ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 25-28 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

PROVIDING SECURE AUTHENTICATION BY GRAPHICAL PASSWORD USING GRABBING TECHNIQUE

S.SARATHKUMAR[1], S.SURENDIRAN[2], M.SANTHOSH SAMUEL[3], [4]M.MARAVARMAN

[1]Adhiparasakthi Engineering College, India, sharath93.k@gmail.com
[2]Adhiparasakthi Engineering College, India, kalamsurendar1992@gmail.com
[3]Madras Institute of Technology, India,federersamuel@gmail.com
[4]Adhiparasakthi Engineering College, India, maravaraman@gmail.com

ABSTRACT

Various graphical password schemes have been projected as alternatives to text-based password. Authentication is the initial stage of information security. Authentication process require users to remember the passwords and recollect them during log-in time. Hence the images are used as a mean for graphical password technique. Images are easily unforgettable than the text password. This paper is evolved on the basis of pass point, cued click point, persuasive cued click point methods. This paper proposes the grabbing technique which includes two viewports. First the viewport should be fixed on two various position of the image. Then we merge the other two points in the image. This is highly secure and authenticated way of providing password than the traditional password methods.

Keywords – Authentication, usable security, grabbing.

INTRODUCTION

Authentication plays a vital role in protecting resources against illegal use. The commonly used authentication system is text passwords. Text based passwords are not secure enough for many applications. That inflict security by access control mechanisms. Also the space needed for text Password is very less. Hence it is easily attacked by the hackers using dictionary Attack. Authentication based on text based passwords has major drawbacks. Most complex authentication process is costly and it needs additional equipment or hardware such as mobile phones to get the verification code. To overcome such drawbacks we used the graphical password. In this paper we have investigated how the security of user authentication can be improved by using image password. The conventional image password systems are pass point, cued click point and persuasive cued click point.

The password technique is classified into 3 major types. They are Knowledge based, Token based and biometrics. Knowledge based is classified into Alphanumerical and Graphical and it's classified into recognition based and recall based technique and it's classified into pure recall and cued recall based techniques. The token based is classified into token, Smart Cards, Keys, Chip implants. Biometrics is further classified into Finger prints, Palm prints, Hand geometry, Face geometry, Voice Recognition, Iris Recognition and Retina Recognition.

PASS POINTS

Based on Blonde's original idea, Pass Points (PP) is a click-based system where a password consists of a sequence of five click-points on a pixel-based image. 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.

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 25-28 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

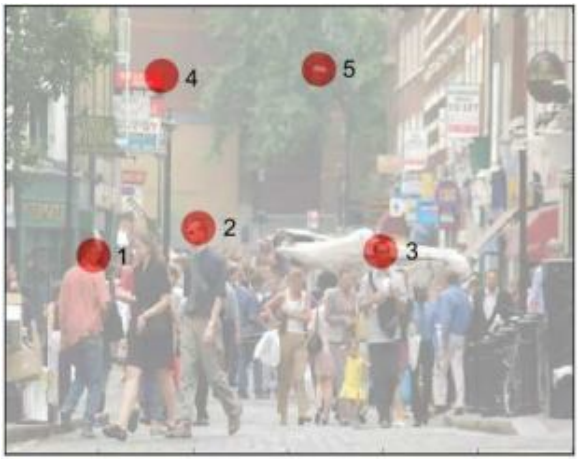

Fig 1: Pass point

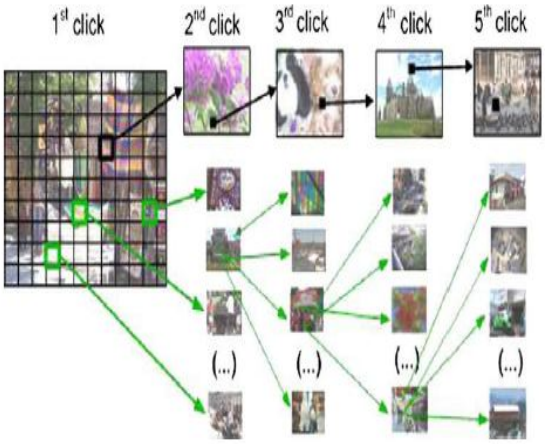

Fig 2: Cued click point

CUED CLICK POINTS (CCP)

The Cued Click Points (CCP) scheme is advanced to Pass Points. In CCP, users click on one point on each of 5 per images rather than on five points on one image. It offers Cued-recall and introduces visual cues that directly alert valid users if they have made a mistake when entering their latest click-point that is the point in which the hackers can terminate their effort and repeat from beginning. Each click results will shows the next-image, in order with sequences of images. 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 decides the next image. If they dislike the resulting images, they could produce a new password involving various click points to get different images.

CCP passwords can be regarded as a choice-dependent path of images. We think about that CCP fits into an authentication model where a user has a client device which displays the images to access an on-line server which authenticates the user.

The images are stored server side with client communication. For implementation, CCP primarily functions like PassPoints. During password creation, a discretization method is used to determine a click-points tolerance square and corresponding grid. For each click-point in a consequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point. With CCP, we will need to determine which next-image to display. A users initial image is selected by the system based on some user characteristic. The sequence is regenerated each time a user enters the password. If a user enters an incorrect click-point, then the sequence of images from that point will be incorrect and thus the login attempt will fail. For a hacker who does not know the correct sequence of images, this cue will not be helpful. We expect that hotspots will appear as in Pass Points, but since the number of images is significantly increased, analysis will require more effort which increases proportionally with the configurable number of images in the system. For example, if attackers identify thirty likely click-points on the first image, they then need to analyse the thirty corresponding second images (once they determine both the indices of these images and get access to the images

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 25-28 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

themselves), and so on, growing exponentially. A major usability improvement over Pass Points is the fact that legitimate users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. The visual cue does not explicitly reveal right or wrong but is evident using knowledge only the legitimate user should possess. As with text passwords, PassPoints can only safely provide feedback at the end and cannot reveal the cause of error. Providing explicit feedback in PassPoints before the final click-point could allow PassPoint attackers to mount an on-line attack to prune potential password subspaces, whereas CCPs visual cues should not help attackers in this way. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.

PERSUASIVE CUED CLICK- POINTS (PCCP)

To deal with the problem of hotspots, PCCP was proposed. 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 placed on the image . Users must select a click-point within the view port. If they are unable to select a point in the current view port, they may press the Shuffle button to randomly reposition the view port. The view port make the users to select more random passwords that are less likely to include hotspots. A user who is firm to reach a certain click-point may still shuffle until the view port moves to the specific location.

Fig 3: Persuasive Cued Click-Points

AUTHENTICATION SYSTEM

Image based Authentication for password has been known since the early days of the Internet, there is little academic literature on prevention techniques. This project deals with guessing attacks like brute force attacks and dictionary attacks. Our project proposes a new technique for providing password in secure manner. This is more complex to hack by the eavesdropper. During registration we have to select a particular category from a list of categories. It shows a list of images related to the category we already selected. From that we pick a image which we select during the registration process. If the previous steps are authenticated then it displays a image with two view ports. Viewport is used to select some portion of the image. It highlights the particular portion of the image and the other portions are blurred. In our project we include two viewports and hence we have to set the viewports in the correct location in order to show that you are the authenticated person. In order to provide more security we include another step called grabbing. In this the particular portion of the image is dragged to some other portion of the image. In this method the starting and the ending portion should be predefined at the time of password creation. If any input is incorrect then it assumes that the password

ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol.2 , No.5, Pages : 25-28 (2013)
Special Issue of ICETCSE 2013 - Held during October 21, 2013,Mysore, India

is incorrect. Also the sequence of image is based on the preceding image. This proposed system also provides protection against key logger spy ware. Since, computer mouse issued rather than the keyboard to enter our graphical password; this protects the password from key loggers.

CONCLUSION

In general people select short and simple textual passwords to remember it easily. It makes Intruder's task easy. Random and lengthy passwords are difficult to remember, but provides more security. Graphical passwords are introduced as alternatives to textual passwords. This paper proposed an authentication system which uses drag and drop method. The usage of well-known tool increases usability and the lengthy password provides security. The memorability and usability of character passwords should be done as future work. The user study should be done extensively using systems. The current study did not concentrate on time requirements. Actually, it is also important that how much time is required to enter a password using the specified tool. It is the future work to find minimum time and maximum time required to enter a password during login.

REFERENCES

[1] Chippy.T and R.Nagendran, "*Defenses against large scale online password guessing attacks by using persuasive click points*" International journal of communications and engineering, March 2012.

[2] 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.

[3] Zhi Li, Qibin Sun, Yong Lian, and D. D.Giusto, „An association-based graphical password design resistant to shoulder surfing attack", International Conference on Multimedia and Expo (ICME), IEEE.2005.

[4] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings ofMidwes Instruction and Computing Symposium*, 2004.

[5] L. Sobrado and J.-C.Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin forUndergraduate Research*, vol. 4, 2002.

[6] Sonia Chiasson, Alain Forget , Robert Biddle, P. C. van Oorschot, "User interface design affects security: patterns in click-based graphical passwords", Springer-Verlag 2009.

[7] 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 USENIXSecurity Symposium*, 1999.