Image based authentication using zero-knowledge protocol

Conference Paper · May 2018

DOI: 10.1109/CATA.2018.8398683

Zarina Mohamad
Universiti Sultan Zainal Abidin | UniSZA
26 PUBLICATIONS **37** CITATIONS
SEE PROFILE

Aznida Hayati Zakaria
Universiti Sultan Zainal Abidin | UniSZA
14 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Wan Suryani Wan Awang
Universiti Sultan Zainal Abidin | UniSZA
15 PUBLICATIONS **24** CITATIONS
SEE PROFILE

IMAGE BASED AUTHENTICATION USING ZERO-KNOWLEDGE PROTOCOL

Zarina Mohamad, Lim Yan Thong, Aznida Hayati Zakaria, Wan Suryani Wan Awang

Faculty Informatic and Computing
Universiti Sultan Zainal Abidin,
Kampus Besut, 22200 Besut,
Terengganu, Malaysia.
{zarina@unisza.edu.my, 034588@putra.unisza.edu.my,aznida@unisza.edu.my,suryani@unisza.edu.my}

Abstract: One of the most critical concerns in information security today is user authentication. There is a great security when using the text-based strong password schemes but often remembering those good passwords is very hard and users writing them down on a piece of paper or saving inside the smart phone. There is an alternative solution to the text-based authentication which is the Graphical User Authentication (GUA) or simply image-based Password based on the fact that humans tend to memorize images better. This type of approach allows users to create and remember passwords easily. However, one big issues that is plaguing GUA is shoulder surfing attack that can capture the users mouse clicks and eavesdropping. In this paper, a new algorithm that using zero-knowledge protocol as the solution to solving the eavesdropping and shoulder surfing attack to provide better system security. In zero-knowledge protocol, users prove that they know the graphical password without sending it. In other words, the user does not send the password to the verifier or reveal it to the people nearby. Hackers who try to eavesdrop the password will be failed since the password is not sent over the insecure channel such as Internet nor reveal. Therefore it is a secured approach to prevent interception by unwanted parties or adversary. The result that is going to be yielded in this project is a secured authentication approach which is user-friendly.

Keywords: Authentication, security, graphical password

1. Introduction

Computer security is the protection of information systems from theft of damage to the hardware, the software, and to the information on them. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. To achieve this, many techniques were introduced and can be categorized as encipherments, routing protocols, digital signature, data integrity and authentication [1].

Authentication can be categorized into two types which is message authentication and entity authentication. Message authentication is the process to authenticate and verify the message to be sent by the sender and not modified or forged by attacker. While entity authentication is the process of identifying a party to the other party where a party can refer to a user, a process or a system. User authentication system is the most common entity authentication system implemented and used.

There are 2 types of user authentication approach too which differ from each other by using different type of password scheme. Text-based password is traditional system which use text as password and the most common password type used until today. On the other hand, Blonder was the first to introduce the concept of graphical passwords in 1996 [2]. Graphical User Authentication (GUA) is an authentication system that make use of graphical password which works by having the user select from images, in a specific order, presented in a graphical user interface (GUI) [3].

Zero-knowledge protocols are one of the family members of entity authentication widely used for identity verification over insecure channels. Zero-knowledge protocols were originally introduced by Goldwasser, Micali and Rackoff (GMR) who have proven these protocols to be important models of computation in both complexity and cryptography [4]. In zero-knowledge protocol, the user does not reveal anything that might endanger the confidentiality of his password. The user proves to the authentication system that he knows the password, without revealing it. The interactions are so designed that they cannot lead to revealing or guessing the password. After exchange messages, the authentication system only knows that the user does or does not have the password, nothing more. The result is a yes or no situation, just a single bit of information.

The proposed system aims to solve problems encountered by currently available graphical user authentication approaches which having big issues that are shoulder surfing attack that can capture the users mouse clicks and eavesdropping[5]. This system uses double-layer security model, which are recognition based image password and zero-knowledge protocol, which had offset the vulnerabilities that they both had on themselves. Since the proposed algorithms hide the true password of user within a set of pictures, the user just have to answer whether the set of images contains his password, thus prevent shoulder surfing and eavesdropping.

2. Literature Review

Graphical User Authentication (GUA) is an authentication using Graphical or Picture as password. Most of the journals from 1995 till 2010 describe that Graphical Authentication Techniques are categorized into three groups which are Pure Recall Based, Cued Recall Based and Recognition Based [3]. All these techniques are of the same concept, in which authenticate user by Graphical based technique. To be details, in a graphical user authentication system, a user needs to choose a memorable image as his password to login or authenticate himself in to the system. The process of choosing memorable images or graphical passwords are depends on the nature of the process of image and the specific sequence of click locations. In order to strengthen the memorize ability of user, images should have meaningful content because meaning for arbitrary things is poor. Memorize ability of password and efficiency of their inputs is two key human factors criteria. Memorize ability have two perspectives which are: How the user chooses and encodes the password? What task the user does when retrieving the password?

In Pure Recall-based Technique, users need to reproduce their passwords without being given any reminder, hints or gesture. Although this category is easy and convenient but it seems that users hardly can remember their passwords. Some examples of the method using this technique would be Draw A Secret (1999) and Qualitative DAS (2007) [3]. Table1 displays some of the example algorithm created based on this technique.

Table 2.1. Pure Recall Based Techniques Ordered by Year

Algorithm	Proposed Year	Created By
Draw a Secret (DAS)	1999	Jermyn Ian et al.
Grid Selection	2004	Juaie Thorpe
Qualitative	2007	Di Lin, et al.

(a) Draw A Secret (DAS)

This method is implemented in 1999 by allowing the user to drawing a simple picture on a 2D grid as in Figure2. The interface is consisting of a rectangular grid of size G*G. Each cell in this grid is represented by discrete rectangular coordinates(x, y). As the figure displayed, the coordinate sequence generated by drawing is:

(2, 2), (3, 2),(3,3),(2,3),(2,2), (2,1),(5,5)

Main point of this method is the drawing or stroke of the password the 2D grid. In this method the stroke should be a sequence of cells which does not contain a pen up event, so password will define as a sequence of stroke, separated by pen up event. In the authentication process, the user must re-draw the picture by creating the stroke in same sequence which done in registration phase. If the drawing touches the same grids in the same sequence, then the user is authenticated [6].

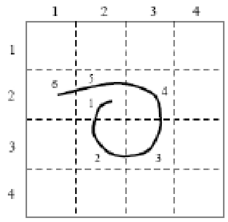


Figure 2.1. Draw a Secret (DAS) method on a 4*4 Grid

The disadvantages is proofed by Goldberg in 2002 had a survey which showed that most of the users forgot their stroke order. On the other hand, he showed that user can remember text password easier than DAS Password. The other weakness is that, the users tend to choose frail graphical passwords that are vulnerable to the graphical dictionary attack [7].

(b) Passdoodle

Passdoodle is a graphical user authentication algorithm by making use of handwritten designs or text, usually drawn with a stylus onto a touch sensitive screen. According to their theory in 1999 paper, Fermyn et al. prove that doodles are harder to crack due to a much larger number of possible doodle passwords than text passwords. Figure 1 will show a sample of Passdoodle password.

Figure 2.2. An Example of a Passdoodle

The issue of recognition prevents widespread use of the Passdoodle are the length and identifiable features of the doodle set the limits of the system. Only a finite amount of computer differentiable doodles can be made. The doodle here is used as the sole means of identification. To maintain security measure of the authentication system cannot simply authenticate a user as the user whose recorded doodle is most alike, rule for a minimum threshold of likeliness and similarity must be set. This prevents the use of blatant guessing to authenticate as a random user.

However efficiency includes speed and accuracy remain top priorities for the system. A complicated recognition design requiring a hundred training samples and minutes of computation to authenticate negates the purpose of the original pervasive design. The proposed system uses a combination of doodle velocity and distribution mapping to recognize and authenticate a doodle [8].

Goldberg and his colleagues [8] developed a Passdoodle algorithm, which was a graphical password comprised of handwritten designs of text, usually drawn with on a screen as input to the system. Their study concluded that users were able to remember complete doodle images as accurately as alphanumeric passwords.

With reference to the [8], they found that people could remember complete doodle images as accurately as alphanumeric passwords, but they were less likely to recall the order in which they draw a doodle than the resulting image. This is the biggest drawback of the system.

In the other research [9], users were fascinated by the doodles drawn by other users, and frequently entered other users' login details merely to see a different set of doodles from their own.

(b) Grid Selection

In 2004, Thrope and van Oorschot further studied the impact of password length and stroke-count as a complexity property of the DAS scheme. In their study, they proofed that stroke-count posed significant effect on the DAS password space. The size of DAS password space decreases significantly with fewer strokes for a fixed password length. The length of a DAS password also has a significant impact but the impact is not as strong as the stroke-count. To improve the security, Thrope and van Oorschot proposed a "Grid Selection" technique. The selection grid is an initially large, fine grained grid from which the user selects a drawing grid, a rectangular region to zoom in on, in which they may enter their password (see figure 3). This would significantly increase the DAS password space.

A user first selects an N x N drawing grid within a much larger selection grid. Then they zoom in and create the secret as per the original DAS scheme. The location of the chosen drawing grid adds an extra degree of complexity to the password as there are thousands of possible drawing grids within the selection grid. This technique in theory could significantly increase the password space by adding up to 16 bits to the password space. To our knowledge no use study of grid selection has been carried out, so it is unclear whether this works as well in practice as expected. A well-known lesson on usable security, in particular for password schemes, is that what engineers expect to work and what users actually make work are two different things [10].

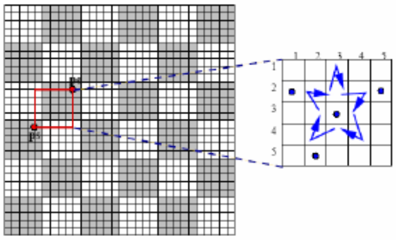


Figure 2.3. A sample of Grid Selection Method

Although this method had significantly increases the DAS password space however, Thrope and van Oorschot didn't solve the lacks of DAS [10].

(c) Qualitative DAS (QDAS)

In 2007, QDAS method introduced as improvement of DAS method. It is created by encoding each stroke. The raw encoding consists of its starting cell and the sequence of qualitative direction change in the stroke relative to the grid. In this method, a direction change is considered valid when the pen cross a cell boundary in a direction different from direction the cross the previous cell boundary. The research shows that, the image which has more area of interest could be more useful as a background image [12] which can be seen in Figure 4.

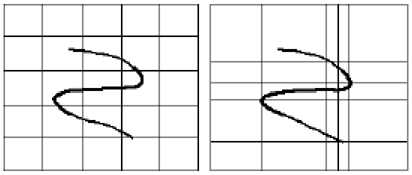


Figure 2.5. A sample of Qualitative DAS Algorithm

The advantages of this model is that it has higher resistant toward shoulder surfing attack. This is because the model uses dynamic grid transformation to hide the process of creating password so this method could be safer that original DAS to shoulder surfing attack. Although this model have more entropy than previous DAS but it has less memorable than the original DAS [12].

In the Cued Recall-Based Technique proposed a framework of reminder, hints and gesture that help the users to reproduce their password or help users to make a reproduction which will be much more accurate. Example would be Blonder Algorithm (1996) and Passpoint (2005) [3]. Table2 shows some of the example algorithm created based on this technique.

Table 2.2. Cued Recall Based Techniques Ordered by Year

Algorithm	Proposed Year	Created By
PassPoint	2005	Susan et al.
Passmap	2006	Vamponski
Background	2007	Paul Duaphi

(a) PassPoint

In 2005, PassPoint created as improved version of Blonder Algorithm by overcome the limitation which was limitation of image. The background picture choice can now be any natural picture or painting but at the same time should be rich enough in order to have many possible click points. One important point is that the image is not secret and has no role other than helping the user to remember the click point. Another advantages of PassPoint is that flexibility that there is no need for artificial predefined click regions with well-marked boundaries like Blonder algorithm [14]. PassPoint system has the potential for extremely high entropy. As any pixel in the image is candidate for a click point so there are hundreds of possible memorable points in the challenge image. There are several researching on the characteristic of this model like predicting probabilities of likely click point which enables predicting the entropy of a click point in a graphical password for a give image like Figure 9[15]

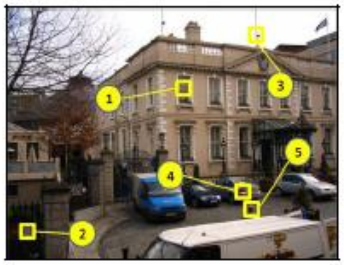


Figure 2.9. A sample of PassPoint method

Users in PassPoint system can create a valid password easily and quickly, but they had more difficulty learning their passwords than alphanumeric users. It takes more trials and more time to complete the practice for newcomers. On the other hand, the login time in this method is longer than alphanumeric method [14].

(b) PassMap

One of the main problems with passwords is that very good passwords are hard to remember and the one which are easy to remember are too short of simple to be secured. From the studies of human memory, we know that it is relatively easy to remember landmarks on a well-known journey. As an alternative example we can use a map of Europe and a user who has never been to Europe before should have no problem memorizing that he wants to one day see the Eiffel Tour in Paris, the Big Ben in London and the Kremlin in Moscow and his PassMap might be to visit all of them one at a time flying in from his hometown [16] (see Figure 10).

Figure 2.10. A sample of PassMap method

The advantages of PassMap method is not very susceptible to "shoulder surfing" as can be clearly seen from Figure8. Noticing a single new edge in a large graph or even an absence of some edge in the map is not a trivial task, for someone just passing by. But it is respect to Brute Force attacks while at the same time considering how good those mechanism are in terms how memorable they are [16].

(d) Background DAS (BDAS)

In 2007, this method proposed by adding background image to the original DAS for improvement, so that both background image and the drawing grid can be used to providing cued recall as you can see in Figure 11 [17].

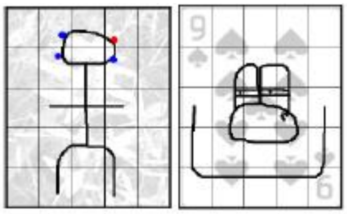


Figure 2.11. A sample of BDAS algorithm

The user starts by using three different ways:

i. The user have secret in mind to begin, and then draw using the point from a background image.
ii. The user's choice of secret is affected by various characteristic of the image.
iii. The mix of two above methods.

With reference to a research on BDAS, memory decaying over a week is one of the major problems in this algorithm. Users had no problem in recreating it in the five minute test but a week later they could not do better than producing the secret passwordas previous. Also shoulder surging and interference between multiple passwords are concerns for BDAS [17].

Recognition Based is one of the most common graphical authentication technique used in the world. Recognition Based involves users select pictures, icons or symbols from a bank of images [18].

During the authentication process, the users have to recognize their registration choice from a grid of image. Research has shown that "90% of users can remember their password after one or two months" [19]. Most of the researches show that majority of users are not adept at drawing graphical passwords in Recall based category and also for recall based algorithm we need to use mouse or drawing input devices. On the other side, regarding to previous research around 90% of users can remember their password after one or two months, so the main focus of this research is on the recognition based category. Table3 lists some of the example algorithm which created based on this technique.

Table 2.3. Recognition Based Techniques Ordered by Year

Algorithm	Proposed Year	Created By
Story	2004	Davies, et al.
Déjà Vu	2012	Dhamija, et al.
Passfaces	2015	Brotstoff, et al

(a) Story

The Story scheme, which requires the selection of pictures of objects which included people, cars, foods, airplanes, sigh-seeing, etc. to from a story line. Story was proposed by Davis, Monrose and Reiter (2004) as a comparison system for Passfaces. Users create a story by selecting a series of pictures. To login, users are presented with one panel of images and they must identify their story images from among set of fake images. Images used for the story scheme can be everyday objects, places, or people. Story introduced a sequential component: users must select images in the correct order. To aid remembrance, users were instructed to mentally construct a story to connect the images in their set. [20][21]

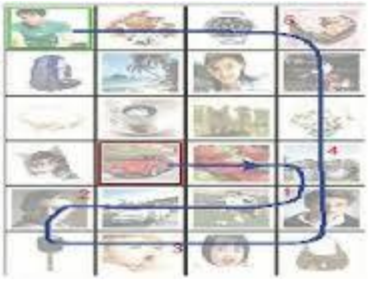


Figure 2.12. Example of Story scheme

Story scheme is very similar to Passlogix v-Go method. Both approach make the remember of password by making a sequence of graphical password that brain easier to remember and recognize as human brain is more sensitive to story than words. Similar to other graphical password, the long login time make Story scheme unpopular.

(b) Deja Vu

Another recognition-based graphical password system is Déjà vu proposed by Dhamija and Perrig, which authenticates the users by choosing pictures among the set of fake pictures. These pictures are presented in a random manner. Each picture is derived from an initial seed and no need to store the pictures pixel by pixel so only the seeds need to be stored in the server. Therefore an authentication server does not need to store the whole picture, it simple needs to store the initial seed.[22]

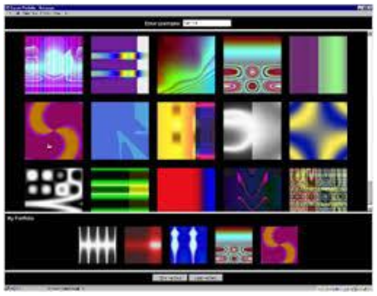
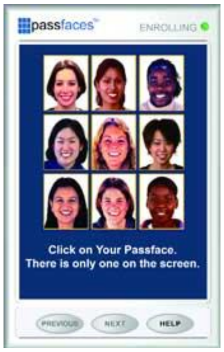


Figure 2.13. Randomly generated images in Déjà vu

Although the average time taken to log into the system longer than that of the traditional text-based password approach, it has a much lower rate of failure.

(c) Passfaces

Passfaces is cognometric method of graphical user authentication. It is based on the measurement of an innate cognitive function of the human brain as brain ability to recognize familiar faces. Similar to traditional text-based password, there is a shared secret between the user and the system. However, instead of relying on users to memorize and recall strings of characters and/or numbers, it use photographs of faces as password and requires only familiarization and recognition on the part of the user [23].



Click on Your Passface.
There is only one on the screen.

Figure 2.14. A sample of Passfaces

The advantage of Passfaces is it is a system that is purely software based and no extra hardware is required. Therefore the cost of implementation of this system is low. The advantage of Passfaces is that it is a wrapper or hash on top of password authentication, not two factor authentication as the author claimed. Although Passfaces is used by United State Congress, it is not a major industry standard.

Zero-knowledge protocols also called as interactive protocols. The protocols are very promising for solving the problem related to verification of identity. They are protocols guaranteed for proving your identity over an insecure medium without giving any information out to eavesdroppers that may enable them to identify themselves as you.

After the main theory introduced by Goldwasser, Micali and Rackoff(GMR) in 1985, A. Fiat and A. Shamir proposed a first practical solution in 1986 which is applicable to the computational power of that time[4]. The scheme of Fiat-Shamir is a trade-off between the number of authentication numbers stored in each security microprocessor and the number of witness number to be checked at each verifications [24].In order to show the logic behind the zero-knowledge protocol, Quisquater and Guillou devised the cave example [1].

Suppose there is an underground cave with a door at the end of the cave that can only be opened with a magic word. Alice claims that she knows the word and that she can open the door. At the beginning, Alice and Bob are standing at the entrance (point1). Alice enters the cave and reaches the fork (point2). Bob cannot see Alice from the entrance. Now the game starts.

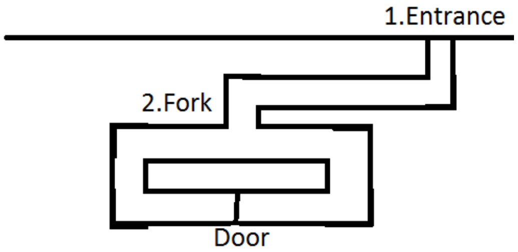


Figure2.15. Cave Example

1. Alice chooses to go either left or right. This corresponds to the sending of the witness(x).
2. After Alice disappears into the cave, Bob comes to the fork (point2) and asks Alice to come up from either right or left. This corresponds to sending the challenge (c).
3. If Alice knows the magic word (her private key), she can come up from the requested side. She may have to use the magic word (if she is on the wrong side) or she can just come up without using the magic word (if she is at the right side). However, if Alice does not know the magic word, she may come up with the correct side if she has guesses Bob's challenge. With a probability of ½, Alice can fool Bob and make him believe that she knows the magic words. This corresponds to the response (y).
4. The game is repeated many times. Alice will win if she passes the test all of the time. The probability that she wins the game is very low if she does not know the magic word. In other words, P = 〖1/2〗 ^N where P is the probability of winning without knowing the magic word and N is the number of times the test is run.

A user authentication mechanism's main goal and the most important requirement is security. Likewise many strategies that exist are primarily for attacking authentication to the system. Therefore schemes must be evaluated according to their vulnerabilities and susceptibility to different attacks because there are no systems that offer perfect security. Shoulder surfing attack refers to obtaining the password of a user when login by direct observation when user not adware or using external recording devices. Most of the graphical password schemes are vulnerable to shoulder surfing attacks. Only a few of recognition-based technique are designed to resist shoulder surfing and none of the recall-based techniques are considered resistant to shoulder surfing [25]. Therefore to overcome these problems, this project aim to research in combination of recognition-based technique and zero-knowledge protocols.

3. Methodology

The development of this system is carried out by applying the methodology of Agile Development. Among the sub-methodologies of Agile Development, Extreme Programming is used. Although implementation of a system based on graphical password techniques with zero-knowledge protocol is also one of the objectives but the system is implemented to show the real working performance of the algorithm rather than being applied or been provided to be used in real business environments or military operations. In extreme programming, every iteration produces the complete system.

(b) Login

User login by recognize his registered password choice. When login, the system will check whether the user is registered to user database by using MySQL query. After found the record of the username is registered, the system displays a set of random image by calling random image from image database. To continue, user has to recognize their password and answer whether his password is in the set or not. Below displays some of the random images set generated by the system.

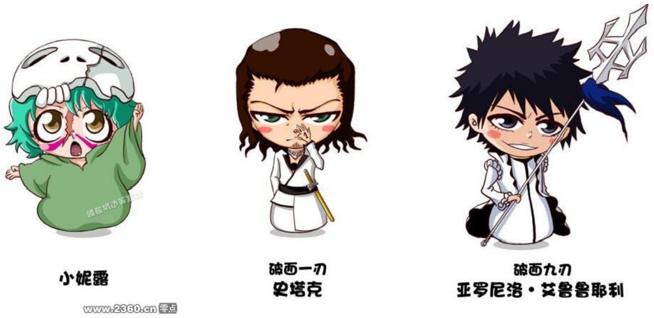


Figure 3.3. Example of a set of random picture

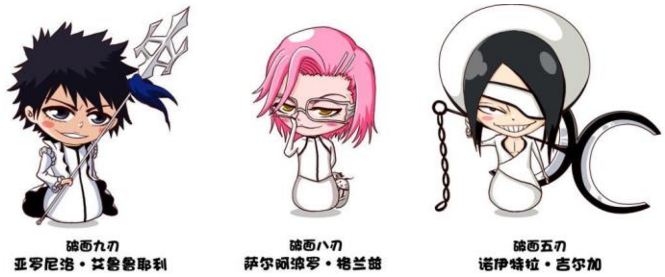


Figure 3.4. Another example of a set of random picture

For instance, the user enters his username which is username123. Then he have to answer the set of random image displayed contains his password or not. In Figure 3.1.3.2 (1), the password chosen by the user is inside the set system displayed. So the user has to answer “yes” to be authenticated. In Figure 3.1.3.2 (2), the password chosen by the user is not inside the set displayed, so the user has to answer “no” to be authenticated.

(b) Authentication

The system will authenticate user whether his answer is correct about the existence of his password in the set displayed. System will set a token to the image set displayed contains user’s registered password to verify that user recognize his password is in displayed image set or not. By using concept of Zero-knowledge protocol, this system only accept input of “yes” or “no” which is similar to 0 or 1 in other Zero-knowledge protocol. Every displayed set is considers a round as in Zero-knowledge. Similar to Zero-knowledge protocol, login is carry on with a few rounds to ensure the security of the user authentication system. If user‘s answers is correct in all round, then he will be authenticated. If his answer is incorrect in any round, he will not be authenticated.

In order to lie, the attacker must guess the value of i in advance, and give $\mathrm{H} = \mathrm{a(Gi)}$ (1) for some a. Since he has no way of doing it, then the authentication system will wrong with probability of ½ in each round. Since the choices are independent, the probability of getting the correct answers in all the rounds is $2^\wedge(-n)$ (2). For instance, let the round of authentication be 5 and each set of images contains 3 images.

Round of authentication, n =5,

Probability to guess correct in all round $= 2^\wedge(-5 * 3)$ (3)

$= 2^\wedge(-15)$ (4)

= 0.0000305 (3 significant figure)

$= 3.05 * \text{〖}10\text{〗}^\wedge(-5)$ (5)

5. Results

The security strength of text-based password is very dependent of the text used. The more complicated and elements it make from, the higher the strength of the password. However, good text-based password is hard to remember because it required the users to remember a random word combined from alphabets and digits. On the other hand, image-based password is easier to remember. Security strength of image-based password is as strong as a well-constructed text-based password. Survey about how long can a user remember their password, either image-based password or text-based password are carried and result is recorded in tables.

On top of that, comparisons are carried out to test the performance and security of the system implemented in this thesis. In graphical user authentication, there are 3 types of technique used to authenticate users which are pure recall-based technique, cued recall-based technique and recognition-based technique. Implemented system is compared to each of the system that belongs to those techniques and results are recorded.

5.1 Results of Survey

In the surveys, a total of 20 different users included children and aged users are invited. They are divided into 2 groups, each group consist of 10 users. Each group is required to register a username and password then login into the system once a week to find out if they can remember their password.

The attribute used to record and survey for 10 different users who use image-based password can be found in Table 5.2. These users are registered with image-based password and login into system implemented in this project. The users are surveyed once every week to check whether they remember their password or not. Users are surveyed and tested by try to login with username and password their registered.

(c) Comparison of Text-based Password Survey and Image-based Password Survey

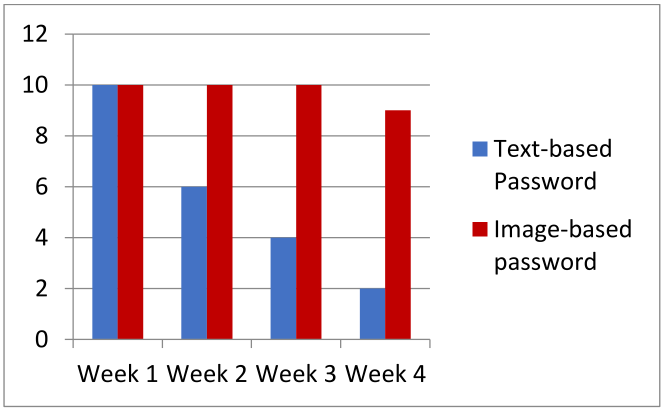


Figure 5.1. Bar chart showing the number of users who still remember their password.

From Figure 5.1, it can be observed that many of the users who use text-based password forgot their password within 2 weeks. The number of users who still remember their text-based password decreases very fast with time. It can be seen that only 2 out of 10 users who still remember their password after 4 weeks. On the other hand, most of the user who use picture password can easily remember their password. The number of users who still remember their image-based password decreases very slow with time. This can be proof by the data that 9 out of 10 users still remember their password after 4 weeks.

5.2 Results of Comparison

Shoulder surfing attack is an attack method use by hacker to obtain victim username and password. This kind of attack is more common in crowded area where it is not uncommon for people to stand behind, example would be queuing at ATM machines. There are also cases where ceiling and wall cameras placed neared ATM machines are used to record keyed pin numbers. The best way to avoid pin number being recorded or remembered by attackers is to properly shield the keypad when entering the pin number. However, in GUA, user cannot simply shield his mouse movement when try to login thus GUA is very vulnerable to shoulder surfing attack. Unlike text-based password which can be masked after user input, image-based passwords in GUA have to use indirect input method to shield the password from shoulder surfing attack.

The implemented algorithm is work by display a set of random images then user has to answer whether his image-based password is in the displayed image set and this process will repeat several times. This indirect input method make this GUA gained higher resistant to shoulder surfing attack because the attacker cannot know which password is user's password. The real user's password is hid within the image set.

Comparison of implemented algorithm and existed algorithm are as below.

(a) Comparison between Implemented System and System that Used Pure Recall-based technique

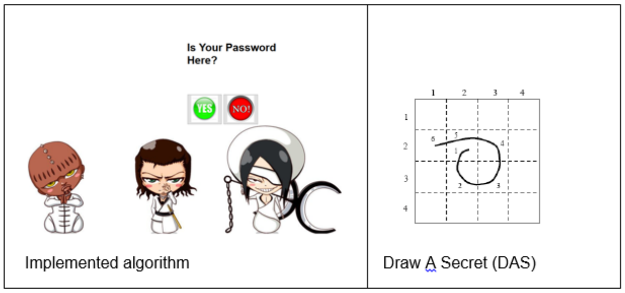


Figure 5.2. Comparison of implemented algorithm and Draw A Secret (DAS)

Draw A Secret (DAS) user input their password by drawing their password out on the space provided using mouse. Attacker can clearly observe the mouse movement from the back and memorize user's password. On the other hand, it is clearly shown on the picture that the invented algorithm using indirect approach to authenticate user whether he know the password or not. The user click on the button of "yes" or "no" instead of directly input his image-based password like DAS do. This indirect approach can mask the mouse action or the drawing action which can prevent shoulder surfing attack.

(b) Comparison between Implemented System and System that Used Cued Recall-based technique

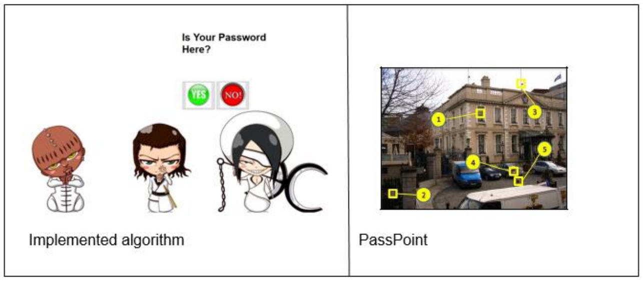


Figure 5.3. Comparison of implemented algorithm and PassPoint

In PassPoint algorithm, users register their password by click on the certain region on the picture provided. To login, user has to click on the same region as when registration using mouse. This login mechanism is very vulnerable to shoulder surfing attack because attacker can see or record the region where user clicks by tracking the mouse movement. On the other hand, invented algorithm didn't involve mouse movement of clicking the registered region thus recording or observing from the back cannot capture any useful information from mouse movement.

(c) Comparison between Implemented System and System that Used Recognition-based technique

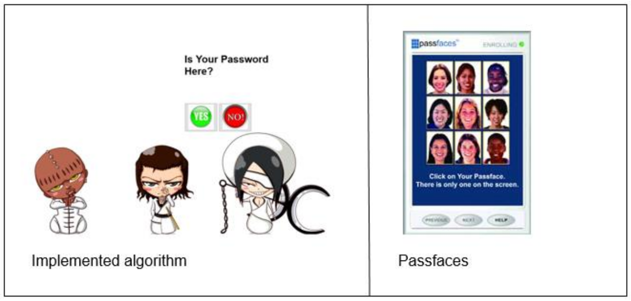


Figure 5.4. Comparison of implemented algorithm and Passfaces

Passfaces is cognometric method of GUA. It is based on the measurement of an innate cognitive function of the human brain as brain ability to recognize familiar faces. This method authenticate user by selecting the face user registered as password when registration. This login mechanism is very vulnerable to shoulder surfing attack because attacker can see or record which face user selected. On the other hand, invented algorithm didn't involve selection of picture nor face thus recording or observing from the back cannot capture any useful information.

Text-based password has to be complicated to have high security strength while image-based password doesn't have to be complicated to have high security strength. Image-based password is easier to remember compare to text-based password. Implemented algorithm has higher resistance toward shoulder surfing attack compare to existed algorithm or method.

6. Conclusion

Nowadays, graphical user authentication is one of the important topic in information technology. Graphical authentication has been proposed as a possible alternative solution to text-based authentication, motivated particularly by the fact that humans can remember images better than text. However, one big issue that is plaguing graphical user authentication is shoulder surfing attack that can capture user mouse click and eavesdropping. Unlike tradition text-based password which can be masked right after user input, image-based password lack of effective way to mask the input of user when login. This thesis had discussed an approach to combine recognition method in graphical user authentication and Zero-knowledge protocol to mask the users input when attempt to login. It increased the resistance of this graphical user authentication system to shoulder surfing attack used by hackers. The application of this algorithm had helped easing business organizations and casual operations in considering security mechanisms used to ensure authentication of users.

The system implemented in this project can indeed provide a very secure graphical user authentication function. To increases security of this system, system should reserve and choose a series of image for user to select as password instead of let users to upload their own image as it is hard to standardize image upload by users. This can make users' password harder to be recognize by hacker who attempt to guess users' password. Research on simplifying Zero-knowledge protocol can help reducing the time taken and amount of system resources used in authenticating user.

7. Acknowledgments

We would like to thank Universiti Sultan Zainal Abidin for the financial support to this project under the Special Research Grant Scheme, SRGS (UNISZA/1/2015/SRGS/5).

8. References

[1] Behrouz A. Forouzan, Cryptography and Network Security, 2008.

[2] Greg E. Blonder, Graphical Password U.S. Patent No. 5559961, 1996.

[3] A.H. Lashkari, F.T., Graphical User Authentication (GUA).2010: Lambert Academic Publisher.

[4] Louis C. Guillou, Jean-Jacque Quisquater, C.G.Guethen(Ed): Advances in Cryptology – EUROCRYPT' 88, LNCS 330.pp. 123-128, 1988.

[5] Arash Habibi Lashkari, Maslin Masrom, Azizah Abdul Manaf, A Secure Recognition Based Graphical Password by Watermarking, 2011 11th IEEE International Conference on Computer and Information Technology.

[6] Jermyn Ian, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords", Proceedings of the Eighth USENIX Security Symposium. August 23-26 1999. USENIX Association 1–14, 1999.

[7] Paul Dunphy, Jeff Yan, "Do Background Images Improve "Draw a Secret" Graphical Passwords?", Proceedings of the 14th ACM conference on Computer and communications security. Alexandria, Virginia, USA. ACM. 36-47; 2007.

[8] Christopher Varenhorst," Passdoodles; a Lightweight Authentication Method ", Massachusetts Institute of Technology, Research Science Institute, July 27, 2004.

[9] Karen Renaud, "On user involvement in production of images used in visual authentication"; Elsevier, Journal of Visual Languages and Computing, 2008.

[10] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi; “Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique”; IEEE Explore, 2008.

[11] Ali Mohamed Eljetlawi, “Study and Develop a New Graphical Password System”, University Technology Malaysia, Master Dissertation, 2008.

[12] Di Lin, Paul Dunphy, Patrick Olivier and Jeff Yan, “Graphical Passwords & Qualitative Spatial Relations”, Proceedings of the 3rd symposium on Usable privacy and security. Pittsburgh, Pennsylvania. ACM. 161-162; July 2007.

[13] Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy;” Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice”, Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA, 2005.

[14] Susan Wiedenbecka, Jim Watersa, Jean-Camille Birgetb and Alex Brodskiyc, Nasir Memon. PassPoints, “Design and longitudinal evaluation of a graphical password system”, Academic Press, Inc. 102-127, July 2005

[15] Ahmet Emir Dirik, Nasir Memon and Jean-Camille Birget, “Modeling user choice in the PassPoints graphical password scheme”, Symposium on Usable Privacy and Security 2007. Pittsburgh, Pennsylvania, USA. ACM. 20-28; July 2007.

[16] Roman V. Yampolskiy, “User Authentication via Behavior Based Passwords”; IEEE Explore, 2007.

[17] Paul Dunphy, Jeff Yan, “Do Background Images Improve “Draw a Secret” Graphical Passwords?”, Proceedings of the 14th ACM conference on Computer and communications security. Alexandria, Virginia, USA. ACM. 36-47; 2007.

[18] Hu, W., X. Wu, and G.Wei, The Security Analysis of Graphical Passwords, in International Conference on Communications and Intelligence Information Security.2010.

[19] Saranga Komanduri, Dugald R. Hutchings. “Order and Entropy in Picture Passwords”, Proceedings of graphic interface 2008. Windsor, Ontario, Canada. Canadian Information Processing Society. 115-122; May 2008.

[20] Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle, Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords, School of Computer Science, Department of Psychology Carleton University, Ottawa, Canada, ACM CCS’09, November 9–13, 2009.

[21] Robert Biddle, Sonia Chiasson, and P.C. van Oorschot, Graphical Passwords: Learning from the First Twelve Years, Carleton University, Ottawa, Canada, ACM, September 27, 2010.

[22] Sonkar S.K., Paikrao R.L., Awadesh Kumar, Graphical Password Authentication Scheme Based On Color Image Gallery, International Journal of Engineering and Innovative Technology (IJEIT) Volum2, Issue 4, October 2012.

[23] Ms. Grinal Tuscano, Aakriti Tulasyan, Akshata Shetty, Malvina Rumao, AIshwarya Shetty, Graphical Password Authentication using Passfaces, Int. Journal of Engineering Research and Applications, ISSN 2248-9622, Vol. 5, Issues 3, (Part 5)March 2015, pp.60-64

[24] Amos Fiat and Adi Shamir, How to prove yourself: practical solutions to identification and signature problems. Springer-Verlag, Lecture notes in computer science, No 263, Advances in cryptology, Proceedings of CRYPTO '86, pp. 186-194, 1987.

[25] Arash Habibi Lashkari, GPIP: A new Graphical Password Based on Image Portions.2014.