PREVENTING SHOULDER SURFING ATTACK IN GRAPHICAL PASSWORD AUTHENTICATION SCHEME

Hammed, M.[1], Adeboye, N. O.[2]

[1]Department of Computer Science, Federal Polytechnic, Ilaro, Ogun State
[2]Department of Mathematics & Statistics, Federal Polytechnic, Ilaro, Ogun State

Corresponding author: Hammed Mudasiru, mudasiru.hammed@federalpolyilaro.edu.ng

ABSTRACT: Authentication based password is very common in computer security and privacy. Most of the traditional passwords are numbers, numbers with alphabets and numbers with alphabets and symbols. That can be easily broken by the attacks such as eves dropping, dictionary attacks, social engineering and shoulder surfing attacks. However, human factors such as choosing bad passwords and keeping passwords in an insecure place are also big problems. In order to address these challenges, several graphical authentication schemes have been proposed, but still shoulder surfing attack increasing. This study proposed multiplication matrix for graphical authentication scheme to reduce shoulder surfing attack. The system attained high degree of accuracy to restrict unauthorized users.
KEYWORDS*:* Graphical authentication, shoulder surfing attack, Multiplication matrix, Password

1. INTRODUCTION

Authentication is the process of determining that the person requesting a resource is the one who he claims to be. Most of the authentication system these days uses a combination of username and password for authentication (Harsh and Farhat, 2013). A password is a form of secret authentication that is used to control access to data. It is kept secret from unauthorized users, and those wishing to gain access are tested and are granted or denied the access based on the password according to that. Passwords are used from ancient times itself as unique code to detect the malicious users. A computer user may need passwords for many uses such as log in to personal accounts, accessing e-mail from servers, retrieving files, databases, networks, web sites, etc.(Dhanashree *et al.*, 2017).The problem with the password is that you have to remember it and it should be kept secret. Each authentication system has their own rules and constraints like password length, password must contain alphabet, and special characters etc. (Harsh and Farhat, 2013) .Normal passwords have some drawbacks such as hacked password, forgetting password and stolen password (Phen-Lan *et al.*, 2008). Therefore, strong authentication is needed to secure all our applications. Conventional passwords have been used for authentication but they are known to have problems in usability and security (Saranya and Bindhu, 2014). Psychology studies have revealed that the human brain is better at recognizing and recalling images than text (Nelson *et al.*, 1977).A graphical password scheme, in which a password is generated through asking the user to click on a graphic or an image provided by the system, is designed (Blonder,1996) . When creating a password, the user is asked to choose four images of human faces from a face database as their own password. In the authentication stage, users must click on the approximate areas of those locations. This method is considered as a more convenient password scheme than textual scheme, for the image can help users to recall their own passwords. (Wiedenbeck *et al.*, 2005).Using images instead of characters will help the user to improve the security as the alphanumeric corpus size is limited. But in the case of graphical password, the size of the corpus is infinity if it is in the case of multiple numbers of images or if it is in the case of multiple points in a single image (Madigan, 1983).There are different existing graphical password techniques proposed by the researchers. Among the graphical password techniques are: Recognition-based techniques, Pure recall-based techniques, Cued recall-based techniques and hybrid techniques. Brute-force and dictionary attacks are the problems associated with the textual passwords. Similarly shoulder surfing attack rendered graphical passwords useless and very expensive to implement. This study proposed a solution to shoulder surfing attack.

2. LITERATURE REVIEW

There are many graphical password authentication schemes which have been proposed by the researchers, they are:

a. Recognition based technique require the user to identify and recognize the secret, or part of it, that the user selected before. Generally during password creation the

users are required to memorize a series of images, and then must recognize their images from among decoys to log in. Phishing attacks are somewhat more difficult with recognition-based systems as a correct set of images must be presented to the user before password entry. Shoulder surfing seems to be of particular concern in recognition-based systems when an attacker is standing behind the user and sees or observes the images selected by users during login (Shraddha and Kishor, 2012).

b. Pure Recall-Based Technique In this category, users have to reproduce their passwords without being given any type of hints or reminder. Although this category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique (Saranya and Bindhu, 2014).
c. Cued Recall-Based Technique: In this category, users are provided with reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to recall based schemes but it is recall with cueing (Dhanashree *et al.*, 2017).
d. Hybrid Schemes: In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome drawbacks of single scheme, such as spyware, shoulder surfing (Dhanashree *et al.*, 2017).

Shoulder surfing attack is a particular concerns of all these approaches when an attacker is standing behind the user to record, see or observe the images selected by users during login.

Related Work

Chiasson et al., (2007), proposed Cued Click-Points (CCP), it was a variation of PassPoints. In this scheme, the next image is displayed based on the basis of the location of the previous click-point. Each image displayed after the first image is a function of the coordinates of the user click points of the present image. When the users click on an incorrect point on the image, then the next image displayed will be wrong. Without the knowledge of correct password, attackers may lead to incorrect images only. However, the users tend to select points within known hotspot regions. However, shoulder surfing attacks remains as an issue in CCP

Chiasson et al., (2008), proposed Persuasive Cued Click-Points (PCCP), which includes persuasive feature to Cued Click- Points. More random passwords can be selected as the cued click points are persuasive. At the time of password creation, the images are slightly shaded except for a random small viewport area positioned on the image. In Persuasive Cued Click- Points, the users have to select a click-point within the viewport. Users can click on the "shuffle" button to reposition the viewport randomly until an ideal location is found by the user. At the time of login, the not shaded images are displayed usually. PCCP eliminates hotspot problem. And also enhances the usability up to an extent. However, shoulder surfing attacks remains as an issue in PCCP.

Gao et al., (2009), proposed a hybrid scheme using CAPTCHA (Completely Automated Public Turing tests to tell Computer and Humans Apart). It retains all the advantages of graphical password schemes and CAPTCHA technology. During the registration phase, users select the images as their password images. For authentication, user is required to differentiate the password images from decoys and complete a test by recognizing and typing the CAPTCHA string below every password images. This scheme is almost impossible to break but still spyware may affect this Hybrid scheme.

Passlogix, (2018), has also developed several graphical password techniques based on repeating a sequence of actions. For example, its v-Go includes a graphical password scheme where users can mix up a virtual cocktail and use the combination of ingredients as a password. Other password options include picking a hand at cards or putting together a "meal" in the virtual kitchen. However, this technique only provides a limited password space and there is no easy way to prevent people from picking poor passwords (for example, a full house in cards).Shoulder surfing attacks also remains as an issue.

3. METHODOLOGY

3.1 Registration phase

During registration phase the user creates an account by providing its information which contains names, sex, phone number and email etc. The user has to choose six images from provided set of images as a pass- image after its information has been stored in the system database. The system stores the six images in form of 2x3 matrix as a template A. Then user will also choose another three images, the system stores this in form of 3x1 matrix as a template B. The matrix in template A and the matrix in template B are multiplied to form a 2x1 matrix M in the database. Multiplication of the two matrices becomes possible because number of columns in matrix A is equal to number of rows in matrix B.

That is A operates on B to yield M . The equation 1 and 2 depict the registered information

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \quad (1)$$

$$B = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \quad (2)$$

$$A\ X\ B = \begin{bmatrix} a_{11}b_1 + a_{12}b_2 + a_{13}b_3 \\ a_{21}b_1 + a_{22}b_2 + a_{23}b_3 \end{bmatrix} \quad (3)$$

In the equation 3, if row 1 and row 2 are denoted as M_1 and M_2 respectively, therefore

$$M_{reg} = A\ X\ B \quad (4)$$

$$M_{reg} = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix} \quad (5)$$

3.2 Authentication Phase

During authentication when a user wants to login with his/her password/PIN generated during registration. The system randomly provides set of images that also contains images selected during registration. Users must be cognitively active when selecting images as a password/PIN and there is a specified time for a user to complete its login action. A user who is unable to complete its login action within a given time, the system will automatically logout such user. System first validates the user's email with images submitted for login, and check if there is commonality between them. The system will finally use six selected images to form matrix **A** and use the three selected images to form matrix **B** and then perform a multiplication of matrix **A** and matrix **B** to form matrix M_{aut} . The system will then checks whether the matrix M_{reg} which was formed during registration is the same with the matrix M_{aut} formed during authentication. If there is a relationship between M_{reg} and M_{aut} then the user will be activated, otherwise the user will be denied access. The shoulder surfing attack is eliminated because the adversary can only see the two matrices i.e. matrix **A** and matrix **B** but the result of multiplication which is matrix M_{reg} can never be known to the attacker. So, it is difficult for the attacker to find the relationship between M_{reg} and M_{aut} . The figure 1 and 2 depicts the system architecture and the data flow diagram for the proposed system.

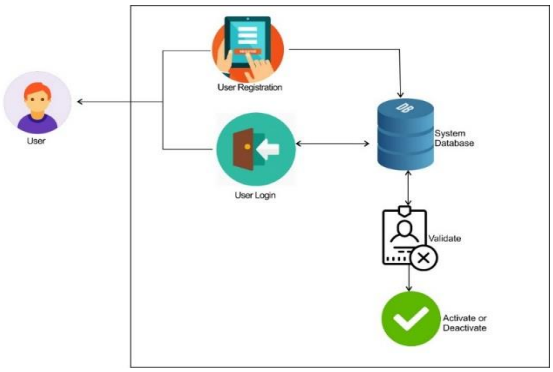

Figure 1: Graphical authentication system

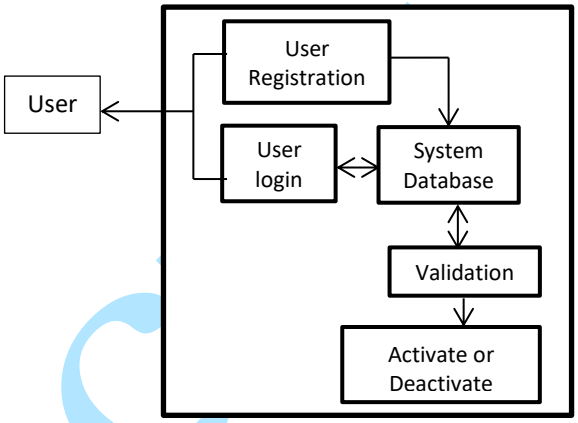

Figure 2: Data Flow Diagram

3.3 Discussion

Every system user submits his/her personal information such as name, phone number, e-mail address etc. and the system stores the information in the database. The figure 3 shows the sign - up page for registration of every user, the system stores every user's information as a template which is stored in the system database.

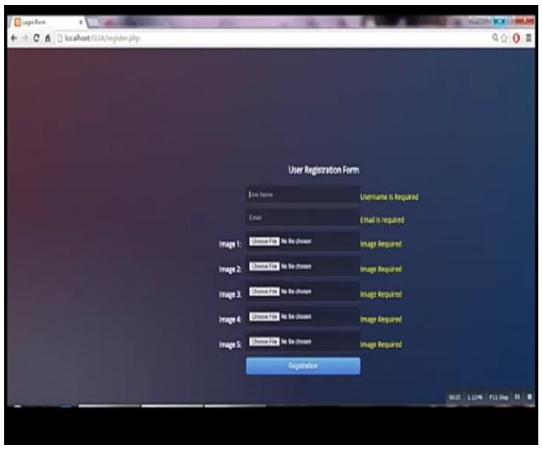

Figure 3: User personal information

The system will pop-up different images and the user will select system six different images, when the images are submitted the system stores them in matrix form. The system will pop-up another set of images and the user will select another three different images which will be multiplied with the

set of six already stored by the system. The result of multiplying two sets of matrices form a multiplied matrix which form a detection system. The figure 4 shows the set of images in the system.

Figure 4: Set of images for user Registration

The set of images are randomly pop – up each time that the user wants to register or login, the system does the randomization in such a way that locations of images cannot be the same at every login. The exact images used for registration must be selected in every login. The system performs multiplication matrix on the selected images. If the registered images match the login images then the user will be activated while the user will be deactivated when login images do not match images. The system prevents shoulder surfing attack by finding the relationship between M_{reg} and M_{aut} .

3.4 Result

The system attained high degree of accuracy when it was tested in software laboratory at federal polytechnic, Ilaro. The system restricts non-register students to use the computers in the laboratory.

3.5 Performance Evaluation

This work was benchmarked with the PassMatrix method, in the PassMatrix the pass-image will be shown on the display, with a horizontal bar and a vertical bar on its top and left respectively. This horizontal bar and a vertical bar of pass–image can be easily captured and memorized by the adversary; that is shoulder surfing attack is still possible in the PassMatrix method. But it was observed that the multiplied matrix is accurate because set of images were randomly generated each time that the user wants to register or login. A multiplied matrix which form a detection system difficult for adversary to easily locate the position of images during login, and equation 3 and 5 cannot be seen by the adversary.

CONCLUSION

In order to protect user's information and property such as personal computer, authentication is required every time the users want to access their personal account and data. However, the strong graphical authentication process in public might result in potential shoulder surfing attacks. Even it cannot be cracked easily as the adversary cracks textual password or PIN method.

REFERENCES

[1] **Harsh K. Sarohi and Farhat U. Khan**, 2013. Graphical Password Authentication Schemes: Current Status and Key Issues. ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784

[2] **Dhanashree K.** 2017. Different Graphical Password Authentication Techniques. *International Conference on Emanations in Modern Technology and Engineering (ICEMTE-2017)* Volume: 5 Issue: 3

[3] **Phen-Lan Lin, Li-Tung Weng and Po-Whei Huang**. 2008. Graphical passwords using images with random tracks of geometric shapes. *Congress on Images and Signal Processing.* 2008

[4] **Saranya R. and Bindhu J.** 2014. A Survey on Different Graphical Password Authentication Techniques. Vol. 2, Issue 12

[5] **Nelson, D.L., U.S. Reed, and J.R. Walling**, 1977. Picture Superiority. *Journal of Experimental Psychology: Human Learning and Memory* 3, Pp 485-497

[6] **G. Blonder**, 1996. Graphical Password. *In Lucent Technologies*, Inc., Murray Hill, NJ,United States Patent 5559961

[7] **S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon**, 2005. Authentication Using Graphical Passwords: Basic Results. *In Human-Computer Interaction International* (HCII 2005), Las Vegas, NV

[8] **S. Madigan**, 1983. Picture memory, in Imagery, Memory, and Cognition: *Essays in Honor of Allan Paivio, J. Yuille, Ed. Lawrence Erlbaum Associates*, ch. 3, pp. 65–89.

[9] **Shraddha S. Banne1, Kishor N. Shedge**. A Review of the Graphical Password Based Authentication Schemes

[10] **E. Stobert, S. Chiasson, and R. Biddle**, 2011. User-choice patterns in PassTiles graphical passwords. *In Annual Computer Security Applications Conference* (ACSAC). IEEE, 2011

[11] **H.C.Gao, X.Y.Liu, S.D.Wang and R.Y.Dai**, 2009. A new graphical password scheme against spyware by using CAPTCHA. *In: Proceedings of the symposium on usable privacy and security*, 15-17 July, 2009

[12] *** Passlogix, http://www.passlogix.com