NOVATEUR PUBLICATIONS
International Journal of Research Publications in Engineering and Technology [IJRPET]
ISSN: 2454-7875
VOLUME 3, ISSUE 3, March-2017

SECURE GRAPHICAL PASSWORD SCHEME

TUSHAR R. MAHORE
Computer Science and Engineering, Government College of Engineering, Amravati, India, mahoretushar@outlook.com

PROF. A.V.DEORANKAR
Computer Science and Engineering, Government College of Engineering, Amravati, India, avdeornakar@gmail.com

ABSTRACT:

In the world of computer applications authentication is the main process of granting access for an individual to get control over the services provided by different service providers. It is the process of identification of particular individual, unique username and password are used. Username and text-based password are the most commonly used technique in authentication, use of this technique is very popular in web applications. Lots of work has been done in the field of authentication. Conventional technique includes the text-based password, which is the combination of alphanumeric letters. On the other side of the authentication Graphical Password techniques are popular among handheld devices, the main motivation behind developing such kind of authentication technique is to provide strong but easy to remember password. Graphical authentication schemes are in use from decades, they have some limitations in early days, but comparatively the schemes which are in use today are secure and trust worthy. In this paper a technique for graphical authentication has been proposed based on the previous work, which can be implemented on the web application. The proposed authentication scheme is made secure using the homomorphic encryption technique to avoid the security issue in database.

KEYWORDS: DAS (Draw-a-Secrete), Homomorphic encryption, PassMatrix, Passfaces.

I. INTRODUCTION:

Conventional technique, in which the combination of username and alphanumeric password is used for authentication is the basic way for granting access to the application. The problem associated with the conventional technique is the selection of alphanumeric password. Alphanumeric password is the combination of uppercase letters, lowercase letters, special symbols and numbers, for example "FJH6900@kert7" is considered as strong password. For generating such kind of passwords instructions are associated with the particular application, they help you to generate strong passwords, which are secured against various types of attacks. It has been made clear that, one cannot use their name or birth date or any kind of personal information, while creating the password. By considering all these aspects one can generate a strong password, which is difficult for cracking by the attackers. But the main issue associated with such kind of password is on the user point of view. Users of the computer applications are not familiar with the security issues, user creates passwords for their ease of use. How badly the user treats the password security is an interesting fact. 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]. One another interesting thing found is that most of the users uses same passwords for their multiple accounts, which gives attackers an advantage. 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 [2]. Again remembering such kind of passwords is the difficult task for those who are not related to the computer field [3]. The text based password are only useful when the password is created by considering all the instructions, i.e. only strong passwords are the most secured passwords to use, and strong passwords are not of the users choice.

Different human authentication techniques includes following types:

1. Knowledge based authentication
2. Token based authentication
3. Biometrics based authentication

Every above mentioned type of human authentication is different in their own way, some of them uses hardware which are expensive for implementation point of view. Some uses tokens for authentication, and some of them are knowledge based, in which the user possessed knowledge is used for authentication. Graphical authentication is knowledge based authentication technique.

In graphical authentication system the issue related to the users are considered and the schemes are created, such that easy remembering passwords can be generated and which will provide security similar to the alphanumeric passwords. Graphical authentication schemes uses the capacity of a human being of remembering images rather than the text, this can be taken as an advantage for creating the authentication scheme based on the images. Lots of

graphical authentication schemes are present in the computer world, such as shown in [4],[5],[6]. Using the human ability of remembering images, a scheme can be developed which generates strong password but which can be easy to remember. The security issue related to the graphical authentication schemes is that, they are vulnerable to shoulder surfing attacks. The proposed scheme is developed in such a way that, to resist the shoulder surfing attack. For shoulder surfing attack the attacker can use recording devices for capturing images on the screen or direct observation.

Graphical authentication scheme which is proposed in this paper is resistant to shoulder surfing attack, and is able to generate strong password. The authentication security is not only about the username and the password, the security also includes various aspects, such as network security, database security and much more. In this paper database security is taken in consideration and an homomorphic scheme, which is a one way encryption technique is given in proposed system. Below mentioned secure graphical authentication scheme is based on PassMatrix technique [7], which is originally implemented as mobile application.

The paper is arranged in the following way, section 2 describes the work done in last few decades for graphical authentication scheme, section 3 describes the proposed scheme, and finally section 4 concludes the paper.

II. RELATED WORK:

Since 1996 when Blonder first introduced the world to the graphical authentication, various advances has been made. In Blonder's scheme, in front of user an image is displayed which is predetermined image on any visual display device which user is using then user has to select one or more positions on image which are already known positions to user in a particular order to access the particular resource [8]. The problem associated with this technique is that users cannot click other positions than known positions. The researches done on the graphical authentication schemes leads to some of the most promising. There are some other schemes are present such as shown in [9][10][11][12][13], which are not that much popular, and they need some additional equipment's or we can say that the hardware. Following are some popular graphical authentication schemes.

A. DAS (DRAW-A-SECRETE):

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

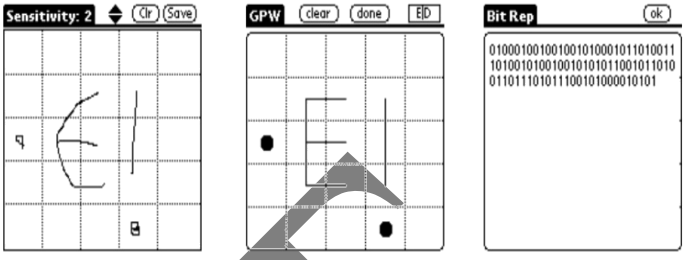

Fig. 1 (a) User inputs desired Secrete. (b) Internal representation, (c) Raw bit string

B. PASSSFACES:

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 set of various faces has to be put in front of user among which the user has to select only those faces which belongs to particular his image 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 pass faces.

Fig. 2 Passfaces system. Left: sample panel from the original system [16]. Right: panel with decoys similar to the image from the user's portfolio [17].

Similar to the Passfaces technique a Story system is proposed by Devis, Monrose, and Reiter [18]. In this scheme a user have to select some images for his/her 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.

C. PASSPOINTS:

Pass Points [19] 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 3, 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.

Fig. 3 Pixel squares selected by users in PassPoints [19].

III. 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.

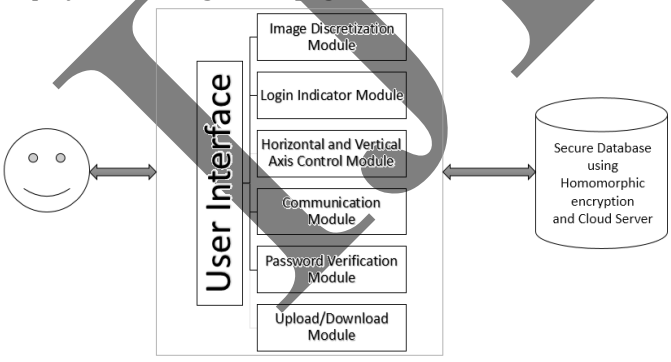

Fig. 4 System Components

A. Image discretization module:

This module divides the image into squares, from which user would choose one as the pass square. The smaller the image is discretized the more the password space is.

B. Login indicator generator module:

It generates a login indicator consisting of several distinguishable characters (such as alphabets and numbers) or visual materials (such as colors and icons) for user during the authentication phase. One principle is to keep the indicators secrete from the people other than the user.

C. Horizontal and vertical axis control module:

There are two scroll bars: a horizontal bar with a sequence of letters and a vertical bar with a sequence of numbers. This control module provides drag and scroll functions for users to control both bars. Users can scroll either bar using the arrows provided to shift one alphanumeric at a time. They can also shift several checks at a time by dragging the bar for a distance. Both the bars are circulative.

D. Communication module:

This module is in charge of all the information transmitted between the client devices and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

E. Password verification module:

This module verifies the user password during the authentication phase. Pass square acts similar to a password digit in the text-based password system. The user is authenticated only if each pass-square in each pass-image is correctly aligned with the login indicator.

F. Upload/Download module:

As the authentication system is implemented as an authentication for the web application which provides the storage space to the user as the cloud service. The user is going to have his/her personal space over the cloud in which one can upload or download his/her files.

G. Database

The database server contains several tables that stores user accounts, passwords (ID numbers of pass images and the positions of pass squares), and the time duration each user spent on both registration phase and login phase. Using FHE the contents in the database is encrypted, and to efficiently check the equality the FHE scheme done the equality check without decryption. This module plays an important role in improving the security in the database.

The system includes two phases, registration phase and authentication phase. In registration phase the user is allowed to select the grid layout as per his/her choice, then the user is supposed to be selecting the pass image, which is used as the password in the authentication phase. Here the more complex the grid selection is, the more complex is the password. At the authentication phase, a login indicator has been generated, and given to the user through various ways, such as audio, visual or

text. Then the user is supposed to be setting the scroll bars to the particular known position of the password, by using the horizontal and vertical axis control module.

IV. CONCLUSION:

We have done a survey on various authentication techniques, which in result leads us to develop such graphical authentication scheme, which is very simple in user point of view, but difficult in attacker point of view. This work is all about the proposed system which in future can be implemented as a web application. The work we have done has been totally done by taking the ease of use priority in consideration. Graphical passwords are more popular among non-technical users, so more research can be done in the field of graphical authentication. Graphical authentication is best for handheld devices, but in this work it has been shown that a simple but effective graphical authentication scheme can be developed for other platforms also, such as web applications.

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) K. Gilhooly, "*Biometrics: Getting back to business*," Computerworld, May, vol. 9, 2005.
3) 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.
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
7) conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.
8) Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng *"A Shoulder Surfing Resistant Graphical Authentication System*" IEEE Transactions on Dependable and Secure Computing 2015.
9) G. E. Blonder, "*Graphical passwords",* in Lucent Technologies, Inc.,Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.
10) 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.
11) 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.
12) 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.
13) A. Bianchi, I. Oakley, and D. S. Kwon, "*The secure haptic keypad: A tactile password system,"* in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ser. CHI '10. New York, NY, USA: ACM, 2010, pp. 1089–1092.
14) 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.
15) Passfaces Corporation. The science behind Passfaces. White paper, http://www.passfaces.com/ enterprise/ resources/white_papers.htm, accessed July 2009.
16) F. Tari, A. Ozok, and S. Holden. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords.
17) In 2nd ACM Symposium on Usable Privacy and Security (SOUPS), 2006.
18) D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.
19) P. Dunphy, J. Nicholson, and P. Olivier. Securing Passfaces for description. In 4th ACM Symposium on Usable Privacy and Security (SOUPS), July 2008.
20) D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In 13th USENIX Security Symposium, 2004.
21) 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.