Enhancing Security of Graphical User Passwords

Ishan Rastogi

School of Computing Science

Sir Alwyn Williams Building

University of Glasgow

G12 8RZ

Masters project proposal

March 28, 2014

Abstract

People usually find it difficult to remember multiple graphical passwords. Passhint Authentication System (PHAS) is a scheme which tries to overcome this problem by providing the users the facility to create hints for each of their password images. This results in increased memorability of the passwords because it provides a cue to the users which aids recall. However, like many other graphical passwords PHAS is prone to shoulder-surfing attacks. An attacker can capture a password by direct observation over few successful authentication sessions. To overcome this problem this paper proposes an Enhanced PHAS (EPHAS) which uses six images instead of four images as used in PHAS. This solution keeps the password length unchanged at four, thus increasing the total permutations to three hundred sixty from just twenty four, thereby increasing the entropy of the password. The extra two images are also used to confuse the attacker by using target image from one challenge set as distractor image from another challenge set depending on the hint provided. To make sure that the memorability of the passwords is not adversely affected by the increase in the number of password images, this paper proposes a usability study conducted on the lines of PHAS. The paper also proposes a guessability study to measure the effectiveness of the solution against shoulder-surfing attacks and to measure the extent to which hints help in guessing the password of a user.

Table of Contents

1 Introduction

Graphical passwords have been considered as an alternative to the conventional alphanumeric passwords for over a decade based on various studies which show that it is easier to recall pictures than words [1-3,6,18]. The dual-coding theory suggests that verbal and non-verbal memory are processed and represented differently in mind [12]. Graphical passwords not only increase the usability of the authentication system by improving the memorability of the passwords, but also improve the strength of the passwords against guessing attacks [9,17,19].

Graphical authentication though proven to be more resistant to brute-force attacks is still susceptible to shoulder surfing and other such attacks where the attacker is observing a genuine user input their passwords, or clicking on their password images [10,13,19]. The aim of this project is to enhance the security of one such graphical authentication scheme, Passhint Authentication System [29]. This will be done by increasing the size of password space while keeping the password length unchanged, thus making it difficult for an attacker to observe or guess the password of a user without increasing the steps required during the authentication phase.

1.1 Steps involved in Graphical Authentication System

Graphical Authentication System (GAS) generally is a two-step process:

- **Registration Phase:** During this step the users create their graphical passwords. The images can be allocated to them by the system; they might need to select the images from a set presented by the system; they might need to upload their own images to be used as passwords; or they may be asked to draw the images to form the passwords
- **Authentication Phase:** During this step the users are required to authenticate their identity by selecting their password images from a set of images displayed on the screen, or reproduce the previously drawn images. This set is called *challenge set.* The subset of challenge set which does not contain the password images is called a *distractor set.*

1.2 Types of Graphical Authentication

GAS can be classified into three main categories based on the memory task involved [7,8]:

- **Cognometric Systems**: They rely on a user's ability to recall a set of authenticator images from among decoy images. These are also known as recognition-based systems or searchmetric systems [8,19]. These systems use various types of visual stimuli like faces, icons, everyday objects, and random art. Figure 1a shows an example of a Cognometric Scheme [25].
- **Locimetric Systems**: These systems rely on user's identifying specific locations on an image. These are also known as cued-recall systems [8]. This feature is aimed to reduce the memory load on the users. Figure 1b shows an example of a Locimetric Scheme [25].

- **Drawmetric Systems**: These systems require the users to draw and upload their authentication images to the system. These are also known as recall-based systems because users recall and reproduce a secret drawing [8]. These systems generally use hand-drawn doodles as authenticators. Figure 1c shows an example of a Drawmetric Scheme [19-21].

Recognition is generally considered to be an easier memory task than recall [4,5].

Figure 1a: Cognometric [23]

Figure 1b: Locimetric [23]

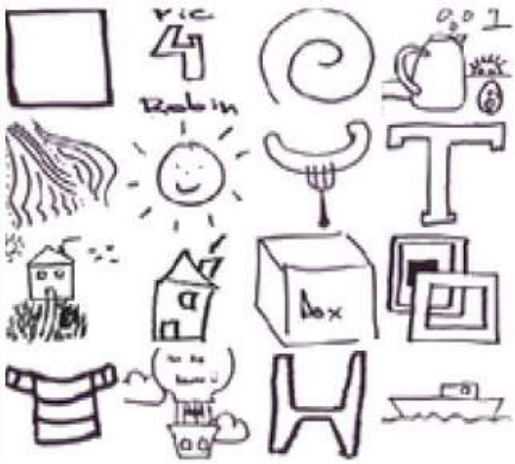

Figure 1c: Drawmetric [21]

1.3 Characteristics of Passhint Authentication System (PHAS) [29]

- **Authentication Type**: Cued-Recall/Recognition. During the registration phase the user has to select four images from a set of images presented by the system and provide a hint for each image to complete the registration. The user still has to identify the target images from the challenge set, but the hint is available to help them recall their password. Hint is displayed at each authentication step.

- **Password Length**: Four images
- **Images Type**: The system provides the user with the options of selecting images from four different sets- art images [8], object images, doodle images [19-21], Mikon images [22].
- **Challenge Set**: During each step of the authentication phase, a challenge set consisting of 15 decoy images and 1 password image is displayed to the user in the form of a 4x4 grid along with the hint.
- **Security**:
    - Challenge sets for a user do not change when the web page is reloaded using the refresh button.
    - Selection of a wrong image in a step results in a challenge set not containing the password image in the subsequent steps.
    - A maximum of four failed attempts before the account is temporarily locked.

1.4 Structure of the Proposal

This chapter provides a brief introduction to Graphical Authentication System (GAS), their types, the steps involved in the authentication system and their shortcomings. It identifies the target authentication system, presents a brief overview of its characteristics, identifies the weaknesses in the current system and provides a brief idea of the aim of the project.

The next chapter formalizes the problem to be addressed by the project and explains the necessity of the solution.

2 Statement of Problem

Recognition based graphical passwords (RBGPs) have always been inherently vulnerable to shoulder surfing attacks [23-25] and other observation based attacks such as malware-based attacks, and phishing attacks because of their visual mode of interaction [13;23-27]. In most of the GASs available the complete password remains on the screen for the entire authentication session. There have been some attempts [17,23] at mitigating the observation based attacks, but these result in various usability challenges to the user.

Even in the Passhint Authentication System (PHAS) a user is required to enter the password by clicking on the target images shown on the screen. Such click-based interaction is easy to view from the naked eye. The password length of four images also makes the system vulnerable to observation-based attacks. An attacker can observe few successful authentication sessions of a genuine user and can deduce the password of the user.

Therefore, this project proposes the use of six images instead of four images as the password. The images used will be of type art and object. This is because PHAS [29] has shown that these images have better memorability (97.5%) when compared to images belonging to doodles and Mikons (95%). The use of six images will result in at least fifteen different password combinations (three hundred sixty permutations), opposed to one combination (twenty four permutations) in the current system. This will improve the entropy of the password by increasing the password space. The other main reason behind using

two extra images is to use these images as a means of confusing the attacker. During the login process each challenge screen may contain one, two or three of the user's password images. The user only has to click on that password image for which the hint is provided even if there is another image from the password set of the user in the displayed challenge set. This means that if an attacker observes the user clicking on a particular image, her attempt to replicate the same might not result in successful login. This is because the system might provide a different hint and therefore now requires a different password image. Also, the image which the attacker might discard as a decoy image after observing a session could be the password image belonging to some different hint.

The project also aims at using timed login during the authentication phase. PHAS identifies mean authentication time at around 15 seconds [28]. Whenever a user is taking more time than usual the session will be dropped. This will be done with the aim of reducing the chances of cognitive attacks [25,28,29]. The lock-out policy which in the current system is implemented for four failed attempts will be reset to three failed attempts, thus reducing the number of attacks possible by reducing the chances of guessing the correct password.

To make sure that the usability of the system is not adversely affected by increasing the number of password images, this project proposes to conduct a usability study with multiple passwords. This study will compare the usability of the existing system to the usability of the modified system, Enhanced Passhint Authentication System (EPHAS). This study will also measure the effects of using six images as the password on the memorability of the password. PHAS has shown the memorability of a four image password to be around 95% [29]. Since the system provides a hint to aid recall it is expected that the addition of two extra images to the password space will not have a significant impact on the cognitive load of a user.

To verify the effectiveness of the system a guessability study will also be conducted on both PHAS and EPHAS and the results will be compared. This will include a study to measure: the effectiveness of the proposed solution against shoulder surfing attacks; the extent to which passwords can be guessed using hints used in the system.

3 Background Survey

This chapter identifies the existing research in the field of GAS and reviews it based on the problem tackled by researchers. The first section of this chapter reviews the research on superior memorability of graphical passwords over alphanumeric passwords. The second section reviews some solutions to mitigate shoulder-surfing attacks on GASs. The third section reviews proposed solutions against guessability attacks.

3.1 Review Based on Memorability of Multiple Passwords

There are very few papers that have studied the memorability of multiple graphical passwords.

Pictures at the ATM: Exploring the usability of multiple graphical passwords by W. Moncur, and G. Leplatre [14]

This paper conducted a research to compare the memorability of multiple graphical passwords to that of traditional 4-digit PINs. The study was performed online and a total of 172 participants volunteered. The participants were randomly distributed into 5 different groups. The control group being the traditional 4-digit PIN using group and the remaining 4 different groups were all graphical password groups, each group using a different technique to aid memorability of the passwords. The users were randomly distributed to one of the groups and were allocated 5 different system generated passwords. Each graphical password was made up of four detailed, colorful, meaningful photographic images from separate semantic categories. The challenge sets used during the retention tests had 10 components – the 4 components forming the password and 6 random distractor components. Three retention tests were carried out with a gap of 2 weeks between each of them. The number of permitted retries for any password was limited to three, to replicate existing PIN mechanisms. The dropout rate for the study was very high at 64.91%, and was attributed to the time consuming nature of the study. The final results suggested that multiple graphical passwords were more memorable than multiple PIN numbers, and that the memorability of graphical password could be enhanced by allowing the users to choose their own password images, and by showing the challenge set against a signature background. Figures 3.1a and 3.1b show example screens from the experiment.

The study though considers passwords to PINs, it still remains unclear on how this compares to text passwords. Also, the PINs used in this study were not associated with any "user accounts", and the study did not take under consideration the serial memory effects, i.e. there was no distraction task between allocating any two passwords.

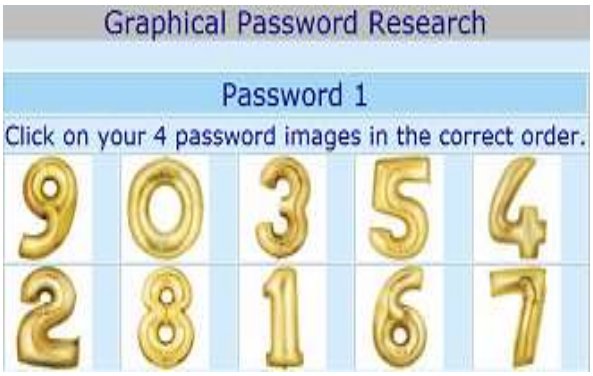

Figure 3.1a: Example Numerical Password Selection[14]

Figure 3.1b: Example Graphical Password Selection[14]

A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords by K. Everitt, T. Bragin, J. Fogarty, and T. Kohno [16]

This paper conducted a study of multiple graphical passwords using faces as visual cue to systematically examine frequency of access to a graphical password, interference resulting from interleaving access to multiple graphical passwords, and patterns of access while training multiple graphical passwords. The study was conducted online over a period of 5 weeks and a total of 110 participants volunteered to take part in the study. The users were provided with 4 system generated passwords, each consisting of 5 passfaces making a total of 20 images for the users to remember. During the authentication phase the users had to select correct image from a challenge set of 9 images presented in the form of a 3x3 grid. Figure 3.1c shows an example authentication screen. A between-subject design was used to conduct the study. Users had 3 attempts to successfully authenticate the system. After analyzing the data obtained using various statistical tools, the following results were obtained:

- Increase in the frequency of use of facial graphical password increased the success rate and reduced the login time and total time.
- Participants who accessed four different graphical passwords per week were 10 times more likely to completely fail to authenticate than participants who accessed a single password once per week.
- Change in method of training can reduce the overall failure rate and total time taken.
- Time required to authenticate can be significantly impacted by frequency, interference, and training even when the failure rate is not.

This study though very comprehensive, strictly focused on the usability of the system chosen facial passwords and did not consider the security of the scheme itself. It also did not consider the security implications due to changes in user behavior when dealing with multiple graphical passwords.

Figure 3.1c: Example Authentication Screen [16]

Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords by S. Chiasson, A. Forget, and E. Stobert [18]

This paper compared the effects of having to remember several text-based passwords and several multiple-click-based graphical passwords (CGPs). The study was performed in controlled laboratory settings with 65 participants. The participants were assigned to use either textual passwords or CGPs. They created six distinct passwords for different accounts and later had to recall each of these passwords. The study was repeated after a period of 2 weeks where the 26 returning participants had to recall passwords for each of their accounts. The dropout rate for the study was around 60%.

The paper hypothesized that CGPs would be easier for the users to recall than text passwords, when users had multiple passwords to remember.

The system was implemented as stand-alone Windows application. The text password required a minimum of 8 characters. In the graphical password scheme used by this study (PassPoints), the users were presented with an image, and a password consisted of 5 click-points on that image. To log in, users needed to select the same 5 click-points in the same order. The system allowed for a tolerance area around each click-point so that approximately correct login attempts were accepted. The different accounts were identified by colored banners at the top of the application window that included a unique icon and the account name. The results from the study suggested that it was much easier to recall PassPoints passwords (95% success rate) than text passwords in short term (68% success rate), it took longer to recall alphanumeric passwords (29.3 seconds to 15.1 seconds in CGP) and it also induced more errors (59% compared to 25% in CGP). It was also observed that PassPoints suffered from clustering (hotspots), i.e. multiple users selecting their click-points in the same regions of image. The study showed that 30% of the passwords had same click-points. This knowledge could be used by attackers to perform brute-force attacks.

Age-Related Performance Issues for PIN and Face-Based Authentication Systems by J. Nicholson, L. Coventry, and P. Briggs. [28]

This paper conducted a study to understand age-related performance issues for PIN and Face-based authentication systems. The study involved providing young adults and old adults with 6 system generated passwords and the retention of the passwords was tested over a period of three weeks. The study first established a baseline performance in which populations of younger and older adults were tested with text-based PINs. The second part of the study used two face-based graphical authentication systems employing young faces vs. old faces as code components. The study was performed in laboratory conditions and total of 36 participants volunteered to participate. The participants were divided in 4 groups: 2 groups of young adults and 2 groups of older adults. The users were required to successful authenticate 5 times. The results obtained from the study suggested that the performance of older adults improved while using old faces as passwords (mean successful attempts 4.05 as compared to 3.14 with young faces), young adults (mean successful attempts: 4.8) performed much better than older adults (mean successful attempts: 3.91), and performance of both age groups was significantly higher with passfaces (means 4.8, 3.91) than with PINs (means 4.13, 3.26). Figures 3.1d and 3.1e show sample screens for both old passfaces and young passfaces.

Figure 3.1d: Sample grid for old faces [28]

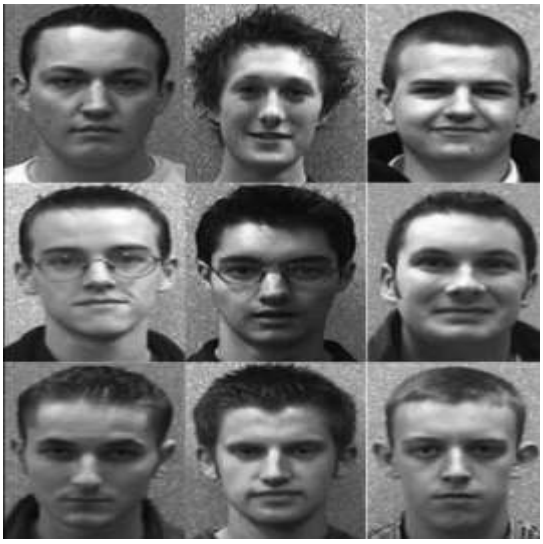

Figure 3.1e: Sample grid for young faces [28]

Passhint: Memorable and Secure Authentication by S. Chowdhury, R. Poet, and L. Mackenzie. [29]

This paper conducted a study of multiple graphical passwords using hints as cues to compare the memorability of different image types: doodles, objects, art, and Mikons, which are generally used in GASs. The study was conducted over a period of two weeks with 40 participants. The users were asked to create four passwords, one from each image category. Each password consisted of 4 images and each image required a hint. During the authentication phase the users were presented with a challenge screen displaying a hint and a challenge set of 16 images, containing 15 distractor images and 1 target image. To successfully authenticate users had to correctly recognize the four images which formed their passwords from four such challenge screens. The results showed that the memorability for art and object images (97.5%) was higher than the memorability for doodles and Mikons (95% each); time taken for authentication was highest for doodles (17.15 sec) and lowest for art images (13 sec); guessability was highest for object images and lowest for art images.

3.2 Review Based on Shoulder Surfing Solutions

Shoulder Surfing Defense for Recall-based Graphical Passwords by N. Zakaria, D. Griffiths, S. Brostoff, and J. Yan [24]

This paper proposed three shoulder surfing defense techniques for recall-based graphical password systems and mainly focuses on Draw-A-Secret (DAS) and Background Draw-A-Secret (BDAS) [25]. The three approaches were:

- Decoy Strokes: Creating real-time strokes alongside of a user's password, which are believable enough that they resemble strokes that could have been drawn by a user. The aim of this technique is to distract an onlooker's attention away from the actual password that is drawn by the user. Figure 3.2a shows a working example of this approach.

- Disappearing Strokes (DS): This solution entails the user stroke being removed from the screen after it has been completely drawn. The idea was to give the attacker less time. Figure 3.2b shows a working example of this approach.
- Line Snaking (LS): Based on the disappearing stroke solution but intended to leave the vital password information onscreen for an even shorter period. The start of the user stroke being removed from the screen as the user is still drawing, giving the appearance of the line snaking towards the user's stylus. Figure 3.2c shows a working example of this approach.

A prototype of the DAS graphical password system was used with all three shoulder-surfing resistance techniques on a PDA, using a 5x5 DAS grid. A study was conducted in a controlled laboratory environment with 68 participants. The participants were randomly assigned to 4 conditions (3 defense techniques and 1 without any defense technique). A set of three passwords of different security levels (weak, medium and strong) was tested for each condition. After analyzing the resulting data from the experiments it was observed that Line Snaking (40% strokes surfed) outperformed Disappearing Stroke (49% strokes surfed), whereas Decoy Stroke (78% strokes surfed) provided little security enhancement whatsoever.

A usability study to identify the easier to use defense technique between DS and LS was performed with 30 participants in a controlled laboratory environment. The result of the study suggested that LS requires more time (8.7 sec) and more attempts (1.3) to login when compared to DS (7.1 sec, 1.1).

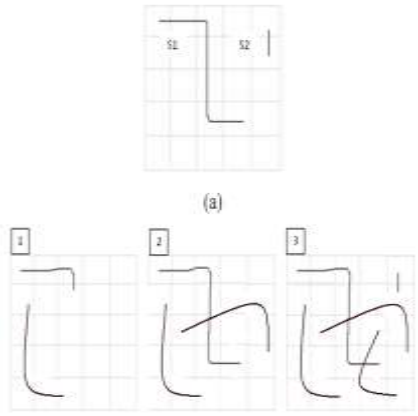

Figure 3.2a: Decoy Strokes[24]

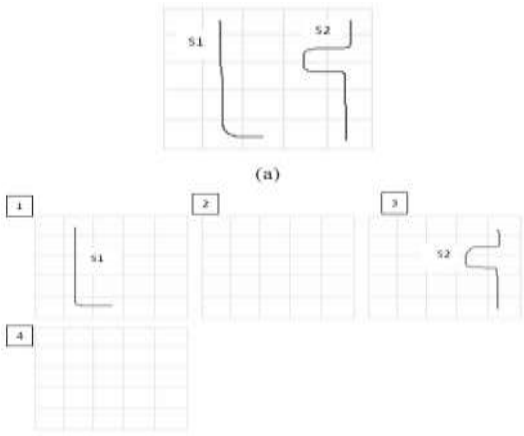

Figure 3.2b: Disappearing Strokes[24]

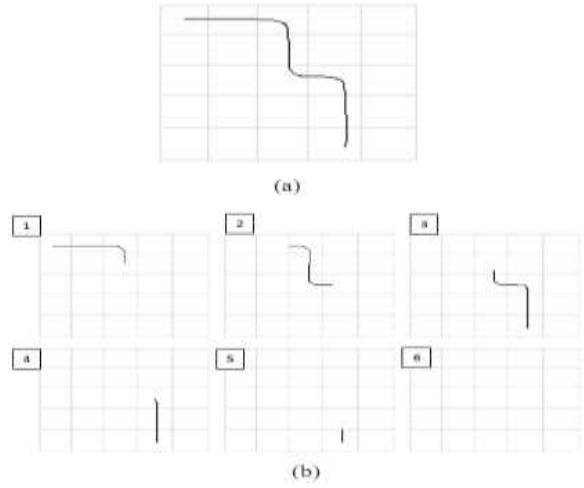

Figure 2.2c: Line Snaking[24]

WYSWYE: Shoulder Surfing Defense for Recognition based Graphical Passwords by R. Khot, P. Kumaraguru, and K. Srinathan [26]

This paper proposed a scheme named WYSWYE (What You See is Where You Enter) where the user identifies a pattern of password images inside a bigger grid and then correctly maps the positions of the identified pattern onto another grid. The idea here is to identify a pattern of N password images inside MxM grid (Challenge Grid) and then map the identified pattern onto a separate NxN grid (Response Grid). The user must first reduce the bigger grid to the size of response grid by mentally eliminating rows and columns that do not contain any of the password images. The user then maps the positions of password images from the reduced challenge grid onto the response grid. Figure 3.2d shows the working of the scheme. Two variants of the proposed scheme were developed:

- Horizontal Reduce (HR): grid is reduced by eliminating only the columns (7x4 grid).
- Dual Reduce (DR): grid is reduced by eliminating one row and one column (5x5 grid).

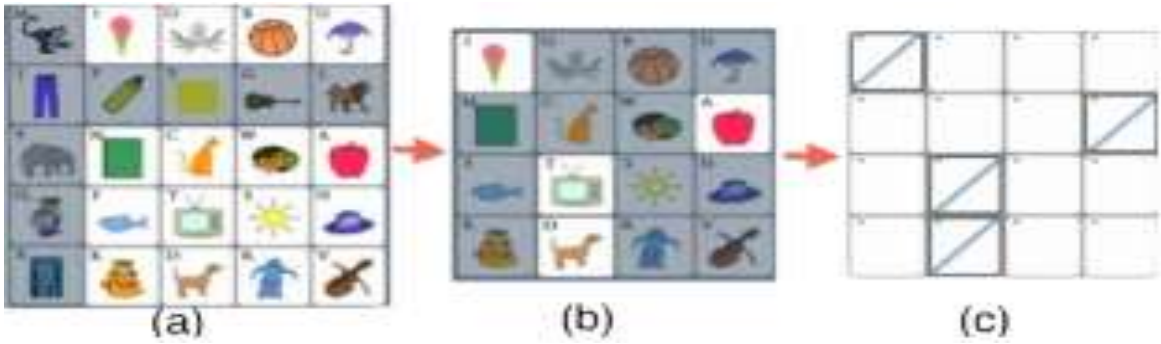

Figure 3.2d: Working of WYSWYE: (a) The user mentally eliminates a row and a column from the challenge grid that does not contain any password images (b)User identifies the position of password images in the reduced grid (c)User maps them onto the response grid [26]

A controlled laboratory experiment to evaluate the usability of the scheme was performed using the repeated-measures design. A total of 24 participants were recruited for the study. The users were divided randomly into 3 groups: horizontal reduce condition, dual reduce condition, and undefended password scheme. After analyzing the results it was observed that: HR and DR techniques resulted in similar accuracy; DR scheme required more time to login than HR scheme; performance improved with practice; participants liked HR scheme more than DR scheme.

A further study to test the security of the techniques against shoulder-surfing attacks was performed using a between-subjects design. A total of 16 participants from the previous study took part. Screen-scraper software was utilized to capture the login information. After analyzing the obtained data it was observed that both DR and HR schemes were more secure when compared to undefended password scheme.

An Enhancement on Passface Graphical Password Authentication by F. Towhidi, M. Masrom, and A. Manaf [27]

This paper proposed an enhancement to make the current PassFace graphical password scheme[25] resistant to shoulder surfing attacks. This was done by changing the method of selecting the password during the authentication phase. In this scheme a unique random text (code) is assigned for each picture and the user needs to input the string of codes corresponding to her password images, instead of directly clicking on the images, to login. Each code consists of two random characters and is displayed below each face. For making the password look random, the S-Passface scheme asks the users to create two different passwords during the registration phase. First password screen contains 18 faces of various men and women, and the second password screen consists of 18 faces of babies and clowns. The authentication screen alternates every session. Each password consists of 4 images selected by the user. Figure 3.2e shows an example login screen.

Figure 3.2e: First Round Login in S-Passface [27]

An online questionnaire based study to analyze the usability of the scheme was conducted with 52 participants. The study followed a between-subjects design and the feedback on certain aspects was collected for both PassFace and S-Passface schemes. The results obtained from the study suggested that most people preferred PassFace (50%) over S-PassFace (43%) when it came to usability, but judged S-Passface (75%) to be more secure than PassFace (22%).

The paper however does not provide any data which suggests that the S-Passface scheme has in fact made Passface more secure.

3.3 Review Based on Solutions for Guessability Attacks

Use Your Illusion: Secure Authentication Usable Anywhere by E. Hayashi, and N. Christin [15]

This paper proposed the use of degraded/distorted images to make graphical password schemes more resilient to social engineering or observation based attacks. The system relied on the human ability to recognize a degraded version of a previously seen image, and the difficulty in mentally reverting from a previously unseen degraded image to the original image. Image degradation provides an effective line of defense against impostors, while being largely unaffected by a low graphical resolution.

A study was conducted to identify the usability of the proposed system. The study was conducted under laboratory conditions using a between-subjects design on mobile phone interface over a period of 4 weeks, and a total of 54 participants volunteered to take part in the study. The users were allowed to select 3 images to be their graphical password images either from the images in the system, or to upload their own images. Once the users selected their images, they were distorted using a non-photorealistic rendering algorithm that eliminates most details in the image, while preserving some features such as color and rough shapes. The users were then divided into 2 groups: 1 with no image distortion and other with image distortion. The users in the distorted-image group were provided with a training session to associate the distorted image with the original image and the meaning of that image. During the authentication phase, the users were required to select their images from a set of 9 distractor images. Intersection attacks were resisted by always maintaining identical decoys in each authentication challenge. Each authentication challenge always remained the same, and the intersection of many challenges revealed nothing about the portfolio. After analyzing the data obtained it was clear that the performance of the users in Use Your Illusion group was comparable to that of the users in non-distorted group, which suggested that users who had been exposed to the original image could easily mentally revert a highly lossy, one-way transform on the image, even when it was not mathematically reversible and conveyed limited information. It was also observed in the study that people found it really difficult to identify the original image from a presented distorted image if they hadn't been exposed to the original image beforehand (almost 60% users guessed images wrongly).

The study however only considered 3 portfolio images and only 27 challenge images which is a very small sample size. The study also does not provide any mechanism to measure the distortion in the images.

Figure 3.3a: Example Training Set[15]

Figure 3.3b: Example Challenge Set[15]

Figure 3.3c: Examples of incorrect semantic meanings[15]

3.4 Conclusion

The background survey suggested that a lot of research has been undertaken in the field of graphical authentication system to make it secure towards attacks such as shoulder surfing [10,11,13,15,25-27] and other observation based attacks [17,23-25,27]. There is however very limited work done to make it easier for the user to recognize their images without decreasing the security of the scheme [29]. The schemes that do propose solutions to mitigate shoulder surfing attacks fail to consider the effects of multiple passwords[2-7,16,18] on the overall usability of the system [10,11,13,15,25-27]. Therefore, it is desirable to design a system which will make it easier for the users to remember their passwords without compromising the usability, or security of the password scheme.

The next chapter describes the implementation of the proposed approach and the evaluation method to be used to justify the solution.

4 Proposed Approach

This section provides the details about the solution and the approach which will be followed to achieve the solution obtain the results.

4.1 Implementing the System

The aim is to develop the EPHAS system. The system will be a website which will be developed using technologies such as PHP, JavaScript, and MySQL and

will be hosted on a Windows server. The images used will be collected from freely available and non-copyrighted image sources over the internet.

The system will consist of two phases. Figure 4b shows the general scheme of the solution:

Registration Phase: Steps to be followed during the registration phase-

- Create a username for the account.
- Select 6 images from a set of images presented by the system to be used as passwords.
- Provide hints to each image. Hints can be in any language but must use Latin alphabets (English letters).
- Hints should be non-obvious, i.e. the users should aim to provide hints which may help them to recall the image but make it very difficult for someone else to guess the image based on the hint.
- A hint could be a maximum of 6 words long.

Authentication Phase: Steps to be followed during the authentication phase-

- The users will be provided with 4 different challenge screens (one after the other).
- Each screen will show a challenge set (16 images) containing a set of distractor images (13-15) and password images (1-3). Only 1 of the password images will be the target image. Figure 4a shows a sample authentication screen.
    - The system will keep a count on the usage of a password image as target image.
    - All the password images will be used as the target images almost equally.
    - The corresponding challenge sets between 2 successive sessions (for e.g.: screen 1 in session 1 to screen 1 in session 2) will share some of the distractor images and password images to minimize the observation and intersection attacks.
    - Refreshing the page will not change the challenge set.
- Hint corresponding to required password image (target image) will be provided to the user to aid the recall.
- Selecting an image on the current screen will take the users to the next screen. If all the choices made by the user are correct, they will be taken to their account.
    - No indication of the choice made by the user will be shown on the screen to make the selection less observable.
- If any/all of the choices made by the user are wrong, they will have to re-attempt the login process.
    - The user will not be notified of wrong choices until the login process is finished.
    - The challenge screens will remain unchanged during a session, to reduce the chances of intersection attacks.
- The login process will be timed. Exceeding the time limit will result in authentication failure and will count as an attempt. This will be done in an attempt to reduce cognitive attacks.
    - The initial time limit will be set to around 15 seconds as reported in PHAS [29] (might be fine-tuned based on further research).

- The system will keep track of the time taken by every user to authenticate.
- The timer for a user will be automatically adjusted to average authentication time taken by that user.

- Maximum of 3 attempts will be allowed before the account becomes temporarily inactive to reduce the chances of brute-force attack.

Figure 4a: Example Authentication Screen

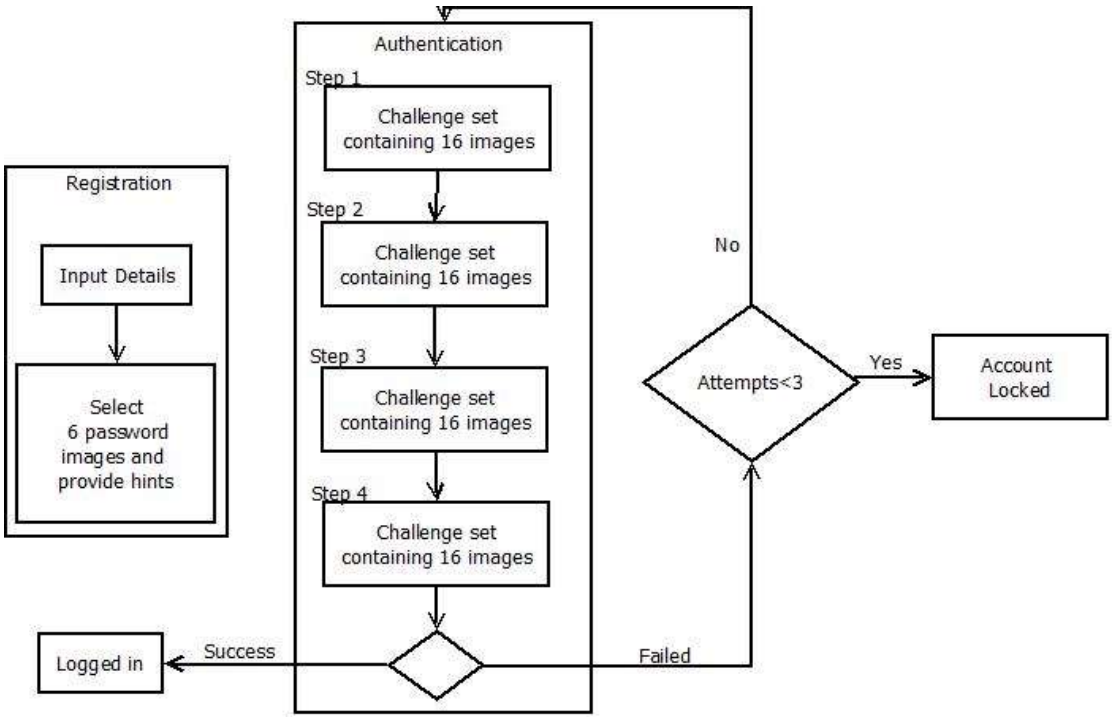

Figure 4b: Scheme of EPHAS

4.2 Usability Study

A usability study of the current system will be performed by and the results will be compared to the available results for PHAS [29] and other GASs [10,11,14,15,21-27].

The study will be conducted in a laboratory environment and will consist of two sessions conducted at a gap of two weeks (figure 4c provides an overview of the process). The experiment will use the independent–measures protocol and will be conducted with at least 30 users:

Entry Questionnaire: Before starting the first session the users will be required to answer an entry questionnaire which will be aimed at collecting the demographic data about the users and their expertise with the different authentication systems.

Session 1: The first session will be divided into three phases- Practice, Password Generation, and Retention. Users will be provided with instructions explaining the registration and authentication process. First, the users will complete a practice session with two trials. For each trial they will create a password and then try login the system. In the password generation phase the users will be asked to create four different accounts and four passwords (images and hints), one for each account. To make sure that users do not select same image for multiple passwords, they will be provided with four different sets of images. During this phase users will be asked to remember their passwords.

To reduce the effects of memory interference and overlapping, users will be asked to complete a distraction task after registering with each password. The registration time for each password will be recorded.

After the password generation phase, the users will be asked to authenticate using each password three times. This will be done in the hopes of making the user more comfortable with the system and to make sure that they remember their passwords. In case of authentication failure the correct password will be displayed. The authentication process will not be timed during this phase nor will the lockout policy be enforced.

Session 2- Retention Test (after two weeks): During this session the users will be asked to authenticate with each password three times. No practice session will be provided in this session.

Data Collected: The following data will be recorded:

- Number of successful logins.
- Number of total login attempts.
- Average login time per user.

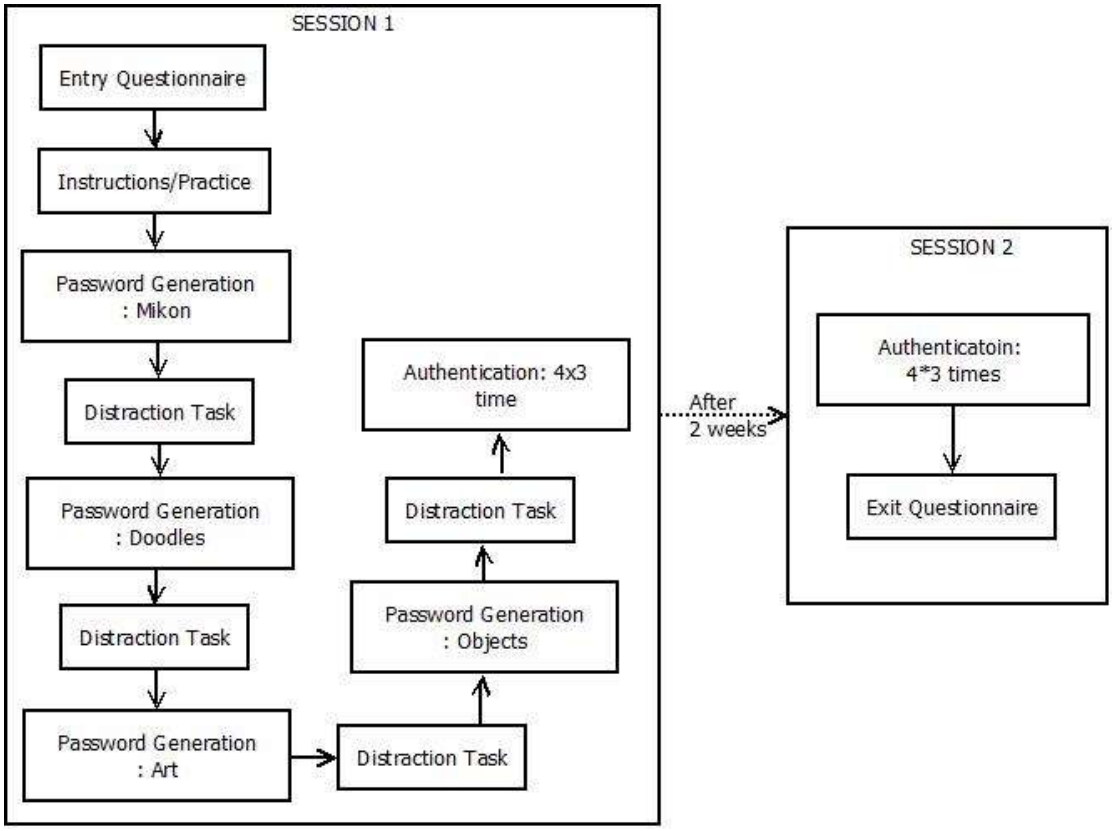

Figure 4c: Process Flow of Usability Testing

4.3 Guessability Study

A guessability study to measure the security of the system against shoulder-surfing attacks will be performed. The same users from the usability study will be asked to participate in the study, since they already have the familiarity with the system. The test will be conducted in lab environment.

The users will be provided with instructions on the steps they would need to follow during the study. The experimenter will act as a victim and the users will play the role of shoulder surfers. They will have the freedom of choosing an optimal viewing position. The users will only be given a single chance to observe each login session, to emulate a casual shoulder-surfing attack. The users will record the password images and the corresponding hints for each session.

To reduce the effects of memory interference users will have to complete a distraction task after observing each password. The success of the attack will depend on the number of password image-hint pair correctly identified.

If the time permits, second phase of guessability study will be performed to identify the security of the proposed system against brute-force attack. This will also be done to examine the extent to which passwords can be guessed using the hints. The test will be conducted in lab environment and will follow think-aloud protocol, to gauge the thought process of the users.

The user will be provided with the account name and the demographic details of the account holder, and will be asked to guess the password based on the hints and the details provided.

The data collected from the test will be number of successful authentications and average time taken.

4.4 Conclusion

After identifying the design and development methodology, and the evaluation criteria it can be observed that the whole project needs to be divided into subtasks, goals and milestones. The next chapter makes and attempt at identifying the major goals and tries to estimate the time required for the completion of each goal.

5 Work Plan

The main activities in the project stage following the submission of the proposal are identified and listed below. A gantt chart is also presented in Figure 5.

Understanding the current PHAS

Duration: 6 days

This phase will provide a complete description of the working of PHAS as implemented at the coding level, and will also include acquiring the rights to use and enhance PHAS.

Requirement Elicitation

Duration: 6 days

This phase will provide a complete description of the desired behavior of the updated system that is being developed.

Design of the System

Duration: 10 days

This phase will include designing the UML diagram for the proposed solution showing the behavior and interaction of the proposed system.

Implementing the System

Duration: 18 days

During this stage the designed solution will be implemented and the solution will be integrated with the existing system.

Testing the System

Duration: 5 days

This phase will include testing the developed solution. The tests will include unit testing, integration testing, and validation and verification of functionalities.

Usability & Guessability Evaluation

Duration: 21 days

After successful testing of the solution it will be evaluated for usability by participants. This will follow the procedures already defined in Chapter 4.

Analysis of the Data Obtained

Duration: 5 days

After the completions of user evaluation, the data obtained will be analyzed. The data obtained from the questionnaires will also be analyzed. The results obtained will help us to compare PHAS with EPHAS.

Writing the dissertation

Duration: 35 days

The final submission of the project stage includes a completed dissertation; hence this phase is absolutely important. Dissertation writing is a time consuming process and therefore it will be performed in parallel with other activities.

Figure 5: Work Plan

5.1 SWOT Analysis

Strengths

- PHAS system is already implemented.
- Hardware and software required for development is available.
- The memorability of multiple PHAS passwords is already established.

Weaknesses

- The introduction of 2 extra images could severely deteriorate the memorability of the passwords.
- Very limited amount of work done to study the results of remembering multiple passwords.
- The working of PHAS system is unknown. This will be solved by understanding and using the system.

Opportunities

- We can make the system secure while maintaining the usability.
- We can understand the effects of using multiple passwords on the users and the strategies used by them to remember their passwords.
- If time permits we can perform statistical tests on the data obtained, which could be important for further research in the field of GASs.

Threats

- Time constraints: there might not be enough time to evaluate the results.

Mitigation Strategy: Work plan in the gantt chart will be strictly followed.

- Novel Approach: the use of six images as password has not been done before.

Mitigation Strategy: Proven processes used in earlier researches [16,18,29] will be followed to minimize the risk of failure.

- Insufficient Requirement Capture: developing the system that does not satisfy the requirements.

Mitigation Strategy: Performing a comprehensive requirement elicitation and using iterative model of software development will help in making sure that the system satisfies the requirement.

6 References

[1] Kirkpatrick, E. A. (1894). An experimental study of memory. Psychological Review, 1(6), 602.

[2] Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. Journal of verbal Learning and verbal Behavior, 6(1), 156-163.

[3] Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words?. Psychonomic Science, 11(4), 137-138.

[4] Kintsch, W. (1970). Models for free recall and recognition (Vol. 124). Models of human memory. New York: Academic Press.

[5] Tulving, E., & Watkins, M. J. (1973). Continuity between recall and recognition. The American Journal of Psychology, 739-748.

[6] Madigan, S. (1983). Picture memory. Imagery, memory and cognition, 65-89.

[7] Raaijmakers, J. G., & Shiffrin, R. M. (1992). Models for recall and recognition. Annual review of psychology, 43, 205-234.

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

[9] Monrose, F., & Reiter, M. K. (2005). Graphical passwords. Security and Usability, 147-164.

[10] Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In Proceedings of the working conference on Advanced visual interfaces (pp. 177-184). ACM.

[11] Weinshall, D. (2006, May). Cognitive authentication schemes safe against spyware. In Security and Privacy, 2006 IEEE Symposium on (pp. 6-pp). IEEE.

[12] Paivio, A. (2006). Mind and its evolution: A dual coding theoretical interpretation. Mahwah, NJ: Lawrence Erlbaum Associates, Inc. __Paivio, A., & Lambert, W.(1981). Dual coding and bilingual memory. Journal of Verbal Learning & Verbal Behavior, 20, 532-539.

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

[14] Moncur, W., & Leplâtre, G. (2007, April). Pictures at the ATM: exploring the usability of multiple graphical passwords. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 887-894). ACM.

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

[16] Everitt, K. M., Bragin, T., Fogarty, J., & Kohno, T. (2009, April). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 889-898). ACM.

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

[18] Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. C., & Biddle, R. (2009b, November). Multiple password interference in text passwords and click-based graphical passwords. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 500-511). ACM.

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

[20] Poet, R., & Renaud, K. (2009). A mechanism for filtering distractors for doodle passwords. International Journal of Pattern Recognition and Artificial Intelligence, 23(05), 1005-1029.

[21] Renaud, K. (2009). On user involvement in production of images used in visual authentication. Journal of Visual Languages & Computing, 20(1), 1-15.

[22] Renaud, K. (2009, August). Web authentication using Mikon images. In Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09. World Congress on (pp. 79-88). IEEE.

[23] De Luca, A., Hertzschuch, K., & Hussmann, H. (2010, April). ColorPIN: securing PIN entry through indirect input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1103-1106). ACM.

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

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

[26] Khot, R. A., Kumaraguru, P., & Srinathan, K. (2012, November). WYSWYE: shoulder surfing defense for recognition based graphical passwords. In Proceedings of the 24th Australian Computer-Human Interaction Conference (pp. 285-294). ACM.

[27] Towhidi, F., Masrom, M., & Manaf, A. A. (2013). An Enhancement on Passface Graphical Password Authentication. Journal of Basic and Applied Scientific Research, 3(2), 135-141.

[28] Nicholson, J., Coventry, L., & Briggs, P. (2013, April). Age-related performance issues for PIN and face-based authentication systems. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 323-332). ACM.

[29] Chowdhury, S., Poet, R., & Mackenzie, L. (2014, April). Passhint: Memorable and Secure Authentication. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM.