A Review on Click Points Graphical Password

Dr.Manmohan Singh [#1], Mr.Devidas S. Thosar[#2]

[#1]*Associate Professor,* [*2]*PhD Student,*

Dr.A.P.J.Abdul Kalam University,Indore

[1]kumar.manmohan4@gmail.com, [2] devidas.svit@gmail.com

Abstract-: Security is main concern in today's scenario. Standard human-computer-interaction approaches is not directly relevant. Security that are usable has exclusive usability challenges for the need of security. Users choosing enhanced password is the significant usability objective for authentication of the system. Most of the client generate easily memorable passwords that can be easy to hack by hackers. Password can be though for user also which are assigned by tough systems. User has to remember his whole password. So researchers replace this methods by other method in which password are made through images. Pictures are easy to remember than textual password. There are many types of graphical password schemes or graphical password software is available in the software market. Our project work combine persuasive cued click points and protocol of password guessing attacks. Project aims to make it tough for hackers to attack password. Users can choose random passwords and also passwords that are complex. This technique can remove many popular security threads.

Keywords: Graphical Password, Security, Persuasive Cued Clicks, Pattern Detection, Authentication

I. INTRODUCTION

There has been a great deal of hype for graphical passwords since two decade due to the fact that primitive methods suffered from an innumerable number of attacks which could be imposed easily. Here I will progress down the taxonomy of authentication methods. To start with I focus on the most common computer authentication method that makes use of text passwords. Despite the vulnerabilities, it's the user natural tendency of the users that they will always prefer to go for short passwords for ease of remembrance [10] and also lack of awareness about how attackers tend to attacks. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks [10][1].To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The idea of Graphical passwords first described by Greg Blonder (1996). For Blonder, graphical passwords have a predetermined image that the sequence and the tap regions selected are interpreted as the graphical password. Since then, many other graphical password schemes have been proposed. The desirable quality associated with graphical passwords is that psychologically humans can remember graphical far better than text and hence is the best alternative being proposed. There is a rapid and growing interest in graphical passwords for they are more or infinite in numbers thus providing more resistance.

Graphical methods of password creation shave a predestined illustration of image. In this image, the series and the tap area chosen are taken to mean as the graphical password. Graphical methods of passwords creation became popular since then. The enviable feature connected in the company of graphical methods of password creation is that it is easy for humans to memorize graphical than text. Hence graphical method is the best substitute that has been proposed so far. Reduction of the guessing attacks and heartening users to select more random and complicated passwords to guess is the most important objective of this work.

II. Literature Review

Online hacking and password breaching is becoming more popular now a days. Passwords can be easily hack by hackers now days by various methods of attacks. They are capable to hack into any important and secret data. The graphical password method is introduced which is more advanced and secure. This idea was proposed by Mr. Greg Blonder. According to theory selecting pattern and the small

particular area from the given images which is a graphical password. After that many password schemes have been designed and are being used. Now coming to the fact that humans are more comfortable in remembering graphical images rather than texts and graphical passwords are more secure when it comes to guessing attacks. It can take many years for guessing passwords. Project's objective is to reduce guessing attacks by guide the users to select more odd and unpremeditated images to make it impossible for any password guessing attack. Dhamija and Perrig proposed a graphical verification scheme. In this system the user will select one of the images from a set of given pictures produced by a program than the user will be required to recognize the selected images in order to be login. Here syste fault is that the server needs to store the details of the portfolio images of each user. Also, the process of choosing a set of pictures from the picture database can be dull and time consuming for the user.

Persuasive Cued Click- Points:To address the issue of PCCP was proposed. As with CCP, a password consists of five click points. During password creation, small view port area that is randomly positioned on the image is darkening. Users must select a click- point from the view port. If they are not capable to select a point in the current viewport, they can press the Shuffle button. The viewport guides users to select more random passwords that are less probable to include hotspots. A user can still shuffle until the view port moves to the specific location, but it is a time consuming and more dull process.

III. SYSTEM OBJECTIVES

- To validate the end user for authentication I usually prefer to adopt the knowledge-based authentication.
- To support the users in selecting better and safe passwords.
- To provide a security to the system.
- To reduce the guessing attacks and assign a strong password to the system.
- To select more random, and difficult passwords to guess

IV. PROPOSOSED APPROACH

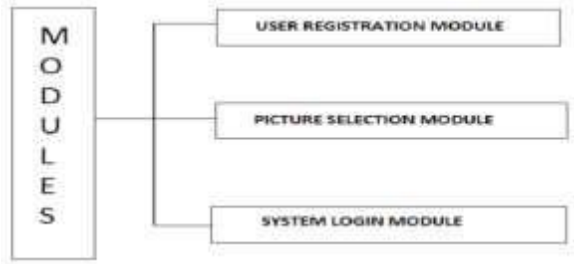

Fig: 1-System Module

Methodology:

1. Sign Up

This feature allows all users including servicemen or product vendors can register their details along with credentials.

2. Login

This feature allows all types of users a secure authentication mechanism in order to get access to the system.

3. PCP password creations:

• Layer 1:- 1st password is set on image through clicking event check attribute height, width, and size and image name.

• Layer 2:- 2nd password is set on image through cropping image with X and Y axis checking.

• Layer 3:- 3rd password is set on select point around images like if I select three point it will be triangle around image. If four it will be a cube (this will check points and shape and also X and Y axis)

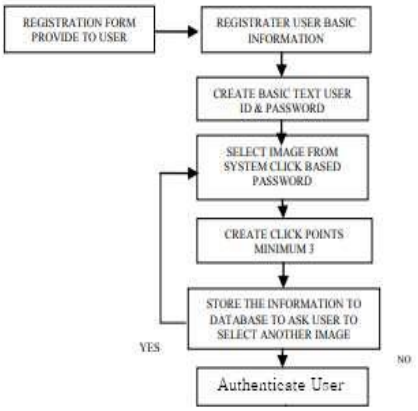

Fig: 2-System Architecture

CONCUSION

Persuasive cued click point plays a vital role for password protection, the graphical password are more protected and are better than the alphanumeric passwords. One most important factor with the graphical passwords is they are very easy to memorize for the user and more protected as well. Online password guessing attacks are more common these days and so the use of more protected password system is needed which brings us to graphical passwords.

REFERENCE

1. Sonia Chiasson , P.C. van Oorschot, and Robert Biddle, “Graphical Password Authentication Using Cued Click Points” ESORICS,LNCS4734,pp.359 374,Springer-Verlag Berlin Heidelberg 2007.
2. Manu Kumar, Tal Garfinkel, Dan Boneh and Terry Winograd, “Reducing Shoulder-surfing by Using Gazebased Password Entry”, Symposium On Usable Privacy and Security (SOUPS) , July 18-20, 2007, Pittsburgh ,PA, USA.
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. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of9th USENIX Security Symposium, 2000. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings of Midwes Instruction and Computing Symposium,2004.
5. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic
6. lletin for Undergraduate Research, vol. 4, 2002.
7. Sonia Chiasson, Alain Forget , Robert Biddle, P. C. van Oorschot, “User interface design affects security: patterns in click based graphical passwords”, Springer Verlag 2009.
8. 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 USENIX Security Symposium, 1999.
9. S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.
10. A. Adams and M. A. Sasse , "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp. 41-46, 1999.
11. 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 USENIX Security Symposium, 1999.
12. Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.
13. Cranor, L.F., S. Garfinkel. Security and Usability. O’Reilly Media, 2005