Volume: 02, Issue: 06, Pages: 906-910 (2011)

Implementing CHC to Counter Shoulder Surfing Attack in PassPoint – Style Graphical Passwords

M. Joshuva
Department of Computer Science and Engineering,
Aditya Engineering College, Surampalem, East Godavari, A.P., INDIA
Email: m.jashua@gmail.com
T. Sudha Rani
Department of Computer Science and Engineering,
Aditya Engineering College, Surampalem, East Godavari, A.P., INDIA
Email: sudha.mahi84@gmail.com
M. Samuel John
Department of Computer Applications,
V.R.Siddhartha Engineering College, Vijayawada, INDIA
Email: write2samuel@gmail.com

----------**ABSTRACT**----------
Graphical passwords are an alternative to existing alphanumeric passwords. In Graphical passwords users click on images than type a long, complex password. Passpoints scheme is one of the Graphical user authentication techniques. In this method the password is represented by multiple clicks on a single image. One of the advantages with Passpoints scheme is that, a user can click on any place in the image as a click point. Graphical authentication suffers a major drawback of Shoulder-surfing. Shoulder-surfing refers to someone observing the user's action as the user enters a password. Due to this, the user's action can be monitored by the attacker or it can be captured using recording devices such as camera. Sobrado and Birget suggested Convex Hull Click (CHC) scheme to counter shoulder-surfing using PassIcons which is different from PassPoint scheme. In this paper, we described how CHC is implemented in Passpoint-sheme to counter Shoulder Surfing Attack.

Keywords – Authentication, Convex Hull Click Scheme, Graphical Passwords, PassPoint System, Shoulder Surfing.

Date of Submission: 18 February 2011 Date of Acceptance: 08 April 2011

I. INTRODUCTION

In these days, some of the computer users are using the Graphical password system for the security of their Information. The graphical Passwords are proposed for the alternative of textual password. Psychological studies support such assumption as the human can remember pictures better than a text [1]. A graphical password is a top secret that user inputs to a computer with the aid of graphical input devices like mouse, stylus or touch screen [2]. The main objective for the graphical password is that the people are better at remembering images than textual or artificial words. Graphical password can be formed in the combination of the image icons and pictures. In other words, 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. For this reason, the graphical password approach is sometimes called as Graphical user authentication. If the image is large and complex, and if it has a good resolution, it is the basis for the graphical passwords [3,4]. An excellent survey of the numerous graphical password schemes that have been developed is [5].

We can classify password systems as

1. Recognition based systems [6, 7],
2. Pure recall based systems [8, 9],
3. Cued recall based systems [3,10,11].

In recognition based systems, a user chooses images or icons or symbols from a large collection; to be authenticated, the users need to recognize their previous choice among a large set of candidates. Dhamija, et al. Presented a scheme based on recognition of computer generated images. In their system, user will be asked to select certain number of images from a set of random pictures generated by a program. Later, user will be required to identify the pre-selected images to be authenticated. Akula and Devisetty [12] provide a variation of this method. The commercial scheme Passfaces [13] uses images of human faces. Davis, et al. studied such systems and found that user password selection is biased by race and gender. Wein-shall and Kirkpatrick [14] worked on a similar recognition based scheme in which users were asked to recognize a set of

Volume: 02, Issue: 06, Pages: 906-910 (2011)

images (100-200) from a database of 20,000 images. Their studies showed that even after one or two months, users could still recognize their graphical passwords with 90% accuracy. This study supports the hypothesis that people remember pictures/images better than alphanumeric strings. Recognition based graphical passwords seem to be easy to remember, but they have a drawback. In order to provide a sufficiently large password space they require many rounds of image recognition for authentication, which is tedious.

In pure recall based graphical password schemes, users need to reproduce their password without being given any hints or cues. Alphanumeric passwords, as well as manuscript signatures, are examples of means of authentication based on pure recall. Jeremyn et al. described a graphical password scheme Draw a Secret" (DAS), where users draw a shape on a grid. Users need to draw approximately the same shape in order to authenticate themselves. Wei-Chi Ku et al. study a variation of DAS. Recent research by Thorpe and van Oorschot [15] describes possible dictionary attacks against DAS. Overall, graphical password schemes based on pure recall are quick and convenient to use, but they seem to have the same disadvantage as alphanumeric password: They are hard to remember with sufficient precision when they have enough entropy to be secure.

The concept of cued recall was introduced in [16]. As the name indicates, users have to recall a password, but the system offers a framework of hints, context, and cues, that help the users reproduce their password or help them make the reproduction more accurate. In the field of computer systems the earliest example of a graphical password scheme based on cued recall was Blonder's patent. Here, the user is shown an image on the screen, and the password consists of a few points that the user chooses in the image (by clicking or pointing). The underlying images in the system help users recall their graphical password click points, but they have no direct role in the password. Authentication is performed by clicking near the previously determined points. In Blonder's scheme the image is partitioned into regions, whose outlines are visible; this results in comics-like images. The user has to click within the correct regions to log in. An extension of Blonder's idea was presented, this system allows natural images, without visible regions; instead, there are several underlying discretization grids (invisible to the user).We may conclude that cued recall is intermediate between recognition and pure recall.

II. PASSPOINT STYLE GRAPHICAL PASSWORDS

Now a days, to access a computer resource, the most common authentication method we are using is traditional ‘username’ and ‘Password’, in which the password is secret alphanumeric word known to the computer and the user. But users have many problems with the alphanumeric passwords. If a password is not used frequently then there is a chance of forgetting and if the password is hard to guess, it is hard to remember. For these reasons the researchers have developed various graphical password schemes.

The PassPoints scheme was first developed by Wiedenbeck, et al. [17] and it is based on the idea of Blonder. Even in Blonder’s approach the password is represented by multiple clicks on a single image. But Wiedenbeck’s PassPoints system overcomes the limitation of Blonder’s scheme, i.e. there are no predefined boundaries around areas of the image where the user can click.

One of the advantages with PassPoints scheme is that a user can click on anyplace on the image. An interface used in PassPoints scheme is shown in Fig. 1.It allows the use of arbitrary images. After clicking on several areas, the sequence is stored. A tolerance region around the chosen click points is calculated. When logging in, the user has to click on points within the tolerance. Generally, users cannot click on the same points that are selected during registration. So, a tolerance is given. This tolerance allows a user to click on nearby locations. For example, if the tolerance is 20X20, users can click on any location within the 20 pixels around (top, bottom, left, right) a click point.

Fig 1: The PassPoints [16] interface

There is another method in which a single click on multiple images is allowed. It is called as Cued Click Points. These schemes are called as cued recall based schemes since the background image can be regarded as a cue to recall the location of clicks chosen as a password.

Along with PassPoints technique, there are other techniques existing [18]. One such technique is Passfaces, in which user chooses four faces from a pool of faces. When logging in , the user sees a 3X3 grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces, the user has to recognize and click anywhere on the chosen face. This procedure is repeated

Volume: 02, Issue: 06, Pages: 906-910 (2011)

with different target and decoy faces, for a total of four rounds. It is observed that Passfaces may be more memorable than alphanumeric passwords. Another similar system suggests that choosing images from a pool of images is a slow process, but the images are easier to remember over time.

Passlogix [19] has developed a similar system. In their method, users must click on areas in the correct sequence in order to be authenticated. Invisible boundaries are defined for each clicked area in order to detect whether a particular area is clicked by the mouse. A similar technique was developed by sfr [20]. Microsoft has developed a comparable graphical password technique where users are required to click on pre-selected areas of an image in a chosen sequence [21].

III. How The Passpoint System Works?

The PassPoints system by Wiedenbeck, et al. is based on the idea of Blonder, in which the password is represented by multiple clicks on a single image.

If a new user wants to register, he has to enter a user name. He/she will be given a set of eight images. We used animals' image, a map, a fruits and veg image, an image with birds, a group of national flags and dog's image, and also things and house image etc. The registration page is as shown in the following fig. 2.

Fig.2: A screen shot of registration page

From these eight images, user has to select one image and then click on one or more areas as a graphical password. Users should remember the order of clicks and they have to produce the same order when they log in. Size of an image used in our application is 431X540.

The PassPoint scheme allows the use of arbitrary images. After clicking on several places (pixels) the sequence is stored. A tolerance region around the chosen click points is calculated. When logging in, the user has to click on points within the tolerance. Generally, users cannot click on the same points that are selected during registration. So, a tolerance is given. This tolerance allows a user to click on nearby locations. For example, if the tolerance is 20X20, users can click on any location within the 20 pixels around a click point.

IV. Shoulder Surfing Attack

Main drawbacks for the current graphical password schemes are the shoulder-surfing problem and usability problem. Even though graphical passwords are difficult to guess and break, if someone directly observes during the password entering session, he/she probably figure out the password by guessing it randomly. Nevertheless, the issue of how to design the authentication systems which have both the security and usability elements is yet another example of what making the challenge of Human Computer Interaction (HCI) and security communities[22].

In computers security jargon, shoulder-surfing refers to the direct observation techniques, such as looking over someone's shoulder, to get information like passwords, PINs and other sensitive personal information. As well as when a user enters information using a keyboard, mouse, touch screen or any traditional input device. Like text based passwords graphical passwords are also vulnerable to Shoulder-Surfing. There are some schemes developed by researchers and the first scheme is developed by Sobrado and Birget [23] in which system displays a number of pass-objects among many different objects. User needs to recognize pass-objects to be authenticated. Second scheme is developed by Man, et al., in which the user needs to select a number of pictures as pass-object, but each pass-object has several variants and each variant has unique code. Third scheme is developed by Hong, et al., and this scheme still uses pass-object. Many techniques are available to counter the shoulder surfing attack. Sobrado and Birget suggested Convex Hull Click (CHC) scheme [24] to counter shoulder-surfing attack in graphical passwords, and it works with pass objects. In the following section we propose a countermeasure which is to be used with Passpoints scheme.

V. Countermeasure for Shoulder Surfing Attack

Our proposed scheme

The Convex Hull Click (CHC) scheme allows a user to prove knowledge of the graphical password safely in an insecure location. To counter the shoulder surfing attack in PassPoint-Style graphical password system we propose a new scheme with the use of Convex Hull Click method. In this scheme, during the time of registration user selects few PassPoints on selected image. The user should remember the sequence of Passpoints when the time of Login process.

Volume: 02, Issue: 06, Pages: 906-910 (2011)

Let us assume that registration process is over, the user selected few PassPoints. And at the time of login the image displays three objects, through these three objects on the image user can mentally create the convex hull. For example the user choose animals image for the login process.

The screens of the login page are shown in the following fig.3 and fig. 4.

Fig.3: A screen shot selected image for clicking

Fig.4: A Screen shot selected image for clicking

After assuming the hull, the user should decide whether the Passpoint is inside the hull or not. If the PassPoint is within the convex hull user need not click the passpoint. But whatever the passpoints that are outside the convex hull that are to be clicked by the user. And for each time of clicking, the three objects will change their place randomly, resulting the hull will be changed to another place of the image. And after clicking all the passpoints in the sequence order, then the submit button will be clicked for the login process. If all the passpoints are within the convex hull, the user has to click only the submit button to enter. From time to time Hull changes its place, so the user will not click the same no. of clicks in the same place. And also with the use of these objects in the login process the attacker's mind can be diverted to see the objects but not the Passpoints. That's why we can counter the shoulder surfing attack.

VI. CONCLUSION

The graphical password system has some important issues. The first issue is that the people are better at memorizing graphical passwords than text-based passwords. And also graphical passwords have a large password space over alphanumeric passwords. Second issue is efficiency; users use the mouse to enter a password, it may be slower than the keyboard. People should spend more time learning and practice the graphical password but by user′s thinking and feeling this kind of graphical passwords will be much easier than alphanumeric passwords. Although graphical passwords are vulnerable to shoulder surfing attacks, our method provides security over this attack.

REFERENCES

[1] Madigan, S. Picture Memory, In John C.Yuille, editor, *Imagery memory and cognition*, Pages 65-89. Lawrence Erlbaum Associates,N.J., U.S.A.1983.

[2] Graphical passwords by Fabian Monrose And Michael K Reiter

[3] J.C. Birget, D. Hong, N. Memon, "Graphical password based on robust Discretization", *IEEE Transactions on Information Forensics and Security* 1(3) (Sept. 2006) 395-399. Earlier version: Cryptology ePrint Archive http://eprint.iacr.org/2003/168, Aug. 2003.

[4] Blonder, G. *Graphical Passwords*, In Lucent Technologies, Inc., MurrayHill,NJ, U.S.Patent, Ed. United States, 1996.

[5] X. Suo, Y. Zhu, G.S. Owen, Graphical passwords: A survey", *21st Annual Computer Security Applications Conference* (ACSAC'05) (2005) 463-472.

[6] Graphical Passwords: Comprehensive study for the Usability features of the Recognition based Graphical Password methods by Ali Mohamed Eljetlawi, Norafida Ithnin. IEEE 2008.

[7] R. Dhamija, A. Perrig, D ejµa Vu: User study using images for authentication", *Ninth Usenix Security Symposium* (2000) 14-17.

[8] I. Jeremyn, A. Mayer, F. Monrose, M.K. Reiter, A.D.Rubin, The design and analysis of graphical passwords", *Proc. 8th Usenix Security Symposium* (1999)

[9] W.Ku, M.Tsaur, A remote user authentication scheme using strong graphical passwords", *IEEE Conference on Local Computer Networks* (2005)351-357.

[10] D. Hong, S. Man, B. Hawes, M. Mathews, A password scheme strongly resistant to spy ware", *Proc. International Conference on Security and Management*, Las Vegas NV (2004) 94-100.

[11] J. Findlay, The visual stimulus for saccadic eye movement in human observers", *Perception* (1980)

7-21.
[12] S.Akula, V.Devisetty, Image based registration and authentication system," *Midwest Instruction and Computing Symposium* (2004).
[13] The Passfaces System", Real User Technology And products (2004) http://www.realuser.com/published/RealUserTechnologyAndProducts.pdf, last accessed on Oct 2010.
[14] D. Weinshall, S. Kirkpatrick, Passwords you'll never forget, but can't recall", *Conference on Human Factors in Computing Systems* (CHI) (2004) 1399-1402.
[15] J. Thorpe, P.C. van Oorschot, Towards secure design choices for implementing graphical passwords", *Computer Security Applications Conference* (2004).
[16] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodsky, N.Memon, Design and longitudinal evaluation of a graphical password system", *International J. of Human- Computer Studies* 63 (2005) 102-127.
[17] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A and Menon, N. *"Authentication using graphical passwords: Effects of tolerance and image choice"*. In Symposium on Usable Privacy and Security (SOUPS). Carnegie-Mellon University, Pittsburgh 2005.
[18] Brostoff, S and Sasse, M.A. Are Passfaces more usable than passwords: A field trial investication. In "people and Computers XIV-Usability or Else"*: Proceedings of HCI 2000(Bath, U.K., Sept.8-12, 2000)*.Springer Verlag, 405-424.
[19] M.Boroditsky, Passlogix Password Schemes http://www.passlogix.com accessed on Oct 2010.
[20] Sfr http://www.sfr-software.de/cms/XX/ pocketpc/sfr-password/index.html,last accessed in Oct 2010.
[21] Paulson, L.D., "*Taking a Graphical Approach to the Password*," Computer, vol.35, pp.19 .
[22] Ali Mohamed Eljetlawi, Norafida Ithnin Graphical Passwords: Comprehensive study for the Usability features of the Recognition based Graphical Password methods. IEEE 2008.
[23] L. Sobrado, J.C. Birget, Graphical passwords", *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4 (2002).
[24] S. Wiedenbeck, J. Waters, L. Sobrado, J.C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme", in *Proceedings of Advanced Visual Interfaces (AVI2006)*, Venice, Italy, 23-26 May 2006.

Authors Biography

M. Joshuva received the M.Sc.(Computer Science) degree from Arts College, Rajahumundry, Andhra University in 2006. He has three years teaching experience and pursuing M.Tech (Computer Science and Engineering) in Aditya Engineering College. His research areas are Network Security, Data Base Management Systems, Data mining and Data Warehousing.

T. Sudha Rani did her M.Tech in Computer Science and Engineering. She is currently working as Assistant Professor in the Department of Computer science and Engineering, Aditya Engineering College, E.G.Dist. She has four years teaching experience. Her research areas are Computer Networks, Cryptography and Software Engineering.

M. Samuel John received the M.Tech (Computer Science) degree from P.V.P.Siddhartha Institute of Technology. He is currently working as Lecturer in the Department of Computer Applications, V.R.Siddhartha Engineering College, Vijayawada, INDIA. He has six years of teaching experience. His research areas are Computer Networks, Cryptography and Network Security and Data mining and DataWarehouseing.