UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

Study of Graphical Password Schemes and "Two Level" Authentication Technique for Software Applications

Mrs.Hemangi Kulkarni
Computer Engineering Department
Pimpri Chinchwad College of Engineering
Pune, India
Hemangikulkarni21@gmail.com

Sonal Ahuja
IT Department
Institute of Management Studies (CD&R)
Ahmednagar, India
sonalahuja11@gmail.com

\

Abstract*— *Login is the basic and primary stage of authentication to any system. For Login users create memorable passwords, so that they remember those passwords when they next need access to the system Users create their own passwords as system generated passwords are difficult to remember. Going with same fact such text based factors are vulnerable to many well known attacks. So an alternative method was designed that used Graphical Passwords that use images or representation of Images as passwords. There are various graphical password schemes and software's in market. Text based passwords are mercilessly broken down so to mitigate the issues with the old methods advanced techniques have been proposed using Graphical Passwords. This paper aims at providing a comparative study of the various advance graphical password techniques available and I have also proposed a system using Cued Click Point Based Authentication for tightening the authentication process of any Online Application

Keywords*— Graphical Passwords, Recognition-Based Graphical User authentication, Recall-Based Graphical User Authentication, Pure Recall-Based Authentication, Cued Recall-Based Authentication, Usability, Security, Cued ClickPoint(CCP)*

I. Introduction

Various graphical password schemes [1] have been proposed as alternatives to text based password. Research has shown textual password has some disadvantages. It is very difficult to remember and easy to hack the textual password. If the textual password is too long or complicated the user may forget the password. They may also suffer from shoulder surfing. To overcome the disadvantage of the textual password, graphical passwords were introduced. Several studies and investigations showed that graphical passwords are more preferable than textual passwords. It is always proved that human brain is better in recognizing and recalling images than text. The graphical passwords are secured and cannot be hacked.

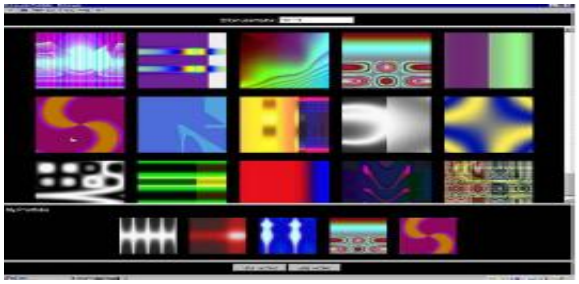
II. Background

There are two approaches used for graphical password authentication, recall based & recognition based. Recall retrieves items from memory with or without any cues, while recognition identifies a memorized match from a provided item. Recognition based & recall based are treated as two different processes, with recognition demonstrated as the task which requires less cognitive effort [10][11].

Recognition Based Technique:

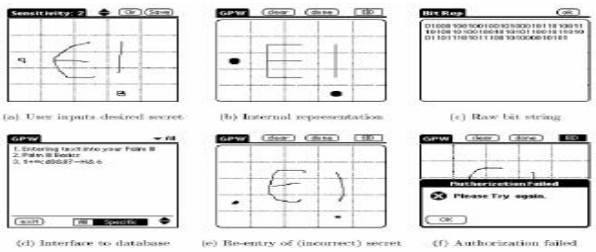
In this technique the user has to select certain number of images from a set of random pictures which are generated by a program. This way the user saves the password. Later for authentication the user must select the images in same order.
This technique needs to store random images as well as the image clicked by user in specific order to compare & authenticate.

1. Dhamija and Perrig[6] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this system, the user selects a certain number of images from a set of random pictures during registration. Later, during login the user has to identify the pre selected images for authentication from a set of images as shown in figure
   1. This system is vulnerable to shoulder-surfing.
   2. 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.

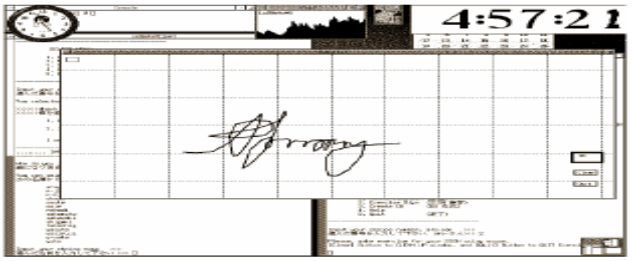


2. Passface is a technique where the user sees a grid of nine faces and selects one face previously chosen by the user as shown in figure 2. Here, the user chooses four images of human faces as their password and the users have to select their pass image from eight other decoy images. Since there are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

3. Jermyn, et al. [11] 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.



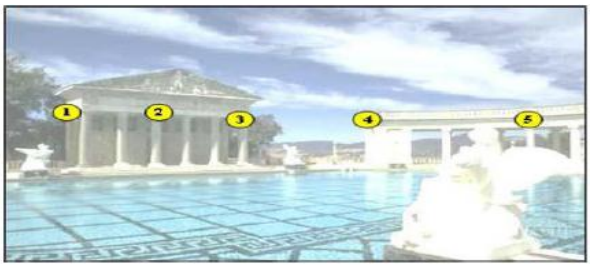
4. Syukri [13] developed a technique where authentication is done by drawing user signature using a mouse as shown in figure 4. This technique included two stages, registration and verification. At the time of registration stage the user draws his signature with a mouse, after that the system extracts 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.



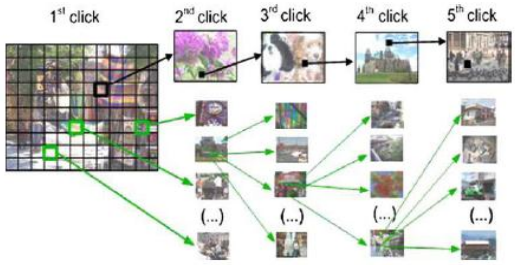
5. Haichang et al [16] proposed a new shoulder-surfing resistant scheme as shown in figure 6 where the user is required to draw a curve across their password images orderly rather than clicking on them directly.

Repeating the selection

1. Pass Points (PP) Pass point (PP)[1] Based on Blonder's original idea Pass Points (PP) is a click-based graphical password system where a password consists of an ordered sequence of five click-points on a pixel-based image as shown inFigure.4 To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points



2. Cued Click Points (CCP) - CCP [1] was developed as an alternative click based graphical password scheme where users select one point per image for five images Figure.5: The interface displays only one image at a time; the image is replaced by the next image as soon as a user selects a click point. The system determines the next image to display based on the users click-point on the current image. The next image displayed to users is based on a deterministic function of the point which is currently selected. It now presents a one to-one cued recall scenario where each image triggers the users memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images.



3. Persuasive Cued Click Points(PCCP)- To address the issue of hotspots, PCCP was proposed [1]. As with CCP, a password consists of five click points, one on each of five images. During password creation, most of the image is dimmed except for a small view port area that is randomly positioned on the image as shown in Figure. 6. Users must select a click-point within the view port. If they are unable or unwilling to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port guides users to select more random passwords that are less likely to include hotspots. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

III. Proposed System

Various software applications doing critical transactions are available online, however in spite of the ease of use of such applications and the convenience that these applications provide, there are some challenges that these applications face. One of such challenges is the issue of security of such systems. This new scheme developed will present a method for increasing security of the information requested by users with the use of Steganography method.

The method will have following features:

1. Encryption/decryption of data
2. Steganography Using Random bit of data
3. Internet Banking application Login, fund transfer and balance enquiry.
4. Graphical Authentication Using Cued Click-Points (CCP)

Details of modules of the system and Project Work Flow are

1. User enters user id and password
2. Data is encrypted and sent to server
3. Server checks the credentials in DB and returns the result
4. Server sends SMS on users registered phone no.
5. Client- it waits for an incoming sms, if the sms is for the same user and imei then the user is shown the CCP images
6. Users gets 5 images in sequence for authentication. Each image is divided into 4*4 matrix user has to click on on point per image and advances to next image. If the user clicks the wrong block, he will be taken to different image that was not used during registration
7. After successful authentication user get the application menu.

IV Analysis of Proposed Scheme

1. Contribution of Cued Click Point

When users log into the system the scheme allows the user to get to the cued click point environment only once the first stage of Text Password authentication is successfully passed.

In the CCP environment the user can select 5 images from the available set of images of his/her own choice. Once the images are selected, the user is required to select a cued click point on each image. Only one cued click point on one single image is permitted. This will

be confirmed and request will be raised that is approved by the admin, approval email or sms is sent to the user. User can now use his textual password to pass the first stage of authentication, then he will be moved to cued click point environment and only after successfully selecting the correct cued click points he will be authenticated and authorized to use the website. This will complete his/her login process.

2. Resistance to Shoulder Surfing

Some proposed password schemes have proved to be shoulder surfing resistant. But they are actually alphanumeric based, which required users to remember and input text characters, or not a good user experience. This proposed scheme uses CCP (Cued Click Points) thus it provides a shoulder surfing resistant scheme, which can overcome the drawbacks noted above. Here there are number of images stored in the database, thus the user can select his own 5 images out of the large database.

3. Password Space
System security largely depends on having sufficiently large password space. This is main defense against a brute force search. Theoretical password space for different length text passwords and CCP passwords with varying parameters

Chars	N	Space
95	6	2^{39}
95	8	2^{53}
95	10	2^{66}

The theoretical password space for a password system is the number of possible passwords that could be generated according to the system specification. A larger theoretical password space indicates lower likelihood that it would be guessed. For text passwords, the theoretical password space is typically reported as 95^n, where n is the length of the password, and 95 is the number of type able characters on the keyboard.

In CCP theoretical password space is calculated as $((w \times h)/t^2)^{c)}$ where the number of places that the user could click (the width (w) multiplied by the height(h) of the image) divided by the size of the tolerance square (t commonly set to 192) is raised to the power of the number of click points.

	w	h	c	space
S5	451	331	5	2^{44}
S6	451	331	6	2^{53}
S7	451	331	7	2^{61}
L5	800	600	5	2^{52}
L6	800	600	6	2^{63}
L7	800	600	7	2^{73}

IV. Usability Experiments

The proposed system is implemented in Java. The tool can be used as a password login scheme replacing that of traditional login schemes.
System has 5 phases:

1. Create 2. Confirm 3.Login 4. Recall-1 5. Recall-2

For each of the phase the usability will be measured in three ways: the time it took participants to complete each phase of the study: the number of errors they made in entering their passwords: their success rates when logging in. Conditions that took less time, had fewer errors, and had higher success rates will be judged to have better usability.
Till now, only the Create and Confirm phases have been tested. The success rates can be obtained by dividing a users number of successful password logins by their total number of password entry attempts. For Create and Confirm phases success rates were as follows

No	Login ID	Profile Create Trials	Times Successful	Times Unsuccessful
1	CCPU1	5	5	0
2	CCPU2	5	4	1
3	CCPU3	5	5	0
4	CCPU4	5	3	2
5	CCPU5	5	4	1

V. Conclusion

The proposed scheme is a graphical password method to develop effective, user friendly and secured method of authentication. In this paper textual password and graphical password together is introduced, as a means of reducing the users worry of using any application without thinking about the security issues. It aims to motivate the user with fun, friendly interface designed to improve user experience and acceptable and secured login. This scheme is a promising technique which can be developed by further studies. Future work should consider higher security

mechanisms, and reducing time consumption. We can in future strengthen the authentication process by adding a sound signature. In the near future, this system is expected to be further tested with actual projects/ websites.

References

1. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, "Graphical Password Authentication Using Cued Click Points" ESORICS , LNCS 4734, pp.359-374,Springer- Verlag Berlin Heidelberg 2007.

2. K.Renaud, "Evaluating authentication mechanisms," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 6, pp. 103–128.

3. C. Herley, P. van Oorschot, and A. Patrick, "Passwords: If We're So Smart, Why Are We Still Using Them?" in Financial Cryptography and Data Security, LNCS 5628, Springer, 2009.

4. R. Morris and K. Thompson, "Password Security: A Case History," Communicaitons of the ACM, vol. 22, no. 11, pp. 594–597, 1979.

5. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, \Graph- ical Password Authentication Using Cued Click Points" ES- ORICS , LNCS 4734, pp.359-374,Springer- Verlag Berlin Hei- delberg 2007.

6. R. Dhamija, and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". In 9th USENIX Security Symposium, 2000.

7. Passlogix, site http://www.passlogix.com

8. J. Bentley and C. Mallows, "How much assurance does a PIN provide?" in Human Interactive Proofs (HIP), LNCS 3517, Springer-Verlag, H. Baird and D. Lopresti, Eds., 2005, pp. 111–126.

9. F. Monrose and M. Reiter, "Graphical passwords," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 9, pp. 157–174.

10. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in 8th USENIX Security Symposium, August 1999.

11. 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.

12. 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.

13. B. Kirkpatrick, "An experimental study of memory," Psychological Review, vol. 1, pp. 602–609, 1894.

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

15. Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing

16. A. Paivio, Mind and Its Evolution: A Dual Coding Theoretical Approach. Lawrence Erlbaum: Mahwah, N.J., 2006.

17. J. G. W. Raaijmakers and R. M. Shiffrin, "Models for recall and recognition," Annual Reviews Psych., vol. 43, pp. 205–234, January 1992.

18. E. Tulving and M. Watkins, "Continuity between recall and recognition," American Journal of Psych., vol. 86, no. 4, pp. 739–748, 1973.

19. J. Anderson and G. Bower, "Recognition and retrieval processes in free recall," Psychological Review, vol. 79, no. 2, pp. 97–123, March 1972.

20. W. Kintsch, "Models for free recall and recognition," in Models of Human Memory, D. Norman, Ed. Academic Press: New York, 1970.

21. E. Tulving and Z. Pearlstone, "Availability versus accessibility of information in memory for words," Journal of Verbal Learning and Verbal Behavior, vol. 5, pp. 381–391, 1966.

22. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, "Design and longitudinal evaluation of a graphical password system". International J. of Human-Computer Studies 63 (2005) 102-127.