International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue 01, Apr 2017

Graphical Password Authentication System (PCCP)

[1]Shubhangi Bhakare, [2]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 a Persuasive Cued Click Points (PCCP) graphical method is presented. In this we encourage users to select more random and so make the password more difficult to guess. This knowledge based authentication based system allows users to select the password with high security. In this system the user selects some images and one or more clicks per image as password. The sound signature used as a supportive system for easy remembrance of the password for the user. A sound signature is selected by the user per image for easy recalling of the click on the image.

Keywords: Authentication, CCP, Graphical password, Passpoint, Persuasive.

I. Introduction

In the proposed work a Persuasive Cued Click Points (PCCP) graphical method is presented. In this we encourages users to select more random and so make the password more difficult to guess. This knowledge based authentication based system allows users to select the password with high security. In this system the user selects some images and one or more clicks per image as password. The sound signature used as a supportive system for easy remembrance of the password for the user. A sound signature is selected by the user per image for easy recalling of the click on the image.

Recently network and computer security has been formulated as a technical problem. Human's are incapable of storing securely high-quality cryptographic keys which having acceptable speed and accuracy when performing these operations. New passwords techniques are developed in password security to protect the system. With the drawbacks of pervious methods i,e token based and biometric based authentication system .New system of graphical password authentication method developed.

II. LITERATURE SURVEY

Information security systems are used to permit authorized people in and to prevent unauthorized people from accessing a certain system. A security system allows authorized people do what they are allowed to do only. Security systems always require a user to identify him/herself. Once the identification process has been successes, the person will have to prove that identity-which is where authentication comes in. Authentication does not have to be able to identify a random person as X, but rather only prove that person X is who he/she says he/she is during the identification process. A graphical authentication method increases security using the innate ability of humans to recognize visual information. Such an approach reduces the trouble of remembering passwords, is relatively cheaper because it does not require extra hardware. We propose a graphical password method for authentication.

2.1 Authentication methods

Present authentication methods can be divided into three main parts:

- Token based authentication.
- Biometric based authentication.
- Knowledge based authentication.

2.1.1 Token based authentication.

Smart cards and bank cards are examples of widely used token based authentication techniques. Here every time user have to carry token with him/her. Also additional cost includes cost of token, replacement fees etc.

2.1.2 Biometric based authentication

Iris scan, Fingerprints, or facial recognition are some examples of biometric based authentication. The major shortcoming of biometrics is that setting up such systems can be costly and the identification process can be slow. This is because of the cost of card readers and scanners for widespread adoption. However, biometrics is known to provide the highest level of security. Biometrics can provide security in military, airports and government.

2.1.3 Knowledge based authentication techniques

Knowledge based authentication techniques are mostly used according to Suo et al (2006), and include text-based passwords. Users often create memorable password that are easy to for attackers to guess and strong password are hard to remember for the users.

2.2 Proposed System

In picture-based password technique, a user is expected to get authenticated by identifying and recognizing the images he/she chose when he/she got registered by the system.

People find it easier to remember pictures in billboards or traffic signs because a picture is said to speak better than a thousand words. When people see pictures, they are able to later remember the pictures through conscious recollection.

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.

III. EXITING SYSTEMS

3.1 *Pass Point*

In the pass point technique user select N click points at time of selecting a password in registration step.

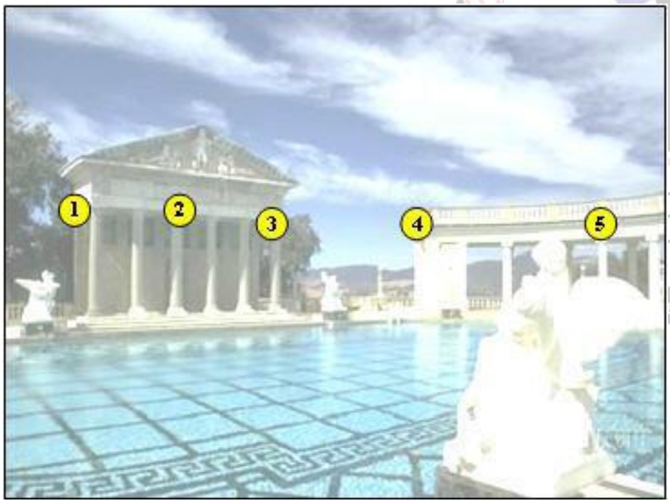


Fig 1 On PassPoints, a password consists of 5 ordered click- points on the image

3.2 *CCP (Cued click points)*

Cued Click Points (CCP) was designed to decrease patterns and to reduce the usefulness of hotspots for the attackers. Rather than five click-points on one image, CCP uses one click-point on five different images as shown in sequence. The next image displayed is based on the location of the previously selected click-points (Fig.2), creating a path through an image set. Users select their images only to the extent that their click-points determine the next image. Creating a new password with different click-points results in a different image sequences.

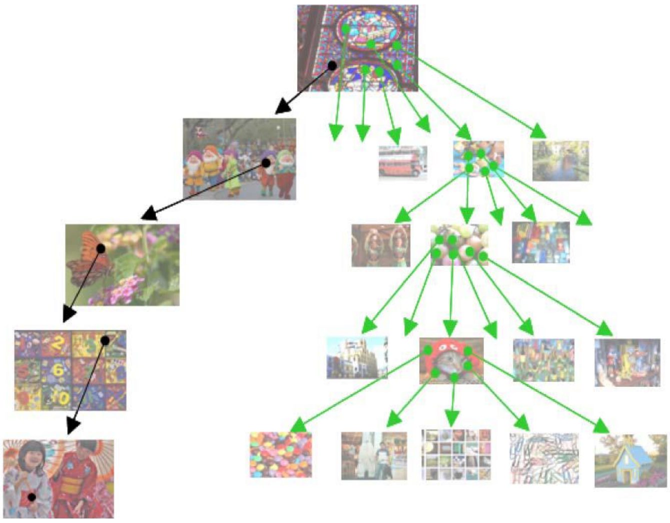
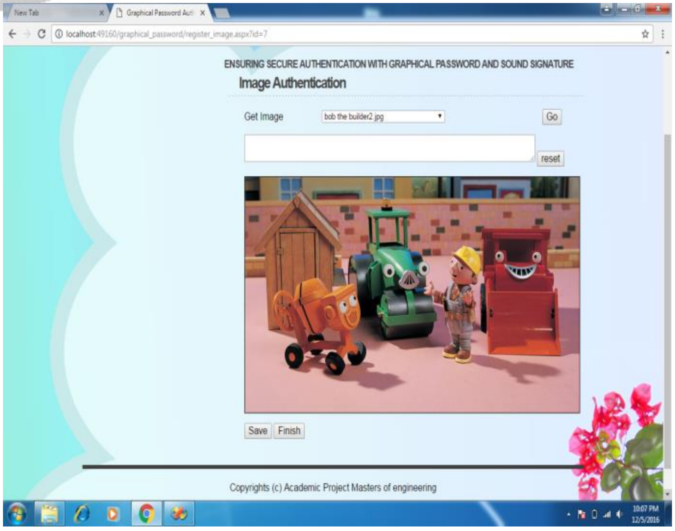


Fig. 2 A user navigates through images to form a Clue click point (CCP) password. Each click determines the next image.

IV. PROPOSED SYSTEM

Using CCP as a base system, we have added a persuasive feature to encourage users to select more 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 (see Figure 3). 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.



localhost:49160/graphical_password/register_image.aspx?id=7

ENSURING SECURE AUTHENTICATION WITH GRAPHICAL PASSWORD AND SOUND SIGNATURE

Image Authentication

Get Image: bob the builder2.jpg

Copyrights (c) Academic Project Masters of engineering

Fig. 3 PCCP Create Password interface.

1. Users will be less likely to select click-points that fall into the known hotspots.
2. The click-point distribution across users will be more

randomly spread and will not form new hotspots.
3. The login success rates will be higher than to those of the original clue click point i,e.CCP system.
4. When tolerance value is low, the login security success rates will increase.
5. Participants will feel that their passwords are more secure with Persuasive cued click point (PCCP) than participants of the original CCP System.

V. SYSTEM DESIGN

The system design consist of three modules such as user registration module, picture selection module and system login module (see Figure 4).

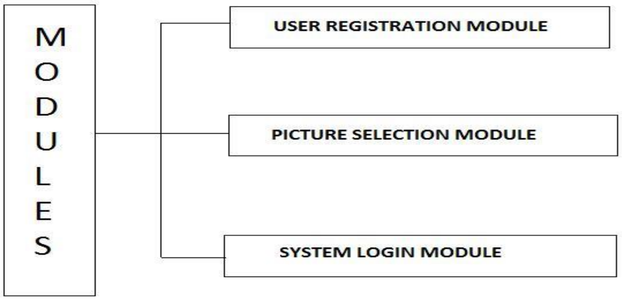


Fig 4 System Design Modules

5.1 In user registration module user enter the user name in user name field and also suitable tolerance value (tolerance value is use to compare registration profile vector with login profile vector). When user enters the user details in registration phase (Fig. 5), these user registration data stored in data base and used during login phase for the verification.

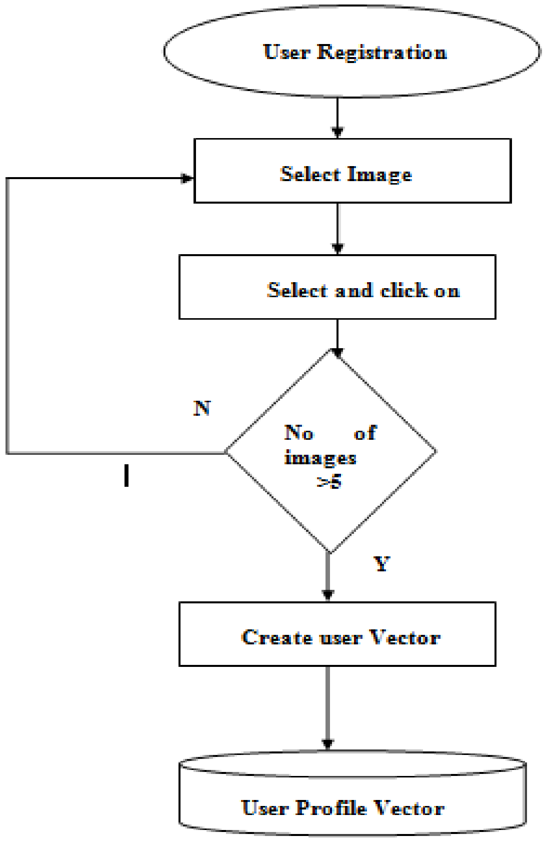


Fig.5 User Registration

5.2 In picture selection phase there are two ways for selecting the picture password authentication.
5.2.1 User defined pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
5.2.2 System defined pictures: In this pictures are selected by the user from the database of the password system.
In picture selection phase user select any image as the passwords and consist of a sequence of click-points on a given image. Users can select any pixels in the image as click-points for their password. Users have to select a click-point within the view port. If they are unwilling or unable to select a point in the current view port, they may reposition the view port by pressing the Save button randomly. The view port directs or guides users to select more random passwords that are less likely to include hotspots.

5.3 In this login procedure (Fig. 6), first user enters the unique user ID as same as entered during registration phase. Then images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within the system-defined tolerance square of the original click-points. After done with all these above procedure, user profile vector will be opened.

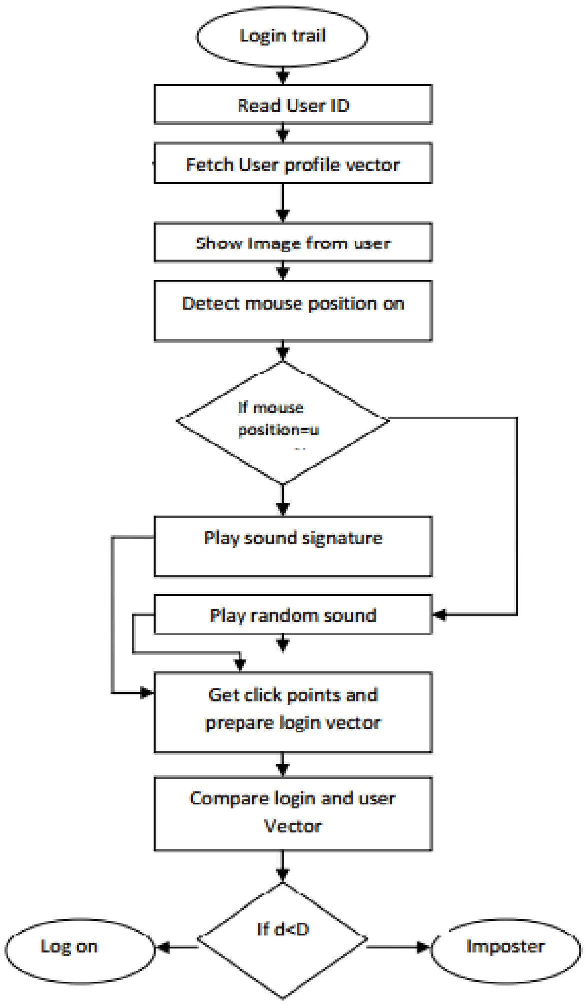


Fig.6 Login Process

5.4 Comparison between login Success rate and security success rates of existing CCP and proposed PCCP Success rates are reported on the first attempt and within the three attempts. Success on the first attempt occurs when the password is entered correctly in the first try, with no mistakes. A success rate within three attempts indicates fewer than three mistakes. Mistakes occur when the participant presses the Login button but the password is incorrect.

	CCP		PCCP	
	Success rate (%)	Security Success rate (%)	Success rate (%)	Security success rate (%)
User1	4/5 (80)	20	3/5 (60)	40
User2	3/5 (60)	40	2/5 (40)	60
User3	5/5 (100)	0	4/5 (80)	20
		20 (mean rate)		40 (mean rate)

TABLE 1 Comparison of PCCP with CCP

VI. CONCLUSION

PCCP encourages and guides users in selecting more random click-based graphical passwords. A key feature in Persuasive cued click point (PCCP) is that creating a secure password is the "path-of-least-resistance", making it likely to be more effective than schemes where behaving securely adds an extra burden on users. The approach has proven effective in the reducing the formation of hotspots, avoid shoulder surfing problem and also provide high security success rate, while still maintaining usability.

We have proposed a approach which uses sound signature to recall graphical password click points. No previously developed system used this approach. This system is helpful when user is logging after a long time. In future other patterns may be used for recalling purpose like touch or smells, study shows that these patterns are very useful in recalling the associated objects like images or text.

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.

[1] 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.

[2] 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.

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

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

[5] http://www.iosrjournals.org/iosr-jce/papers/Vol12-issue2/G01223946.pdf?id=11

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

[7] www.ijesrt.com/issues pdf file/Archi...0AND PASSFACES.pdf

[8] https://www.ijsr.net/archive/v2i10/MDIwMTMzNjY=.pdf

[9] http://www.ijact.in/index.php/ijact/article/download/302/253

[10]www.ijcsits.org/papers/vol3no52013/8vol3no5.pdf

[11]http://jpinfotech.org/wp-content/plugins/infotech/file/upload/pdf/5663Persuasive-Cued-Click-Points-Design-Implementation--and-Evaluation-of-a-pdf.pdf

[12]http://irjmwc.com/wp-content/uploads/2013/07/COIM-012.pdf

[13]www.ijreat.org/Papers 2013/Issue5/IJREATV1I5036.pdf

[14]https://www.scribd.com/document/261946351/20-Graphical

[15]https://www.scribd.com/document/335753548/Secure-Authentication-Using-Click-Draw-Based-Graphical-Password-Scheme

[16]http://www.chennaisunday.com/Java%202012%20Base%20Paper/Persuasive%20Cued%20Click-Points.pdf

[17] http://www.ijarse.com/images/fullpdf/342.pdf.