

2.3 Recall-based Techniques

For authentication, recall-based techniques demand a user to regenerate something that he or she created or previously picked during the registration phase. Specifically, there are two kinds of recall-based techniques, which are:

- Reproduce a drawing,
- Repeat a selection.

2.3.1 Reproduce a Drawing

In this group of authentication algorithms, a user is asked to draw a sequence of picture originally proposed by the user during the registration phase.

2.3.1.1 Draw a Secret (DAS)

Jermyn, et al. proposed a authenticate technique based on reproduce a drawing scheme, called “Draw a Secret” (DAS).DAS features on allows user to draw or sketch their unique password.

“We propose and implement a second scheme, called “Draw a Secret"(DAS), which is purely graphical, the user draws a secret design (the password) on a grid.(I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.)”

Firstly, a user is order to sketch a simple picture on a 2D grid. The coordinates of the grids occupied by the stroke are saved in the order of the drawing. During authentication stage, the user is asked to reproduce the picture. If the sketching contacts the same grids with the same sequence, hence, the user will be authenticated. In this case, Jermyn, et al. had recommend that given feasible-length passwords in a 5 X 5 grid. After the analysis, it is proven that the full password space of DAS is greater than that the full text-based password space.

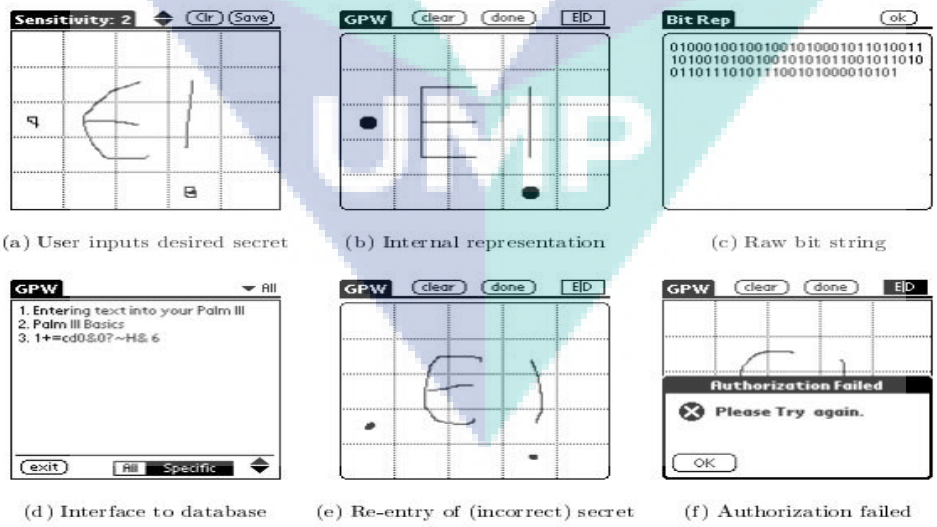


Figure 8: DAS algorithm

"In commonplace textual password schemes, users choose passwords that are easy to recall. Since memorable passwords typically exhibit patterns, they are exploitable by brute-force password crackers using attack dictionaries. This leads us to ask what classes of graphical passwords users find memorable. We postulate one such class supported by a collection of cognitive studies on visual recall, which can be characterized as mirror symmetric (reflective) passwords. We assume that an attacker would put this class in an attack dictionary for graphical passwords and propose how an attacker might order such a dictionary. We extend the existing analysis of graphical passwords by analyzing the size of the mirror symmetric password space relative to the full password space of the graphical password scheme of Jermyn et al. (1999), and show it to be exponentially smaller (assuming appropriate axes of reflection). This reduction in size can be compensated for by longer passwords: the size of the space of mirror symmetric passwords of length about L + 5 exceeds that of the full password space for corresponding length L ≤ 14 on a 5 × 5 grid. This work could be used to help in formulating password rules for graphical password users and in creating proactive graphical password checkers.(J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium. San Diego, USA: USENIX, 2004.)"

Afterward, Thorpe and van Oorschot evaluated the memorable password space of the DAS scheme proposed by Jermyn. They suggested the theory of graphical dictionaries and investigate the possibility of a brute-force attack by implement such dictionaries. They illustrate a length parameter for the DAS type graphical passwords and state that the password length of 8 or greater on a 5 x 5 grid may be less vulnerable to dictionary attack than text-based passwords. They also justify that the space of mirror symmetric passwords is relatively lower than the full DAS password space. Due to human recall symmetric picture better than asymmetric picture, it is expected that a considerable portions of users will preferred mirror symmetric passwords. If this phenomenon occurs, essentially the security of the DAS scheme could be extensively lower than formerly believed. However, this limitation can be deal with by using longer passwords length.

"We examine the role of and relationships between the number of composite strokes, grid dimensions, and password length in the DAS password space. We show that a very significant proportion of the DAS password space depends on the assumption that users will choose long passwords with many composite strokes. If users choose passwords having 4 or fewer strokes, with passwords of length 12 or less on a 5 x 5 grid, instead of up to the maximum 12 possible strokes, the size of the DAS password space is reduced from 58 to 40 bits. Additionally, we found a similar reduction when users choose no strokes of length 1. (J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.)"

In turn, Thorpe and van Oorschot further explore the impact of stroke-count and password length as a complexity property of DAS mechanism. Their research showed that stroke-count brings the greatest impact for the DAS password space. For instance, the size of DAS password space decline gradually with lesser strokes for a fixed password length. The length of DAS password itself also has certain of impact but the influence is not as intense as the stroke-count. To enhance the security, Thorpe and van Oorschot developed a "Grid Selection" technique. Selection grid is an initially huge, fine grained grid from which the user may mark out a drawing grid (sort of a rectangular region) to zoom in on, later on, they should draw their password in that certain area. This technique would undoubtedly improve the DAS password space.

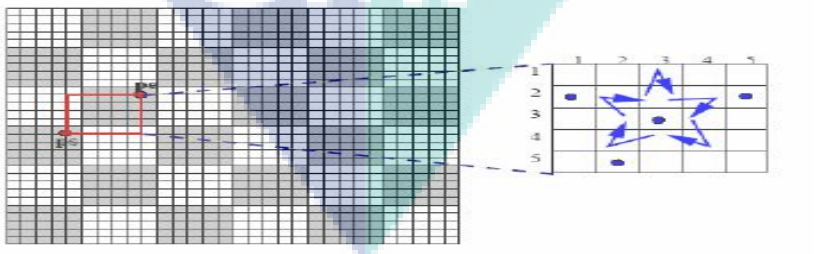


Figure 9: User selects a drawing grid.

2.3.1.2 Passdoodle

"Password security often fails in practice because users select predictable passwords. We conducted a study to explore the use of hand-drawn doodle password ("passdoodle"). Our findings show that users could recall all visual elements of the doodle as well as they could recall alphanumeric passwords, but most could not perfectly redraw their selected doodles. Users perceive passdoodles as easier to remember than alphanumeric passwords; however, they prefer whichever authentication method they perceive to be more secure.(J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.)"

Goldberg et al. did a research in which they developed a technique called "Passdoodle". This is a graphical-based password scheme involved of handwritten designs or text sketching, mostly, it is drawn with a stylus on a touch sensitive screen. Their studies concluded that users may able to memorize a complete doodle images as precisely as alphanumeric passwords. Simultaneously, the user studies also stated that people are less likely to remember the sequence in which they drew a password. However, these studies were done by paper prototype instead of proper computer programs, moreover, result verifications were done by human rather than computer. Therefore, the precision and correctness of this study is still unclear.

2.3.1.3 Signature Authentication

"In order to realize a more reliable user identification system using mouse, we propose a new system to identify users using a complex figure object, signature. New techniques we utilize in our system are as follows: the normalization of input data, the adoption of new signature-writing-parameters, the evaluation of verification data using geometric average means and the dynamical update of database. We have implemented our user identification system and conducted experiments of the implemented system. The successful verification rate in our system is 93%.(A. F. Syukri, E. Okamoto, and M. Mambo,

"A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science(1438), 1998)"

Syukri, et al. develops a system where authentication is executed by recognize user sketching their signature using mouse. Basically, this technique comes with two stages, registration and verification. During the registration phase, user asked to draw their signature, and then the system will derive the signature area (either magnify or scale-down signatures as well as rotates the image if needed, these processes also known as normalizing). Later on, the information will store into the database. For the next stage, verification phase collects the user input, and undergo normalization again, immediately program will extracts the parameters of the pass image. After that, the system conducts verification by a dynamic update of database and applying geometric average means. According to the studies, the degree of successful rate was satisfying. The biggest favored element of this approach is that there is no requirement to memorize the password since it is the user's signature and signatures are often difficult to imitate. However, not every user is familiar with adopting mouse as their writing tool. Therefore, the signature can sometime be hard to drawn for some users. One possible solution to address this problem would be to implement a pen-like input gadget, but adding new device to the current system can be costly.

2.3.2 Repeat a Selection

In this group of authentication algorithms, a user is demand to repeat a sequence of actions originally proposed by the user during the registration phase.

2.3.2.1 Blonder's Algorithm

"G. E. Blonder (1996) is the originator of the graphical passwords. In his scheme, he introduced a technique that allow user to hit on a few areas on an image that is displayed on the screen. If all the selected spots are tapped correctly, the user will be authenticated.(Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah Kutty Mammi, "Usability Features of Graphical Password in Knowledge Based Authentication Technique",2009)"

Blonder proposed a graphical password scheme in which an authentication session is conduct by require the user click on a few of region on a picture. During authentication, the user must hit on the approximate areas of those specific positions. On the others hand, image is able to aid the users for recall their passwords. Thus, this scheme is considered as a more convenient way than unassisted recall (such as text-based password).

Besides that, Passlogix (an enterprise software company) has developed a graphical password system based on Blonder's algorithm. In their system, users asked to click on various items in the picture with the correct order of sequence to be authenticated. Invisible boundaries are designate for each component in order to detect whether a pass-item is clicked by user. However, this technique only serves a limited range of password space and there is no straightforward way to prevent user from selecting poor passwords.

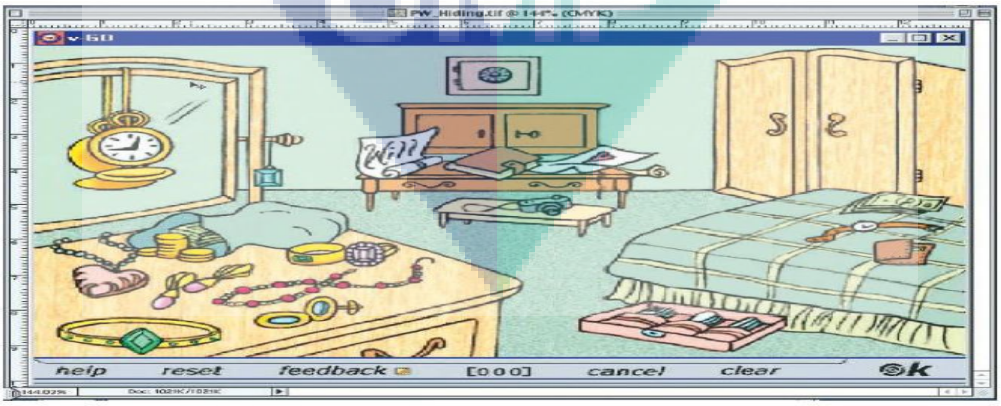


Figure 10: A recall-based technique developed by Passlogix.

2.3.2.2 PassPoint

"Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters. We have designed a new and more secure graphical password system, called PassPoints. (S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon,"Authentication using graphical passwords: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.)"

The "PassPoint" system is created by Wiedenbeck, et al. which extended the Blonder's idea by remove the predefined boundaries and allowing arbitrary images to be implement. As a result, a user can click on any position of an image to create the password. A tolerance level is calculated by each chosen pixel. For authenticated phase, a user must click within the tolerance pixels and also following the correct sequence. This technique is based on the discretization method proposed by Birget, et al. Since any picture can be used and due to a picture may consist of hundreds to thousands memorable locus, the possible password space is relatively huge.

"The results show that the graphical password users created a valid password with fewer difficulties than the alphanumeric users. However, the graphical users took longer and made more invalid password inputs than the alphanumeric users while practicing their passwords. In the longitudinal trials the two groups performed similarly on memory of their password, but the graphical group took more time to input a password. (*S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system, 2006)"*

Wiedenbeck, et al. conducted a user study, in which a batch of participants were demand to use text-based password, while the other batch was asked to use the graphical password. The result stated that graphical password consume fewer attempts for the user than alphanumerical passwords. However, graphical-based password users had more

difficulties adopt the password, and take more time to insert their passwords than the alphanumerical users.

Later Wiedenbeck, et al. also undergoes a user study to figure out the effect of tolerance level during the re-authenticating phase, and the effect of picture choice in the system. The result showed that accuracy for the password is decreased significantly after applying smaller tolerance for the user clicking points, but the selection of images do not make a big difference. Above all, it is believable that the system is able to function with a large variety of images.

2.4 Security Factors

2.4.1 Brute Force Search

"Brute-force search or exhaustive search, also known as generate and test, is a very general problem solving technique that consists of systematically enumerating all possible candidates for the solution and checking whether each candidate satisfies the problem's statement.(Yasmeen Farouk, Tarek ElDeeb and Hossam Faheem, "Massively Parallelized DNA Motif Search on FPGA", 2011)"

The main protection against brute force search is to create a sufficiently huge password space. In particular, text-based passwords come with a password space of 94^*N*, where *N* is the length of the text-based password, while 94 is the total number of printable characters from keyboard excluding SPACE. On the others hand, graphical password schemes have been proved to provide a password space that may similar to or larger than a text-based passwords. In fact, recognition based graphical passwords will tend to contain smaller password spaces than the recall based mechanism. Literally, it is harder to perform a brute force attack against graphical based passwords than text-based passwords due to some reason. For instance, the brute force attack programs have to able automatically generated precise mouse motion to imitate user input. Overall, it is plausible to explain that a graphical password is less susceptible to brute force attacks than a text-based password.

2.4.2 Dictionary Attacks

"A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary. (E-crime Expert blog, http://ecrimeexpertblog.wordpress.com/tag/dictionary-attack/, last accessed in November 2013)"

Due to recognition based graphical passwords engage with mouse input instead of keyboard, it will be unwise to perform dictionary attacks against this kind of graphical passwords. On the others hand, the recall based graphical passwords, it may possible to carry out a dictionary attack but it still will be much more complex and harder to perform than a text based dictionary attack.

2.4.3 Spyware

"Spyware is software that aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.(Sarah A. Cherry," The Effects of Spyware and Phishing on the Privacy Rights of Internet Users",2005)"

Markedly, key logging or key listening spyware is unable to crack the graphical passwords. Yet, it is not clear evidence show that whether mouse tracking spyware will capable to crack the graphical passwords. However, it is obvious that alone with mouse motion is not enough to break through graphical passwords. It is due to such information has to be interact with other crucial information, such as timing information as well as window size and position,

2.4.4 Shoulder Surfing

"Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. It is commonly used to obtain passwords, PINs, security codes, and similar data. (Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, "Reducing Shoulder-surfing by Using Gaze-based Password Entry", 2007)"

Admittedly, just like the text-based passwords, most of the graphical-based passwords are susceptible to shoulder surfing or even vulnerable in some case. While at this point, there are a few recognition-based scheme are designed to be free from shoulder-surfing attack. Conversely, none of the recall-based based scheme is considered as should-surfing resistant.

2.4.5 Guessing

"Password guessing attacks are the widest spread and threatening attacks on every browser login and peer to peer systems. (Ms. Resmipriya M G, "An Efficient Approach for Preventing Online Password Guessing Attacks", 2012)"

Unfortunately, it is undeniable that graphical passwords are always tending to predictable. For instance, studies on the Passface method have proven that user often pick predictable and weak graphical passwords. Generally, more research and exploration efforts are required to carry out in order to figure out the nature of graphical-based password establish by real world users.

2.5 Comparison between Various Types of Password

Table 1: Taxonomy for graphical password

Techniques	Usability		Security	Reliability
	Authentication Process	Memorability	Possible Attack Methods	
Text-based password	Type the password, process is very fast.	Rely on password. Random and complex passwords are hard to memorize for long time.	Dictionary attack, brute force search, guess, spyware, shoulder surfing, etc.	Quite high since it is only insert by keyboard.
D´ej`a Vu	Pick several pictures out of numbers of choices. Takes longer time than text password.	User study showed that more people tend to remember pictures than plain text-based passwords.	Brute force search, guess, shoulder-surfing	Very High, user only requires clicking on desired picture.
Sobrado and Birget algorithm	Click within the area bounded by registered pass objects, can be very fast if object number is little.	Will be hard to remember when huge numbers of objects are involved.	Brute force search, guess.	High, user need to estimate the area of effect.
Man,et al algorithm	Type in the code according to the variant of registered pass objects, not so fast when user needs to recall the every single of variant password.	Users demand to memorize both variant picture objects and their codes. Even difficult than text-based password.	Dictionary attack, brute force search, guess, spyware, shoulder surfing, etc.	Same as text-based password.

Passface	Recognize and choose the registered pass pictures; takes longer than text based password.	Faces are easier to memorize for long time, but the choices always are very predictable.	Brute force search, guess, shoulder, surfing.	Same as D´ej`a Vu.
Jansen et al.	Enters the registered images in the appropriate sequences, slower than text-based password.	Pictures are organized to help users to remember.	Brute force search, guess, shoulder surfing.	Depend on the area of thumbnail, too small may causing false negative.
Draw a Secret (DAS)	Draw the picture on a 2D grid.	Relies on what users draw. User studies proven the drawing sequence are hard to memorize.	Dictionary attack, shoulder surfing, guess.	Normal, it is difficult to redraw an exactly identical picture, the error tolerance is the key.
Signature Authentication	Draw signature using mouse or drawing device.	Very easy to remember, but hard to recognize by computer.	Guess, shoulder surfing, dictionary attack.	Need a reliable signature recognition program to execute this technique.
Blonder's algorithm, Passpoint	Click on several registered locations of a picture in the right sequence.	Easy to remember.	Guess, brute force search, shoulder surfing	Relies on the tolerance level of pixel number, can be unreliable if the pixel number is too large.

2.5 Summary

Above all, huge number of user studies has suggested that human can recall graphical password better than conventional text-based password even over a long period of time. Obviously, this can be described as the main advantage of graphical password. Furthermore, several graphical password techniques have been proven able to provide a password space similar to or greater than text-based passwords. Although there are research exists in this field, yet, the number of research has been done to investigate the exact difficulty of breaking a graphical password is very less. Furthermore, there are only handfuls of study on the possible method for cracking graphical passwords. In other words, there is no actual evidence to justify whether graphical password in general is less or more secured than conventional text-based password. This question has to be determined by case basis, depending on relevant algorithms and implementations of system. General speaking, more research efforts are required to reveal and comprehend the nature of graphical passwords at the moment. Undeniably, every type of GUAS comprised with particular strength and do come with certain limitation as well as some usability constraint. For this reason, much more user studies and research are required for GUAS techniques to reach higher degree of maturity and usability in order to develop an improved alternative authentication system. In conclusion, I believe that there is no best graphical password mechanism exist but better.

CHAPTER 3 METHODOLOGY

3.1 Introduction

Specifically, to build a system to be effective, it should grant the intended users the ability to accomplish their tasks in the best way possible. The exact principle applies to graphical user authentication system as well. In order for this system to work proficiently, it must be able to let users utilize it accurately and effectively. Graphical passwords, which consist of clicking and dragging activities on the pictures has become the alternative technique in knowledge-based authentication environment rather than traditional approach which is textual-based approach. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. This is referred to as shoulder surfing and is a known risk, the development for the GUAS will take considerations from the previous related studies and thus make improvement from the currently available authentication method.

After a comprehensive studies and exploration about the existing graphical password schemes, we had list out and discussed several features for research continuity in this area. Moreover, based on the findings from the literature review, we can perceive about the basic concept of a graphical password scheme and the limitation of it. Hence, for this project we will attempt to discover a new GUAS algorithm to deal with the existing GUAS weaknesses such as shoulder surfing issues.

Above all, in this chapter we will discuss about the detail of methodology used for this project. Thus, we are able to identify on selected methodology and the stages used to establish this project. Furthermore, we will also introduce a brand new shoulder surfing resistant GUAS algorithm as well as which technique or tools are applies when conducting the project. In addition, we will generalize on which software and hardware is utilized to carry out the development of this project. Lastly, a Gantt chart is available to be review on this chapter as well.

3.2 System Development Methodology

The methodology that will be implementing for this whole project will be the Rapid Application Development (RAD). RAD is a scheme of methodology that able to facilitate the system development process to become faster and higher quality. Moreover, RAD tends to address both limitations of the conventional development methodologies, which are: tediously long development process and the difficulty to understand a system only through a paper-based description. Besides that, RAD methodologies attempts to improve the Systems Development Life Cycle (SDLC) stages, hence, the procedure part of the system development is way more rapidly before hands into the users. The crucial elements lies beneath this approach is to make sure the users gain better understand about the system through interactive and simultaneous revisions, which bring the system closer to what is needed.

The primary concepts and benefits in the RAD environment are high system delivery speed, high quality in term of user requirement and lower cost needed. Systems development using the RAD will able to fulfill the needs of the users more proficiently and require low maintenance fee.

In particular, the RAD methodology recommends that developer may apply some specific techniques or software tools to hasten the system development phases, such as CASE (Computer-Aided Software Engineering) tools, JAD (Joint Application Design) sessions, visual programming languages (e.g., Visual Basic), and code generators that automatically construct programs from design specifications. Above all, RAD has proven to be a valuable system development methodology.

The RAD methodology had distributed into four separate phases as shown in figure 11, which are, requirements planning, user design, construction and cutover respectively.

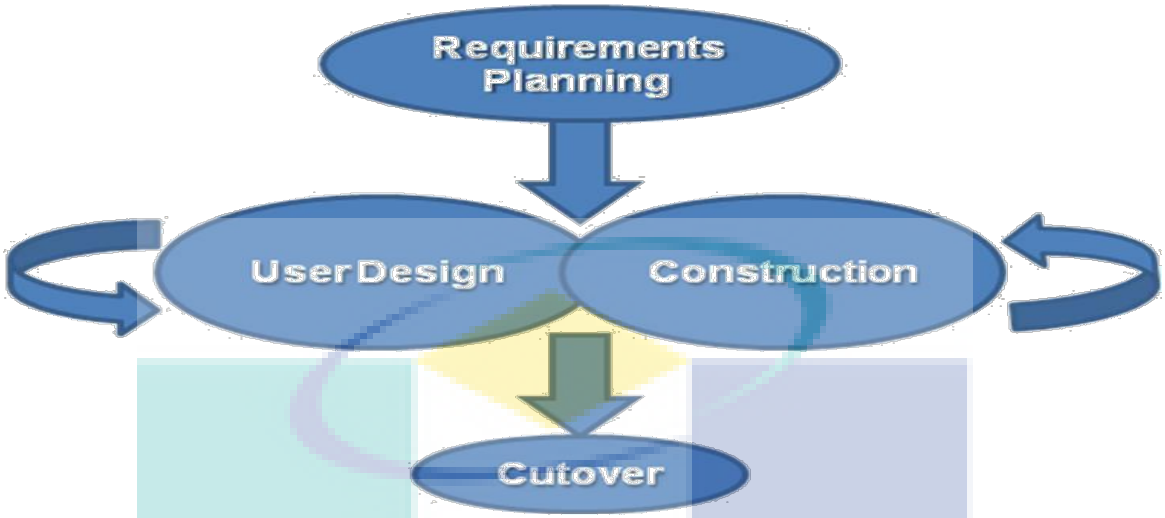


Figure 11: RAD phases

3.2.1 Requirements Planning Phase

The first stage in the RAD methodology is requirements planning. This stage engages with reviewing the areas that are apparently essential to the system which is being constructed. The review will generate a solid overview, covering the specifications and outlining the operation performed by the system. When executed accordingly, through this phase should deliver a display of how the proposed system functions. Furthermore, it should also clearly characterize the scope of the system, including its limitations and capabilities.

For requirement planning phase of this project, the objective and scope will be defined first and foremost. Afterward, the data and requirement collection step will be intake. In the research phase, relevant information for the project will be studied and gathered. Basically, the approach used and requirements have to be verified in order to proceed the project and acquire the expected outcomes. The information retrieval channel consists of the document and journal review. Simultaneously, the comparative study will be performed to evaluate the current situation and produce the general element that should implement in the new GUAS scheme.

3.2.2 User Design Phase

The second stage is termed as the user design stage. This involves an intensive look of business activities that correlate to the system being developed. During this phase, users communicate with systems analysts and develop models as well as prototypes that represent all system input, output and process. User design is a constant interactive procedure that allows users to customize, understand, and ultimately approve a working model of the system that fits their requirements.

In this phase, we aim to design a sophisticate system GUI that takes account in principle will be applied to increase the degree of user friendliness presented by system. In additional, the prototype will be built to promote the further customization and enhancement process. usability and system reliability issues. Several of human and computer interaction

3.2.3 Construction Phase

The third stage is named as construction. In construction stage of RAD model, the code is building with the concept from design phase as the base. This construction allows designers to program key parts of the system and immediately test features with user feedback. As key pieces of the system are built and tested, the overall project comes together. Differ from SDLC, in RAD, however, users persist to participate and available to suggest adjustment or enhancements as actual screens or reports are being established.

In this phase, we will start implement the coding part and complete the system GUI. After the system is coded, the program will be tested and refine to improve the system. Besides that, the GUAS beta will be released for a number of selected system testers and user feedback is collected in order to enhance the system performance.

3.2.4 Cutover Phase

The fourth and final stage of RAD is cutover, it is similar with the final stage of the SDLC the implementation phase. At this point, the new software system is finalized and installed. While comparing with the traditional SDLC methods, the entire process is compressed. RAD facilitates the movement of system development process; hence, the new system is assembled, delivered, and placed in operation much rapidly.

As the last stage, this project will deploy and install the finalize version of system. Furthermore, the constant periodic system testing and improvement will be undergoing to prevent any software flaw or programmed loophole is presented.

3.3 Move Your Secret Algorithm (MYS)

To conquer the weaknesses of text-based password, authentication method such as two factor authentication and graphical-based password have been implemented. At the same time, application tools and input devices such as stylus and touch-screen that permit had made the usage of the graphical user authentication system more conveniently. However, most of the GUAS are susceptible to shoulder-surfing. A malicious observer can acquire the password by observe directly or by record the user's authentication session. Markedly, this situation is referred as shoulder surfing and is a known risk nowadays, the concern is raised when authenticating session takes place in public places. Obviously, this is been a limitation that difficult to overcome. In this chapter, I will be proposing a new algorithm of GUAS name as Move Your Secret (MYS), in which able to resist against shoulder surfing attacks as well as possess high level of usability and reliability. This is a combination of recognition-based and recall-based approaches. In this technique, the user will be demanded to move and drag the mouse along their preregistered pass picture according to a specific sequence. Basically, the procedure of MYS divided into three stages: registration, login session, and system authentication process. For the prototype designation as shown in the coming section, it is completed with the aid of Visual Basic 2008.

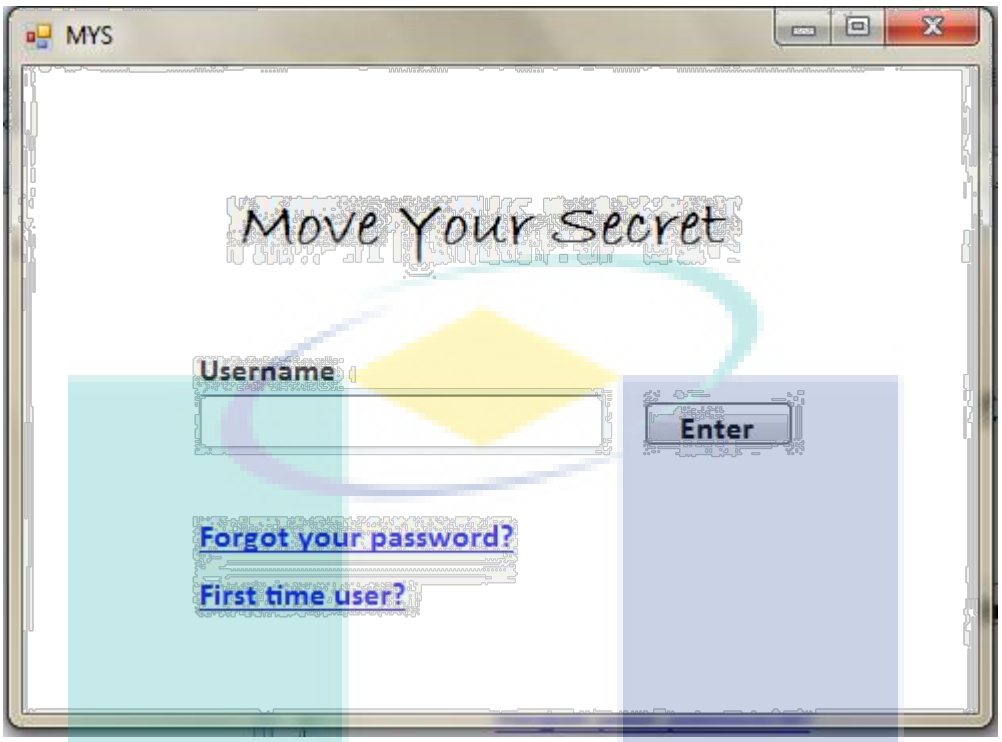


Figure 12: Interface of MYS homepage.

3.3.1 Registration

In this stage, first of all, the user is required to provide a valid text-based username for future login usage. After verify the validity of username, user can continue the pass picture selection based on their intuition. As refer to figure 14, it is a screen shot of registration session (note that, this is a basic prototype GUI and only for illustrational purposes). On this point, the users have to memorize not only the picture itself but also the sequence of selection. Hence, the system will require the users to reinsert the pass picture selection to ensure the users had entered the pass picture that they truly desired. Finally, after the confirmation, registration process is successful and data will be appended to the database.

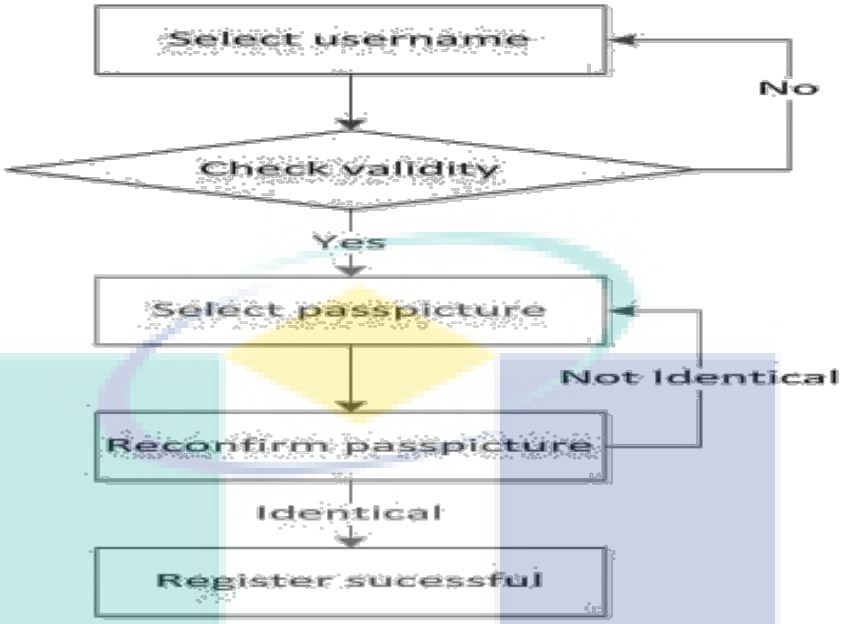


Figure 13: Flowchart for register session.

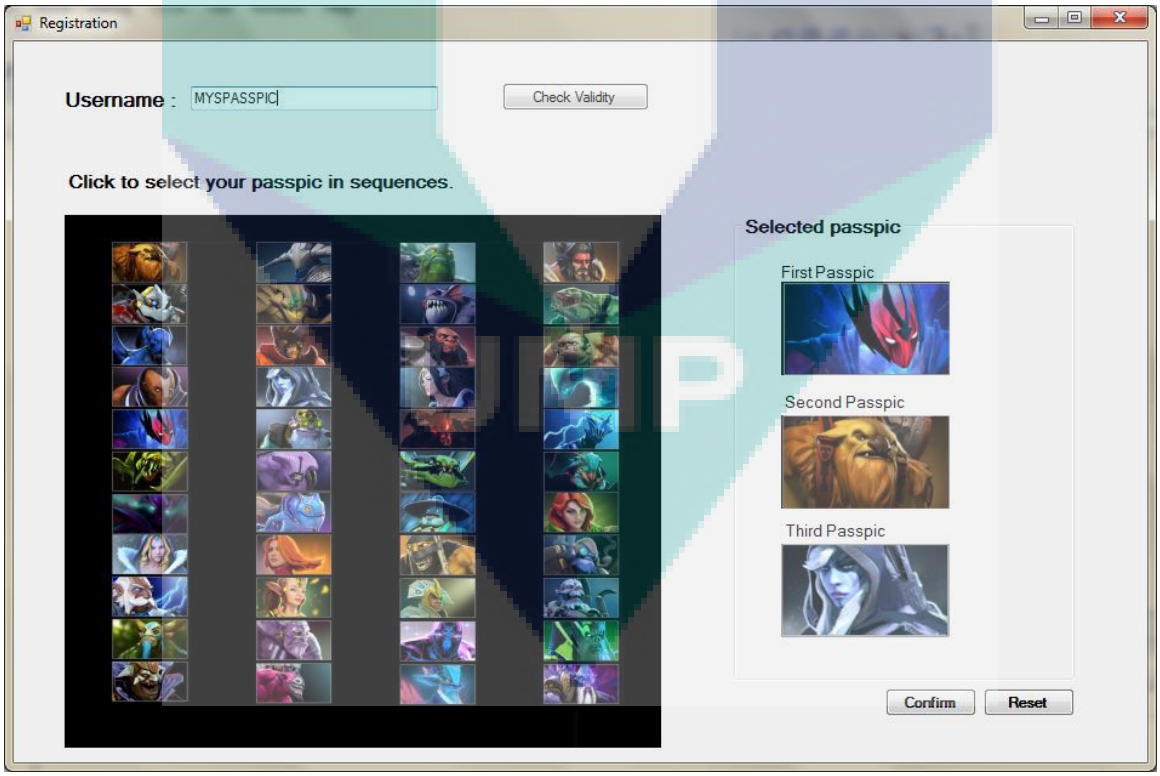


Figure 14: Screen shot of registration interface.

3.3.2 Login Session

After the registration, the user is able to login to the system through the authentication session. Firstly, the user needs to insert the username on the homepage of the system. After verified existence of username, user will be redirect to the MYS authentication page. MYS authentication page will consist of a 5x5 grid in which occupied with 25 pictures. The picture grid consists of the preregistered picture and some random decoy image. In order to authenticate, the user needs to drag and move the mouse among the picture, the movement of mouse should go through the pass picture and follow the specific sequence that him/her preselected when register session. This algorithm is able to deal with mouse tracking software and shoulder surfing attack due to several factor:

- The mouse movement is randomly generated by user as long as it does meet the sequence required, user will be authenticated.
- The arrangement of picture is scramble up and come with different order for every login session to improve the strength of security.
- Since the user can move and draw the line according to their wishes, it is almost impossible to figure out the exact user's pass picture by shoulder-surfing attack.

As refer to the figure 16, it shown the example of a user had drawn the line through the pass picture by following a specific preregistered sequence. Clearly, the order of mouse movement to draw the line for authentication process is not fixed. Hence, users are able to draw the line based on their intuition and the sequence of pass picture is untraceable by password cracker or shoulder-surfer.

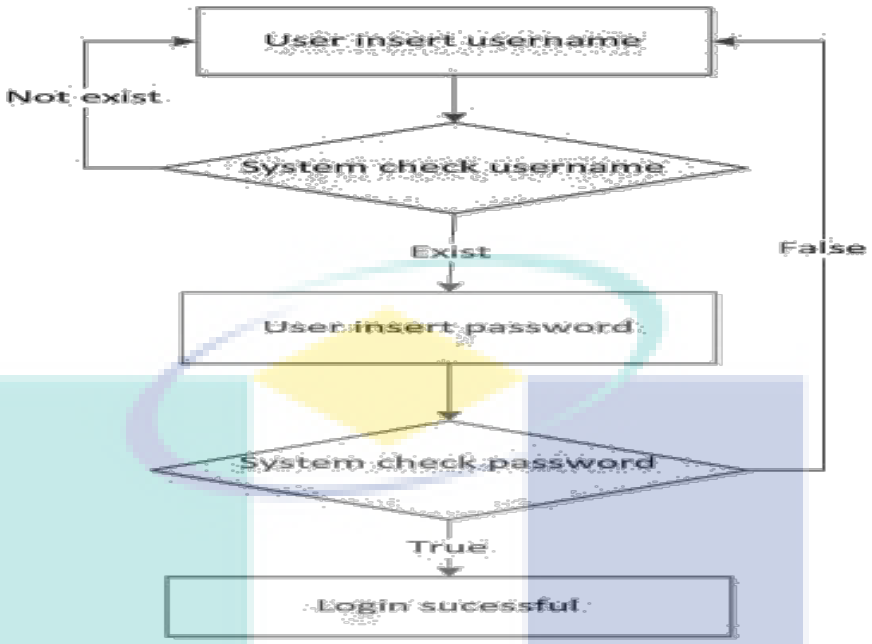


Figure 15: Flow chart of login session.

Figure 16: Screen shot of login session interface.

3.3.3 System Authentication Process

After the user had inserted the appropriate username, the authentication process will officially launch. At first, the system will retrieve the user information such as the pass picture that preregisters by the user from database for further verification. While user starts to move the mouse and draw the line among the pass picture grid, once the line contact with any picture, at the meantime, it will trigger the pass picture verification mechanism. The flow of authentication procedure and decision will follow the step according to the flow chart as shown in figure 17. As stated, the users had been empowered the ability to draw and generate their very own pass picture line. Hence, in order to prevent the false positive and less vulnerable to the brute force attack, the system had programmed the tolerance of error for this system as 5 moves which means that any further movement without hitting the correct pass picture, the authentication process will be terminated immediately. The authentication mechanism will be dismissed instantly and considered as fail trial. Note that, every failed authentication session only will be informed to the user right after they click on the confirmation button. This measure is applied to avoid the malicious cracker trying to guess the pass picture from the fail trial, since they are incapable to figure out where is the incorrect step they had taken.

When the moment the line had touched the correct first pass picture, the system will verify it and cease the first stage of authentication. For the next step, the system is repeating the flowchart but apply the second pass picture as the new verifying factor. Lastly, the authentication process is successful when all three pass picture is verified.

On the others hand, once the users realize that they had insert three of their pass picture correctly, they are feel free to draw some decoy image or scrambled up the lining of picture gird before they click the confirmation button. This is due to the nature of system, once the user is authenticated, the system will stop to record and analysis any line movement. Markedly, this action can be act as confusion and distraction to the shoulder surfer and password cracker, hence, the strength of security for this algorithm is raised significantly.

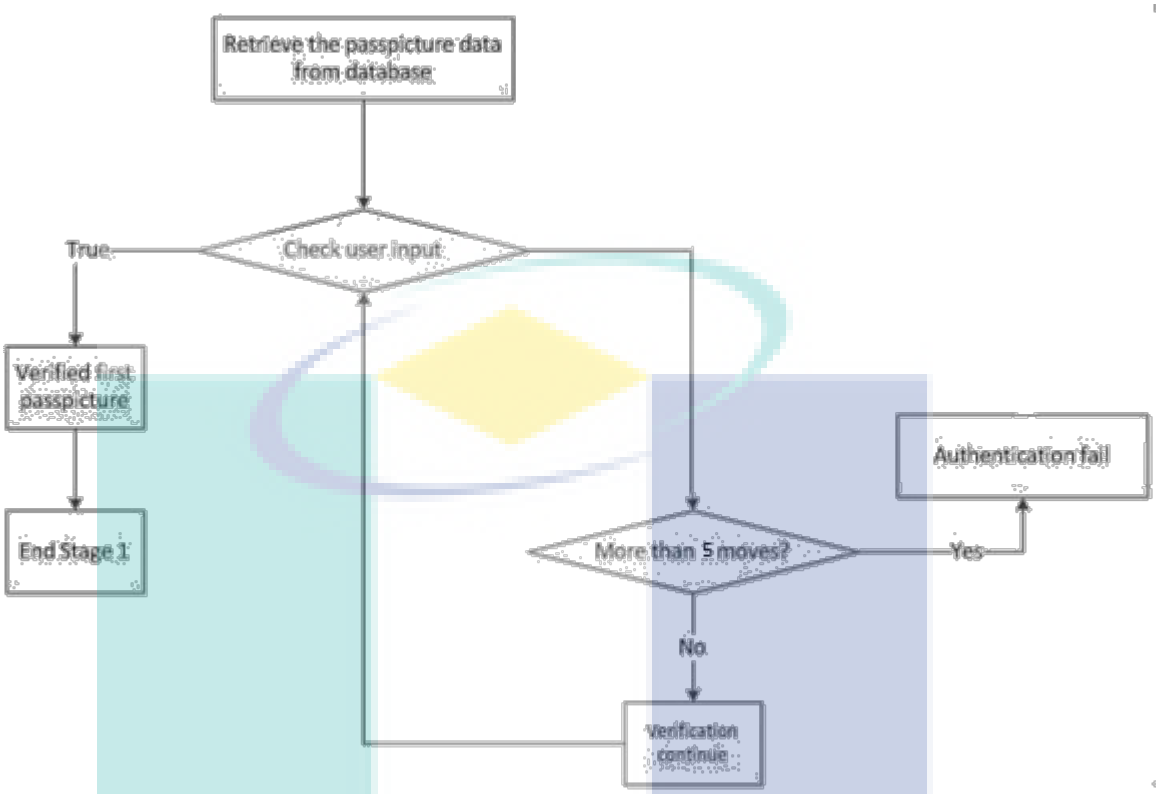


Figure 17: Flow chart of authentication process for first stage.

3.4 Hardware and Software Requirement

Indeed, a development of a system demands a few of appropriate software and hardware to facilitate the procedure. Following had outlined the requirement software and hardware for the development phase of system.

3.4.1 Software Requirement

Software	Purpose
Microsoft Word 2010	To prepare the proposal and documentation works.
Microsoft Visio 2010	To design the flow chart.
Microsoft Project 2010	To develop the gantt chart.
Microsoft Power Point 2010	To create the slide show for presentation use.
Adobe Reader	To view the related article regarding the project.
Microsoft Windows 7 Operating System	The OS environment for develop the system.
Microsoft Visual Studio	To design and create the prototype GUI interface.

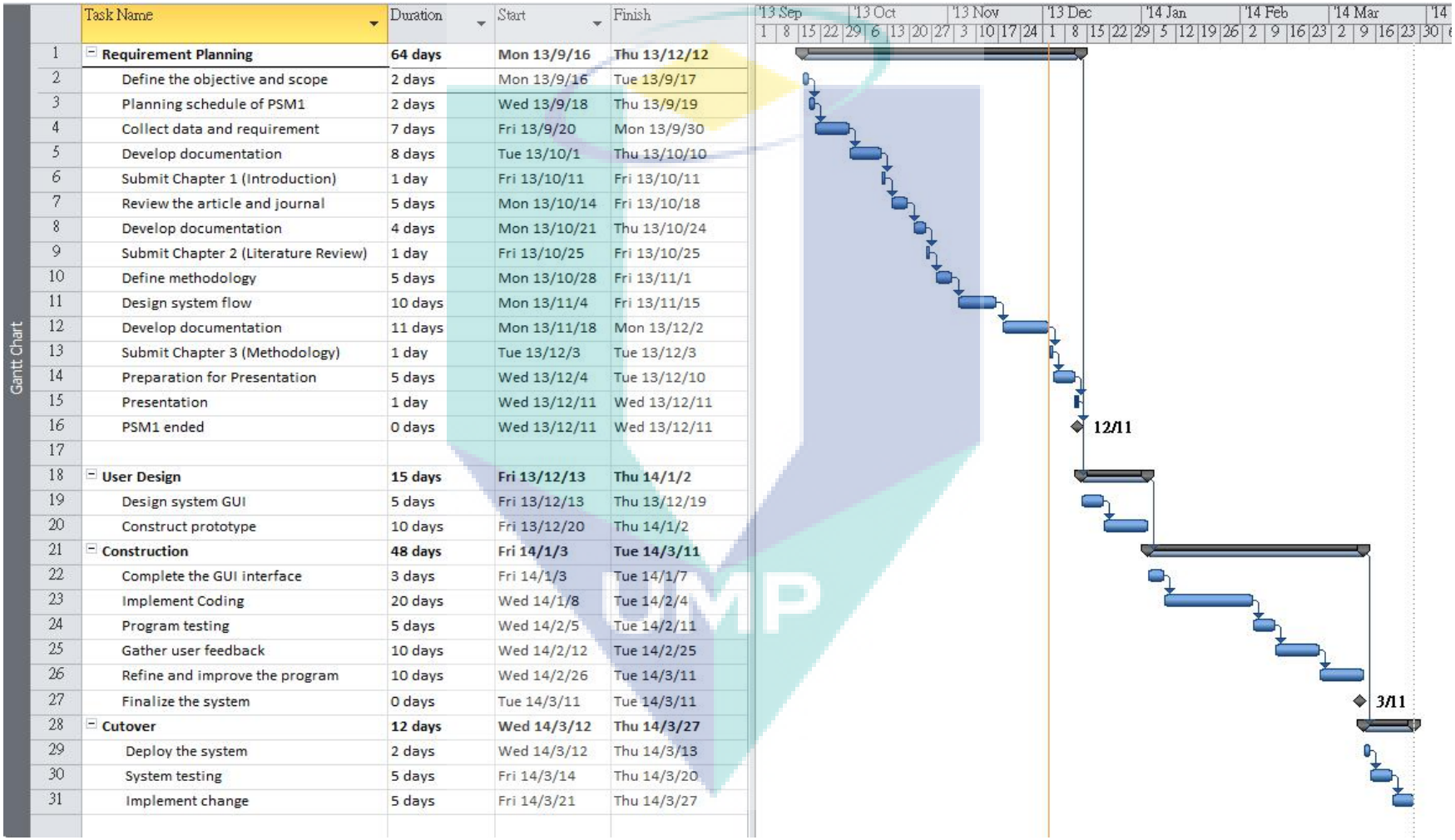
Table 2: Software requirement

3.4.2 Hardware Requirement

Hardware	Purpose
ASUS A43S	To prepare documentation and develop the system.
Seagate External hard disk 500GB	To back up the project file and data.
Imation pen drive 4GB	To transfer data

Table 3: Hardware requirements

3.5 Gantt Chart



	Task Name	Duration	Start	Finish
1	**Requirement Planning**	**64 days**	**Mon 13/9/16**	**Thu 13/12/12**
2	Define the objective and scope	2 days	Mon 13/9/16	Tue 13/9/17
3	Planning schedule of PSM1	2 days	Wed 13/9/18	Thu 13/9/19
4	Collect data and requirement	7 days	Fri 13/9/20	Mon 13/9/30
5	Develop documentation	8 days	Tue 13/10/1	Thu 13/10/10
6	Submit Chapter 1 (Introduction)	1 day	Fri 13/10/11	Fri 13/10/11
7	Review the article and journal	5 days	Mon 13/10/14	Fri 13/10/18
8	Develop documentation	4 days	Mon 13/10/21	Thu 13/10/24
9	Submit Chapter 2 (Literature Review)	1 day	Fri 13/10/25	Fri 13/10/25
10	Define methodology	5 days	Mon 13/10/28	Fri 13/11/1
11	Design system flow	10 days	Mon 13/11/4	Fri 13/11/15
12	Develop documentation	11 days	Mon 13/11/18	Mon 13/12/2
13	Submit Chapter 3 (Methodology)	1 day	Tue 13/12/3	Tue 13/12/3
14	Preparation for Presentation	5 days	Wed 13/12/4	Tue 13/12/10
15	Presentation	1 day	Wed 13/12/11	Wed 13/12/11
16	PSM1 ended	0 days	Wed 13/12/11	Wed 13/12/11
17				
18	**User Design**	**15 days**	**Fri 13/12/13**	**Thu 14/1/2**
19	Design system GUI	5 days	Fri 13/12/13	Thu 13/12/19
20	Construct prototype	10 days	Fri 13/12/20	Thu 14/1/2
21	**Construction**	**48 days**	**Fri 14/1/3**	**Tue 14/3/11**
22	Complete the GUI interface	3 days	Fri 14/1/3	Tue 14/1/7
23	Implement Coding	20 days	Wed 14/1/8	Tue 14/2/4
24	Program testing	5 days	Wed 14/2/5	Tue 14/2/11
25	Gather user feedback	10 days	Wed 14/2/12	Tue 14/2/25
26	Refine and improve the program	10 days	Wed 14/2/26	Tue 14/3/11
27	Finalize the system	0 days	Tue 14/3/11	Tue 14/3/11
28	**Cutover**	**12 days**	**Wed 14/3/12**	**Thu 14/3/27**
29	Deploy the system	2 days	Wed 14/3/12	Thu 14/3/13
30	System testing	5 days	Fri 14/3/14	Thu 14/3/20
31	Implement change	5 days	Fri 14/3/21	Thu 14/3/27

3.6 Summary

According to the Chapter 2, we determine a graphical password based on three basic principles, which are: security, usability and reliability. Security, according to the earlier section, can be evaluate based on several important extent; they are brute force search, dictionary attacks, guessing spyware and shoulder surfing. Brute force attacks and guessing can be avoided by a large password space. Obviously, password space is considerably large in MYS, since any pictures from the database can be used and there could be countless possible combinations for a password. Moreover, dictionary attack is useless for this kind of technique due to only picture involve for the authentication phase. Since there is no exact mouse motion during the authentication phase, hence it is futile to record the mouse motion. Furthermore, MYS technique also deals with the shoulder surfing attack, since it is hard to figure out exactly which picture the user is referring to in the picture grid and the decoy picture may change randomly for every login session. For usability, the pass picture memorability is noticeably higher if compare with conventional alphanumeric password due to the usage of picture. Besides that, the login session taken fairly short of time since user only requires to move the mouse and draw the line. The reliability of MYS rather greater as compare with other GUAS, MYS had provided the border for each picture to ensure that user will not mistakenly touched the picture that he or she not favors thus causing authentication failure. Hence, we can conclude that MYS is a better GUAS algorithm that able to fulfill the objective of the project.

CHAPTER 4 IMPLEMENTATION

4.1 Introduction

In chapter 4, it will propose the development and implementation of the framework as well as the model introduced in chapter 3. Hence, it will reveal the process and implemented algorithm, thus, sketching the work flow and model. Furthermore, we will be approach to the source code that involved during the development of this project.

4.2 Move Your Secret (MYS) Interface

Apparently, most of the system functionality and program architecture had been described on previous chapter. On this section, we will introduce and explain the detail of the MYS interface which may include GUI of Homepage, Registration, Authentication and etc.

4.2.1 Homepage

Figure 19 displays the homepage of Move Your Secret (MYS) system. The designation of homepage is intended for the first stage of verification before the authentic users can proceed to the next phase. First and foremost, the users are required to insert their username in the textbox provided. Thereafter, once the users hit on the login button, the system will read the username and compare with the database information. If the inserted username is matched with any single of username that residue in the database, the particular user will be redirect to the Authentication page. On the others hand, if the inserted username does not exist in the database, the user will be prompt with a message box that demand user to enter an available username. As for the first time login user, they can click on the Registration button and proceed to Registration page and create their own MYS account.

Figure 19: The homepage interface

4.2.2 Registration Page

Before a user is able to fully utilize the MYS system, they will need to preregister themselves to the system by providing an available username and select the pass-picture that they would like to be adopt for the authentication phase. Once the user had validate their username is available, they can move on to the 5x5 pass-picture grid and select 5 of them from it. Otherwise, the user will be prompt to provide a valid username. Note that, the username is not case sensitive.

In order to select the pass-picture, the user are requirement to click on it and double confirm the selection before it is put into the picture slot with specific sequence. During the process, the user are feel free to remove their selection and reinsert everything with the "CLEAR" button. Apparently, users are able to select same image as their pass-picture, which mean that they could have 5 same images as their pass-picture but this action is not recommended since it would be easily guess by malicious hacker. The general interface is shown on figure 20 as below.

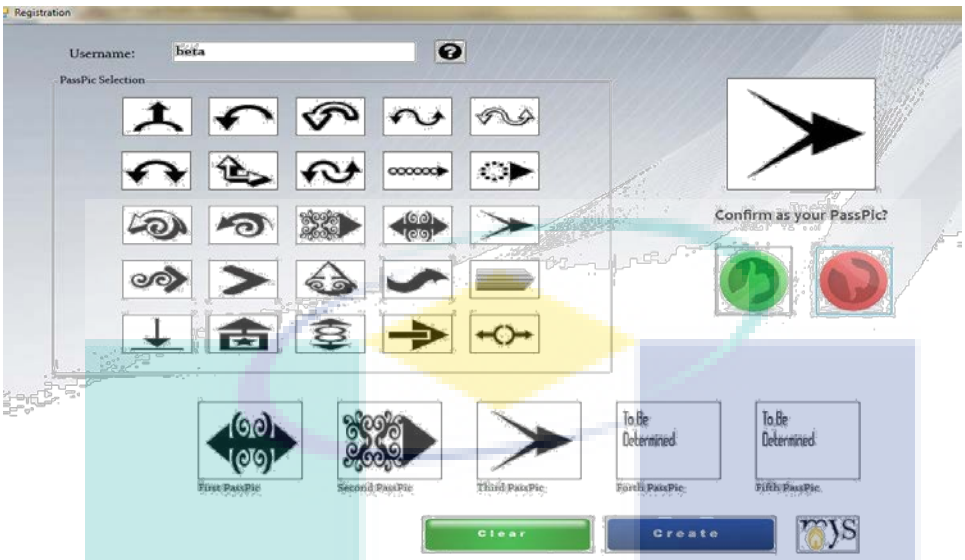


Figure 20: The registration page

4.2.3 Authentication Page

Basically, then authentication page is plain and simple, it only presenting a 5x5 picture grid which require user to insert their pass-picture to verify their authenticity. Once the user move their mouse inside the picture grid, it will detain a trace associated with the mouse movement. The trace can be stacked and will not causing any authentication failure, the only rule is that user need to pass through their preselected image in the specify sequence within 5 moves.

In term of picture grid reconstructing, every single time the user login, the pass-picture will be in random order. In additional, the picture are being resized and rotated to even confuse the shoulder surfer. When the user had confirm their pass-picture had inserted correctly, they can click on the login button and redirect to the content page or they will be sent back to the homepage if the inserted pass-picture is not being recognize.

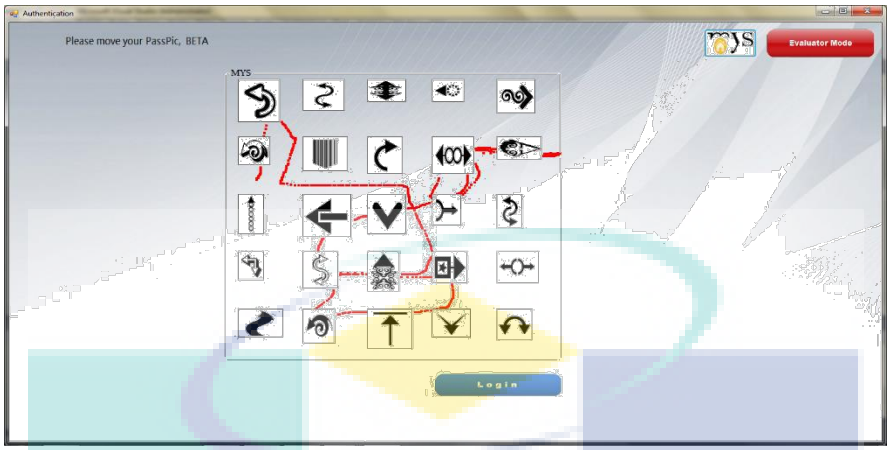


Figure 21: The authentication page

Besides that, this system had prepared an additional mode for the convenient and ease of use for evaluator to assess the system and figure out how the exact programming running behind the scene. This mode can be activate by clicking on the Evaluator Mode button, afterward, it will display the status, current move used and the pass-picture of the particular account beside the picture grid to assist evaluator to adapt to the system.

Figure 22: Evaluator mode

4.2.4 Others

Other than the main interface described above, this system do furnish with the tutorial feature. The tutorial walks through the basic idea of MYS and assists the user adapt to the newly introduced system configuration that people might not familiar with.

Figure 23: Tutorial page

4.3 Coding

In this section, we are about to discuss some coding related tasks include database usage, debugging and managing the source code as well as employment of the build system. MYS had been supported by some fundamental source code in order to perform its functionality perfectly.

4.3.1 Login Code

For the login source code, basically, the system will communicate with the database and examine the compatibility of the user inserted username with the database information. If the username is valid, the user will be redirect to the authentication page, otherwise, will the user will be prompt with an error message box and require user to reinsert a valid username. Besides than redirect the user, it will relocate the particular user pass-picture information to the appropriate web control in the authentication page.

```
Private Sub Form4_Load(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles MyBase.Load

    con.Dispose()
    con.Close()

    dbProvider = "PROVIDER=Microsoft.Jet.OLEDB.4.0;"
    dbSource = "Data Source =PSMDB.mdb"
    con.ConnectionString = dbProvider & dbSource
    con.Open()
    sql = "SELECT * FROM PSM"
    da = New OleDb.OleDbDataAdapter(sql, con)
    da.Fill(ds, "PSM")


    inc = -1
    MaxRows = ds.Tables("PSM").Rows.Count
    If inc <> 0 Then
        inc = 0

    End If
```

Figure 24: Code for database connection

```
Private Sub PictureBox2_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles PictureBox2.Click
    If TextBox1.Text = ("") Then
        MessageBox.Show("Please insert username!", "Login", MessageBoxButtons.OK, MessageBoxIcon.Error)
    Else
        TextBox1.Text = StrConv(TextBox1.Text, VbStrConv.Lowercase)
        Dim i As Integer
        Dim flag As New Boolean
        For i = 0 To MaxRows - 1
            If CStr(ds.Tables("PSM").Rows(i).Item(0)) = TextBox1.Text Then
                flag = True
                Form5.Label13.Text = CStr(ds.Tables("PSM").Rows(i).Item(0))
                Form1.Label16.Text = CStr(ds.Tables("PSM").Rows(i).Item(0))
                Form1.Label13.Text = CStr(ds.Tables("PSM").Rows(i).Item(1))
                Form1.Label14.Text = CStr(ds.Tables("PSM").Rows(i).Item(2))
                Form1.Label15.Text = CStr(ds.Tables("PSM").Rows(i).Item(3))
                Form1.Label9.Text = CStr(ds.Tables("PSM").Rows(i).Item(4))
                Form1.Label10.Text = CStr(ds.Tables("PSM").Rows(i).Item(5))
            End If
        Next
        If flag = True Then

            MessageBox.Show("Proceed to user authentication phase.", "Login", MessageBoxButtons.OK, MessageBoxIcon.Information)
            Me.Hide()
            Form1.Show()


        ElseIf flag <> True Then
            MessageBox.Show("Invalid username!", "Login", MessageBoxButtons.OK, MessageBoxIcon.Exclamation)
        End If
    End If
```

Figure 25: Code for username checking

4.3.2 Registration Code

In general, registration code is performing based on the picture box value and the assigned tag value. When a user click on a picture from the picture grid, the action will send the detail of the specific picture to the confirmation picture box such as the resource number and the tag value.

```
Private Sub PictureBox1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles PictureBox1.Click
    PictureBox26.Image = My.Resources._0
    PictureBox26.Tag = 0
End Sub

Private Sub PictureBox2_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles PictureBox2.Click
    PictureBox26.Image = My.Resources._1
    PictureBox26.Tag = 1
End Sub

Private Sub PictureBox3_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles PictureBox3.Click
    PictureBox26.Image = My.Resources._2
    PictureBox26.Tag = 2
End Sub
```

Figure 26: Code for passing value to confirmation picture box

Afterward, when the user click on the confirmation button, the picture will be pass to the next section of picture slot and ready to be commit in the database. First of all, the system will check which particular of sequence slot had not been filled with pass-picture and send the pass-picture to the appropriate placement, thereafter, the pass-picture tag value will be transfer to a label control and ready for further usage.

```
Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles Button1.Click

    If PictureBox26.Tag = "88" Then
        MessageBox.Show("You haven choice any PassPictures!", "Registration", MessageBoxButtons.OK, MessageBoxIcon.Error)

    ElseIf PictureBox27.Tag = "100" Then
        PictureBox27.Image = PictureBox26.Image
        PictureBox27.Tag = "99"
        Label5.Text = PictureBox26.Tag
    ElseIf PictureBox27.Tag = "99" And PictureBox28.Tag = "100" Then
        PictureBox28.Image = PictureBox26.Image
        PictureBox28.Tag = "99"
        Label6.Text = PictureBox26.Tag
    ElseIf PictureBox28.Tag = "99" And PictureBox29.Tag = "100" Then
        PictureBox29.Image = PictureBox26.Image
        PictureBox29.Tag = "99"
        Label7.Text = PictureBox26.Tag
```

Figure 27: Code for verify the picture box status

4.3.3 Data Storing Code

MYS had employ Access 2013 as its main database storage to gather and maintain user information. If the username and pass-picture are filled correctly, when the user click on the Save button, it will deliver the username and tag value of picture to the database for further usage. Hence, the database will be updated with a new row of user information regarding the username and pass-picture chosen. After the successfully of account creation, the system will pop up a notification message box to inform the user.

```
    If flag <> True Then

        Dim xx As New OleDb.OleDbCommandBuilder(da)
        Dim dsNewRow As DataRow

        dsNewRow = ds.Tables("PSM").NewRow()

        dsNewRow.Item(0) = TextBox1.Text
        dsNewRow.Item(1) = Label5.Text
        dsNewRow.Item(2) = Label6.Text
        dsNewRow.Item(3) = Label7.Text
        dsNewRow.Item(4) = Label12.Text
        dsNewRow.Item(5) = Label13.Text

        ds.Tables("PSM").Rows.Add(dsNewRow)
        da.Update(ds, "PSM")
        MaxRows = ds.Tables("PSM").Rows.Count
        inc = MaxRows - 1

        Dim home As MsgBoxResult
        home = MessageBox.Show("MIS account created sucessfully.Back to home?", "Registration",
        If home = MsgBoxResult.Yes Then
            Application.Restart()
        Else

        End If
    End If
End If
```

Figure 28: Code for storing data and create the account

4.3.4 Authentication code

The main procedure operating among the authentication page is mostly happen inside the picture grid and the interactive between users with the pass-picture. Firstly, when the user move their mouse inside the picture grid, it will detain a red movement line associate with their mouse response.

```
Public Class Form1
    Dim count As Integer = 0
    Dim down = False
    Dim mybrush = Brushes.Red
    Private _pictureBox As Object

    Private Sub GroupBox1_MouseDown(ByVal sender As Object, ByVal e As System.Windows.Forms.MouseEventArgs) Handles GroupBox1.MouseDown
        down = True
    End Sub

    Private Sub GroupBox1_MouseMove(ByVal sender As Object, ByVal e As System.Windows.Forms.MouseEventArgs) Handles GroupBox1.MouseMove
        If down = False Then
            GroupBox1.CreateGraphics.FillEllipse(mybrush, e.X, e.Y, 5, 5)
        End If
    End Sub

    Private Sub GroupBox1_MouseUp(ByVal sender As Object, ByVal e As System.Windows.Forms.MouseEventArgs) Handles GroupBox1.MouseUp
        down = False
    End Sub
```

Figure 29: Code for the line drawing

Furthermore, once the mouse enter and leave a pass-picture, it will be record as a move, thus, verify whether the pass-picture is the preregister pass-picture or otherwise by comparing the tag value of the pass-picture with the database record.

```
Private Sub PictureBox1_MouseLeave(ByVal sender As Object, ByVal e As System.EventArgs) Handles PictureBox1.MouseLeave

    If Label1.Text = ("Start") And count < 5 Then

        If PictureBox1.Tag <> Label3.Text Then
            count = count + 1
            Label6.Text = count
        ElseIf PictureBox1.Tag = Label3.Text Then
            Label1.Text = ("Pass")
            count = 0
            Label6.Text = count
        End If
```

Figure 30: Code for counting move

```
ElseIf Label1.Text = ("Pass") And count < 5 Then

    If PictureBox22.Tag <> Label4.Text Then
        count = count + 1
        Label6.Text = count
    ElseIf PictureBox22.Tag = Label4.Text Then
        Label1.Text = ("Pass2")
        count = 0
        Label6.Text = count
    End If

ElseIf Label1.Text = ("Pass2") And count < 5 Then

    If PictureBox22.Tag <> Label5.Text Then
        count = count + 1
        Label6.Text = count
    ElseIf PictureBox22.Tag = Label5.Text Then

        Label1.Text = ("Pass3")
        count = 0
        Label6.Text = count
    End If
```

Figure 31: Code for checking the status of authentication

Lastly, the user are require to finalize their input by click on Login button. The button will translate all of the movement and information given by user to verify the authenticity of the user's identity.

```
Private Sub PictureBox32_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles PictureBox32.Click
    If Label1.Text = ("Sucess") Then

        Me.Close()
        Form5.Show()

    ElseIf Label1.Text = ("Fail") Then

        MessageBox.Show("Incorrect MYS detected! Return to login page!", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Exclamation)
        Application.Restart()

    ElseIf Label1.Text = ("Start") And Label6.Text = ("0") Then

        MessageBox.Show("You haven insert any PassPic!", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Exclamation)

    ElseIf Label1.Text = ("Pass") Or Label1.Text = ("Pass2") Or Label1.Text = ("Pass3") Or Label1.Text = ("Pass4") Or Label1.Text = ("Start") Then

        MessageBox.Show("Incorrect MYS detected! Return to login page!", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Exclamation)
        Me.Close()
        Form4.Show()
    End If
End Sub
```

Figure 32: Code for the login button

4.4 Summary

In general, this chapter had outlined the interface design and source code implementation of the project. Apparently, we can divide MYS techniques into three stages: registration, login and authentication. Likewise, each stage will requires a different mechanism and peculiar source code to carry out the capabilities of MYS. The user may start and terminated the program in their convenience. To be brief, registration phase will record the user input and store the values into Access database. Login phase will check the existing datasets with user input and proceed to authentication stage. Afterward, In order to be authenticated, the users are required to move their mouse within the picture grid and the movement will be record, hence, compare with the registered datasets to justify the pass-picture authenticity.

CHAPTER 5 RESULT AND DISCUSSION

5.1 Introduction

In general, this chapter will derive the clarification in regard to the results and finding from statistical analysis. Besides that, the statement of trade-off and constraint met between security as well as efficiency during development of project will be disclosed through this chapter. Suggestion about the space and resolution for improvement in order to secure employment for the future development of this project will be provided on this chapter as well.

5.2 MYS Perspective

In this section, we will investigate the MYS graphical password mechanism from several perspectives. Basically, we focus primarily on security and usability but also take into consideration the system as well as communication issues. For security, we will explore on password space and the strength of the password. Meanwhile, for usability, we are study on the ease of registration and ability of authentication.

Specifically, the password space for recognition based techniques technically depends on the size of the picture content. Obviously, the likelihood of creating a weak password are immerse in recognition based password. Broad range of recognition based technique disregard the order of the selection, hence, they usually comprise rounds of authentication phase with users undergo and examine several pages of images. Hence, the password space for recognition based technique is of total number of pictures multiple with number of rounds of authentication:

$$\text{Password Space} = (s \times n)$$

n: Number of pictures in each page

s: Number of rounds of authentication

Simultaneously, MYS take in account of sequencing and ordering the pass-picture selection. Besides that, the repetition of pass-picture is allowed in MYS as well. The password space is considerably massive in this environment. As a result, the password space of MYS is based on:

$$\text{Password space} = T^n$$

T: Total number of pass-picture selection

n: Number of user selected pass-picture

T = 25, n = 5, hence the total password space for MYS will be:

$$25^5 = 9{,}765{,}625$$

The huge number of password space is literally unbreakable by a simple guess from malicious hacker. Thus, we can determine that MYS is a very secure scheme in term of password space meanwhile MYS also able to deal with shoulder surfer issues.

A major criticism among the users regarding usability of graphical passwords is that the password registration and login process are time exhausting and tiresome, especially in recognition-based approaches. For instance, during the registration stage, a user require to choose number of images from a large set of selections. During authentication phase, the user has to browse through large amount of images to identify a few pass-picture, hence, user may experience the process is tedious. Meanwhile, MYS had grouping and well- arrange all of the pass-picture in a 5x5 picture grid when presenting in authentication phase, the user can efficiently scan through all the image and figure out the location of their pass-picture in second. Another major complaint is that it is not easy to sketch pattern with mouse. As for MYS, instead of require user to draw the exact lining to authenticate themselves, MYS only involve some mouse movement to verify a user identity which can remove the burdensome of mouse drawing in this case.

5.3 Test Plan Result

5.3.1 Homepage

The homepage of MYS comprise of numbers of button and textbox to carry out the functionality. After plenty of testing procedure being conducted, the results we acquired from the homepage are as following:

No	Test Case	Expected Results	Remark
1	The username textbox able to input with a string of characters.	The users are manage to key in any characters into the box.	True
2	The 'Login' button function to redirect legitimate users to the authentication page.	The button check the username validity and forward the user to authentication page if it is valid.	True
3	The 'Sign Up' button redirect user to the registration page.	Registration page is shown and database connection established.	True
4	The link label 'What is MYS' forward user to the tutorial page.	Tutorial selection page is shown.	True

Table 4: Testing result of homepage interface

5.3.2 Registration

Table 5.2 show the results we obtained from the testing event from registration process.

No	List of Test Case	The Expected Results	Remarks
1	The new users can enter their own case insensitive username in the textbox provided.	The user manage to insert username and before store into database all of the letter will be alter to lowercase.	True
2	User able to check the availability of their username before creation of account by click on '?' button.	The button will compare the user input with database data and inform the result to user.	True
3	The user can select their desired pass-picture from the picture grid.	The picture will be send to confirmation box when user click on it.	True
4	The users can click on the 'clear' button to get flush all of the previous selection	All of the selected pass-picture slot will be empty and the tag value will be removed	True
5	The 'Save' button will create the account	The system will verify the pass-picture number and the username availability hence save all the information into database for further usage	True

Table 5: Testing result of registration process

5.3.3 Authentication

Table 6 show the results we obtained from the testing event from authentication process.

No	List of Test Case	The Expected Results	Remarks
1	The users will any to draw on the picture grid and know their mouse movement.	Any mouse movement on the picture grid will detain a red tracing.	True
2	Maximum of 5 moves between the pass-picture connections to meet the next sequence pass-picture.	Once the mouse enter and leave a pass-picture it will be consider as a move had been taken, if the move is more than 5 and did not meet the next pass-picture system will mark the attempt as fail trial	True
3	User can click on the 'login' button to justify their final input.	The button will proceed the user to content page if user had input correct pass-picture	True
4	Evaluator mode will be enable by clicking on the button.	The interface will show the current status, moves used and the pass-picture of the particular user beside of the picture grid.	True

Table 6: Testing result of authentication process

5.4 Summary

MYS is an innovative approach in terms of practicing the user's own behavior as the authentication mechanism. In this chapter, the test case have demonstrated that employment of user's mouse movement as an authentication technique is plausible, yet simple to be enforced.

CHAPTER 6 CONCLUSION

4.1 Future Planning

Since this is only the first part of the project and it is considered a new prototype for graphical password authentication which still at its very early stage, obviously, there are plenty of future works required in order to facilitate the development of system. They should include but not limited to:

1. The future plan aim to enhance the prototype to transform into a real system with good usability, security and reliability features. Besides that, the propose GUAS, MYS will be run as web based application as well.

2. Moreover, the questionnaire survey will be distributed to evaluate the system usability where the questionnaire concentrates on the whole system evaluation, system layout and usability features.

3. Adding more user's biometric parameters and factors into the registration process would certainly be an improvement, examples such as: recording the users typing patter alone with the mouse motion, or the eye fixation during different activities. Nevertheless, biometrics as an authentication technique is still at its very early stage, there is still much more work to do.

4. Furthermore, it should provide a comprehensive training session to users, this is due to GUAS is not widely adopted nowadays and the newly propose technique is not familiar by most of the users. Hence, the training session should be come with the system as a packet.

4.2 Summary

For the past decade, the interest in applying graphical passwords had grown as an alternative to the conventional text-based passwords. In this thesis, we have conducted comprehensive studies about the existing graphical password scheme. The current existing graphical password techniques can be differentiate into two categories which are: recognition-based and recall based techniques. A comparison of current existing graphical password techniques is presented in Table 1.

Although the main argument for GUAS is that human are often better at remember graphical-based object rather than text-based passwords, yet, the actual user studies are very limited in order to provide some convincing evidence to uphold this argument. Meanwhile, our introductory analysis had suggested that it is harder to crack graphical passwords utilizing the traditional attack methods such as dictionary attack, spyware or brute force attack. However, since our society is not widely adopting the graphical-based password yet, the vulnerabilities and susceptibility of graphical passwords are still not completely discovered in most of the respects.

The proposed technique: MYS, or move your secret, a shoulder surfing resistance method, addressed many of the existing problems of the traditional GUAS. For instance, the new technique is able to overcome mouse tracking attack as well as shoulder surfing issues, meanwhile, it still retains the huge password space and therefore it is considered to be more secure than the existing graphical password methods. However, the user study of the new technique MYS was complete by paper prototype rather than computer systems, verifications were accomplished by human instead of computer. Therefore the result accuracy and consistency of this study is still remaining ambiguous. Hence, the further investigation is considered as our future work.

Overall, the current GUAS techniques are still remain on the premature stage. Plenty of research and user studies are required for GUAS to achieve higher degree of maturity and practicality.

REFERENCES

1. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.
2. M. Kotadia, "Microsoft: Write down your passwords," in ZDNet Australia, May 23, 2005.
3. Gilbert, "Phishing attacks take a new twist," in CNET News.com, May 04, 2005.
4. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 33, pp. 168-176, 2000.
5. R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, 1967.
6. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-
7. World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.
8. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwest Instruction and Computing Symposium, 2004.
9. D. Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can'tRecall," in Proceedings of Conference on Human Factors in Computing Systems (CHI).
10. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.
11. D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme stronglyresistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.
12. S. Man, D. Hong, and M. Mathews, "A shoulder-surfing resistant graphicalpassword scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
13. RealUser, "www.realuser.com," last accessed in October 2013.
14. T. Valentine, "An evaluation of the Passface personal authentication system,"Technical Report, Goldsmiths College, University of London 1998.
15. T. Valentine, "Memory for Passfaces after a Long Delay," Technical Report, Goldsmiths College, University of London 1999.
16. S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords: a field trial investigation," in People and Computers XIV - Usability or Else: Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

17. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical passwordschemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

18. W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.

19. W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture Password: A Visual Login Technique for Mobile Devices," National Institute of Standards and Technology Interagency Report NISTIR 7030, 2003.

20. W. A. Jansen, "Authenticating Users on Handheld Devices," in Proceedings of Canadian Information Technology Security Symposium, 2003.

21. T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images," in Human-Computer Interaction with Mobile

22. Devices and Services, vol. 2795 / 2003: Springer-Verlag GmbH, 2003, pp. pp. 347 - 351.

23. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

24. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Passwords," in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.

25. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in Proceedings of the 20th Annual Computer Security Applications Conference. Tucson, Arizona, 2004.

26. J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.

27. J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in 20th Annual Computer Security Applications Conference (ACSAC). Tucson, USA.: IEEE, 2004.