ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

New Graphical Password and Pair Based System to Avoid Shoulder Surfing Attack

Tejashri Dumbre[1], Prof. S. A. Kahate[2]

M.E. Student, Dept. of Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, SPCOE, Otur, Pune, Maharashtra, India[2]

ABSTRACT: Nowadays computer as well as information security is the most significant challenge. Authorized users should access the system or information. Authorization can't occur without authentication. For this authentication various techniques are available. Among them the most popular and easy is the password technique. Password ensures that computer or information can be accessed by those who have been granted right to view or access them. Traditional password technique is a textual password which is also called alphanumeric password. But these textual passwords are easy to crack through various types of attack. So to overcome these vulnerabilities, a graphical password technique is introduced. As name suggests in this technique images (pictures) are used as a password instead of text. Also psychological study says that human can easily remember images than text. So according to this fact, graphical passwords are easy to remember and difficult to guess. But because of graphic nature, nearly all the graphical password techniques are vulnerable to shoulder surfing attack. So here, a new graphical password authentication technique is proposed which is resistant to shoulder surfing and also other types of possible attacks to some extent. It is a combination of recognition and recall based approach.

KEYWORDS: Graphical Passwords, Authentication, Shoulder Surfing Attack, Authorization.

I. INTRODUCTION

Today, authentication is achieved through the use of password technique. To prove and maintain the identity every user uses a password authentication [1]. From last decades textual password have been the most widely used in authentication. Combination of upper-case, lower-case letters and numbers is the strong password and hard to memorize and recollect. So, user select the short password or they write down the passwords for future instead of random alphanumeric string as password. Also to remember easily, here the passwords are kept simple like personal names, family member names, birth dates, pet names, phone numbers etc. and so vulnerable to various types of attacks like easy to guess, brute force, dictionary attack, shoulder surfing, hidden camera, social engineering and malicious softwares like keylogger, spyware etc.To overcome these limitations users can use the strong (complex) password. But it is difficult to remember. So to memorize easily users write the password on paper and so it is easily available to anyone. So to reduce the shortcomings of textual passwords a new technique is developed which is a Graphical Password and Pair-based system which reduces the shortcomings of textual password.

Graphical Password: As name indicates in this, various types of images or shapes are used as password. Also psychological study says that images can be easily remembered by human than text [4 -7]. Human brains can process images easily. Because of this human characteristic, graphical passwords are superior to textual passwords. As images are used it is resistant to dictionary attack, keylogger, social engineering etc. There are two types of graphical password techniques: Recognition based and Recall based. In Recognition based, various images are presented to the user and from that user has to recognize the right images in a correct sequence. In Recall based, user has to reproduce something that he/she has been created or selected during registration.**Pair-**

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Based System: At the time of registration user has to enter password. The minimum length of password is 8 characters. So at the time of login we create session password based on users original password entered at the registration time by using 8x8 matrix grid provided on login page.

II. RELATED WORK

In this, user is presented with a set of random images during registration. The user has to select the particular number of images from this set as a password. During authentication, user has to recognize those preselected images in a correct sequence.

1.1. Jensen et al. technique [8]: This technique is proposed for mobiles, PDAs. First user is required to select a theme (E.g. Cats and Dogs, Sea and Shore etc.). Images based on theme are shown to user in 5 x 6 grid and also each image is displayed in thumbnail size. To form a password user has to select the images in a sequence. The user needs to recognize the previously selected images and touch it using stylus in a correct sequence for authentication. The number of images here are limited only to 30, so the size of the password space is small. A number is assigned for each image and a sequence of selection will produce a numerical password. Sometimes this numerical password is shorter than the textual password. So to overcome this problem user can select two images at a time on single click to increase a password space size. But this will become more difficult and complex for user.

1.2. ImagePass technique [9]:In this, during registration user is presented with a grid of 30 images. The user has to select images as a password. During login user is presented with a grid of 4 x 3 which is a combination of real and decoy images. From the grid user has to select the real images in a correct sequence for authentication. The image positions will vary at every login. It is not strongly resistant to shoulder surfing as grid is only of size 4 x 3 and also the password images are fixed. So those can be easily seen and remembered by attacker.

1.3. ColorLogin technique [10]: In this, background color is used to decrease the login time. Multiple colors are used to confuse the imposters, but easy to use for authorized users. It is resistant to shoulder surfing attack but the password space, here, is less than text-based password.

1.4. Blonder technique [11]: The graphical passwords were originally described by Blonder. In this, a predetermined image with predetermined tap regions is shown to the user. During registration, for password creation user has to click those tap regions in a particular sequence. For authentication, user has to click the approximate areas of those tap regions in the predefined sequence. The image can assist the user to recall the password and so this scheme is considered as more convenient than textual password. The drawback of this is memorable password space. The user cannot click where he wants because of predetermined tap regions. Also background of image is very simple.

1.5. PassPoints technique [12]: To overcome the limitations of Blonder technique, this technique was proposed. In this, any natural picture/painting is used, which helps the user to remember the click points. Here no need of predefined click points like Blonder technique. During registration, to create a password user can click on any place on the image. The tolerance around each chosen click point is calculated. For authentication, user has to click within tolerances of chosen click points in a correct sequence.

Our proposed technique is easy and resistant to all types of possible attacks specially shoulder surfing to some extent. We have tried here to balance the trade-off between usability and security metrics.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

III. PROPOSED SYSTEM

The proposed system is a modified version of existing system to overcome the limitations of it. It has also two phases.

Proposed System authentication consists of a registration phase and an authentication phase as defined below:

a. Registration Phase:

In this stage, the user creates an account which contains a username and a password. In proposed system, pair-based and graphical password included. For pair-based system user has to enter one password length of minimum 8 character which generates 4 character minimum session password at the login phase.The password consists of only one pass-square per image for a sequence of n images in graphical password. The number of images (i.e., n) is decided by the user after considering the trade-off between security and usability of the system [13]. The only purpose of the username is to give the user an imagination of having a personal account. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either choose images from a provided list or upload images from their device as pass-images. Then the user will pick a passsquare for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

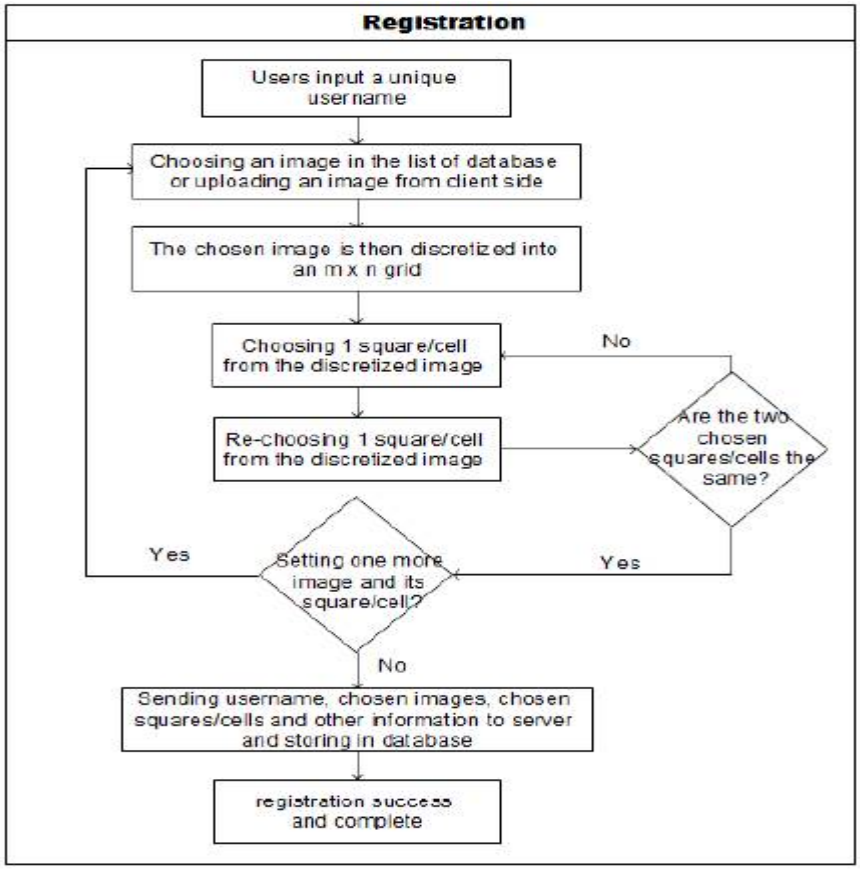

Fig. The flowchart of registration phase in PassMatrix.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

b. Pair-based Scheme: 8x8 matrix is used to represent alphabets, digits and special symbols to the user so user has to select session password by using grid. E.g. Length of the password is 8 and password is ABCDEQRS. Now we will make pairs as AB CD EQ RS .so the session password length is 4. User will select row containing character A and column containing character B. And intersection of that row and column is inserted into the password field likewise all the pairs are selected into the grid and password is entered. This new password is valid only for that session and is stored in the user log on server. The session password and 8x8 grids is sent to the server. On the server side this session password is cross checked with the user's original password [14].

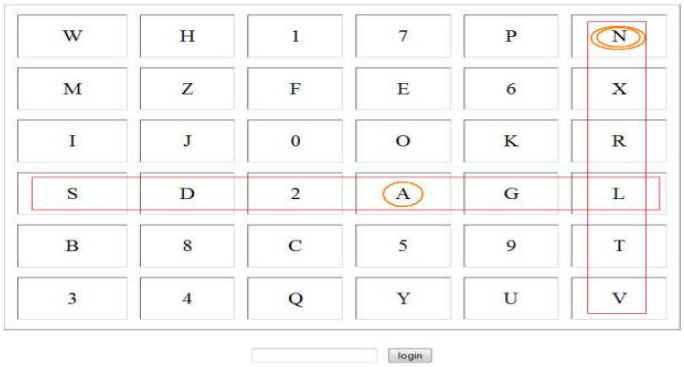

Fig. Pair-based system

c. **Authentication Phase:** At the authentication phase, the user uses his/her username, password and login indicators to log into PassMatrix. The following describesall the steps in detail:

1. The user has enter his/her username which was created in the registration phase.
2. Next, random pass-image will be shown on the user display with vertical and horizontal bar on its left and top respectively. To solve the challenge, the user scroll the bars to select the pre-selected pass-square of the image. For example, if the indicator is (e,10) and the pass-square is at (5, 7) in the grid of the image, the user shifts the character ”e” to the 5th column on the horizontal bar and ”11” to the 7th row on the vertical bar

Fig. The permutations of alpha-numeric in horizontal and vertical bars are randomly generated for each image.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

3. Repeat the step 1 and 2 for another login phase.
4. The communication module gets user account information.
5. Finally, for each image, the password verification module verifies the alignment between the passsquare and the login indicator.

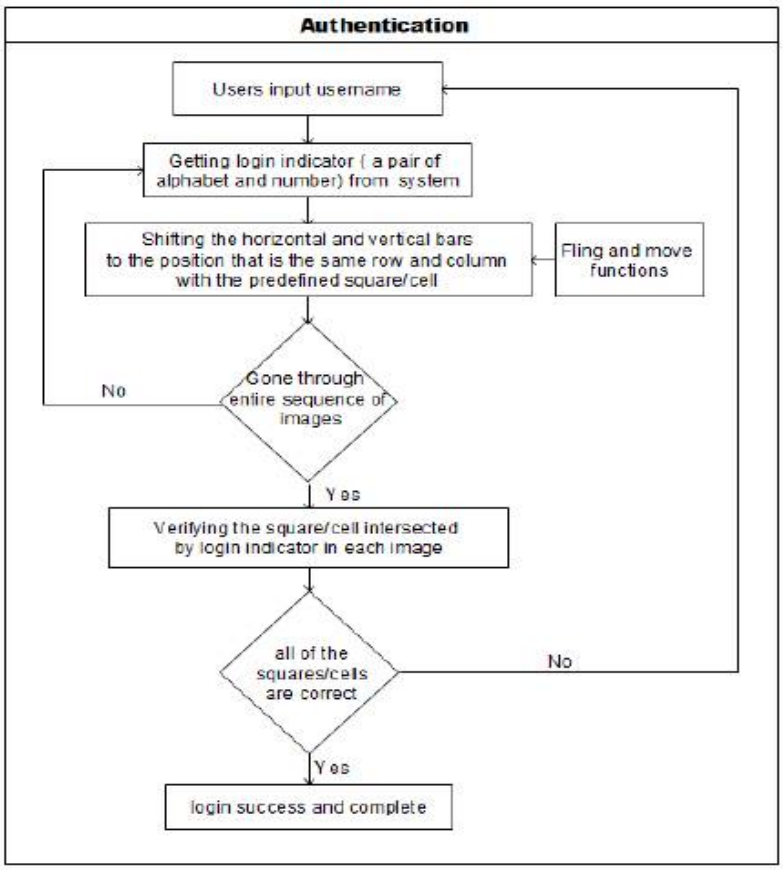

Fig. The flowchart of authentication phase in PassMatrix.

III. ANALYSIS OF THE SYSTEM

A proposed system provides a strong security against brute force and guessing attacks as it has a good combination of two types of graphical passwords. It is difficult to guess the password system by a person or by a computer by trying millions of possibilities. It has a very large password space. In pair-based system, it provides a new password for each session and need not to transfer password form server each time for authentication purpose that's why Session password scheme provides more security than the other existed systems. Also proposed system analysed by collected data to evaluate the effectiveness of the proposed system.

a. Accuracy: for analysis of the proposed system calculate the accuracy.
First accuracy = successful attempts in the first try/total attempts. (1).
Total Accuracy=successful attempts/total attempts. (2).

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

b. Usability: The usability perspective is measured by the amount of time users spent in each PassMatrix phase.

IV. CONCLUSION

Proposed system is a combination of graphical and pair-based approach. It is more usable and secure as compare to previous graphical password authentication systems. As password space is very large it provides the security against brute force attack. It is easy to use. Passwords can be created and memorized easily. Randomization in both the authentication steps provides strong security against shoulder surfing. Overall our system is resistant to all other possible attacks also. This system can be used for highly secure systems. In future, one more addition possible to our system is, if the user forgets any password that password is mailed to user's registered mail id and such a message will be sent to user's registered mobile number also. So user can get the system updates although he is offline. Thus, in future, our system can be made more secure and easy to access.

REFERENCES

[1]. Renaud. "Evaluating authentication mechanisms". In L. Cranor and S. Garnkel, editors, Security and Usability: Designing Secure Systems That People Can Use, chapter 6, pp.103-128. O'Reilly Media, 2005.
[2]. D. Florencio and C. Herley. "A large-scale study of WWW password habits". In 16th ACM International World Wide Web Conference (WWW), May 2007.
[3]. XiaoyuanSuo, Ying Zhu, G.Scott. Owen, "Graphical Passwords: A Survey", Department of Computer Science Georgia State University.
[4]. Kirkpatrick. "An experimental study of memory". Psychological Review, 1:602-609, 1894.
[5]. S. Madigan. "Picture memory". In J. Yuille, editor, Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.
[6]. A. Paivio, T. Rogers, and P. C. Smythe. "Why are pictures easier to recall than words?" Psychonomic Science, 11(4):137-138, 1968.
[7]. R. Shepard. "Recognition memory for words, sentences,and pictures". Journal of Verbal Learning and VerbalBehavior, 6:156-163, 1967.
[8]. W. A. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.
[9]. "ImagePass - Designing Graphical Authentication for Security" Martin Mihajlov E- business Department Faculty of Economics BorkaJerman-BlaziJozef Stefan Institute Ljubljana, Marko IlievskiSeavus Group 2011.
[10]. HaichangGao, Xiyang Liu, Ruyi Dai, "Design and Analysis of a Graphical Password Scheme", International Conference on Innovative Computing, Information and Control (ICICIC), 2009, pp. 675 – 678.
[11]. Susan Wiedenbeck, Jim Waters, Jean - Camille Birget and Alex Brodskiy, Nasir Memon. PassPoints,"Design and longitudinal evaluation of a graphical password system", International Journal of Human-Computer Studies, 63(1-2): 102-127, July 2005.
[12]. Reshma D. Kadam , Swapnil D.Koshti , Amol R.Gawde, Prashant C. Kamble ,"Authentication Schemes for Session Passwords using Hybrid and Paired based Techniques"- Multidisciplinary Journal of Research in Engineering and Technology Volume 1, Issue 2, Pg.175-182, M12-1-2-7-2014