IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

A Persuasive Cued Click-point based Authentication Mechanism with Dynamic User Blocks

D.Anu Radha

Computer Science and Engineering,
C.Abdul Hakeeem College of Engg. And Tech
Vellore, Tamilnadu, India.

Abstract

The usability goal for knowledge-based authentication systems is to guide the users in creating graphical passwords to implement better security. Instead of having the security level being fixed for all the applications, The PCCP with dynamic user blocks approach presents a more feasible way of varying the security level depending upon the user's requirements. While guiding the user to choose the click points, the proposed system lets the user to select the security level needed. In order to help the user to memorize the password audio support can also be provided. Thus the system influence the user to create a click based graphical password, which is more random, so that it will be more difficult for the hackers to guess it.

Keywords: *PCCP with dynamic user blocks, Persuasive technology, Password registration, User login process.*

1. Introduction

To validate the end user for authentication we usually prefer to adopt the knowledge-based authentication, which involves text based passwords. The text based passwords are vulnerable to be hacked. The attackers can easily guess the text passwords with other details of the system. If we want to avoid this, the system can assign a strong password, which the attacker cannot guess. But the system assigned passwords are very difficult to memorize and remembered by the user. The study on the graphical passwords states that the click point passwords are hard to guess by the attacker and easy to remember for the users. So the password authentication system should encourage the strong password selection while maintaining the memorability of the user.

This paper proposes the idea of persuasive cued click point authentication with dynamic user blocks. This scheme influence the user to set a random password which cannot be guessed and also being graphical, the user can easily remember. In practical situations the same user will require different level of security for different types of applications over internet. But the existing system provides a concrete security level, which is same for all users and applications. It sets the threshold range as a fixed one whose size cannot be changed. In the proposed system the size of the threshold area is set by the user, depending upon his/her current requirement, with the help of dynamic user blocks. To increase the memorability of the user, audio support can also be provided, i.e. each click point is randomly associated with an audio sound. So that genuine user can be alarmed for wrong clicks. The previous works does not answer this problem of helping the user to remember the graphical password.

The background of the research work is outlined in the next section. The Persuasive Cued Click Point mechanism and its proof are discussed in section 3. The concept of this proposal is described in section 4. Section 5 briefs about the security analysis of this scheme with the help of PCCP method proofs. The possible extensions are listed out in section 6.

2. Background

Even though text passwords are the most popular user authentication method, they have security and usability problems. The alternatives for text based passwords such as biometric systems and tokens have their own drawbacks [9],[10],[11]. A graphical password scheme using click point offers the best alternative for the text password, and is discussed in this paper.

2.1 PassPoints

This system was developed early in the evaluation of graphical passwords, and in this, the user is given with an image. The click points on the image are used as the password for user authentication. The user has to remember the order and position of the click points. The click points are not stored as such, but as a hashed value.

For correct validation, discretization square is used which is the tolerance area around the original click point. The

user should click on the discretization area. Here, the system does not have any influence over the selection of the click points. The user is free to set the password which the user can easily remember. Since it is being very simple, it can easily be attacked.

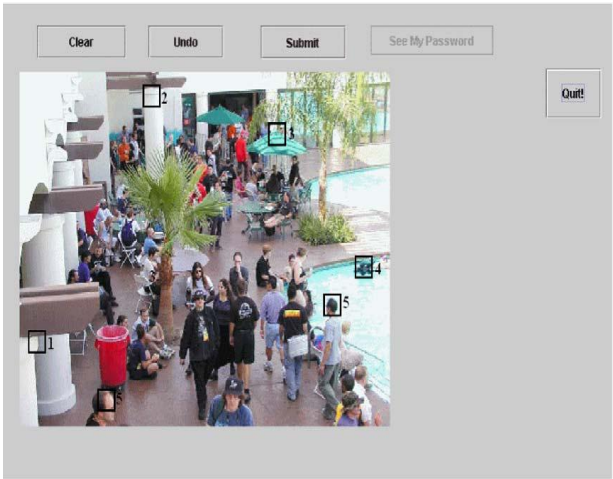

Fig1: PassPoints with discretization area.

2.2 Cued Click Points (CCP)

The cued click point method uses a series of images for click point password creation. The position of the click point on the previous image decides the next image to appear. It offers cued-recall and introduces visual cues that 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).

The image used has the size 451x331 pixels and a tolerance square of 19x19 pixels. The candidate image or image, thus have approximately 400 squares. To have better discretization, 3 overlapping squares are assigned.

So, in a candidate grid there could be 1200 squares. If a click on the first image is correct (by considering the tolerance squares), the user gets the next correct image. Once the user practiced with the usage of click point password, user can readily understands when he/she clicks the wrong point, by looking at the next image.

In this scheme also user is free to select the graphical password without system's intervention. So the attackers can easily guess the hot spot, which is the area where most of the users will tend to click. If the hacker is succeeded in guessing the hot spots in the images then the hacker can log in to the system easily.

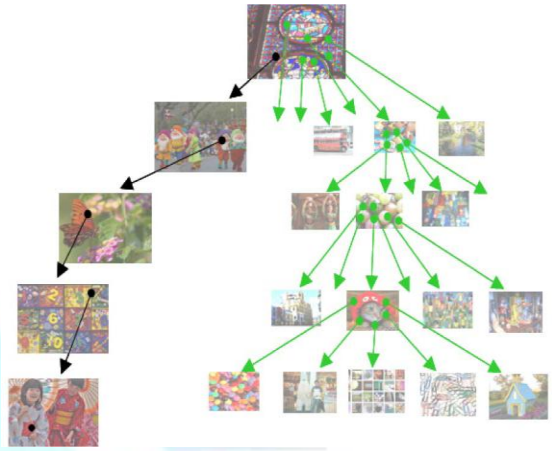

Fig2: User navigation in creation of CCP password.

2.3 Persuasive Technology

Persuasive Technology used to motivate and influence people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, not the system-generated passwords.

Even though the users are guided, the resulting passwords must be memorable. This persuasion makes the password stronger by avoiding the hot spots in almost all the cases. The click points are more randomly scattered to avoid the correct guess by the attackers.

3. Persuasive Cued Click Points (PCCP)

Using a skewed password distribution the attackers can guess the password in the previous graphical password schemes. Without the system guidance most of the users clicks on the hotspot in each image. In this method the system influence the user to select more random clicks, and also maintains the user memorability.

In this scheme when the image is displayed the randomly selected block called the view port only clearly seen out. All the other parts of the image are shaded, so that the user can click only inside the view port.

This is how the PCCP influence the user to select the position of the click point. The view ports are selected by the system randomly for each image to create a graphical password. It will be very hard for the attackers to guess the click point in all the images.

The users are allowed to click anywhere in the view port. There is an option for changing the viewport position also. This option is called the Shuffle. There is a limit on the number of times the shuffle option to be used.

While users may shuffle as often as desired, this significantly slows password creation. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images.
Like PassPoints and CCP, login click-points must be within the defined tolerance squares of the original points. The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications.

Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. Whereas text passwords have very skewed distributions resulting in an effective password space much smaller than the theoretical space, PCCP is specifically designed to significantly reduce such skews. The recall studies of the PCCP approach proved that remembrance of the graphical password is much better than the text-based passwords.

Fig3: PCCP Create Password interface. The viewport highlights part of the image

4. PCCP with Dynamic User Blocks

In PCCP approach the image of size 451x331 pixels is segmented in to approximately 400 blocks of size 19x19 pixels. This block is called the tolerance block or the threshold range. Since the threshold area is fixed in PCCP method, the security level provided by it is rigid and concrete in nature.

There may be some situations where the security levels need to be decreased. In those situations this PCCP method will not be feasible. To address these requirements, a new system is proposed, where the user can decide how strong the security of the system should be.

The tolerance area or the threshold area determines the level of security of the target system. For each click point, it is enough for the user to click in the threshold area of that click point during login. If the threshold area is larger, then the security level is smaller and vice versa.

4.1 Password Registration

In this approach, the user provides the threshold range say n (in pixels), where 18<n<101. This user defined threshold value is saved for future login.The view port remains the same as that of the PCCP method. But the threshold area is made variable in this proposal. For each threshold area the system assigns a sound tone. Now, the image is ready to be displayed. When the image is displayed, only the view port portion of the image is visible which is random. Thus the system influences the user to select the click points to avoid the attacker guessing of the hot spots. When the user clicks on the view port, the assigned sound tone is played. The click points and the relevant sound tones are stored for future usage.

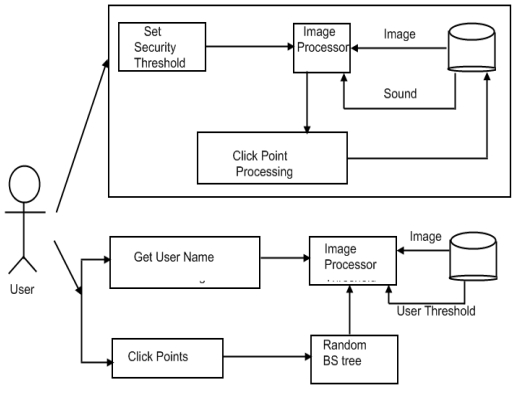

Fig4: PCCP with Dynamic user blocks –Architecture

4.2 User Login

To login to the system the user enters the name first. Then the images stored are displayed without the viewport separation. Now the user has to click on the correct threshold area. This can be checked by hearing the sound tone. Once the user get practiced with click points and sound tones, then, if the user by mistake clicks on a different threshold area, a different sound tone will be heard. With this difference the user can understand that he has clicked in a wrong position.

In the previous works, if any one of the clicks is wrong also, the system may not intimate in the middle of the login. At the end of login process only the user will come to know that a wrong click is given. And also which one is wrong is also not known to the user. To avoid these difficulties sound tones can be used.

This can be useful only to the genuine user not to the attacker. Because the sound tones are repeated for other threshold areas also, the attacker does not know which block gives a particular sound.

5. Security Analysis

In this section a discussion on how the proposed system may behave for password guessing attack and capture attack.

5.1 Password guessing attack

The most basic guessing attack against PCCP is a brute force attack, with expected success after exploring half of the password space (i.e., with a theoretical password space of 2^{43}, success after 2^{42} guesses). However, skewed password distributions could allow attackers to improve on this attack model. We now consider how these could be leveraged in guessing attacks.

PassPoint system hotspots of small number of users can be collected and an attack dictionary can be formed, with the use of server-side information. Then this dictionary details can be used for the guessing of the click point in an image. But this does not work in PCCP with dynamic user blocks scheme, because the view port does not include the hot spot in almost all cases. If the attackers gain the access to hash table entry of the passwords, they cannot correctly predict the original password, which are kept in a different database.

5.2 Capture attacks

Password capture attacks occur when attackers directly obtain passwords (or parts thereof) by intercepting user entered data, or by tricking users into revealing their passwords. For systems like PCCP, CCP, and PassPoints (and many other knowledge-based authentication schemes), capturing one login instance allows fraudulent access by a simple replay attack.

All three security schemes (PP, CCP, PCCP) are vulnerable to shoulder surfing threat. Observing the approximate location of click points may reduce the number of guesses necessary to determine the user's password. User interface manipulations such as reducing the size of the mouse cursor or dimming the image may offer some protection, but have not been tested.

Malware is a major concern for text and graphical passwords, since key logger, mouse logger, and screen scraper malware could send captured data remotely or otherwise make it available to an attacker.

For social engineering attacks against cued-recall graphical passwords, a frame of reference must be established between parties to convey the password in sufficient detail. One preliminary study suggests that password sharing through verbal description may be possible for PassPoints. For PCCP with dynamic user blocks, more effort may be required to describe each image and the exact location of each click-point. Graphical passwords may also potentially be shared by taking photos, capturing screen shots, or drawing, albeit requiring more effort than for text passwords.

6. Future Work

The following aspects can be added to the concept discussed above.

6.1 Varying the total number of click points

In order to improve the total security strength of the target system the number of click points used can also be increased while creating the graphical passwords. This can be achieved by setting the number of click point to be received from the user as a predefined value, say v. A number of view ports, which is equal to v are made visible on the image, for the user to click on it.

As soon as the clicks are selected by the user, different sounds are associated with them. While logging on the user is prompted with respective sounds for every click on each image. This will improve the security of the system, but at

the same time it will increase the time consumed for registration and login.

6.2 View port size

The effective password space is determined by the area of the view port of all images displayed for the password creation. The password strength is increased with the password space. So to create a strong graphical password, which cannot be guessed easily, the area of the view port should be higher. It can be done by combining the adjacent user blocks to form the view port. This idea may increase the strength of the password but this will decrease the user memorability of the password.

6.3 Discretization of view port

In some occasions the user may accidentally click the point which is very near to the viewport, while logging in. If the user is genuine then he/she must be correctly logged in. Since we follow a very strict validation method, which requires the user to click on the view port, the genuine user cannot be allowed to use the application.

To avoid this situation, we can compute the discretization are for the view port displayed on each image. The user clicks are tolerated up to the discretization area. But this may reduce the robustness of the system.

7 Conclusion

The goal of a good authentication system is to provide a maximized of effective and secure password space. Here in this system the click point on the image have the scope of the view port area and since the view port cannot be exploited, the password created will be robust. Since shuffling of the view port increases the time for registration of new users, it is limited.

The graphical click point passwords are more random and strong, so that no hacker can guess it, but easy to remember. The security strength is decided by the user himself, depending upon the requirement. The audio sound accompanied with every click helps the genuine user to identify the wrong clicks. The attacker does not know the difference between right and wrong clicks with the sound.

This paper gives an idea of having a effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security level.

8 Acknowledgements

This paper was developed by having [1] as the base idea and lab studies done the implementation of [1] are taken as proof for this paper. Sonia Chiasson and her friends, Members of IEEE, are honorably well acknowledged here for their fruit full research work.

9 References

[1] 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", IEEE DEPENDABLE AND SECURE COMPUTING, March/Arril 2012.

[2] S. Chiasson, R. Biddle, and P. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[3] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing Users towards Better Passwords: Persuasive Cued Click- Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. 2008.

[4] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple Password *Interference* in Text and Click-Based Graphical Passwords," Proc. ACM Conf. Computer and Comm. Security (CCS), Nov. 2009.

[5] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2010.

[6] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords," Int'l J. Information Security, vol. 8, no. 6, pp. 387- 398, 2009.

[7] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.

[8] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[9] L. Jones, A. Anton, and J. Earp, "Towards Understanding User Perceptions of Authentication Technologies," Proc. ACM Workshop Privacy in Electronic Soc., 2007.

[10] L. O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," Proc. IEEE, vol. 91, no. 12, pp. 2019-2020, Dec. 2003.

[11] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.