IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. IV (May-Jun. 2014), PP 104-108
www.iosrjournals.org

Online Password Guessing Attacks by Using Persuasive Click Point with Dynamic User Block

P. Kalaivizhi[1], Dr. S. Thiru Nirai Senthil[2]
[1]*M.Tech(CSE), Prist University, CSE, Puducherry.*
[2]*Professor & Head, Dept.of Prist University, Puducherry.*

Abstract: *The goal of knowledge-based authentication system is to guide the users in creating graphical passwords. User often creates memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for user to remember. So the researchers of modern days use alternative methods where graphical pictures are used as a password. Human brain is good in remembering picture than textual character. Various graphical password techniques are used, now PCCP with dynamic user blocks approach presents a more feasible way of varying the security level depending upon the user's requirements. The proposed system lets the user to select the security level. In order to help the user to memorize the password audio support can also be provided. The system influence the user to create a click based graphical password, which is more random, so that it will be difficult for the hackers to guess it.*

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

I. Introduction

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 based password. To avoid this, the system can assign a strong password, which the attacker cannot guess. But the system assigned passwords are difficult to memorize and remembered by the user. Unfortunately, these passwords are broken mercilessly by intruders by several simple means such as masquerading, Eaves dropping and other rude means say dictionary attacks, shoulder surfing attacks, social engineering attacks. To mitigate the problems with traditional methods, advanced methods have been proposed using graphical as passwords. The graphical password 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 with dynamic user blocks. This scheme influence the user to select the random password which cannot be guessed and also being graphical, the user can easily remember. But the existing system provides a concrete security level, which 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 the genuine user can be alarmed for wrong clicks. The existing work does not answer this problem of helping the user to remember the graphical password. The major goal of this work is to reduce the guessing attacks as well as encouraging users to select more random, and difficult passwords to guess.

II. Background

Graphical passwords were first described by Blonder. Since then, many other graphical password schemes have been proposed. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA). An example of a graphical password uses an image on the screen and lets the user choose a few click points; these click points are the "password", and the user has to click closely to these points again in order to log in.

Graphical password systems can be classified as either recognition-based (image based scheme), cued recall-based (image based scheme) or pure recall-based (grid based scheme).

2.1Recall based techniques:

In this section we discuss recent there types of click based graphical password techniques:

1. Pass Points (PP)
2. Cued Click Points (CCP)

3. Persuasive Cued Click- Points (PCCP)

A graphical password scheme using click point offers the best alternative for the text password, and is discussed in this paper.

2.1.1 Pass Points

This system was developed early in the evaluation of graphical passwords, and in this, the user is given with an image. The user can click any click point in the image and it is used as a password. 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. The user should click on the discretization area. 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.

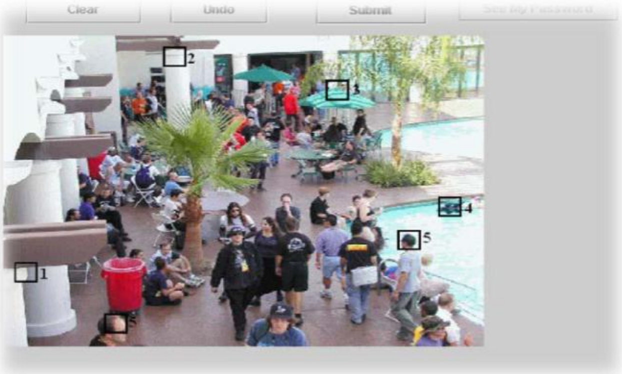


Fig1: PassPoints with discretization area.

2.1.2 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.

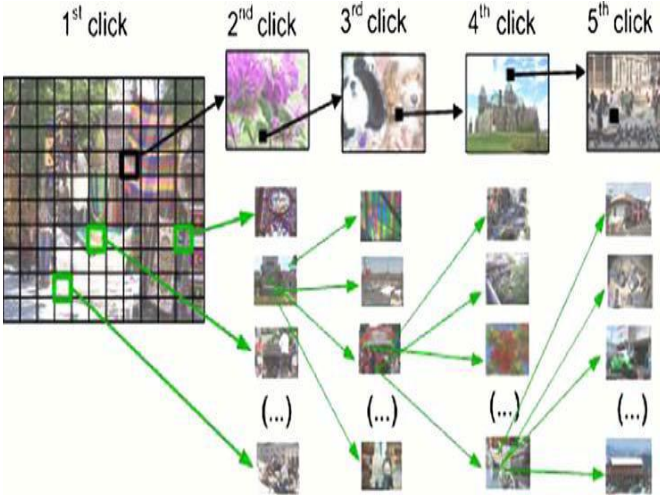
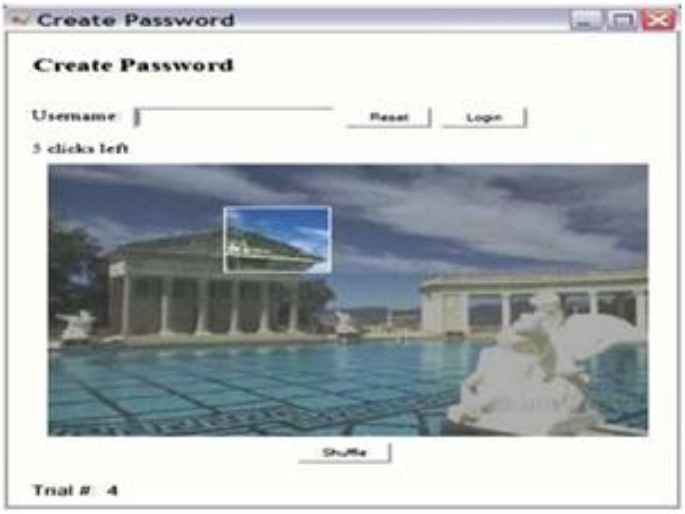


Fig2: Cued Click point



5 clicks left

Trial # 4

Fig3: PCCP with password creation interface. The viewport highlights part of the image

2.1.3 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. A user who is determined to reach a certain click-point may still shuffle until the view port moves to the specific location, but this is a time consuming and more tedious process.

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.

III. 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.

3.1 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.

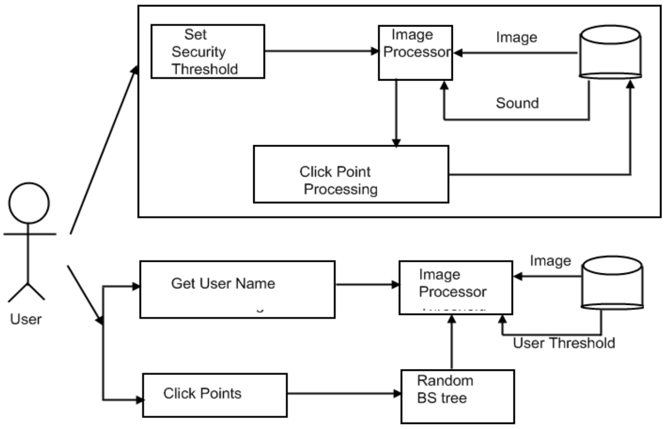


Fig4: PCCP with Dynamic user blocks –Architecture

3.2 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 can 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.

IV. Discussion

These are some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. More research is needed in this area Overall; we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

Guessing

Unfortunately, it seems that graphical passwords are often predictable, a serious problem typically associated with text-based passwords. More research efforts are needed to understand the nature of graphical passwords created by real world users.

Shoulder Surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. At this point, only a few recognition based techniques are designed to resist shoulder-surfing.

Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phasing web site to obtain Graphical passwords would be more time consuming.

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.

V. Future Work

5.1 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 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.

5.2 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.

5.3 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.

VI. Conclusions

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. 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.

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]. Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto, 'An association-based graphical password design resistant to shoulder surfing attack‟, International Conference on Multimedia and Expo (ICME), IEEE.2005

[3]. S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in *Proceedings ofMidwes Instruction and Computing Symposium*, 2004.

[4]. L. Sobrado and J.-C. Birget, "Graphical passwords," *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, vol. 4, 2002.

[5]. 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.

[6]. I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A.D. Rubin, "The Design and Analysis of Graphical Passwords," in *Proceedings of the 8th USENIX Security Symposium*, 1999.

[7]. S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.

[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]. 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.

[10]. Alain Forget, Sonia Chiasson, and Robert Biddle,"Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords", ACM 978- 1-60558-929-9/10/04, April 10 – 15, 2010.