Improved Authentication Scheme Using Persuasive Cued Click Points

Dhanashree Kadu
M.E. Computer Department,
Shree L.R. Tiwari College of Engineering,
Mumbai University, India

Shanthi Therese
Assistant Professor,
Thadomal Shahani College of Engineering,
Mumbai University, India

Anil Chaturvedi
Assistant Professor,
Shree L.R. Tiwari College of Engineering,
Mumbai University, India

Abstract: Authentication plays very important role in information security. Strong text-based password schemes used for authentication which have several drawbacks. Sometimes text based passwords are difficult to memorize. Graphical authentication has been proposed as a possible alternative solution to text-based authentication. Graphical pictures could be used for authentication which have various advantages over text based password. Graphical passwords having two main issues as Shoulder surfing and hotspot. In this paper we have proposed a graphical password authentication system which is best alternative for text password. Persuasive Cued click point (PCCP) is best alternative to old graphical password system. PCCP is combination of five click points on particular five images. PCCP is clubbed with new technologies like mobile phones & Emails.. The proposed work (IPCCP) enhances the persuasive cued clicked points based method with major change, having an additional 5 bit binary OTP generation on user registered mobile phone as input for each point.

Keywords: *Authentication, graphical passwords, Persuasive Cued Click Point (PCCP), hotspot.*

*****

I. INTRODUCTION

A password is secret form of authentication data that is used to control access to a resource. It is kept secret from those not allowed access, and those wishing to gain access are tested whether or not they know the password and granted or denied access accordingly. Some drawbacks of text based password appear like stolen the password, forgetting the password, and weak password.

Strong authentication method is needed to secure all our applications as possible. Graphical password have been proposed as a possible alternative to text-based, motivated particularly by the fact that humans can remember pictures better than texts. The objective of this paper is to Improved Authentication Scheme Using Persuasive Cued Click Points. Persuasive Cued Click Points scheme is effective for the reducing the numbers of hotspots and shoulder surfing attacks. The main objective of the project is to provide a two way authentication to the users by using Persuasive Cued Clicked point's technique and OTP.

II. OVERVIEW OF GRAPHICAL PASSWORD AUTHENTICATION SYSTEMS

One of the best password authentication systems was text based or alphanumerical based password has several problems. One of the main problem with text based password is it was ridicules to remember several text password for different account. Then introduction of biometric password [3] and token based password was considered as alternative of the text based password, but it again has several drawbacks like cost and unavailability issue. To overcome the disadvantages of text based password and token based password the invention of graphical password is introduced. Initially there were following graphical password authentication systems:

A. Pass point.
B. Cued Click Point (CCP).
C. Persuasive Cued Click Points (PCCP).

But this system had again disadvantage of hot spot problem and shoulder surfing attacks. To overcome the disadvantage of hot spot problem invention of Persuasive cued click point is made.

A. Pass Point: The pass point system for password authentication. The concept of the pass point was as simple as just clicking five point on single image and combination of this point as a password. In this user has to select five points from single image and at the time of password selecting and during the time of login user has to repeat the same sequence of the points from single image. But the main security problem with this was the HOTSPOT [1], the area where the user clicks. User choose the easy to memorable passwords to which can be easily guessed by

hacker. To avoid this problem the next method is implemented.

B. Cued Click point: To overcome the disadvantage of the pass point authentication system the cued click point is invented. Cued click point [1][2] has the same concept as of the pass point but the main difference between them is passing five points on five different image one point per image.

C. Persuasive-cued click point (PCCP) The persuasive cued click point [1][2] is the addition of the persuasive feature to cued click point. It allows user to select less portable password. It has two more function as shuffle and viewport, when users creates a secret word, the images are a little monochromic except for viewport for to avoid known hotspots the viewport. The most useful benefit PCCP is make complex system to hackers. Users have to choose clickable area within the area and cannot click outside of the viewport unless they press the shuffle button to randomly reposition the viewport. When password gets created users may shuffle many times as he want. Only during the password generation, the viewport & shuffle buttons are displayed. After secrete word generation process, graphical images are presented to users casually without viewport & shuffle button. Then user has to choose exact clickable area on particular image.

III. PROPOSED SOLUTION & PROPOSED MODEL

The two way authentication needs to be developed for the users by using Persuasive Cued Clicked points technique and OTP, which can be effectively used for any system for secure login and but difficult to be guessed by attacker.

A. Registration Process:
B. Login Process:
Proposed model contains following points:

Proposed system provides a two way authentication to the users by using Persuasive Cued Clicked point's technique and OTP.
The user has to register him by entering his user name; mobile number and IMEI number and email ID.
Then user will have to select the five images with which he wants to generate the password by clicking one point on each image. After the five clicks unique password is generated and the registration process is completed.
Now every time the user wants to login will have to enter the username and select the continue button.
After user selects login, user will receive the binary OTP containing 5 bit binary code on his mobile.
Now user want to select the same points which he had selected at the time of registration for the images when the bit in the OTP is 1 and select any other point except the point select while registration for the image when the bit in the OTP is 0.
Only if the user has followed this process correctly, he/she will get the access to the system using login.

SYSTEM ARCHITECTURE

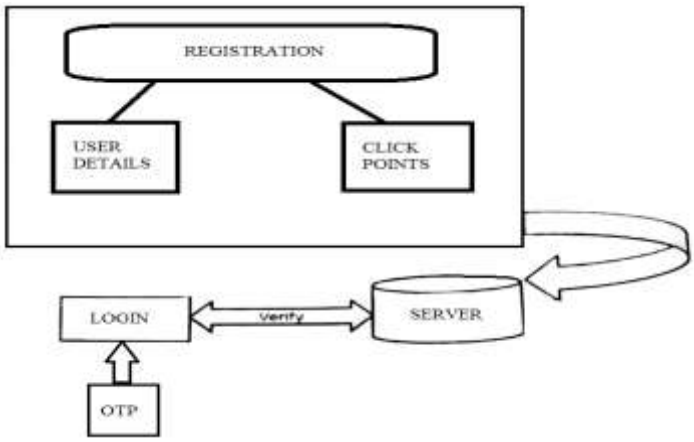

Fig 1.System architecture of proposed model

IV. FLOW

- In user registration module user can enter the user name in user name field which is also suitable tolerance value .When user entered all user details in the registration phase, these user registration data stored into data base which used during login phase for the verification.

- In the picture selection phase users selects 5 images as passwords and consist of one click-point on each image. The users may select any points in the image as click-points for their password.

- During password creation in that most of the image dimmed except for small view port area that is randomly positioned on image. Users have to select the click-point within the view port.

- To make password more secure Advanced Encryption Standard (AES) technique is used and password can be generated, authenticated & protected easily.

- During system login, the user will receive a binary OTP like "01110", the images are displayed normally, without viewport, and the users have to repeat the sequence of clicks in OTP order.

- User want to select the same points which he had selected at the time of registration for the images when the bit in the OTP is 1 and select any other point except the point select while registration for the image when the bit in the OTP is 0.

- If the clicked order matches with the OTP order then the user will able to access the further page, else if does not matches then the user will be redirected to login page.

V. CONCLUSION

The human brain is very efficient to remember the graphical passwords than of the text based passwords. Also the graphical passwords are recognizable to the user. An authentication system is to help user's select better passwords and thus increase the effective password space. Improved Persuasive Cued Click-Points (IPCCP) approach has tried to reduce the formation of shoulder surfing attack. This approach is effective at reducing the formation of hotspots and patterns; therefore it increases the effective password space. So, it is the better user authentication method by solving usability and security issues. The Improved Authentication Scheme Using Improved Persuasive Cued Click Points system is very efficient to use. This system founds very secure and flexible to use. This system allows very attractive GUI to user so user finds very attractive and convenient to use this type of password. This system also can be used as to provide higher level security to the text based password. This system is very cheap as compared of as biometrics system.

REFERENCES

[1] Neha Singh, Nikhil Bomanwar "Improved Authentication Scheme Using Password Enabled Persuasive Cued Click Point, 2015, IEEE.

[2] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Middle, P.C.van Oorschot "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism, 2012, IEEE.

[3] Arash Habibi Lashkari, Farnaz Towhidi, Dr. Rosli Saleh, Samaneh Farmand ,"A complete comparison on Pure and Cued Recall-Based Graphical User Authentication Algorithms", 2009, IEEE

[4] Maslin Masrom, Farnaz Towhidi, Arash Habibi Lashkari, "Pure and Cued Recall-Based Graphical User Authentication", 2009, IEEE

[5] Muhammad Daniel Hafiz, Abdul Hanan Abdullah, Norafida Ithnin, Hazinah K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique", 2008, IEEE.

[6] Fatehah M.D., Mohd Zalisham Jali & Wafa M.K., Nor Badrul Anuar, "Educating Users to Generate Secure Graphical Password Secrets: An Initial Study" 2013, IEEE.

[7] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey" 2005, IEEE.