International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 04 Issue 02 | 2020

Pixel Based User Authentication System

Mr. A.K.Zambre[1], Ms. Vaishnavi D. Chaoudhari [2] ,Ms. Mayuri P. Kolte[3], Ms. Aarti G. Khodke [4], Ms. Nikita A. Shelke[5]

[1, 2, 3, 4, 5] Department of Computer Science & Engineering, Dr. V. B. kolte College of Engineering, Malkapur , India

ABSTRACT

The password security is very important in a our day to day life there are various techniques are available for password protection .cued click point is the click- based graphical password techniques it is also cued -recall techniques of graphical password. The traditional text based passwords are mainly forgotten by user so, many users write down their passwords on papers, note books etc. User chooses simple and less passwords than long and complicated passwords. As an alternative to text based passwords, graphical password have been selected as a password. Because, human can easily remember visuals better than the alphabet. In cued click point method user click on one point per image for the sequence of images. The Second image is based on the earlier click point the password Which is easy to remember is choose by user so it become easy to recognize by the attacker. But the password those are assign by powerful system are not easy to remember for user .in this paper our focus is on to make evolution in graphical password authentication system by using CCP including its security and usability in these authentication method our main goal is to support the user while selecting correct password, thus increasing security by expanding the more effective password space. The pixel based user authentication system deals with the authentication this software help to user to make his account more secure.

Index items/ keywords – Cued Click Point (CCP), Graphical passwords, authentication, persuasive technology, usable security.

1. INTRODUCTION

Authentication is the process to identify user allow to get access particular system or resource .the password user attention .Method encourage less predictable passwords To maintain memorability and security in this paper We propose CPP for graphics for password authentication for graphics password authentication It consists of click point as per which image for the sequence of images the image is displayed is based on earlier click point so user receive immediate implicit feedback they feedback are on correct path while login in correct account CPP provide both security and usability . the text based passwords have usability and security issues that create problems to user that’s why there is a need to use alternative technique to overcome this type of problem there is a difficulty to remember the text based password to overcome these problems we made this graphical password system passwords like first name pets In this paper, We proposed Cued Click Point for graphical password authentication. The CCP proposed alternative to pass point techniques. In CCP techniques the user click on point on each and every image rather than on five points on one image. The CCP offers cued recall and introduces name, parents name are easily remember so, they are easily gain by attacker. Pictures and images are generally easy to remember and recognize than the text. Visual cues which instantly alert valid user , if user have made mistake when entering their latest click point as they choose their password it also make attack based on host spot analysis more challenging

2. LITERATURE SURVEY

2.1 Graphical Password Authentication System

A graphical password authentication scheme is silly similar to pass point scheme .The GPAS is based on “Knowledge based authentication” type of authentication scheme. And in “Knowledge based authentication” type of authentication scheme the server give a task to house by requesting him/her to reproduce same fact or select a same sequence of images which he/she given to the server at the time of registration. Here the password given by user is considered as a piece of information give to the server at the time of registration and at the time of authentication. It is explained through a Mobile Banking domain.

2.2 Why pixel based passwords?

The efficiency is most important in password systems user want to have a quick access the time to input a graphical password by highly skilled ,automated user can be predicted by the Fit’s law .the Fit’s law state that “the two point towards a target depend on the distance and the sized of the target”. Greater distance has smaller target lead result in slower performance**.**

In the text based password authentication flaws in aspect of usability and security that bring problems to the user and difficulty in remembering text passwords The system can be problematic if user forgot the point of click The system can be become complex with the increased number of images. to overcome these problems we have to use alternate mechanism like pixel based password.

2.3Cued Click Point technique

We proposed and examine the username of cued Click Point (CCP) it is one type of Cued-recall graphical password technique in which users click on one point per image per sequence of images and the next image is based on previous click point. We present the result of an initial user study, which revealed positive results CCP performance is very good in terms of speed accuracy and no. of errors .User connect CCP to pass point it tells while selecting and remembering only one point per image was easy and showing each image triggered their memory of where the corresponding point was located. Also, we suggested that greater security is provided by CCP than pass point because no. of images may increase work load to attackers and a sequence of images then the next image is display which based on previous click point.so the user receives immediate implicit feedback as to they are the correct way when logging in their account. Security and usability are improved by using CCP.

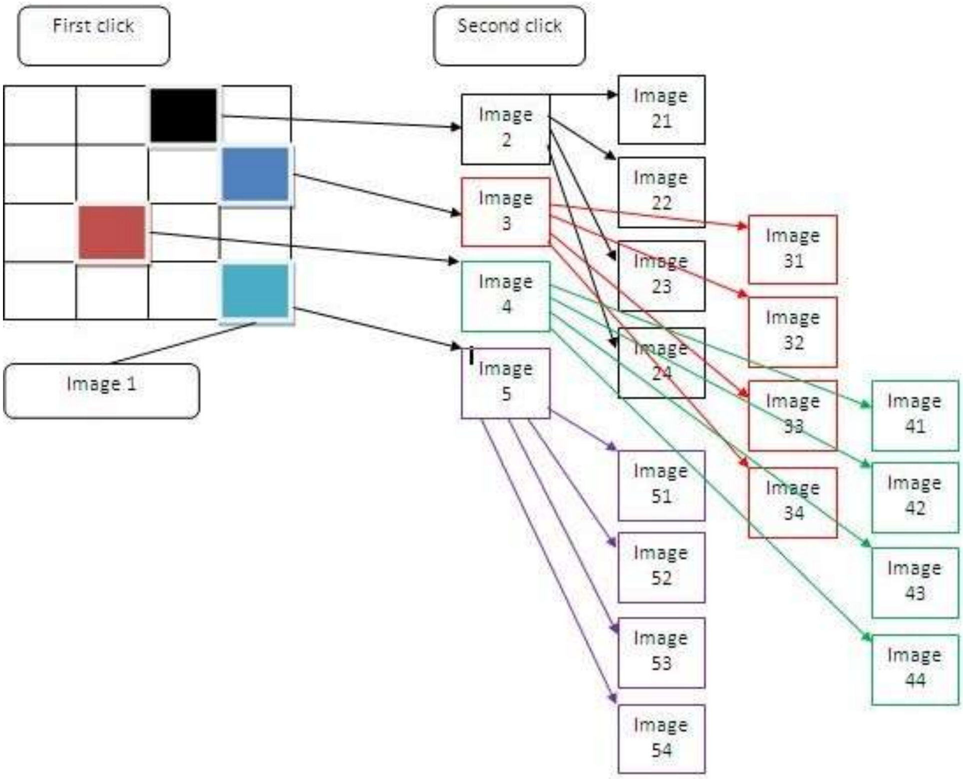

Fig.1.graphic password authentication

3. CONCLUSION

In our project, we have conducted complete study of existing techniques of graphical passwords our approach is to provide a scheme that will able to satisfy the need and requirements of the users. To achieve such a conditions the usability and the security features must be balanced. Also in this topic we present a method to generate strong authentication string which is usable in common users passwords authentication system.CCP is very useful and it provide higher security using hotspot technique. By taking advantage of ability of user to recognize images and the memory trigger associated with see new images.CCP is more secure than the previous graphical methods of authentication. it also increase the workload for attacker by forcing them to first a quire image set of each user, and then analyze for hotspot on each of these images.CCP has advantages over password schemes in terms of usability, security and memorable authentication mechanism

4. REFERENCE

[1] Magalhães, S. T., Revett, K. and Santos, H. D.: Password Secured Sites - Stepping Forward With Keystroke Dynamics, Proceedings of the IEEE International Conference on Next GenerationWeb Services Practices, IEEE CS Press, Seoul, South Korea, 2005.

[2] Magalhães, S. T. and Santos, H. D.: An Improved Statistical Keystroke Dynamics Algorithm, Proceedings of the IADIS Virtual Multi Conference on Computer Science and Information Systems, 2005.

[3] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memo, N.: Authentication using graphical passwords: Basic results, Human-Computer Interaction International (HCII 2005), Las Vegas, and July 25-27, 2005

[4] Blonder, G. E.: Graphical password, U.S. Patent Number 5.559.961, 1996.

[5] The science behind PassfacesTMDavies, D., Monrose, F. and Reiter, M. K.: On User Choice in Graphical Password Schemes, 13th USENIX Security Symposium, 2004.

[6] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K. and Rubin, A.: The Design and Analysis of Graphical Passwords, ??, 1999

[7] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, P.C. van Oorschot, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism", IEEE Trans, Vol 9, Issue2.

[8] Chiasson, P. van Oorschot, and R. Biddle, “Graphical password authentication using Cued Click Points,” in European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September2007.

A. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for information security,” Transactions on Information Forensics and Security (TIFS), vol. 1, no.2.

[9] D. Nelson, V. Reed, and J. Walling, “Pictorial Superiority Effect*,”* Journal of Experimental Psychology: Human Learning and Memory, vol. 2, no.5.

A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, “Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems,” International Journal of Human-Computer Studies, vol.63.

[10] E. Tulving and Z. Pearlstone, “Availability versus accessibility of information in memory for words,” Journal of Verbal Learning and Verbal Behavior, vol.5.

[11] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, “PassPoints: Design and longitudinal evaluation of a graphical password system,” International Journal of Human-Computer Studies, vol.63.

[12] Birget, J.C., D. Hong, and N. Memon. “Graphical Passwords Based on Robust Discretization.” IEEE Trans. Info. Forensics and Security, 1(3), September2006.

[13] Dirik,A.E.,N.Menon,andJ.CBirget.“Modelinguser choice in the Pass Points graphical password scheme”. ACMSOUPS, 2007.

[14] Thorpe, J. and P.C. van Oorschot. “Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords.” 16th USENIX Security Symposium,2007.