ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

EVALUATION OF USER AUTHENTICATION USING PERSUASIVE CUED CLICK POINTS (PCCP)

T. Ramyaramkumari
Research Scholar, Department of Computer science and Engineering, Bharath Institute of Higher Education and Research, Bharath University
Email:ramyaramkumari89@gmail.com

Received on: 15.10.2016 *Accepted on: 22.11.2016*

Abstract

Access to computer system is often based on the use of alphanumeric password but users have difficulty in remembering long password and also it reduces security since users reuse the same password for different systems or reveal other passwords as the users try to log in. Various graphical password schemes have been proposed to overcome the problems of text-based passwords. This paper presents integrated evaluation of Cued Click Point and Persuasive Cued Click Point.

Keywords: Authentication; Graphical password; Usable security.

1. Introduction

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service. In general password is a secret word or string of characters that is used for user authentication to prove identity, or for access approval to gain access to a resource. The easier a password is for the user to remember generally means it will be easier for an attacker to guess but the strong system-assigned passwords are difficult for users to remember. A password authentication system should encourage strong passwords and the authentication schemes allow user choice while influencing users to assign stronger passwords. In this system, the selection of weak password which is easy for attackers to predict is a more tedious task and discourages the users from making such choices. In effect, this approach undergoes the selection of more secure password by using various graphical password schemes. Rather than increasing the burden on users to remember long text passwords, it is easier to click the images which are assigned as passwords for the legitimate user. Image password with cued click points is a new way to have secure passwords, easy to remember and which is difficult for the attacker to guess. Systematic examination provides integrated evaluation of Cued Click Points (CCP) with Persuasive Cued Click Points (PCCP) covering issues such as usability, accuracy and security. Persuasive

Cued Click Points is prudent before practical deployment of new security mechanisms. The paper is organized as follows: Section 2 provides the related work about providing authentication using images. Section 3gives the overview of Cued Click Points and Persuasive Cued Click Points. Section 4 describes integrated implementation of Cued Click Points and Persuasive Cued Click Points. Section 5 describes the conclusion of this paper.

2. Background and Related Work

Users must select and remember passwords to protect an ever-increasing number of accounts. Systems sometimes provide on-screen advice on how to create more secure passwords (e.g., select something memorable that would be difficult for others to guess), give feedback about password choice (e.g., with a password strength meter), or force users to create passwords that comply with specific system-defined rules (e.g., the password must include both letters and numbers). Despite these strategies, users often select weak passwords. This occurs partially because users misunderstand the advice or requirements, underestimate the risks, and because limitations of human memory mean that the user must employ coping mechanisms in order to reduce the burden of remembering so many passwords. These coping mechanisms may include reusing passwords across several accounts, using predictable alphanumeric combinations, or storing passwords in an easily accessible, insecure location. The most popular user authentication method is using the text passwords which have security and usability problems. Alternative models such as biometric systems and tokens have their own drawbacks. In Pass Points, passwords consist of a sequence of five click-points on a given image where the users mayselect any pixels in the image as click-points for their password. In order to login in this case, the sequence of clicks has to be repeated in the correct order, within a system-defined tolerance square of the original click-points. Although Pass Points is relatively usable the security weaknesses make passwords easier for attackers to predict. S. Chiasson et.al [1] proposed Pass Points in which the sequence of click points in an image is assigned as passwords where even an authenticated user finds it hard to remember. In order to overcome the problem, Persuasive Cued Click Point approach is used. PCCP forms fake hotspots for unauthenticated user and leads the users to wrong sequence of images and finally displays as invalid password. A. Forget et.al [2] proposed the effectiveness of the security provided by various password creation policies. This is accomplished by modeling the success rate of current password cracking techniques against real user passwords. Data sets were collected from several different websites. This work focus on actual attack methodologies and real user passwords quite possibly makes this one of the largest studies on password security. The results meant for standard password creation policies such as minimum password length and character set requirements. L. O'Gorman et.al [4] compared Passwords, Tokens, and Biometrics for User Authentication. The password has been the standard means for user authentication on computers. However, users are required to remember more, longer passwords, it is evident that a more convenient and secure solution to user authentication is necessary. This work examines passwords, security tokens and biometrics of all authenticators and then finally compares these authenticators and their password combinations. The effectiveness against several attacks and suitability for particular security specifications are detected. R. Biddle et.al [6] proposed a comprehensive review of graphical passwords in order to protect secret information from sensitive and various applications. In this work Secured authentication system was incorporated since it contains security and confidentiality. Secured Authentication Protocol System using images ensures confidentiality and ensures authentication using server. Even if it is assumed that the cryptographic primitives are perfect, the security goals may not be achieved. The system itself may have weaknesses that can be exploited by an attacker in network attacks.

3. Cued Click Point

Graphical passwords offers an alternative to text-based passwords that is intended to be more memorable and usable because graphical passwordsrely on our ability to more accurately remember images than text. In Cued Click Points (CCP), passwords consist of a click points on a sequence of given images. Users may select any point in the image as click-points for their password. To log in, the legitimate users selects the correct click points in the correct sequence of images. Each click must be within a system-defined tolerance region of the original click-point. The usability and security of this scheme was evaluated by the original authors and subsequently by others. It was found that although relatively usable, security concerns remain.

3.1 Persuasive Cued Click Point

Providing implicit feedback in Cued Click Points before the final click-point could allow the attackers to mount an online attack to prune potential password subspaces, whereas PCCP's visual cues will not help attackers in this way. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image. Persuasive Cued Click Points has the advantage of minimizing the formation of hotspots across the users since click points are more randomly distributed. An online attack could be thwarted by limiting the number of incorrect guesses per account. Providing instructions while creating secure passwords using password managers or providing tools such as strength meters for assigning passwords had only limited success. The problem with such tools increases the workload of the users while creating secure passwords. In PCCP, creating a less guessable password is the easiest course of success.

4. Implementation

4.1 Cued Click Points

The primary security problem in various graphical password authentication schemes is hotspots in which different users tend to select similar click-points as part of their passwords. Attackers who gain knowledge of these hotspots through harvesting sample passwords or through automated image processing techniques can build attack dictionaries and more successfully guess Pass Points passwords. A dictionary attack consists of using a list of potential passwords and trying each on the system in turn to see if it leads to a correct login for a given account. To reduce the security impact of hotspots and further improve usability, an alternative click-based graphical password scheme called Cued Click-Points is proposed.

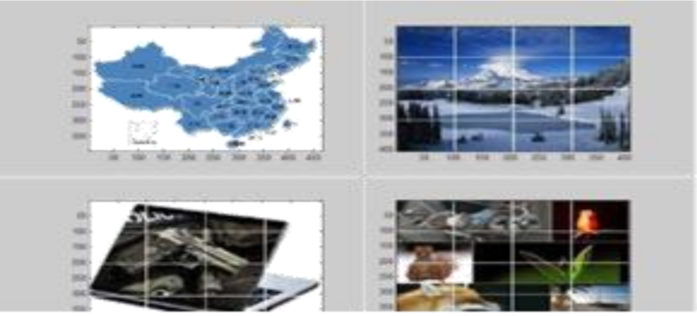

Fig.1.User navigates through images to form a CCP password. Each click determines the next image.

CCP implies that remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on by guesses, if attackers suddenly see an image basically those attackers do not recognize, whether their previous click-point was correct or incorrect. However, to an attacker without knowledge of the correct password, this cue is meaningless. Even though this clue is meaningless, unauthorized users may guess the click points by selecting the click points randomly and continuously. Implicit feedback of passwords was the main drawback of this method. If an attacker selects the wrong click points by continuous and random guesses then the next image (Fig. 1) which is assigned as password will not be displayed. Thus, security issues are still reported in CCP.

4.2 Persuasive Cued Click Points

Persuasive Cued Click Points is effective at reducing hotspots where hotspots are the areas of the image where users are more likely to select click points and also avoids patterns formed by click-points within a password. In PCCP, explicit indication of authentication failure is provided after the final click-point (Fig. 2) to protect against incremental guessing attacks. When the authorized user selects the correct click points which are assigned as their passwords then the users are allowed to log in their account.

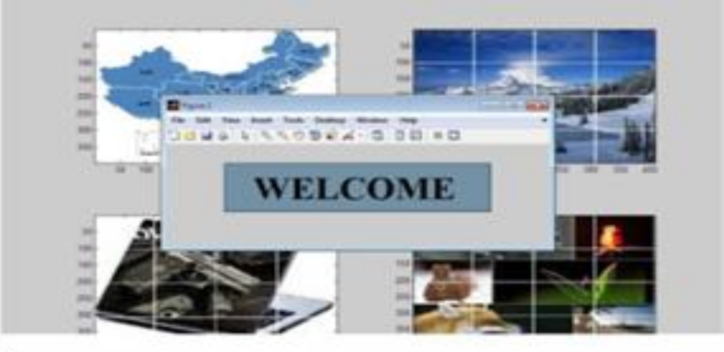
WELCOME

Fig.2. User navigates through images to form a PCCP password. Each click determines the next image

Persuasive Cued Click Point approach forms fake hotspots for unauthenticated user in order to lead the user to wrong sequence of images (Fig. 3) and finally displays as invalid password. PCCP reduces the formation of hotspots and patterns which leads to increase the effective password space. The attacker's task is more difficult in PCCP because not only the popularity of hotspots is reduced but the sequence of images must be determined and each relevant image collected making a customized attack per user.

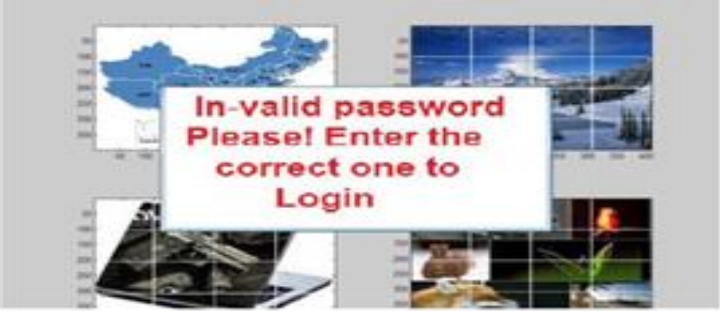
In-valid password
Please! Enter the
correct one to
Login

Fig.3.Fake hotspots for leading the attackers to wrong sequence of images.

5. Conclusion

Pass Points passwords are more robust than text passwords (assuming distinct background images). Often, the usability of a system is tested in isolation but in the case of passwords this is especially problematic because user behavior may change as users accumulate passwords. Users could more easily remember sequence of click-based graphical passwords than text passwords. In Pass point, sequence of click points in an image will be more difficult even for an authenticated user to remember. In Cued Click Point algorithm remembering only one click point per image appears easier for authenticated user than having to remember a sequence of click points on one image but still faces security problemsdue to implicit feedback of wrong click points. Persuasive Cued Click Points approach forms fake hotspots for unauthenticated user and leads them to wrong sequence of images and finally displays as invalid password. Thus explicit indication of invalid password after the final click point reduces the hotspots formed in the images and also increasing the security issues.

6. Scope for Future Work

For future work, challenge response interactions can be added in this project. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. Further access will be granted with the valid response. It can also limit the chances of entering the wrong passwords. Other image format can be used as passwords. Future work for PCCP includes testing PCCP for multiple password interference and conducting a field study to examine multiple password interference.

7. References

1. Elizabeth Stobert, Sonia Chiasson, Member, IEEE , Student Member, IEEE, Alain Forget, Robert Biddle, Member , IEEE, and Paul C.vanOorschot, Member, IEEE“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, March/April 2012.
2. Alain Forget, Sonia Chiasson, P.C van Oorschot, Robert Biddle, Influencing users towards better passwords: Persuasive Cued Click Points, April 2008.
3. Jim Waters, Susan Wiedenbeck, Jean-Camille Birget, Alex Brodskiy and NasirMemon, PassPoints: Design and longitudinal evaluation of a graphical password system International Journal of Human- Computer Studies Vol.6, No. 3, pp 102-127, April 2005.
4. L.O’Gorman, “Comparing Passwords, Tokens, and Biometricsfor User Authentication”, Proceedings of IEEE, Vol. 91, No. 12, pp. 2019-2020, December 2003.

5. M. Weir, M. Collins, S. Aggarwal andH.Stern, "Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords", Proceedings of ACM Conference on Computer and Communication Security (CCS), July 2010.
6. R. Biddle, A. Forget, E. Stobert, P. van Oorschot, and S. Chiasson, "Multiple Password Interference in Text and Click-Based Graphical Passwords", Proceedings of ACM Conference on Computer and Communication Security (CCS), November 2009.