www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 6 Issue 1 Jan. 2017, Page No. 20090-20095
Index Copernicus Value (2015): 58.10, DOI: 10.18535/ijecs/v6i1.41

Graphical Password as an OTP

Veena Rathanavel[1], Swati Mali[2]
[1]Student M.Tech, Department of Computer Engineering,
K J Somaiya College of Engineering, Mumbai.
veena.r@somaiya.edu
[2]Assitant Professor, Department of Computer Engineering,
K J Somaiya College of Engineering, Mumbai.
swatimali@somaiya.edu

Abstract: **The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, some researchers have developed authentication methods that use pictures as passwords known as graphical password. This paper provides additional layer of security to normal textual password by using graphical password for authenticating the user. As graphical passwords are vulnerable to shoulder surfing attack hence one-time generated password is sent to users mobile. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP).The OTP will be the information of the items present in the image to be clicked by the user. The users will authenticate themselves by clicking on various items in the image based on the information sent to them. Additionally, it provides accessibility to visually impaired people.**

Keywords: Graphical password, Authentication, Security, One-Time Password, Visually impaired.

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. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember. Motivated by the promise of improved password usability and security, the concept of graphical passwords was proposed in 1996. Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. Graphical passwords (GP) use pictures instead of textual passwords and are partially motivated by the fact that humans can remember pictures more easily than a string of characters. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface. Graphical passwords may offer better security than text-based passwords because many people, in an attempt to memorize text-based passwords, use plain words. The idea of graphical passwords was originally described by Greg Blonder in 1996. An OTP is a set of characters that can act as a form identity for one time only. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker.

2. Literature Review

Graphical based passwords schemes can be broadly classified into four main categories:

2.1 Recognition Based System

In recognition based systems which are also known as cognometric systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generates then unaided from memory.

Dhamija and Perrig [1] proposed a graphical authentication scheme based on the Hash Visualization technique. In their system, the user is asked to select a certain number of images from a set of random pictures generated by a program. Later, the user will be required to identify the preselected images in order to be authenticated. The results showed that 90% of all participants succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS. The average log-in time, however, is longer than the traditional approach. A weakness of this system is that the server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

"Passface" is a technique developed by Real User Corporation [3]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces (figure 1). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

Figure 1: Passfaces

2.2 Pure-Recall Based System

In recall-based system users need to reproduce their passwords without being given any reminder, hints or gesture.

Blonder [9] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. Passlogix [10] has developed a graphical password system based on this idea. In their implementation, users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse.

The "PassPoint" system by Wiedenbeck, et al. [11] extended Blonder's idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of their chosen pixels and also in the correct sequence

2.3 Clue-Recall Based System

Cued recall based systems which are also called Icon metric Systems. In cued recall-based system, a user is provided with a hint so that he or she can recall his/her password.

Oorschot, and Robert Biddle [12] proposed clued click point. In CCP, users click on one point on each of c = 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. As shown in Figure 2, each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images they could create a new password involving different click-points to get different images.

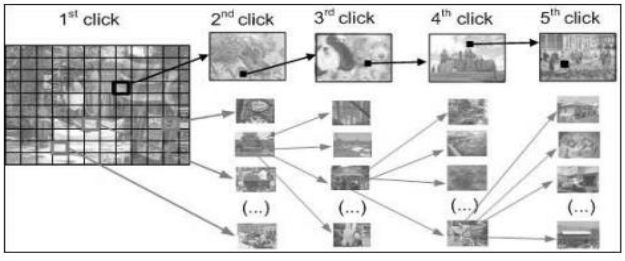

Figure 2: Clue Click Point

2.4 Hybrid System

Hybrid systems are typically the combination of two or more schemes. Like recognition and recall based or textual with graphical password schemes.

Click-Draw Based Graphical Password Scheme [14]: This scheme (CDGPS) combines the merits of PassPoints, DAS and Cued Click Points. Specifically, there are two operational steps in *CD-GPS*: that is, image selection and secret drawing. In the step of image selection which refers to the concept and technique from the choice-based schemes, users are required to choose several images from an image pool in a fixed story-sequence (i.e., selecting and remembering the ordered sequence of images like a story) and then further select some of them (e.g., one or two images) for the following step. The step of secret drawing, which refers to the concepts and techniques from both the click-based and the draw-based schemes, requires users to click-draw something (e.g., a digital number or a letter) on their selected images. In the second step, users should draw their own secrets by using series of clicks.

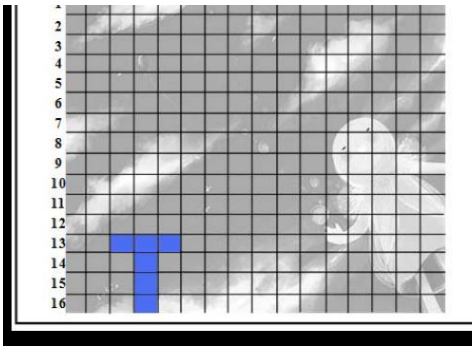

Figure 3: Letter 'T' drawn by a user in the step of secret drawing.

2.5 Existing System

Generation of secure one-time password based on image authentication[16]: Here, The user will be asked to enter his user name, previously selected images (for authentication) and his email. An OTP will be generated following the submission and will be sent to the email id. The user has to enter the particular OTP communicated through mail. If OTP get verified then he will be directed to the home page.

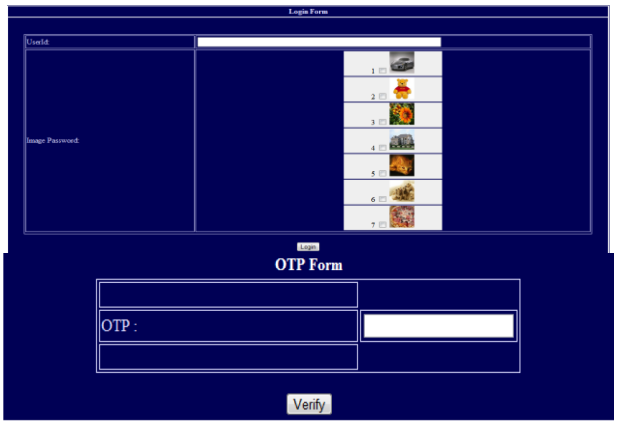

Figure 4: Existing System

3. Security Issues

3.1 Brute Force Attack

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords

tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords.

3.2 Dictionary Attack

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. Overall, graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

3.3 Guessing Attack

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. For example, studies on the Passface technique have shown that people often choose weak and predictable graphical passwords. Nali and Thorpe's study revealed similar predictability among the graphical passwords created with the DAS technique. More research efforts are needed to understand the nature of graphical passwords created by real world users.

3.4 Spyware Attack

Except for a few exceptions, key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether "mouse tracking" spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

3.5 Shoulder Surfing Attack

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition-based techniques are designed to resist shoulder-surfing. None of the recall-based based techniques are considered should-surfing resistant.

3.6 Social Engineering Attack

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

4. Proposed System

Graphical Password as an OTP is based on Passlogix graphical password scheme which is a recall based graphical system. This system is an approach towards more reliable, secure, user-friendly, and robust authentication. It also tries to reduce the various attacks on graphical password and aims to provide a secure authentication.

In addition to the normal way of authentication that is user id and password this system uses graphical password scheme to provide more secured authentication. Here the user needs to provide textual password first and then the user needs to click on few items from an image. The items to be clicked are a one-time password (OTP) which will be sent to the user's mobile number by a text message from a database. The user must click on the sent items on the image provided in order to be authenticated. In addition this system also tries to authenticate the visually impaired people.

This system consists of two phase Registration phase and Login phase to authenticate the user.

4.1 Registration Phase

In Registration phase user registers with the system by providing user id, password and Mobile Number. This information will be then stored in a database which will be used to authenticate the user during login phase.

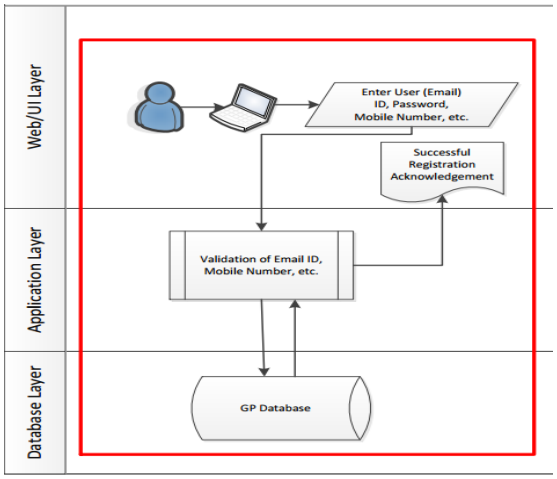

Figure 5: Registration Phase

4.2 Login Phase

In Login phase the user is asked to enter user id and password and an image with several items is displayed to the user. The system then validates the user id and password in the database. If the data matches then the system sends some items from the image to be clicked to the user's mobile number as an OTP. Then the user must click the items in the image in proper sequence. If the user doesn't click the image in some speculated time then the OTP expires. Then a new image is loaded and a new OTP will be send to the user. If the user clicks on time then the system verifies whether the user has correctly identified and clicked the items in correct sequence. If it matches the user is authenticated. Otherwise, whole process will be repeated. If the user is visually impaired (blind people) can hear an audio clip about which items from the image to be clicked. As the user mouse over the items in the images he/she will hear an audio saying the name of the items then the user needs to click on the appropriate items from the image to get authenticated.

DOI: 10.18535/ijecs/v6i1.41

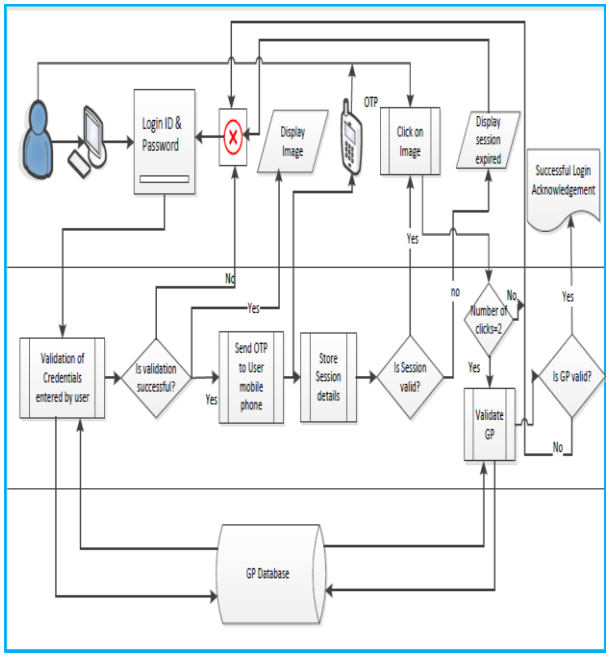

Figure 6: Login Phase

5. Implementation

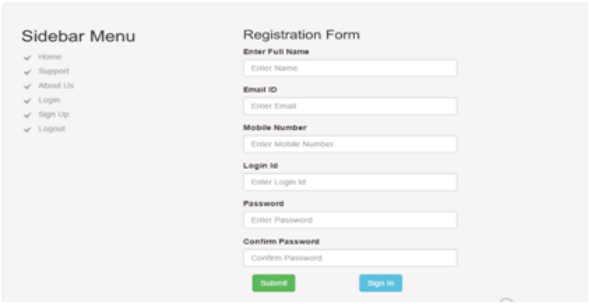

Figure7:Registration

In fig.7 The user is creating a new account. During account creation the user will have to enter his details such as login id, e-mail id, password, Mobile number. User has to enter login ID and password during Login.

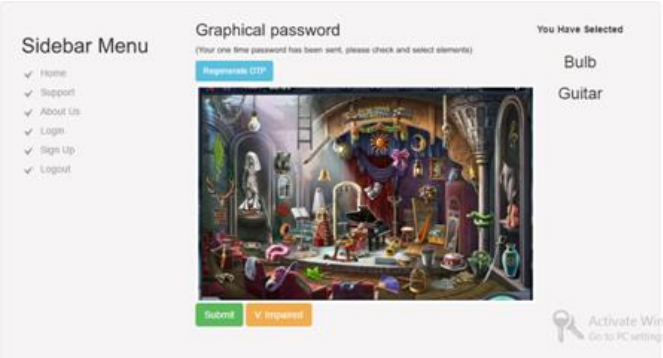

Figure 8: Selecting correct items sent as OTP from images

The user has to click the two items i.e the OTP send to his mobile number from the image in order to get himself authenticated. Here, the user is restricted with two clicks only. The user needs to click on the two items in any order within the two clicks. If he miss the two clicks then the user will not be able to click on any other items from the image.

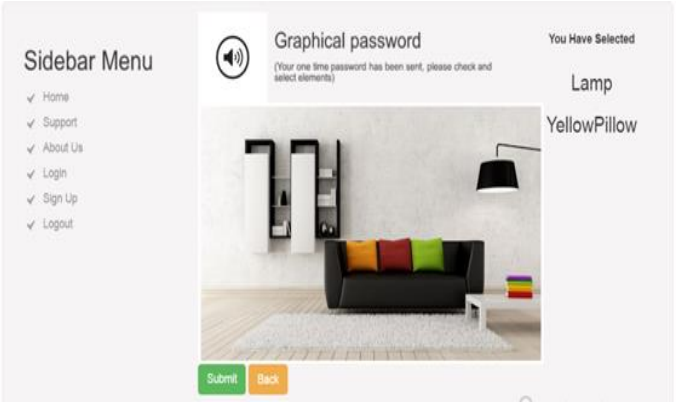

Figure 9: Graphical Password for visually impaired people

This system also tries to provide accessibility to visually impaired people. When the graphical password page is loaded at the bottom there is a button called "V Impaired" for visually impaired. When you click on this button a new image is displayed along with a audio clip. The user has to hear the audio clip before the click. As soon as you mouse over on the audio clip it will ask the user to click on any two image items. Now each and every image item has a associated audio clip about itself which will be played on mouse over i.e if you move your mouse over sofa the audio clip will say "sofa" etc. As the user move the mouse over various items in the image he will hear the audio clip related to each item. Then he have to click the two item respectively. For example the audio clip ask the user to click on "lamp" and "yellow pillow".

6. Security Analysis

- By allowing users to choose their own passwords can enable a personalized attack where the probability of guessing the user's password by a person who knows the user might be higher than other attackers. However, system assigned images lead to usability issues derived mainly from the difficulty of remembering random images. Due to these conflicting problems, a new balanced approach has been adopted that benefits from the advantages of both techniques. The idea is to give the system selected image and system generated OTP. This reduces the the task for users to remember the images they selected.

- As this system provides multilevel authentication i.e text based password as well graphical password it overcomes the potential attack that may exploit the password space size and dictionary attack.

- This system tries to overcome guessability, observeability, and recordability of the users password by generating One time password as OTP expires after certain time.

- This system tries to avoid shoulder surfing attack. As items to be clicked is directly sent to user's personal mobile number and other person cannot overlook the password and cannot copy and re-enter the password because the password expires after certain period. Also it is possible that bot can perform random clicks or click on each and every item present in the image. So the proposed system will restrict the number of clicks

for the user. In this way this system tries to provide more secure authentication.

TABLE 1: COMPARISON WITH EXISTING SYSTEM

Graphical Password Scheme/Technique	Resistance to Possible Attacks				
	BruteForce Attack	Dictionary Attack	Guessing Attack	Shoulder SurfingAttack	Phishing Attack
Blonder Scheme	Y	N	Y	Y	N
Pass Point	Y	N	Y	Y	N
Pass Face	Y	Y	Y	Y	N
Man et.al Scheme	Y	N	N	Y	N
Picture Password Scheme	Y	N	Y	Y	N
Graphical Password as an OTP	Y	Y	Y	Y	Y

7. Conclusion

This system aims to provide addition layer of security to the normal authentication system by using graphical password scheme. Additionally, it provides accessibility to visually impaired users. This system tries to avoid shoulder surfing attack, dictionary attack, brute force attack, guessing attack by generating one time password. This one time password is sent to user's mobile number by a text message from a database. The user must click on the sent items on the image provided in order to be authenticated. It requires large number of images in order to be secure and this will actually slow down the user authentication process.

8. Future Work

This system can be extended by sending the one time password to user's *whatsapp* account for authentication. Future work could include a user study with larger and more varied participants to validate the collected results and a more detailed analysis of this scheme.

References

[1]. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of9th USENIX Security Symposium, 2000.

[2]. D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in Proceedings of International conference on securityand management. Las Vergas, NV, 2004.

[3]. RealUser, "www.realuser.com," last accessed in February 2016.

[4]. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedingsof the 13th Usenix Security Symposium. San Diego, CA, 2004.

[5]. W. Jansen, "Authenticating Mobile Device Users Through Image Selection," in Data Security, 2004.

[6]. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[7]. J. Thorpe and P. C. v. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords," in 20th Annual Computer SecurityApplications Conference (ACSAC). Tucson, USA.: IEEE, 2004.

[8]. A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference onInformation Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

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

[10] Passlogix, "www.passlogix.com," last accessed in February 2016.

[11]. S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-ComputerInteraction International (HCII 200). Las Vegas, NV, 2005.

[12]. P.C. van Oorschot1 , and Robert Biddle, Sonia Chiasson, "Graphical Password Authentication Using Cued Click Points", Springer , June 2007.

[13]. Rohit Jagtap, Vaibhav Ahirrao, Vinayak Kadam, Nilesh Aher, "Authentication schemes for session password using color and special characters", International Journal of Innovations & Advancement in Computer Science (IJIACS), ISSN 2347 – 8616, Volume 3, Issue 2 April 2014.

[14]. Yuxin Meng, "Designing Click-Draw Based Graphical Password Scheme for Better Authentication", IEEE , 2012.

[15]. Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", IEEE, 2005.

[16]. Himika Parmar, Nancy Nainan and Sumaiya Thaseen, "Generation of Secure One-Time Password based on Image Authentication", CoNeCo, pp. 195–206, 2012.

[17]. Suo, Xiaoyuan, "A Design and Analysis of Graphical Password." Thesis, Georgia State University, 2006.

[18].Sukhvinder Kaur, "A Graphical Approach of Authentication in Grid Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2016.

[19]. Xiaoyuan Suo Ying Zhu G. Scott. Owen, "" Graphical Passwords: A Survey", IEEE, 2005.

[20]. Vinit Khetani, Jennifer Nicholas, Anuja Bongirwar, Abhay Yeole, "Securing Web Accounts Using Graphical Password Authentication through Watermarking", International Journal of Computer Trends and Technology (IJCTT), volume 9 number 6– Mar 2014.

[21]. Ms.Vaishali Baviskar, , Mayur Sanpurkar, Amit Patel, Makarand Jadhav, Gaurav Modi, "M-Banking using Steganography and Cued Click Points ", International Journal of Enhanced Research in Management & Computer Applications, Vol. 2 Issue 4, April-2013.

Author Profile

Veena Rathanavel has received the B.E. degrees in Computer Engineering from K C College Of Engineering in 2012. And currently pursuing M.Tech from K J Somaiya College of Engineering.