GRAPHICAL PASSWORD AUTHENTICATION USING IMAGE SEGMENTATION FOR A SECURE PERSONAL MOBILE PLANNER SYSTEM

[1]Phang Hui Hui, [2]Mohd Rizuan Baharon, [3]Syarulnaziah [4]Anawar, Ariff Idris
[5]Hairol Nizam Mohd Shah[2], [6]Aine Mac Dermott
[1,2,3,4,5]Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.
[6]Department of Computer Science, Liverpool John Moores University, L3 3AF, Liverpool, United Kingdom.

Presented at International Symposium on Research in Innovation and Sustainability 2019 (ISoRIS '19) 28 -29 August 2091, Penang, Malaysia.

ABSTRACT**:** *A password authentication mechanism is the most common authentication method. However, some of these mechanisms such as textual or alphanumeric passwords have their own weaknesses. In addition, critical systems such as a personal mobile planner system require a strong authentication mechanism to protect users' information from being disclosed to outsiders. Therefore, a graphical password authentication using image segmentation is proposed in this paper. This graphical password leverages the image segmentation approach for simplicity and eases to memorize. The paper proposes a secure authentication approach by providing three security levels. The proposed authentication method is implemented and tested in a personal mobile planner system. This system allows a user to choose the segmented image to be a password. With the aid of such a system, the proposed authentication mechanism is validated. The result shows that the proposed authentication mechanism offers better advantages and solves some limitations in the existing textual or alphanumeric password.*

Index Terms: Mobile Device, Authentication, Graphical Password, Image Segmentation

I. INTRODUCTION

Nowadays, user authentication is an essential issue in the field of information security. Authentication is a process of deciding whether a user should be allowed to access a system or resource [1]. The authentication process includes the validation of user information with the database information. Users will be granted to access the system if the information matches the database information [2]. The form of authentication that is most frequently used is a password. A password is a form of secret authentication that is used to verify access to records. Password has been used as the unique code to identify the malicious users and to secure computer operating systems, mobile phones and others. In some systems, the password is encrypted to protect its confidentiality [3, 4].

A good password requires some characteristics to be fulfilled such as minimum password length, alphanumeric, and containing symbols. To meet such characteristics leads to some flaws such as hard memorizing the difficult password. Otherwise, the created password could easily be hacked or guessed by attackers [4]. It is difficult to memorize a long password. This leads to the user's tendency to create a simple, short, and insecure password that causes the credential data to be vulnerable to outside attacks. In contrast, a graphical password that uses image segmentation has been developed and it is an alternative way by making the password more memorable and more secure [5]. In this paper, an authentication mechanism based on segmenting the images is proposed and the images will be segmented into numerous fragments [6]. A psychological study says that an individual can remember images easily compared to text [7]. The rest of this paper is briefly described as follows. Section 2 explains the background of the related works. Section 3 illustrates the proposed authentication mechanism to be implemented by the personal mobile planner system. Section 4 demonstrates the application settings and experimental results of our scheme are given in detail, and discussions on the scheme's performance are presented. Finally, the conclusion is given in section 5.

II. RELATED WORK

An alphanumerical password is the most common authentication mechanism [8, 9]. In the year the 1960s, alphanumeric password was first introduced for security purpose to secure confidential data. There are some characteristics for alphanumeric passwords have been proposed such as the password should be at least 8 characters, should not be simple and relate to the user, should not be a word that can be easily found in the dictionary, and should use the combination of upper-case, lower-case letters and digits [9]. However, the alphanumeric password has some vulnerability and usability limitations such as a long and difficult password are hard to be memorized, while a short and simple password is easy to be guessed and hacked by the attackers [8]. The alphanumeric password which has a short and simple password does not fulfill the requirements of a password that are related to the field of security and memorability [10]. Hence, the alphanumeric password should be improved in terms of its password length to strengthen its security performance. A password length is a policy that prevents the user from selecting passwords that are too short and simple. Based on the password policy, the length of the password should be at least 6 to 8 characters. Some system only requires a shorter length such as a 4-digit PIN (Personal Identification Number) number while some enforce user to choose a longer password that is at least or equal to 8 characters [11]. In addition, the usage of longer passwords will increase the time taken for a hacker to crack a hashed password if a database is being compromised [12].

On the other hand, Draw A Secret (DAS) is one of the graphical password authentication schemes which requests the user to draw a pattern on a 2D grid of size $G \times G$. The pattern may contain single strokes or multiple strokes depending on user preferences. The values of touch grids are stored in the order of drawing [7]. During the authentication process, the user needs to redraw the pattern in the same way as it was drawn in the registration stage. If the redraw pattern matches the same grids in the same sequence, then the user is granted to access the system [13]. Figure 1 shows the example of the DAS scheme.

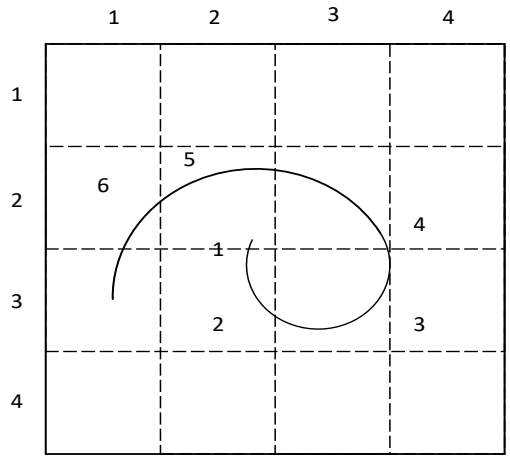

Figure 1: DAS Scheme

However, the DAS scheme also has some disadvantages. One of the disadvantages is hard to memorize the exact and accurate stroke order. It is difficult to redraw the same pattern as it was drawn before. This causes the user fails to recall the password and cannot log in to the system. Moreover, this scheme is not user-friendly and will bring some difficulties to the user. If the user is not familiar with some input devices such as a mouse or joystick, then the user will be struggling while using the authentication scheme [14]. In contrast, a graphical password could provide a strong authentication mechanism to a user and protects the user data from unauthorized access to the user's system. The main objective of graphical password authentication by image segmentation is to provide strong security and a simple interface to the system. It provides a unique method which is image segmentation [10].

Furthermore, segmentation of an image in a graphical password authentication mechanism requires the user to select a number of grids on this image. When the number of grids is inserted in a correct sequence, the user is authenticated to access the system [5]. The image is segmented based on the grid size. The segmentation of images depends on the difficulty level. For example, an image can be segmented into a matrix of 6×6, 8×8 or 9×9 [15]. Each piece of a segmented image and each segment of the empty grid is associated with a unique number [10].

This paper proposes an authentication method which is graphical password authentication using image segmentation. This authentication mechanism will be embedded in a schedule planner system for validation purposes. An image will be segmented into the grid and let the user choose a specific segmented image as a password. Users will be granted to access the system when the selected password matches the password during the registration stage. To ensure the security level of the password, the password will be hashed before storing in a database. This authentication method could overcome the problem of other authentication methods such as hard to memorize and vulnerability to brute force attacks.

III. THE PROPOSED AUTHENTICATION MECHANISM

In this section, an authentication method by graphical password authentication using image segmentation is proposed in order to develop a better and a secure personal mobile planner system as shown in Figure 2. The authentication method has a simple user interface that is user-friendly and easy to use. Using an image as the password can let users memorize a password easily compare to textual or alphanumeric characters. The security assumption of this authentication technique is based on the hacker hard to guess the correct order of the password and thus, hard to hack the system. Therefore, this system can protect the daily routine of users from being exposed to attackers.

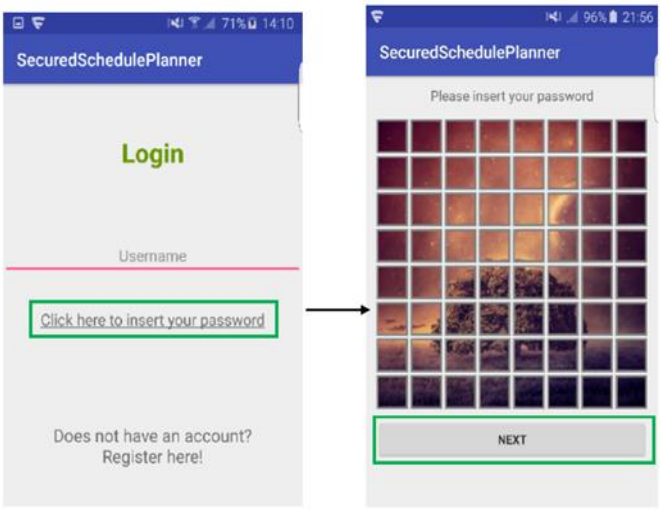

Figure 2: The Proposed Authentication Mechanism

The data processor data flow for graphical password authentication using image segmentation for a secured personal mobile planner system is shown in Figure 3.

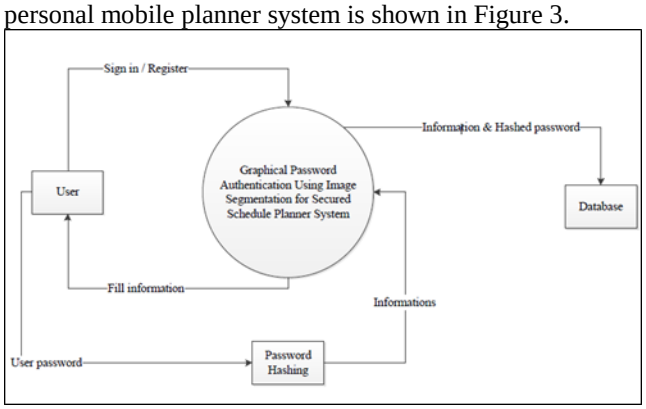

Figure 3: Data Flow Diagram

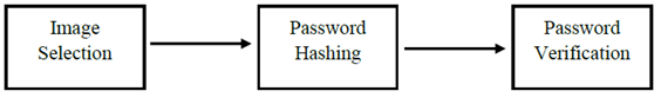

Figure 4: Graphical Password Authentication using Image Segmentation Design

Figure 4 shows the outline for the design of graphical password authentication using image segmentation. There are three modules for the design which are image selection, password encryption, and password verification. These three modules are the focus part of this paper to develop an authentication method by using an image segmentation approach.

A. Image Selection

An image is a visual representation of an object, it is a picture that has been created and stored in electronic form. For the image selection part, a default image is segmented into $8 \times 8$the grid and produces a total of 64 pieces of segmented images. The 64 pieces segmented image is used as user password input. User selects at least six pieces of the segmented image that they wish to remember a password. Figure 5 shows an image that has been segmented into 64 pieces of segmented images.

Figure 5: Default Segmentation Images in 8×8 Grid

The effectiveness of a password against brute force attack or guessing can be measured by using the concept of password strength. The password strength in this paper is measured depending on the size of the image segmentation and the length of the password. The following shows the formula to calculate the strength of the password.

$$L = \frac{H}{(log_2 N)} \quad (1)$$

Where L = length of the selected password, H = strength in bits and N = size of the set.

B. Password Hashing

Hashing is a type of algorithm which takes any size of data and turns it into another string and length of data which is known as a hashed password. Hashing performs a one-way function on a password so that the data cannot be reversed. Without hashed password, any passwords that are stored in the database can be stolen if the database is being compromised. If attackers get the plain text of the password, they can compromise the system and steal the credential information of the user. Therefore, by applying a hashing algorithm to a user's passwords before storing them in the database, it can prevent an attacker from retrieving the passwords in plain text and can secure the password.

To make the password hashing more secure, it requires to have a unique salt per password. Salt is a random string of data used to modify a password hash. The addition of salt can make it more difficult for an attacker to break into a system by using password hash-matching strategies. This can prevent an attacker from guessing the password by using dictionary attacks or Rainbow Table lookups attack. Therefore, the password hashing part for this system will be adding salt to the hashed password to increase the security level of the password.

C. Password Verification

Password verification is an important process because it will determine the identity of a user and only allow an authenticated user to enter the system. For the password verification process, if the hashed password from the login phase is identical to the hashed password stored in the database, the user will be authenticated and have the right to access the system. On the other hand, if the hashed password from the login phase is different from the hashed password that is stored in the database, the user is failed to authenticate and cannot log in to the system. The following is the code used for password verification.

```
if (password_verify($password, $UserPassword))
```

where $password = password that user enter in login form and $UserPassword = hashed password in database. So, if $password is the same as $UserPassword, then the user is authenticated and can log in to the system successfully.

IV. RESULT AND DISCUSSION

This section demonstrates the result of password strength selection based on the proposed segmented images in 8×8 grid. The following result shows the steps for identifying the password strength.

Claim 1: The strength of a password.

Let the length of the selected password, $L = 8$, and the size of the set, $N = 64$. Based on the Equation (1),

$$H = L \times log_2 N = 8 \times log_2 64 = 48$$

Thus, the bits of strength is 48 bits. This result shows that the password strength of the minimum requirement of a password is 48 bits of strength. 8 selected segmented images are chosen as a minimum requirement for a low password strength based on the traditional password key length.

Claim 2: Weak Password Strength.

Let the length of the selected password, L such that $8 \leq L \leq 12$, and the size of the set, $N = 64$. Based on the Equation (1),

$$H = L \times log_2 N = 8 \times log_2 64 = 48$$
$$H = L \times log_2 N = 12 \times log_2 64 = 72$$

From the above calculation, the password strength for the weak password is approximately 48 to 72 bits of strength.

Claim 3: Medium Password Strength.

Let the length of the selected password, L such that $13 \leq L \leq 21$, and the size of the set, $N = 64$. Based on the Equation (1),

$$H = L \times log_2 N = 13 \times log_2 64 = 78$$
$$H = L \times log_2 N = 21 \times log_2 64 = 126$$

From the above calculation, the password strength for the medium password is approximately 78 to 126 bits of strength.

Claim 4: Strong Password Strength.

Let the length of the selected password, $L > 21$, and the size of the set, $N = 64$. Based on the Equation (1),

$$H = L \times log_2 N = 22 \times log_2 64 = 132$$

From the above calculation, the password strength for a

strong password is approximately from 132 bits strength. Such a setting has fulfilled the minimum requirement of key length for AES which is 128 bits. Figure 6 summarizes the number of selected segmented images compared to the password strength.

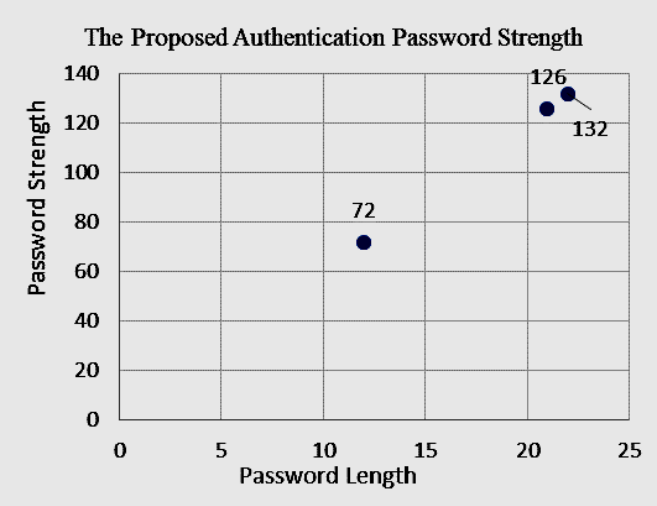

Figure 6: The selection of segmented images versus the Password Strength.

There are many different possible password strengths that can be produced by the default segmented images. However, the number of segmented images can be changed by changing the grid size. For example 9×9, the grid will produce 81 segmented images or 10×10 the grid will produce 100 segmented images. As the number of grid increase, the number of segmented images will also increase. There will be more varied choices of passwords and an increase in password strength. As the password strength increase, the brute force attack will become more difficult. Hence, this can increase the security level of authentication of the system and it will increase the level of difficulty to guess the password.

V. CONCLUSION

In conclusion, graphical password authentication using image segmentation is the best authentication mechanism with tremendous advantages. This mechanism is better in terms of security and easy to memorize compared to textual authentication or alphanumeric authentication. This mechanism can provide a highly secure authentication approach by having features such as using image segmentation as a password, indicating password strength, and hashing function. A secure personal mobile planner system is produced to validate the proposed graphical password authentication which can be used to record the daily life or private life of mobile device users in a secure and protected way.

ACKNOWLEDGMENT

This work has been supported under Universiti Teknikal Malaysia Melaka research grant PJP/2019/FTMK(2B)/S01673. The authors would like to thank Universiti Teknikal Malaysia Melaka and all members of the C-ACT, INSFORNET, and CeRIA research groups for their incredible support in this project.

REFERENCES

[1] S. Ramanan and B. J. S, "A Survey on Different Graphical Password Authentication Techniques," *International Journal of Innovative Research in Computer and Communication Engineering (An ISO Certified Organization)*, vol. 3297, no. 12, 2007.

[2] N. A. Lal, S. Prasad, and M. Farik, "A Review Of Authentication Methods," *International Journal of Scientific & Technology Research*, vol. 5, no. 11, pp. 246–249, 2016.

[3] Richard Duncan, "An Overview of Different Authentication Methods and Protocols," *SANS Institute InfoSec Reading Room*, 2001.

[4] S. S.Ganorkar and P. H. V. Vyawahare, "International Journal of Advance Engineering and Research Development," *International Journal of Advance Engineering and Research Development*, vol. 5, no. 03, pp. 504–508, 2018.

[5] R. Kolay, A. Vora, and V. Yadav, "Graphical Password Authentication Using Image Segmentation," *International Research Journal of Engineering and Technology(IRJET)*, vol. 4, no. 3, 2017.

[6] P. A. S. Sana Ansari, "Implementation of Authentication Mechanism Using Image Segmentation for Web based," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 8, pp. 15619–15625, 2016.

[7] M. A. S. Gokhale and V. S. Waghmare, "The Shoulder Surfing Resistant Graphical Password Authentication Technique," *Procedia Computer Science*, vol. 79, pp. 490–498, 2016.

[8] M. Anwar and A. Imran, "A comparative study of graphical and alphanumeric passwords for mobile device authentication," *CEUR Workshop Proceedings*, vol. 1353, pp. 13–18, 2015.

[9] P. Jadhao and L. Dole, "Survey on Authentication Password Techniques," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 3, no. 2, pp. 67–68, 2013.

[10] R. Koul, T. Kumar, A. Dhongade, R. Malpani, and R. Deshmukh, "GPSI : Graphical Password by Segmentation of Image," vol. III, no. Xi, pp. 57–59, 2016.

[11] L. Zhang-Kennedy, S. Chiasson, and P. Van Oorschot, "Revisiting password rules: Facilitating human management of passwords," *eCrime Researchers Summit, eCrime*, vol. 2016–June, pp. 81–90, 2016.

[12] R. Hicock, "Microsoft Password Guidance," 2016.

[13] Y. D. S. Arya and G. Agarwal, "Impact of Background Images on the DAS (Draw- A- Secret) Graphical Password Authentication Scheme," no. figure 1, pp. 47–50, 2011.

[14] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of Graphical Password Authentication Techniques," *International Journal of Computer Applications*, vol. 116, no. 1, pp. 975–8887, 2015.

[15] S. Ansari and Prof. Avinash Shrivas, "Implementation of Authentication Mechanism Using Image Segmentation for Web based," pp. 15619–15625, 2016.