PASSWORD-PERSUASIVE CUED CLICK POINTS: ADVANCED SECURITY FOR DESKTOP-BASED APPLICATIONS

ROMIL GANDHI AND VINAYAK SHINDE
Shree L. R. Tiwari College of Engineering, Department of Computer Engineering, Thane – 401 107, India
romil.gandhi@gmail.com, vdshinde@gmail.com

SACHIN BOJEWAR
Vidyalankar Institute of Technology, Department of Information Technology, Mumbai – 400 037, India
sachin.bojewar@vit.edu.in

ABSTRACT: This paper presents the concept of persuasive (graphical) cued click points (PCCP), and discusses their usability and evolution. A local survey regarding the largest issue in security was conducted with developers of various applications. This paper also describes the disadvantages of PCCP for desktop-based applications. The system proposed in this paper is different from PCCP in terms of usability and security. PCCP is a web-based system that does not provide the functionality required by desktop-based applications. To this end, this paper provides the concept of text-based password with PCCP that can be used to protect such applications.

KEYWORDS: Authentication, Keyloggers, PCCP, PPCCP, Reversers, RE, Security.

INTRODUCTION

The main concept underlying graphical cued click points is to eliminate text-based passwords and allow users to authenticate themselves through clicks. It is easy to use, and allows users to log in more quickly than password-based schemes. Owing to a few loopholes in graphical cued click points, a persuasive cued click points (PCCP) password protection scheme was proposed to reduce the hotspot, which is a weak point in an image that can be easily guessed by reversers or hackers. However, there remains a loophole that can help penetrate the system. The PCCP system will be discussed in Section III. The main concept of the system proposed is not to implement a web-based protection scheme, but instead to provide a similar level of security for desktop-based applications. In this paper, we propose a system called password-persuasive cued click points (PPCCP), which helps secure desktop-based applications by using the concepts of PCCP.

EVOLUTION OF PCCP

Text-based passwords were the first form of methods of authentication. In these, users have a maximum of two or three credentials, such as user ID/username and password, which are used for authentication. However, people find it difficult to remember different sets of passwords for different sites. Furthermore, since these provide the only protection to users against illegal access, passwords should not be stored or written anywhere. Hence, the concept of click points was invented. This involves selecting multiple points on an image to be authenticated to log in. This technique is called pass point, and consists of five clicked points in sequential order on an image. The user is required to click these points in sequence in order to log in. A tolerance region is

predefined for each click point. The disadvantage of this method is hotspots. This means that hackers attempt to enter coordinates that are likely to be the point in an image. Thus, through trial and error, the probability of a hacker logging into a user's account increases.

However, a single image cannot be used for protection, and the idea of using multiple images was proposed. Here, the user needs to remember and select multiple points on multiple images, where each image has one click point. As humans find it easier to remember click points rather than passwords, these schemes are more effective than text-based password schemes. Another method in the same vein is cued click points (CCP), which is more secure than both text-based passwords and pass points. CCP involves multiple images and a system-defined image. The user can select images as well as points on each image. If a user selects the wrong point on the first displayed image, random system defined images will be shown. However, if the user selects the correct point on a displayed image, the next image will be from the ones chosen by him/her in the selected sequence. The process continues until three or five images, selected by the user at the time of registration, have been correctly clicked.

The problem related to CCPs is that users generally create a pattern to remember the passwords. Therefore, a hacker can gain access to the system through trial and error. To reduce hotspots, the system should help the user select points in a more random manner, which can ensure greater security. This idea was first introduced by Fogg and is known as "Persuasive Cued Click Points" (PCCP) [1].

PCCP

PCCP [1][4][5][6] has all the functionalities of CCP [7] and the additional functionality of being persuasive. This additional functionality helps the user select random points to avoid common hotspots. The system provides a random window to the user to select points. This random window is called "viewport." The user only selects a point from this window, and can shuffle the window by pressing the "shuffle" button. This button is only available at the time of registration. Hence, for every image selected by the user to log in, the window is randomly defined by the system and provided to the user. In this manner, the probability of hotspots is reduced.

The functionality of CCP [7] is shown in Fig. 1. Every correct click leads to the next image, which eventually leads to successful login, and an incorrect click leads to a random system image. Persuasive CCP provides an additional functionality, as shown in Fig. 2.

EXISTING SYSTEM

Pass point, CCP, and PCCP are existing systems that are sufficient to provide security except when a keylogger is used. If installed on a remote PC, the keylogger can keep track of mouse and keyboard events, and can send the mouse coordinates to the recipient's (hacker's) email address. All existing systems are normally defined as web-based systems as the registration option is provided to the user.

PROPOSED SYSTEM

The proposed system is desktop based and comes with protection against keyloggers and debuggers. The system checks an application to determine whether any debuggers, disassemblers,

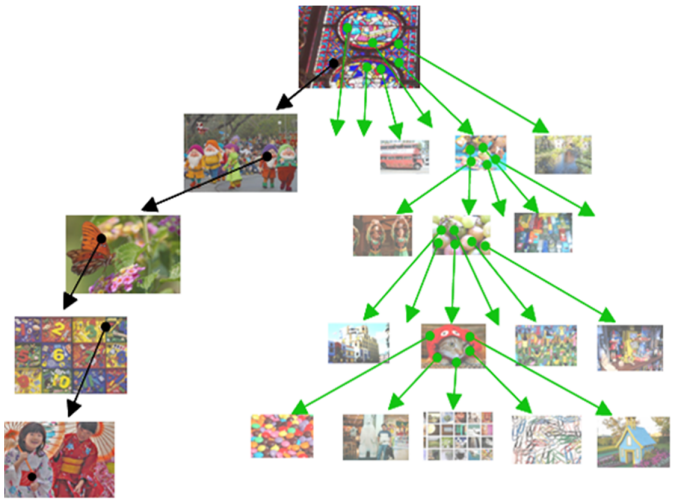

Figure 1 [1]. : Incorrect selection leads to random images

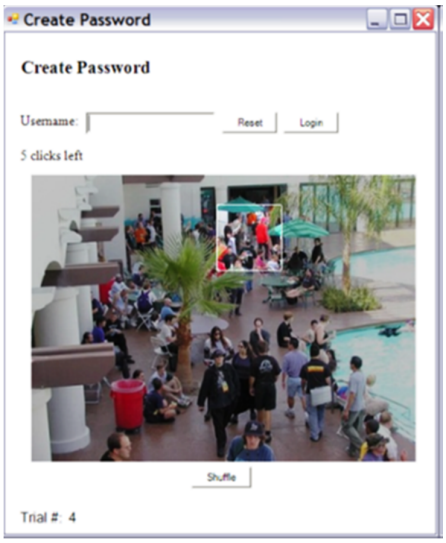

Figure 2 [1]. : Shuffle button helps to select different windows from which user can select the click point

or keyloggers are available and it terminates the application and attempts to uninstall it. This system is called password-persuasive cued click point (PPCCP) [1] [4] [5] [6]. The benefit of this application is that when software is sent to a customer, it is accompanied by a booklet containing pictures that show the points for the user to log in for the first time. The user will have separate images and different click points. The user can then choose whether he/she wants authentication

each time the relevant application runs. If the user chooses to be authenticated every time, he/she has the option to change the password and set images of his/her choice on which to select click points. The persuasive functionality helps the user select points in viewport or to shuffle the viewport by pressing the "shuffle" button [1].

This concept combines click points with password support [8], which means that the user is required to click on the correct point on an image and then enter the password. The application does not prompt the user for the password, nor does it show a password box. The user simply needs to enter the password. If the password is correct, the system moves to the next image. The user repeats the procedure—clicking on the correct point entering the password—until the login procedure is complete. The login procedure normally consists of three or five images to be authenticated. The viewport selected by system can be changed, depending on the security needed for an application [3].

The system also has a time frame [2] within which the user needs to enter the password after correctly clicking an image. Hence, the chances of shoulder surfing, dictionary attacks, or brute force are negligible [2].

The system is developed with the intention of enhancing security for the software development industry, and is a step forward in securing desktop applications against crackers.[1]

SURVEY

Before developing this system, it was necessary to conduct a survey to discover small glitches that normally occur in security following its development by different developers.

Table 1. Problems experienced by developers

Detection of all RE tools	Encryption/decryption algorithms are not strong	Demo version is not developed separately	The logic of serial key is in program itself
40%	-	-	-
-	20%	-	-
-	-	20%	-
-	-	-	20%

As Table 1 shows, detection of RE[2] seems to be the major issue, and there are many RE tools available online. It is thus easy for a hacker to crack the application. Hence, the proposed system will check for existing cracking tools in an application and, if any are found, will terminate and uninstall the application without user intervention, though it will notify the user. Legitimate users

[1] "Crackers" here refers to people who reverse the application in search of a key, serial, make patch, or keygens in order to illegally operate the full version of the application.
[2] RE (reverse engineers) here refers only to people who crack a program to illegally procure its full version.

can scan the system to locate the problem by using antivirus programs. The automatic uninstallation is intended to protect the user's system from crackers.[1]

CONCLUSION

The PCCP system provides adequate security for web-based systems. It is easier to use than text-based password schemes. However, it is not feasible for desktop-based applications because it does not consist of techniques such as detection of RE tools and keyloggers. When we install an application on a system, the security required by the application is considerably different from web application. There is a requirement for a security measure that is sufficiently feasible to use and protect the application. PPCCP is the one of the solutions that attempts to enhance security by covering loopholes and by providing a better and easy interface compared to conventional techniques.

RESEARCH AND FUTURE SCOPE

The proposed system can enhance security and provide a new approach to ensure security. There are many features that can be introduced in the proposed system in order to fulfil user demands of security for desktop applications. The combination of text-based passwords and PCCP will enhance security, as a module to detect the presence of debuggers and keyloggers and the automatic uninstallation of suspicious applications and the removal of keyloggers will help improve security.

REFERENCES

S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. van Oorschot, "Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism," *IEEE Transactions on Dependable And Secure Computing*, Vol. 9, No. 2, 2012.

M. S. Umar, M. Q. Rafiq, and J. A. Ansari, "Graphical user authentication: A time interval-based approach," *IEEE International Conference on Signal Processing, Computing and Control (ISPCC)*, 2012.

E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical passwords," *ACSAC '10*, Austin, Texas USA, Dec. 6–10, 2010.

S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *Int. J. Inf. Secur.* Vol. 8, pp. 387-398, 2009.

S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points, *British Computer Society*, 2008.

S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. C. van Oorschot, "Multiple password interference in text passwords and click-based graphical passwords," *ACM CCS'09*, Chicago, Illinois USA, Nov. 9–13, 2009.

U. D. Yadav and P. S. Mohod, "Adding persuasive features in graphical password to increase the capacity of KBAM," *IEEE International Conference on Emerging Trends in computing, Communication and Nanotechnology (ICECCN 2013)*.

G. Agarwal, S. Singh, and A. Indian, "Analysis of knowledge-based graphical password authentication," *The 6th International Conference on Comnputer Science & Education (ICCSE 2011)*, SuperStar Virgo, Singapore, August 3–5, 2011.