Click Based Authentication For Accessing Web Accounts

Rohit Urade, Roshan Kumar, Dinesh Gawande, Sejal Jawade, Ashwini Awchat

Abstract— **The project aims to develop a good Authentication system that supports users in selecting good passwords easily for accessing different web accounts. Normally user has to memorize their text password at registration process and recall at login time, but text based passwords are used mostly for providing security, but they are unsafe to dictionary attacks, shoulder surfing,etc. A graphical password is alternative to text-based passwords, because people are better at memorizing graphical passwords than text-based passwords. In this project, for click based authentication we have used CCP (cued click points) technique, where Pixel co-ordinates on image are fixed as the password.**

This project is to provide superior authentication system to user by using images in there system as graphical passwords, and then storing authentication Credentials of web accounts in application. Next time when user login, user has to click on any web accounts then user will directly get login into there web accounts without entering authentication Credentials manually again.

Keywords— **Graphical Passwords, Computer Security, Authentication, Cued Click Points, Shoulder Surfing.**

I. INTRODUCTION

In this paper, a new click-based graphical password scheme for accessing web accounts called Click Based Authentication For Accessing Web Accounts. It can be viewed as a combination of PassPoints and Passfaces.

A password consists of one click-point per image for 'n' number of images in sequence. Next image shown to user is based on the previous click-point so users receive immediate implicit feedback, whether they are on the correct path. This Process offers both usability and security to user.

Click Based Authentication is a proposed alternative to PassPoints. In proposed System, users click one point on each of images rather than on different points on one image. Cued-recall offers instantly alert valid users if they have made a mistake when entering their latest click-point at which point they can cancel their attempt and retry from the beginning.

Each click results in showing a next-image, in effect leading users down a "path" as they click on their point's one after other. A wrong click takes down user to an incorrect path, this leads to indication of authentication failure. Users can choose their images only to the extent that their click-point dictates the next image.

II. LITERATURE SURVEY

Dhamija and Perrig [1] proposed a graphical authentication scheme where the user has to identify the pre-defined images to prove user's authenticity. In this the user selects a number of images from a set of random pictures displayed during registration. After registration process, the user has to login and identify the pre-selected images for authentication from a set of images as shown in figure 1. This system is unsafe from shoulder-surfing.

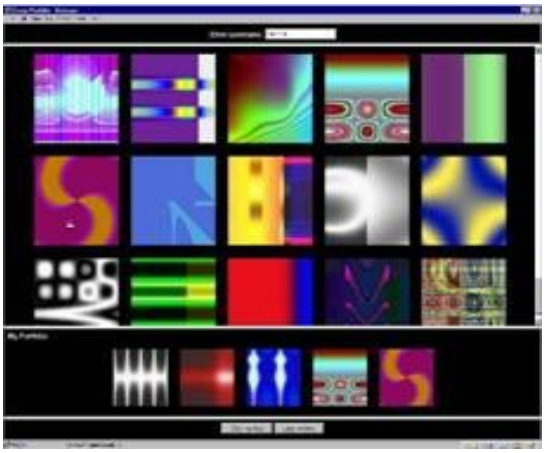

Figure 1: Dhamija and Perrig - Random images

Passface [2] is a technique where grid of nine faces is displayed to user and selects one face previously chosen by the user as shown in figure 2. Then, the user chooses four images as their password and the users have to select their pass image from eight other images. Since there are four selected images, this process has been done for four times.

Figure 2: Example of Passfaces

ISSN: 2278 – 1323

Jermyn [3] proposed a new technique called "Draw-a-Secret" (DAS) as shown in figure 3. Where the user has to draw the pre-defined picture on a 2D grid. If the drawing line touches the same grids in the same pattern, then the user is authenticated and given access to perform actions. This authentication scheme is unsafe from shoulder surfing.

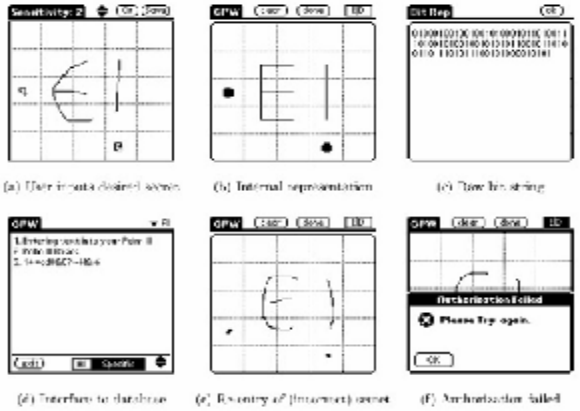

Figure 3: Jermyn - DAS technique

Haichang's [4] proposed a new shoulder-surfing resistant scheme as shown in figure 4. Where the user is required to draw a path or curve across their password images rather than clicking on them directly one by one. This graphical scheme is combination of DAS and Story schemes to provide authentication to the user.

Figure 4: Haichang's shoulder-surfing technique

III. PROPOSED SYSTEM

Aim of the project is to implement the Security features that can avoid Data Dictionary attacks in both the server and client side. To control the data dictionary attacks that occurs in direct internal way to the server and client. Graphical based password authentication is implemented where Pixel co-ordinates are fixed as the password. CCP (cued click points) techniques are added for more security.

Texts passwords are the most commonly used technique for authentication and have several drawbacks. Graphical passwords provide a promising alternative to traditional alphanumeric passwords due to the fact that humans can remember pictures better than text.

Our proposed system allows user choice while attempting to influence users to select complex passwords. It makes user not to select a weak password (easy for attackers to predict) it becomes more complex for attacker, due to this users are forced from making such choices.

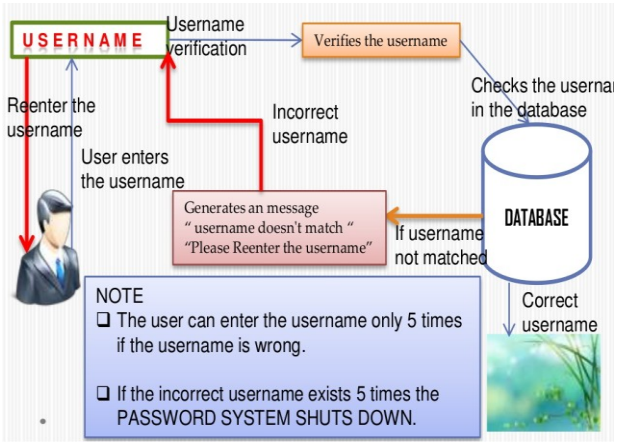

Figure 5: Verification of User

A simple graphical password authentication system that consists of a sequence of 'n' images and the user have to select the click points associated with one of the 'n' image in correct sequence for successful login. The user is permitted to click the pixel only five times, if the proper pixel co-ordinates don't match then the account of user will be blocked and need to contact the admin for activation of account again. So this process leads the hackers more tedious to enter server.

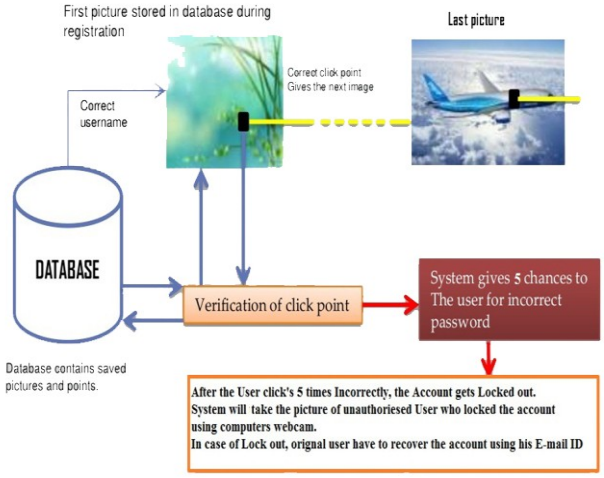

Figure 6: Account lock at unsuccessful login

When user select image and when he clicks on image then the image stored in database and click point is verified. If matched then it give access to new window or else it give user other chance to select correct image and correct click point to open application.

If user click's more than 5 times the account gets locked, then the system immediately take the picture of unauthorized user who locked the account using computer webcam, and store the picture in database.

The account can be recovered via registered email id, a verification code will be sent from unlock account form to the registered email id.

ISSN: 2278 – 1323

The verification code will be generated by the system randomly. When that code is entered in that form, the code in data base and entered code will be matched if it matches then the account gets unlocked.

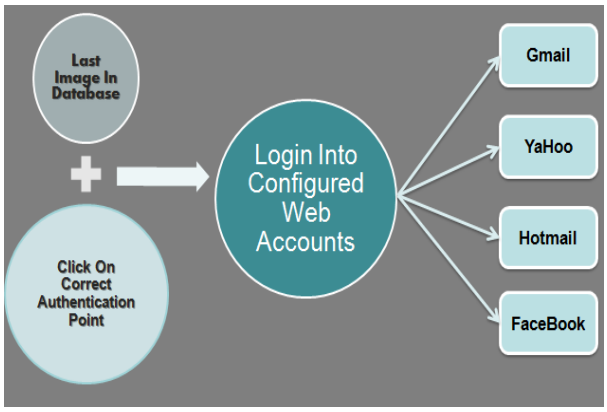

Figure 7: Login into Configured web accounts

After successful login the registered user gets access to login there 5 different web accounts (Gmail, Yahoo, Facebook, Rediffmail, Hotmail ...).

Here the user has already stored the Email-id and password of Web accounts, when user click on any web account (Gmail) then user should directly get login into there web accounts without entering authentication Credentials manually.

IV. SNAPSHOT OF OUTPUTS

Figure 8: Login Screen

Figure 9: New User Registration Form

Figure 10: Setting-up Lock code, No of images & Click point

Figure 11: Login screen For User after Putting Lock Code

Figure 11: Storing credentials to login next time automatically

ISSN: 2278 – 1323

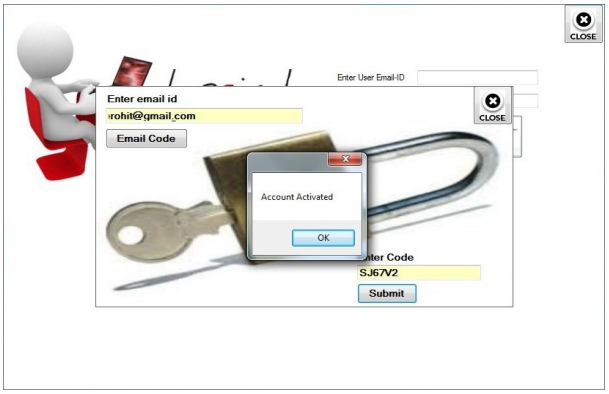

Figure 12: Recovery of Locked Account via Email

V. CONCLUSION

In this paper, a more secure graphical password authentication system is used to access different web accounts automatically without entering credentials every time manually in login page of web accounts.

The main reason for adaption of graphical password is that people are better at memorizing graphical passwords than text-based passwords. The system combines graphical password scheme along with a handheld device to form a new method of multi-factor authentication. This authentication scheme ensures the protection from threats such as key loggers, hotspot, shoulder surfing etc.

It offers a more secure alternative to PassPoints Authentication. This mechanism can be used for securing number of system which has highly confidential data.

It increases the workload for attackers by forcing them to first acquire image sets for each user, and then perform hotspot analysis on each of these images which was selected by user.

VI. FUTURE SCOPE

[i] It can be used to secure centralised servers which requires authentication like FTP Server, Web accounts, online banking, etc.

[ii] A virtual keypad can be provided through which password can be entered and can define some special characters in the character set for text passwords.

[iii] For graphical passwords we can draw images or symbols on the virtual screen and can use those images as passwords.

[iv]We can also implement this in mobile with android operating system.

[v] It can also be used in Folder Locker or an external gateway authentication to connect the application to a database or an external embedded device

VII. REFERENCES

[1] R.Dhamija and A. Perrig. "Déjà Vu: A User Study Using Images for Authentication". Proceedings of 9th USENIX Security Symposium, 2000.

[2] Real User Corporation: Passfaces. www.passfaces.com

[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin."The design and analysis of graphical passwords" in Proceedings of USENIX Security Symposium, August 1999.

[4] HaichangGao, ZhongjieRen, Xiuling Chang, Xiyang Liu UweAickelin, "A New Graphical Password Scheme Resistant to Shoulder-Surfing" 2010 International Conference on CyberWorlds.

[5] Aswathy Nair, Theresa Rani Joseph, Jenny Maria Johny— A Proficient Multilevel Graphical Authentication System *(IJSETR)* Volume 2, No 6, June 2013

[6] Priti Jadhao, Lalit Dole—Survey on Authentication Password Techniques. (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013

[7] Navnath D. Kale, Megha M. Nalgirkar—An Ample-Range Survey on Recall-Based Graphical Password Authentication Based On Multi-Line Grid and Attack Patterns. (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013

[8] Priti C. Golhar , Dr. D.S. Adane—Graphical Knowledge Based Authentication Mechanism. (IJARCSSE) Volume 2, Issue 10, October 2012 ISSN: 2277 128X

[9] K. Semmangaiselvi1, T.Vamsidhar2, KothaHariChandana*, B. Krishna Priya*and E. Nalina—An Effective Secure Environment Using Graphical Password Authentication Scheme. (IJECS) *Volume 2 Issue 2 Feb 2013 Page No. 383-490*

[10] *ASN Chakravarthy* , Prof. *P S Avadhani,* P. E. S. N Krishna Prasad *,N.Rajeev and D.Rajasekhar reddy "*a novel approach for authenticating textual or graphical passwords using hopfield neural network" Advanced Computing: An International Journal (ACIJ), Vol.2, No.4, July 2011.

ISSN: 2278 – 1323