Safe and Secure Graphical Authentication System

Tushar R. Mahore[1], Prof. A. V. Deorankar[2]

[1]Computer Science and Engineering Department, Government College of Engineering, Amravati, India
[2]Computer Science and Engineering Department, Government College of Engineering, Amravati, India

Abstract: ***Authentication is one of the main aspects in the computer applications, to grant access to particular individual authentication is the process to do that. Lots of research has been done in the development of such authentication scheme, which are simple in user's perspective and is secure in attacker's perspective. Early days of computers belong to the authentication which is based on the text passwords, text-based passwords are the most commonly used authentication scheme in the world. Now days text-based passwords are way too much popular for authentication. On the other hand with the development of handheld devices Graphical Passwords got more attention in the authentication process. The reason behind development of graphical passwords is, they are easy to remember as compared to the text-based passwords. Everything on the internet needs authentication in the way of providing services to the user, so it is important to make sure that the security issues related to the authentication must have been solved by the authentication system. In this way to develop the authentication scheme which is easy to understand and difficult to crack, this research paper is all about. This paper focuses on the research done in the field of graphical passwords and finally we propose a graphical authentication system based on some previous work done. In this paper we are going to see how we can add more security to the authentication process by using the homomorphic encryption in the database.***

Keywords: Draw-a-Secrete (DAS), Passfaces, PassPoints, Homomorphic encryption

1. Introduction

Computer applications need some way to identify the type of user for granting access to the services provided by the particular application. The process of identification is known as the authentication process. Different authentication techniques have been developed in last few decades. Among these techniques text-based password authentication is the most popular one. The reason behind the popularity of text-based passwords is that it promises to provide more security with the selection of strong password. On the other hand in most of the condition where user actually selects passwords, the strong sides of the text-based passwords don't work. What it means is that, choosing strong password is never the priority of the user, how badly they treat the password. In many situations, according to the study by Ofcom, the UK communications watchdog, has putted in front some statistics which reveal just how badly the general public treat password security. According to Ofcom's "Adults Media Use and Attitudes Report 2013" report, a poll of 1805 adults aged 16 and over discovered that 55% of them used the same password for most websites [1]. Practically choosing a strong password and remembering it is not usually the choice of user who does not belong to the computer or have any kind of relation to the computers [2]. Normally selecting the strong password is what the combination of the alphanumeric characters, i.e. it includes some uppercase letters, numbers and some special characters, which in result stays strong against the brute-force attack. But from the user's perspective selection and remembering the strong password is the most difficult task, coz they have multiple accounts, on various websites. Therefore always creating different password for different sites and remembering them is really a tuff task. According to a survey it is found that in most cases user sets same password for his/her different account. In that way, attacker only needs to hack only one password and he gets access to the user's all accounts. According to an article in Computer world, a security team at a large company ran a network password cracker and surprisingly cracked approximately 80% of the employees' passwords within 30 seconds [3]. In general text-based passwords are only useful when they are strong, and is entered in the safe place, so the shoulder surfing attack is not possible.

There are three types of human authentication techniques present, as follows;

- Knowledge based authentication
- Token based authentication
- Biometrics based authentication

Knowledge based passwords are those in which what you know is important, i.e. based on the knowledge possessed by the human the authentication has been done. Token based authentication is based what you have, i.e. any kind of card or device which can be used for the identification. For example, an ID card of an employee in the company, this is used for the attendance of the employee. And the third method is the biometric based, in which what you are is important, i.e. fingerprint or retinal scanner is used for the identification.

To solve the problems associated with the text-based passwords, graphical passwords gets more attention, this is because the capacity of human to remember images more than the text. It is found that human being can remember lots of things and in more efficient way by using the images. Lots of graphical authentication schemes have been developed in last few decades as shown in [4], [5], [6], [7]. All of these schemes have some advantages and some disadvantages, taking all these into consideration we have proposed a scheme which is secure and easy to understand. The security is the main issue on the internet. Mainly on the internet the process of identification is very important, in the way of identification we need particularly some of the private information related to the individual. The credentials of the user is very sensitive, it can be used against the user, so the protection of such information is very important. Now to protect such information we don't have too much security. The credentials of a user is stored in the database, so we have to focus on the security of the database also.

The remaining paper is arranged in the following manner part 2 discusses the literature review, part three discusses various attack models, part 4 gives the overview of the proposed system and finally part 5 concludes the paper.

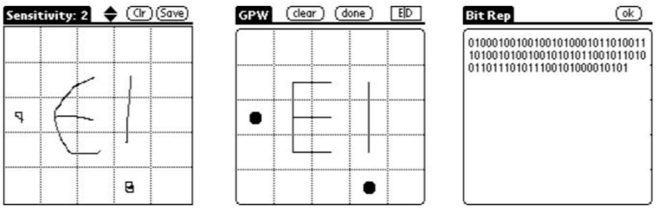
2. Literature Review

As authentication is the important part of the computer field lots of research has been done in last few decades, and various techniques have been developed which day by day increases the security. This paper mainly focuses on the graphical authentication schemes, from which few are discussed, which are more popular. There are other interesting techniques present such as shown in [8], [9], [10], [11], [12], [13] which are not graphical based but needs additional hardware such as audio, gyroscope, vibration sensor etc. Let's see few of the popular graphical authentication schemes.

In 1996 the first idea of the graphical password scheme has been proposed by Blonder. In Blonder's scheme, an image is displayed in front of the user which has predetermined images on any visual display containing device. Then the user has to select particular positions on the image in particular order to access the particular resource [3]. The disadvantage of this technique is that the user cannot click other position than the known position. Mainly there are two types of graphical password schemes i.e. recall based and recognition based. Following are some of the techniques which are more popular than the others.

2.1. Draw-a-Secrete (DAS)

Draw-a-Secrete (DAS) [6] in 1999 was proposed by Jermyn et al. This is an example of recall based graphical password technique. In this scheme the picture is drawn on the grid. This scheme allows users to draw set of gestures for authentication. The drawing of the user is mapped to the grid on which the orders of co-ordinate pair used to draw the password are recorded in a sequence. Following Figures are directly extracted from [6]. The problem associated with this scheme is, it is vulnerable to the attacks like, Multiple Accepted Passwords, Graphical Dictionary Attacks, Shoulder Surfing Attacks.



```
010001001001001010001011010011
101001010010010101011001011010
011011101011100101000010101
```

Figure 1: (a) User inputs desired Secrete, (b) Internal representation, (c) Raw bit string

2.2. Passfaces

Passfaces [14] is one of the most studied scheme, due to its simplicity and easy to implementation way. User pre-selects a set of human faces. At the time of login a set of faces has been presented to the user, among these faces user must select the faces belonging to their set. User has to go through several such rounds, and for successful login, each round must be executed successfully. A study Tari et al. [15] shows that password entry for passfaces using keypad rather than mouse is less vulnerable to the shoulder surfing attack. The following figure shows the example of passfaces. Similar to the passfaces a story system which is proposed by Davis, Monrose and Reiter [16] has been developed in which users first select a sequence of images for their portfolio. Then for log in, users are presented with one panel of images and they must identify their portfolio images from among decoys. Story introduced a sequential component: users must select images in the correct order. To aid memorability, users were instructed to mentally construct a story to connect the everyday images in their set. This scheme is pretty much helpful in the way of memorizing the passwords.

Figure: Passfaces system. Left: sample panel from the original system [16]. Right: panel with decoys similar to the image from the user's portfolio [17].

2.3. Déjà Vu

In Déjà Vu [16] scheme user selects set of images for their portfolio and memorizes it, the images are selected form the random art image set. For the login purpose the user must recognize images belonging to their predefined portfolio from a set of decoy images. Figure 3, shows the example of the Déjà Vu scheme. Déjà Vu was asserted [17] to be resistant to dictionary attacks because few of the images from the set are selected by multiple users. Participants found it difficult to identify their portfolio and those with the same images gave different descriptions from each other.

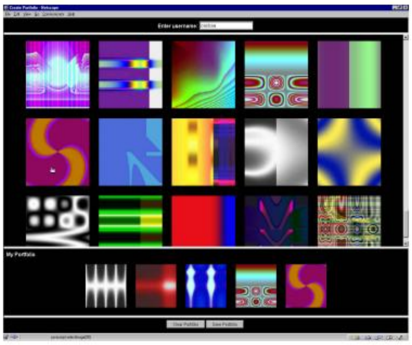


Figure 2: Déjà Vu [17]

2.4. PassPoints

PassPoints [7] scheme is introduced in 2005 by Susan Wiedenbeck et al. at that time the hand held devices have high graphical resolutions and color pictures. In this scheme the user has to click on the set of predefined pixels on the predestined photo, as shown in Figure 4, with the correct sequence and within their tolerant squares during the login stage. As in this scheme user has to select the pixels by using the mouse click, the scheme is vulnerable to the shoulder surfing attack. One of the advantages of the PassPoints scheme is that user can select any random image, as compared to the work done previously in this kind of techniques.

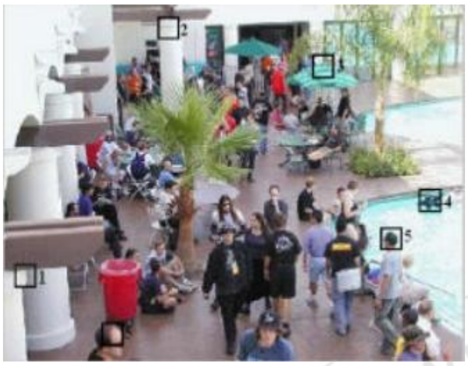


Figure 3: Pixel squares selected by users in PassPoints [7].

2.5. Fake Pointer

To avoid shoulder surfing attacks with the help of video capturing, FakePointer [17] was introduced in 2008 by T. Takada. Below Figure 5, shows the use of FakePointer. The user will get answer indicator every time for the authentication process. In other words the user has two secrets for authentication. PIN as a fixed secret and an answer indicator as a disposable secret. The answer indicator is a sequence of n shapes if the PIN has n digits. Every time at login, the image of numeric keypad with 10 numbers is presented to the user, with each key on the top of randomly picked shape. The numeric keys can be moved circularly but not the shapes using left or right arrow keys. For authentication the user must repeatedly move the keys until the first digit of the PIN overlaps the first shape of the answer indicator.

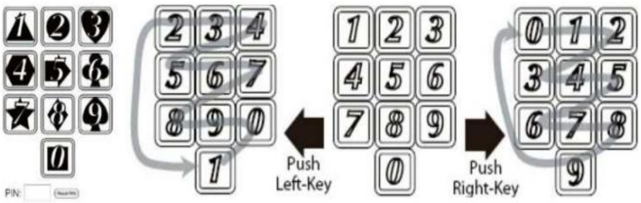


Figure 4: FakePointer where user moves the numeric keys circularly using right and left arrow keys.

3. Attack Models

In this section we are going to take a look on the possible attacks on the authentication schemes.

- Eavesdropping attack
- Man-in-the-Middle attack
- Brute Force attack
- Insider attack
- Keylogger
- Shoulder surfing
- SQL injection

In eavesdropping, an attacker observes and taps the information that goes on the wire and uses it for the future purpose. It is kind of a replay attack, it can be network eavesdropping or offline eavesdropping. MITM is a kind of eavesdropping attack, in this attack an attacker comes in between the customer and the website and all the communication goes through the attacker. He can alter, delete, copy the data transferred between the host and the client. Brute force attack is the type of attack in which the attacker tries all the possible combination to gain access to the particular user account. This is the most common attack used by the attackers, in text-based passwords if the password is weak then the brute force attack is possible. Another type of attack is the insider attack, in which a particular authority from the inside of an organization hacks the user credentials. Keylogger is one of the popular tools used to hack the user accounts. In this attack the keylogger tool keeps tracks of the key strokes and from which attacker can gain access to the credentials of the user. The most common type of attack is the shoulder surfing attack, in this attack the attacker can directly observes the entered password or uses the external video recording devices to gain access to the user credentials. SQL injection is the type of attack in which an SQL query is fired externally into the database, which in result gives credentials to the attacker.

All of the above mentioned attacks are the most common attack, any authentication which is developed considers all the above attacks, and makes their system better. Among all of the authentication schemes not each and every system is made secure from all of the above attacks. The following proposed system considers all the attacks and resists most of them.

4. Proposed System

The proposed system is based on the PassMatrix scheme which has been recently developed by Hung-Min Sun, Shiuan Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng in 2016. In this authentication scheme to make it shoulder surfing resistant scroll bars are used and one time password is generated. The following figure shows the components of the System. The system is proposed to be implemented on the web. The difference in this method and the earlier proposed method is that, the login indicator is generated once, and all the images for authentication is displayed on a single web page.

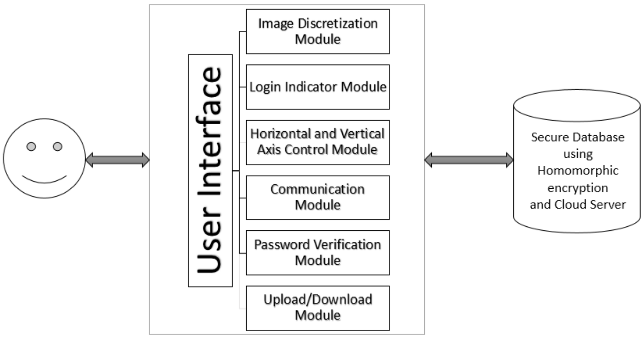

User Interface
Image Discretization Module
Login Indicator Module
Horizontal and Vertical Axis Control Module
Communication Module
Password Verification Module
Upload/Download Module
Secure Database using Homomorphic encryption and Cloud Server

Figure 5: Authentication scheme modules

The very first module in this system is the image discretization module, in which image is divided into grid as per the user specification of the number of rows and columns. Then the second module is the login indicator module, in which the login indicator is generated for the one time use, for authentication. Horizontal and vertical axis control module helps to resist from the shoulder surfing attack. The other modules are communication, password verification, upload/download modules which are used for communication between database server and client server, then verification of the password and the upload/download module is used for the storage space. The last and very important module is the Homomorphic encryption database, here the total credentials of the user is stored in encrypted format. The proposed system has two phases which are registration phase and the login phase. In the registration phase the user has to create his own password from the given images or his own choice of image. In the login phase the process of authentication has been done and the user is redirected to the upload/download page.

5. Conclusion

From the above survey on various graphical password schemes and the attack models we have concluded that, there is a need of development of such authentication scheme which resists most of the attacks models. The proposed system can be implemented in the future work. Graphical authentication is the new way of the authentication on web applications, to provide more security we think that graphical authentication schemes are supposed to be used.

References

[1] "55% of net users use the same password for most, if not all, websites. When will they learn?" https://nakedsecurity.sophos.com/2013/04/23/users same-password most-websites/

[2] S. Sood, A. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 1–7.

[3] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, 2005.

[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[5] "Realuser," http://www.realuser.com/.

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no.1-2, pp. 102–127, 2005.

[8] A. De Luca, M. Harbach, E. von Zezschwitz, M.-E. Maurer, B. E. Slawik, H. Hussmann, and M. Smith, Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers," in Proceedings of the 32Nd Annual ACM Conference on Human Factors in Computing Systems, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 2937–2946.

[9]] E. von Zezschwitz, A. De Luca, and H. Hussmann, "Honey, i shrunk the keys: Influences of mobile devices on password composition and authentication performance," in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI '14. New York, NY, USA: ACM, 2014, pp. 461–470.

[10] A. Bianchi, I. Oakley, V. Kostakos, and D. S. Kwon, "The phone lock: Audio and haptic shoulder-surfing resistant pin entry methods for mobile devices," in Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction, ser. TEI '11. New York, NY, USA: ACM, 2011, pp. 197–200.

[11] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in Proceedings of the SIGCHI Conference in Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.

[12] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp '12. New York, NY, USA: ACM, 2012, pp. 611–612.

[13] G. E. Blonder, "Graphical passwords", in Lucent Technologies, Inc.,Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.

[14] Passfaces Corporation. The science behind Passfaces. White paper, http://www.passfaces.com/ enterprise/resources/white_papers.htm, accessed July 2009.

[15] F. Tari, A. Ozok, and S. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In 2nd ACM Symposium on Usable Privacy and Security (SOUPS), 2006.

[16] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.

[17] T. Takada, "fakepointer: An authentication scheme for improving security against peeping attacks using video cameras," in Mobile Ubiquitous Computing, Systems, Services and Technologies, 2008