PASSWORD AUTHENTICATION SYSTEM

[1]Shubhangi Bhakare, [2]Prof. Richa Sharma,

[1]M.Tech Student, [2]Professor, [1,2]Siddhivinayak College of Science and Hr. Education, Alwar, India.

[1]bshubhu@yahoo.com, [2]sharrma.richa02@gmail.com.

Abstract: In this paper comparison of exiting authentication system with a Persuasive Cued Click Points (PCCP) graphical method is presented. Previous system has their own drawbacks such as usability and security problems. Text based system have also security problems. Biometric systems have their own drawbacks. So we are providing alternative to these existing password authentication systems is Persuasive Cued Click Point (PCCP) authentication system. In this we encourage users to select more random and so make the password more difficult to guess.

Keywords: Authentication, Biometric, Graphical password, Toke.

I. INTRODUCTION

The most commonly and widely used computer authentication method is alphanumerical (Text Based) usernames and passwords. This method has been shown to have significant drawbacks. For example, generally at the time of registration users tend to choose passwords that can be easily remembered or guessable. On the other hand, if a password is hard to guess, then it is often hard to remember. To address such type of common problem, some researchers have been developed for authentication methods that use pictures as passwords.

Graphical password method is motivated by the fact that humans can remember pictures more easily than the text. Pictures can be easily remembered or recognized as compared with the text. If the number of images are large than the possible password space in graphical scheme is more than that of the alphanumerical password so it gives better resistance to the dictionary attacks. Because of these advantages the interest in the graphical password is increasing day by day. Graphical passwords can be used at workstations, web log-in application also in ATM machines and mobile devices etc.

II. EXISTING SYSTEM

A. Text-Based Passwords

In recent years, the traditional alphanumeric or text-based password have been clearly demonstrated. The users of password often aren't much aware of the security. They habitually use similar words as their password and that's why making it guessable. They need to use alphanumeric, lowercase, and uppercase to set a strong password which is difficult for the users to remember. The password which is typed by using keyboard or mouse can easily identified using key stroke, mouse movement and shoulder movement.

B. Biometric Security System

In case of the biometric security system the disadvantages are: Retinal scan and Iris Recognition system needs additional support of hardware and so they are very costly. Hand geometry and Fingerprint needs scanner device and these techniques are pointless for arthritis rheumatics, injury, dirtiness, , and roughness. In the Facial recognition system the accuracy result is very low and also it needs camera as additional device.

While considering the signature recognition, we need touch panel and optical pen. The accuracy is very less for signature recognition since the signatures are often changeable and easy signature is easily hack able and guessable.

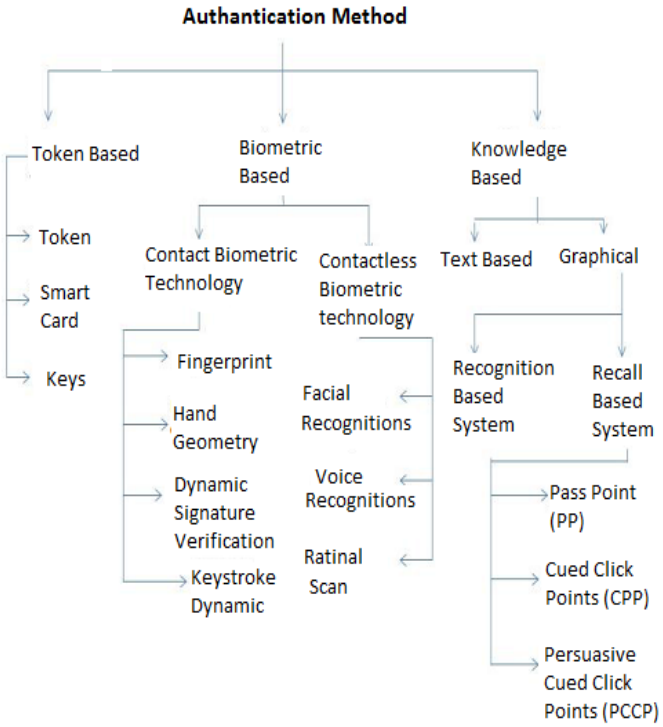

Fig.1 Methods of Authentication

III. PROPOSED SYSTEM

Password is a technique that requires users to select a predetermined set of images on the visual display presented in a GUI (Graphical User Interface). A user is only authenticated if he/she enters some images only in particular sequences. This ability to easily recall pictures by humans can be used for authentication in the similar way to the text passwords. Users can select elements appearing on a screen as part of their graphical password. These elements can be mathematical symbols, shapes, or touch/point some areas of an image to be authenticated. In addition to graphical password we have added sound signature to help in remembering the password. No system has been devolved uptil now which uses sound signature in graphical password authentication. Study also says that sound signature can be used to recall facts like images, text etc. In daily life we see various examples of remembering an object by the sound related to that object.

IV. OVERVIEW OF PROPOSED SYSTEM

Considering CCP as a base system, we have added a interesting persuasive feature to encourage users to select more safe and secure passwords, and to make it more hard to select passwords where all five click-points are hotspots. Specifically, when users created a password, the images were displayed for selection of click points . The images are selected by the user from drop down box to avoid known hotspots, since such information could be used by attackers or hackers to improve guesses and could also lead to the formation of the new hotspots. Users were required to select a click-point within viewport and they are not allowed click outside of this viewport. If they were unable to select a click-point in this region, they may press the “save” button to select another image. While users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. The save button and list of images only appeared during password creation.

V. CONCLUSION

To overcome the problem of old password authentication system such as security, hacking the password, we have given alternative to this is the Persuasive Cued Click Point (PCCP) authentication system. A key feature in PCCP is that creating a harder to guess password is the path of the least resistance, likely making it more effective than schemes where secure behavior adds an extra burden on users. The approach has proven effective at reducing the formation of hotspots and patterns, thus increasing the effective password space.

REFERENCES

[1] Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism presented by Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Student Member, IEEE, Alain Forget, Robert Biddle, Member, IEEE, and Paul C. van Oorschot, Member, IEEE, March/April 2012

[2] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, "Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism," Technical Report TR-11-03, School of Computer Science, Carleton Univ., Feb. 2011.

[3] P.C. van Oorschot and J. Thorpe, "Exploiting Predictability in Click-Based Graphical Passwords," J. Computer Security, vol. 19, no. 4, pp. 669-702, 2011.

[4] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-Surfing Resistance with Eye-Gaze Entry in Click-Based Graphical Passwords," Proc. ACM SIGCHI Conf. Human Factors in Computing Systems (CHI), 2010.

[5] P. Dunphy, J. Nicholson, and P. Olivier, "Securing Passfaces for Description," Proc. Fourth ACM Symp. Usable Privacy and Security (SOUPS), July 2008.

[6] B. Pinkas and T. Sander, "Securing Passwords against Dictionary Attacks," Proc. Ninth ACM Conf. Computer and Comm. Security (CCS), Nov. 2002.

[7] A. Duchowski, Eye Tracking Methodology: Theory and Practice, second ed. Springer, 2007.

[8] D. Florencio and C. Herley, "A Large-Scale Study of WWW Password Habits," Proc. 16th ACM Int'l World Wide Web Conf. (WWW), May 2007.

[9] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," Proc. Fourth Symp. Usable Privacy and Security (SOUPS), 2008.

[10] Iranna A M, Pankaja Patil, "Graphical password authentication using persuasive cued click point", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, July 2013

[11]https://www.ijareeie.com/upload/2013/july/20_GRAPHICAL.pdf

[12] http://documents.mx/engineering/implementation-of-knowledge-based-authentication-system-using-persuasive-cued-click-points.html

[13] www.ijarse.com/images/fullpdf/342.pdf

[14] www.enggjournals.com/ijet/docs/IJET13-05-03-004.pdf

[15] www.ijcttjournal.org/Volume16/number-3/IJCTT-V16P124.pdf

[16]https://www.ijsr.net/archive/v2i10/MIwMTMzNjY=.pdf

[17]www.ijdcst.com/pdf/Implementation%20of%2...20Authentication.pdf

[18] https://www.acsac.org/2005/papers/89.pdf

[19] Suo, Xiaoyuan, "A Design and Analysis of Graphical Password." Thesis, Georgia State University, 2006. http://scholarworks.gsu.edu/cs_theses/27

