IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

A Survey Paper on Authentication for Shoulder Surfing Resistance for Graphical Password using Cued Click Point (CCP)

Monali Pawar[1], Prof. G.S Mate[1], Soni Sharma[1], Sonam Gole[1], Snehal Patil[1]

Information Technology, JSPM's Rajarshi Shahu College of Engineering, Tathawade, Pune, Maharashtra, India[1]

Abstract: In today's world authentication plays a vital role. The most common method used for authentication is textual password. There are various limitations for textual passwords, they are exposed to shoulder surfing attack however strong textual passwords are tough to memorize. Shoulder surfing and hotspot attack are two main problems in graphical passwords. So as an alternative Graphical Passwords are introduced to resist the Shoulder surfing attack. In order to address the above mentioned attacks the new scheme highlights cued click point (CCP), Using graphical password as input and grid lines for image point verification. The objective of this system is to provide security using normal login and graphical password. This system can be used in the field such as banking application, military application, civilians, forensic labs, etc.

Keywords: Authentication, Graphical password, Shoulder surfing, Hotspot, Cued click point.

I. INTRODUCTION

In current state it is very important to secure system. Where the need of authentication is required for high security, there are various methods to provide authentication like password authentication but this type of authentication cannot provide in the fields like banking application, military, forensic labs, etc. [1]. The most widely adopted technique in authentication is Textual passwords are hard to memorize and recollect [1]. Textual passwords are attacked by Masquerading, Eaves dropping, Dictionary attack, Shoulder surfing attack, Spyware and Guessing attack [7]. To overcome this drawback graphical passwords were introduced.It is recognized that humans can remember images for long duration than textual representation. Using graphical password user is able to set up a complex authentication password and is able to recollect it, even if the memory is not activated periodically [3].

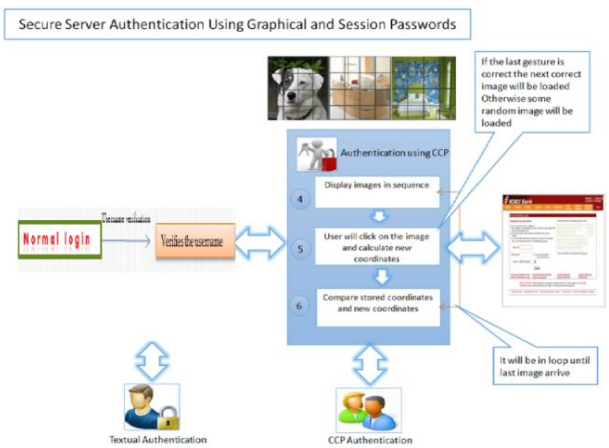

Fig.1Architecture of Authentication using cued click point

This paper focuses on the issues and eliminates them resulting more secure, reliable and useable for users.

II. LITERATURE SURVEY

In graphical based password authenticationPass Point, Cued Click Pointstechniques are used. In Pass Point Graphical password scheme consist of five different click points on given image.[1]To generate password user selects on any pixel in the image. The only limitation is hotspots [7] while attacker can easily guess the password because pattern formation takes place as a secret code for remembrance so the attacks are easily possible. Cued Click Point uses one click point on five different images in sequence instead of five click points on one image.[2]. The next image will be demonstrated on the basis of previously selected point.This method reduces pattern realization attack but hotspots problem is still present.

In Defense against large scale online password guessing attack by using persuasive cued click point [1]by T, R.Nagendran.Proposed the method at the time of registration the randomly selected block of the image called the view port. This view port clearly seen out and all the other parts of the image are shaded, so that the user can select click point only inside the view port of the image. The system casually selects the view port for every image to generate graphical password. But, this system leads to lengthy registration process and still the attacks like dictionary attacks cannot be overcome.

In Even or Odd: A Simple GraphicalAuthentication System [2] by N. López, M. Rodríguez, C. Fellegi, D. Long.Proposed that many portable devices need a simple

authentication system to protect them from being used by an unauthorized person such as a thief. The security of traditional methodssuch as pin codes or passwords is limited by shoulder surfing[7] where a casual or intended observer observes an authentication session and derives all information necessary for authentication. Graphical authentication [6] systems have been developed to anticipate this attack. But this method uses challenge-response scheme, a user is presented with a row of typically three faces and needs to decide whether the number of "friends" is even or odd. Hence, security issue is not resolved.

In a shoulder surfing resistant graphical password scheme," in Proceedings of International conference on security and management by S. Man, D. Hong, and M. Mathews,Proposed a system in which the User should rate colors from 1 to 4 and he can remember it as "RGBY". The login interface consists of grid of size 4×4. This grid contains digits 1-4 placed randomly in grid cells. The interface also contains strips of colors. The color grid consists of 2 pairs of colors. Depending on the ratings given to colors, we get the session password. But the color rating of RGBY Model is hard to remember at the time of login and the interface is quite difficult to understand to the normal user.

In Authentication Schemes for Session Passwords using Color and Images [4] by M. Shreelatha, M. Sashi proposed a Session passwords can be used only once and every time a new password is generated. Session passwords are generated based on this secret pass[3].The session password consists of alphabets and digits. The first letter in the pair is used to select the row and the second letter is used to select the column. The intersection letter is part of the session password But this technique is proposed to generate session passwords using text which fails to resist shoulder surfing.

In Highly Secure Authentication Scheme [5] By Ushir Kishori Narhar, Ram.B.Joshi.The objective is to provide highly secure authentication scheme by using user name with graphical password using persuasive cued click points along with biometric authentication using finger nail plate [6]. The scope of the scheme is limited to three fingers only and also for high security purpose where it is very important to keep tight security like [7] military application, forensic labs, civilian, banking applications, etc. But Biometrics such as face and fingerprints can easily be recorded and potentially misused by biometrics experts without user's consent.

In Improved Authentication Scheme using Password Enabled Persuasive Cued Click Points [6] By Neha Singh, Nikhil Bomanwar.Shoulder surfing andHotspot are the two main issues in Graphical passwords. Sonia Chiasson proposed the method of a persuasive cued click point [1] which reduces the hotspot problem, but provides no security mechanism for shoulder surfing attack [1]. In order to address these issues, The proposed work enhances the pervasive cued click point based method with a major change, having a invisible password input for each point .Moreover concept of fingerprinting [5] is used to ensure that the system is securely used by users. But this method suffers from issues like Reverse Engineering [2] attacks which involve detection of Key logger [7] and decompiler running on the system of users.

InA Shoulder Surfing Resistant GraphicalAuthentication System[7] By Hung- Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh . Proposed a system based on authentication for passwords is used largely in applications for computer security and privacy. With web applications and mobile apps[2] piling up, people can access these applications anytime and anywhere with various devices. Attackers can observe directly or use external recording devices to collect user'scredentials [1]. To overcome this problem, we proposed a innovative authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal [4] and vertical bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks. But this System does not resist the shoulder surfing attack and also vulnerable to smudge attack.

Recall Based Techniques

In this section we discuss recent three types of click based graphical password technique:

1. Pass Point (PP)
2. Cued Click Point (CCP)

Pass Point (PP)

Based on Blonde's original idea, Pass Point (PP) is a click-based graphical password system [3]. This system consists of ordered sequences of five click points on a pixel based image. In ordered to log in user must click within system defined tolerance region for each click point. This point forms the pattern on the image to help user remember their password click points.

Cued Click Points (CCP)

CCP was developed as an alternative to textual password and used with graphical passwords. In this scheme user selects one point per image for five images. Only one image is displayed at a time, next image replaces the previous one as soon as the user selects the click point[7].

The sequence of images is determined by the user while registration, while the appearance of images is decided as per the click points. Secondly, if the user enters and incorrect click point during login, next image displayed will also be incorrect. Authorized user who see an unrecognized image know that they made an error with the previous click point. However, this feedback is not helpful to an attacker who does not know expected images of sequence[7].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

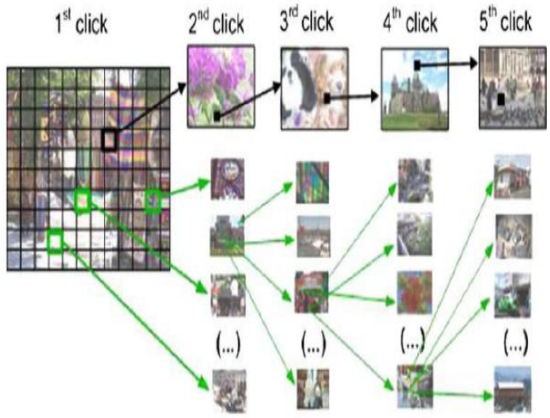

Fig 3. Cued Click Point

III. PROPOSED SYSTEM

As per our studies from above mentioned literature surveys the existing systems fail to resist the shoulder surfing attack. To overcome the above mentioned attacks, we have come with the new authentication technique which provides two layer protections. They are

1. Login
2. Graphical Password

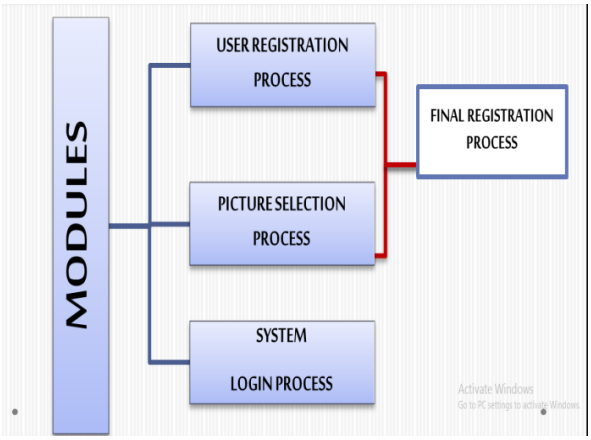

Fig: 4 Block Diagram for Proposed System

1. Login

User will have to register for the normal textual password. User needs to provide simple login details like user id and password and then after first layer verification, he will be diverted to next window which is graphical password.

2. Graphical Password

After login process is done, we are moving towards graphical password and provide second layer security.
Graphical password does a good job in helping users to recollect and remembering their password.

Registration

During registration, the user will select the number of images to be displayed. He will also select the matrix size (splits) per image. If the users click on incorrect region within the image, a different image will be shown.

Login

While login, the user will select 1 point from first image, the correct selection will divert him to second image which is stored into database. Similarly, after the second collect selection, third image will be displayed and will be stored in the database and the user will be in login into the system.

If the user tries to prompt the points which are not there in the database, he will be diverted towards the wrong image. After such three preemptions, the system will be blocked for that user for some time.

IV. FUTURE SCOPE

This system can be used for various security systems like system login and logout process in banking, web locking system, folder locking system, etc.
Like most of the other graphical password authentication system shoulder surfing is vulnerable to the guessing attacks. To overcome this problem the user can upload their own images to make it more difficult for attacker to guess it.

REFERENCES

[1] Chippy.T, R.Nagendran "Defense against large scale online password guessing attack by using persuasive cued click point" International Journal of Communications and Engineering Volume 03– No.3, Issue: 01 March2012.
[2] N. López, M. Rodríguez, C. Fellegi, D. Long.
[3] "Even or Odd: A Simple Graphical Authentication System" IEEE LATIN AMERICA TRANSACTIONS, VOL. 13, NO. 3, MARCH 2015.
[4] 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.
[5] M. Shreelatha, M. Shashi. M Anirudh,Md.Sultan Ahamer, V Manoj Kumar "Authentication scheme for session password using color and images " International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011.
[6] Hung- Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh 2015 International Conference on Computing Communication Control and Automation." Highly Secure Authentication Scheme".
[7] "Improved Authentication Scheme Using Password Enabled Persuasive Cued Click Points". 978-1-4673-7910-6/15/$31.00_c 2015 IEEE.
[8] DOI 10.1109/TDSC.2016.2539942, IEEE Transactions on Dependable and Secure Computing."A Shoulder Surfing Resistance Graphical Authentication System..Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Chen