ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

User Authentication Using Graphical Password Scheme: A More Secure Approach Using Mobile Interface

D. D. Walanjkar, Prof. Vaishali Nandedkar

ME (Computer), PVPIT, Bavdhan, Pune, India

Assistant Professor and Head, Department of IT, PVPIT, Bavdhan, Pune, India

ABSTRACT: Textual password is most coomn method use for password authentication. In today's use of internet is increasing day by day. For security purpose the user selects password, that password are text based passwords or graphical passwords. Most of the user uses text based password because that are easy to remember. But main disadvantage of using text based passwords are many attacks can happen like eavesdropping attack, dictionary attacks, denial of service attacks. To overcome the disadvantages of text based password new graphical passwords are used. Click based graphical password scheme offers a novel approach to address the well known image hotspot problemin popular graphical password systems, such as PassPoints, that often leads to weakpassword choices. So to provide user friendliness and also the protection from various security attacks use of graphical password is important. In this, graphical password scheme, the click event isperformed on various points on same or different images.

KEYWORDS: Graphical passwords, password guessing attacks, security primitive, random question generator, CaRP.

I. INTRODUCTION

The graphical password is new technique which is more secure than text based passwords. In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or on different image. Or user can also selects sequence of images. Graphical passwords offers protection against the dictionary attacks which is major security threat in online applications. Graphical passwords also provide protection against the relay attacks.

The main motivation for graphical passwords is the hypothesis that people are better at remembering images than artificial words. Visual objects seem to offer a much largerset of usable passwords. For example user can recognize the people which he knowsfrom thousands of faces; this fact was used to implement an authentication system. Asanother example, a user could choose a sequence of points in an image as a password;this leads to a vast number of possibilities, if the image is large and complex, and if ithas good resolution.

To overcome the shortcomings of textbasedpasswords, graphical passwords have been proposed. Inmost of the schemes, graphical password employs graphicalpresentations such as icons, human faces or custom images tocreate a password. Human brains can process graphical imageseasily. Graphical passwords claim to be superior to the textbased passwords due to this human characteristic. Thesemethods assume if the number of possible pictures issufficiently large, the possible password space of a graphicalpassword scheme may exceed that of text-based password andtherefore it is virtually more resistance to attacks such asdictionary attacks.Many graphical password schemes are already introduced. Graphical password techniques can beclassified into two categories; recognition-based and recallbased.In recognition-based systems, a series of images arepresented to the user and a successful authentication requirescorrect images being clicked in a right order. In recall-basedsystems, the user is asked to reproduce something that he orshe created or selected earlier during the registration. The pastdecade has seen a growing interest in using graphicalpasswords as an alternative to the traditional text-basedpasswords.

The paper covers the graphical password used in authentication system; there are chances of attacks on graphical password also so to overcome this new technique introduced random question generation; after user gives right answers to question which are provided to him/her then only user can enter into the system.

10.15680/ijircce.2014.0212053

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

II. LITERETURE SURVEY

The need for graphical password is increasing day by day because graphicalpasswords are easy to recall and less likely to being written down also it has greater potential to provide a more symbol space than text based passwords.Many researchers are working on the concept of graphical passwords, some of them also introduced new ideas and some of them are still working to introduce new ideas to provide more secure approach related to graphical passwords. Already, there are many schemes have been proposed in present times. The first idea of graphical password has been given by Blonder in 1996. 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[5]. The disadvantage of this method is that users cannot click other positions than known positions so this also works same as text based passwords.A PassPoint[6] method the idea of Blonder's scheme is used t and further extended to overcome the drawback of Blonder's method.In PassPoints[6] the predefined boundaries of images are eliminated and arbitrary images are allowed to be used. Because of this when user wants to create password he can click on any place on image without restriction of any boundaries. After the password is created a tolerance around each chosen pixel is calculated, then for authentication of user, the user must click within the tolerance of theirchosen pixels and also in the correct sequence when user wants to access restricted resource or any application which is restricted.

In Cued Click Points (CCP), a cued-recallgraphical password technique [7], in this technique, a password is composed of oneclick-point per image for a sequence of 5 images. The nextimage displayed is based on the previous click-point so usersreceive immediate implicit feedback as to whether they are onthe correct path when logging in. A wrong click leads down anincorrect path, with an explicit indication of authenticationfailure only after the final click. The advantage of CCP over PassPoints is the fact that authorized usersget feedback about an error when trying to log in within a second.When users see an incorrect image, they know that the latestclick-point was incorrect and can immediately cancel currentattempt and the process is strated again from beginning.

Grid basedschemes are also proposed which uses recall method. A technique called "Draw A Secret" (DAS) [8]where a user draws the password on a 2D grid. Thecoordinates of this drawing on the grid are stored in order.During authentication user must redraw the picture. The useris authenticated if the drawing touches the grid in the sameorder. The major drawback of DAS is that diagonal lines aredifficult to draw and difficulties might arise when the userchooses a drawing that contains strokes that pass too close to agrid-line. Users have to draw their input sufficiently awayfrom the grid lines and intersections in order to enter thepassword correctly. If a user draws a password close to thegrid lines or intersections, the scheme may not distinguishwhich cell the user is choosing. A system where authentication is conducted by having the userdrawing his/her signature using a mouse [9]. The biggestadvantage of this approach is that there is no need tomemorize one's signature and signatures are hard to fake.However, not everybody is familiar with using mouse as awriting device; the signature can therefore be hard to drawn.A graphical authenticationscheme [10] in which the user selects certain number of imagesfrom a set of random pictures during registration. Later userhas to identify the pre-selected images for authentication. Theusers are presented a set of pictures on the interface, some ofthem taken from their portfolio, and some images selectedrandomly. For successful authentication, users have to select'their' pictures amongst the distracters.

Passface is a techniquedeveloped by Real User Corporation based on the assumptionthat people can recall human faces easier than other pictures[11]. Here the user is asked to choose four images of human facesfrom a face database as their password.These techniques have the potential to fill the gaps leftbetween traditional authentication techniques, including tradeoffsbetween security levels, expense and error tolerance. Butunfortunately there is a common weakness in the abovegraphical password schemes: They are all vulnerable toshoulder-surfing attacks. To address this issue, a graphical password technique [12]. In theirscheme, the system first displays a number of 3 pass-objects(pre-selected by a user) among many other objects. To beauthenticated, a user needs to recognize pass-objects and clickinside the triangle formed by the 3 pass-objects.

A Scalable Shoulder-Surfing ResistantTextual-Graphical Password Authentication Scheme (S3PAS) [13].In this scheme, user is provided with the login-image whichconsists of 93 printable characters. To login, the user mustfind all his/her original pass-characters in that image and thenmake some clicks inside the invisible triangles which arecalled

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

pass-triangles. The pass-triangles are created by 3original pass-characters following a certain click-rule. In thisscheme, user pass-character lies inside the pass-triangle. If theuser password length is k then he has to click k-times insidethe invisible pass-triangles. In S3PAS if the size of every pass trianglearea is too large, attackers are able to click inside theright areas with higher probabilities. A recognition-based graphical password schemeColorLogin[14], it is implemented in an interesting game way toweaken the boring feelings of the graphical authentication.ColorLogin uses background color, a method not previouslyconsidered, to decrease login time greatly. Multiple colors areused to confuse the peepers, while not burdening thelegitimate users. The scheme is resistant to shoulder surfingattack but password space is smaller than text-basedpasswords. Another shoulder-surfingresistant algorithm in which a user selects a number ofpictures as pass-objects[15]. Each pass-object has several variantsand each variant is assigned a unique code. Duringauthentication, the user is challenged with several scenes.Each scene contains several pass-objects and many decoyobjects.The user has to type in a string with the unique codescorresponding to the pass-object. However, these methodsforce the user to memorize too many text strings, and theirshoulder-surfing resistant property is not strong either. In realscenario, these approaches are under-utilized as theauthentications are usually complex and boring for users.

One more method based on recognition based scheme is ClickAnimal[1]. This is a captach scheme, in this 3D models of horse and dog are used to generate 2D animals with different colors, textures poses and arranges them on background such as grassland. When the animals are arranged on background, some animals may be overlapped with each other but main parts are not overlapped in order to identify by human. The ClickAnimal has a smaller password space than ClickText[1], in ClickText the alphabets are displayed but alphabets are not overlapped user can easily clicks on them to create or select password. Here when user click on any alphabet then location is tracked to check whether user clicks on correct character. ClickText[1] is also the recognition based scheme to generate graphical passwords

III. EXISTING SYSTEM

In existing system [1], CaRP (Captch as aRaphical Password) is used to authenticate the system. Here, the graphical password is used to authenticate the user instead of text based password. When user enters into the system then user enter the userID after that system generate the image, user then perform click events, if the click events matches with the system database then user authentication is successful otherwise authentication fail. Following figure illustrates the above procedure:

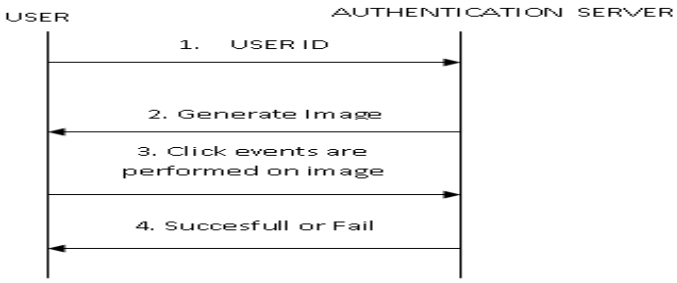

Fig.1 Flow chart of CaRP process.

But the problem with this method is that any person can concentrate and get the password when user is clicking on the image. So new method is introduced to multiple existing system problems, that method is discussed in section IV.

IV. RELATED WORK

Dhamija and Perrig[11] proposed a graphical authentication scheme where the user hasto identify the pre-defined images to rove user's authenticity. In this system, the user selects acertain number of images from a set of random pictures during registration. Later, during loginthe user has to identify the pre-selected images for authentication from a set of images as shownin figure 1. This system is vulnerable to shoulder-surfing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

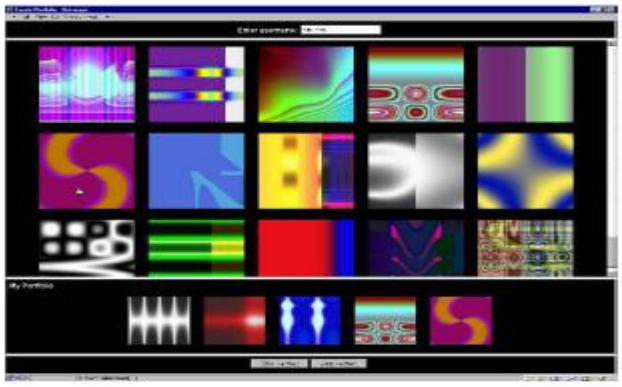

Figure 1: Random images used by Dhamija and Perrig

Passface [12] is a technique where the user sees a grid of nine faces and selects one facepreviously chosen by the user as shown in figure 2. Here, the user chooses four images ofhuman faces as their password and the users have to select their pass image from eight otherdecoy images. Since there are four user selected images it is done for four times.

Figure 2: Example of Passfaces

Jermyn, et al. [13] proposed a new technique called “Draw- a-Secret” (DAS) as shown in figure 3 where the user is required to re-draw the pre-defined picture on a 2D grid. If the drawing touches the same grids in the same sequence, then the user is authenticated. This authentication scheme is vulnerable to shoulder surfing.

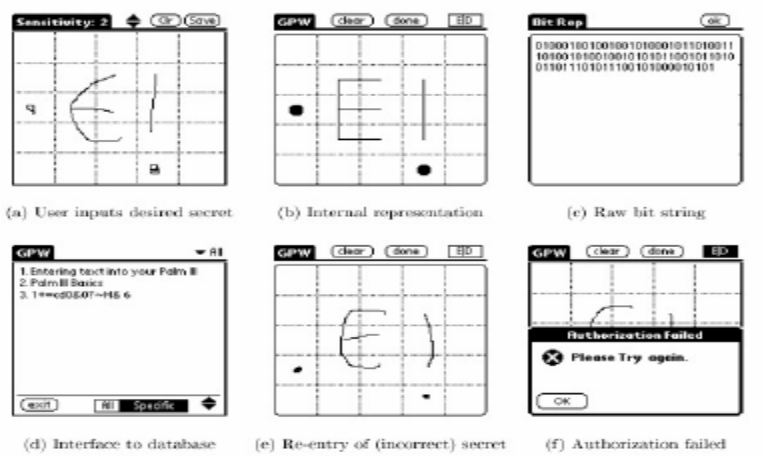

Figure 3: DAS technique by Jermyn

10.15680/ijircce.2014.0212053

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Syukri [14] developed a technique where authentication is done by drawing user signature using a mouse as shown in figure 4. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts the signature area. In the verification stage it takes the user signature as input and does the normalization and then extracts the parameters of the signature. The disadvantage of this technique is the forgery of signatures. Drawing with mouse is not familiar to many people, it is difficult to draw the signature in the same perimeters at the time of registration.

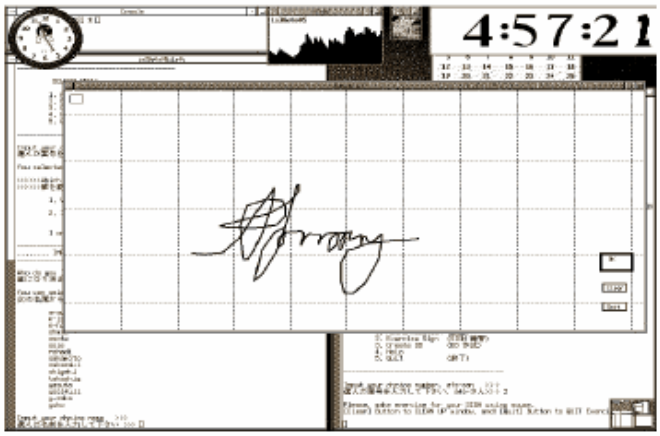

Figure 4: Signature technique by Syukri

Blonder [15] designed a graphical password scheme where the user must click on the approximate areas of pre-defined locations. Passlogix [16] extended this scheme by allowing the user to click on various items in correct sequence to prove their authenticity.

Haichang et al [17] proposed a new shoulder-surfing resistant scheme as shown in figure 5 where the user is required to draw a curve across their password images orderly rather than clicking on them directly. This graphical scheme combines DAS and Story schemes to provide authenticity to the user.

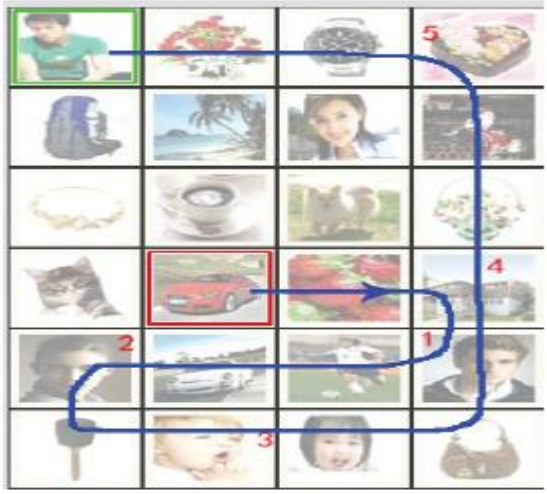

Figure 5: Haichang's shoulder-surfing technique

V. PROPOSED WORK

In this proposed system we use same CaRP scheme toauthenticate the user. But to provide more secure approach mobile interface is introduced. Proposed system includes the following two models:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

A] Random Question Generation:

If any unauthorized/ Untrusted persons know pattern of click based graphical password, then easily enter into the system. To overcome this problem, the proposed method introduces generation of random questions. For this user answers questions (20) asked in registration process. Then save graphical password and question with their respected answers in database.

B] Mobile Interface for answering generated question:

In Login process, after user enter the click based password if it is correct then any two questions from the saved questions during the registration process are send on mobile from registered questions. If user able to correct answer then only login get successful.

The system architecture is shown in fig.6;

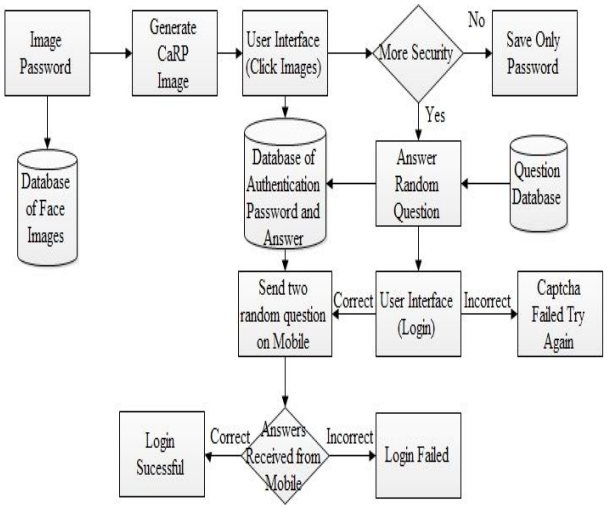

Fig.6System Architecture of Proposed System.

Algorithms

Suedo pair matching algorithm

Input : row characters up to uses input and session user id Sid

Output: session string for password matching

Step 1: Retrieve initial password from database of Xi user

Step 2: load grid GUI with 36 characters and numbers

Chars ={a,b,c,d……z},{0,1,2……..9}

Step 3: Take a two characters from Sid

sessionP $= \sum_{k=0}^{n}(k = 2)$

Step 4: Read the clickthrough from grid as r[] and c[]

Step 5: foreach(j:r.length)

Foreach (k:c.length)

If(sessionP.equals(j,k))

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Session follow;

Step 6: Repeat this step when Sid!=NULL.

Step 7: if all sessions==Sid then

Login success;

VI. CONCLUSION

Authentication system will develop by graphical password scheme, which is based on click based graphical authentication scheme. In authentication process system will allow to store the database of user and it will be in the form of image click by user. User will click on different points on same image or different image.Click based graphicalpassword scheme provides protection offers protection againstonline dictionary attacks and relay on passwords, which have been for long time amajor security threat for various online services. A proposed method is introduced random question generation to provide more secure approach to authenticate an user.

ACKNOWLEDGMENT

I like to acknowledge my vigorous thanks to Prof. Nandedkar for providing giving suggestions which helped me a lot in my research work and I also want to thanks our friends and classmates for helping me in this research work by giving me there timely suggestions and feedbacks on my research work.

REFERENCES

[1] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as Graphical passwords- A New Security Primitive Based on Hard AI Problems", IEEE transactions On Information Forensics And Security, Vol. 9, No. 6, June 2014.
[2] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey", 21st Annual Computer Security Applications Conference (ASCSAC 2005).Tucson, 2005.
[3] Md. Asraful Haque, Babbar Imam, Nesar Ahmad, "2-ound HybridPassword Scheme", International Journal of Computer Engineering andTechnology (IJCET), Vol. 3, Issue 2, July-September (2012), page. 579-587.
[4] D.Weinshall and S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall", in Proceedings of Conference on uman Factors inComputing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.
[5] G. E. Blonder, "Graphical passwords", in Lucent Technologies, Inc.,Murray Hill, NJ, U. S. Patent-5559961, Ed. United States, 1996.
[6] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy,and Nasir Memon, "Passpoints: design and longitudinal evaluation of agraphical password system", International Journal of Human-ComputerStudies, 63:102–127, July 2005.
[7] Sonia Chiasson, P.C. Van Oorschot, and Robert Biddle, "GraphicalPassword Authentication Using Cued Click Points", 12th EuropeanSymposium on Research in Computer Security (ESORICS), 2007, pp.359-374
[8] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and AvielD. Rubin, "The design and analysis of graphical passwords",Proceedings of the 8th USENIX Security Symposium Washington, D.C.,USA, August 23–26,1999
[9] A. F. Syukri, E. Okamoto, and M. Mambo, "A User IdentificationSystem Using Signature Written with Mouse", in Third AustralasianConference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[10] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images forAuthentication". In 9th USENIX Security Symposium, 2000.
[11] R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th
USENIX Security Symposium, 2000.
[12] Real User Corporation: Passfaces. www.passfaces.com
[13] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., "The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.
[14] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer- Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.
[15] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.
[16] Passlogix, site http://www.passlogix.com.
[17] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing