INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 1791 - 1795
RECEIVED: 09-03-17 PUBLISHED: 24-03-17.
March 24, 2017

CUED CLICK POINTS GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

[1]M.Sugavanam, [2]Mr.T.Karthikeyan
[1]UG Scholar, Dept Of computer science and Engineering,Sri Balaji Chockalingam Engineering College, Arni,.
[2]H.O.D/ Assistant Professor, Dept of computer science and Engineering, Sri Balaji Chockalingam Engineering College, Arni.

Abstract

Click cued points is a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. The next image is based on the previous click-point. Performance was very good in terms of speed, accuracy, and number of errors. Users preferred CCP to Pass Point, saying that selecting and remembering only one point per image was easier, and that seeing each image triggered their memory of where the corresponding point was located. CCP also provides greater security than Pass Points because the number of images increases the workload for attackers. Various graphical password schemes have been proposed as alternatives to text-based passwords. Research and experience have shown that text-based passwords are fraught with both usability and security problems that make them less than desirable solutions. Psychology studies have revealed that the human brain is better at recognizing and recalling images than text. Graphical passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope. We propose a new click-based graphical password scheme called Cued Click Points (CCP). It can be viewed as a combination of PassPoints ,Passfaces , and Story . A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security. Users could quickly create and re-enter their passwords. Another feature of ccp is the immediate implicit feedback telling the correct user whether their latest click-point was correctly entered.

1. INTRODUCTION:

Normally, Passwords are used for, (a) Authentication (Establishes that the user is who they say they are), (b) Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and (c) Access Control (Restriction of access-includes authentication & authorization). Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point per image. In addition user is asked to select a sound

signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image.System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.

Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each of 5 images rather than on five points on one image. 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). It also makes attacks based on hotspot analysis more challenging. After some time, biometric and token based password authentication systems were introduced as an alternatives to the text password but again it has its own drawbacks as it requires extra hardware setup and cost to setup new system for it. After some time, as alternatives for all those methods introduced is graphical password authentication system as it is very cheap and best. As well as per psychological studies user can remember graphical passwords very well than text passwords. Graphical password is of three types: Click based graphical password scheme, Choice based graphical password scheme, Draw based graphical password scheme. In this paper proposed here, user clicks on single point of five images coming one after one in random sequence.

User has to click five points on five images at the time of login process. While register user sets five click points to pass during login process. While registering user sets five images from image pool or from local drive. Based on image selection system generates the new signature. While user come to login phase he has to select the point over the image then system again generates the new signature for that point and if both signatures are same then and then user can be said ad authenticated user. Otherwise system will go in finite loop and show multiple wrong images to click. In mid of these images system inserts the right image to give one more chance to authenticate the user.

2. RELATED WORK:

We propose and examine the usability and security of Cued Click Points (CCP), a cued-recall graphical password technique. Users click on one point per image for a sequence of images. The next image is based on the previous click-point. We present the results of an initial user study which revealed positive results. People use passwords for their security. Generally, everyone uses textual password. Textual password is combination of alphabets and numbers. People keep textual password as name of their favorite things, actors or actress, dish and meaningful word from dictionary.

More often the computer systems are access based on alphanumeric passwords. However users are difficult to remember long and randomized passwords, so that they create simple, short and insecure password.Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords.

Many portable devices need a simple authentication system to protect them from being used by an unauthenticated person such as a thief. The security of traditional methods such as pin codes or password.

3. TECHNICAL RIDE

User Interface Design:

This module is the user interface design for the user to access the secure system. It consists of user registration and user login. After registration and login, there is option to choose number of images and give click points for each chosen image. The user password is retrieved by using the image click points. In user registration module user enters the user name in user name. When user entered the all user details in registration phase, this user registration data is stored in data base and used during login phase for verification.

Picture Selection Module:

In picture selection phase user select any image as passwords and consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. Users must select a click-point in the image and proceed on the next image.

Cued Click Point (CCP):

In this method instead of selecting five points on an image, user selects one point per image for five images. next image as soon as a user selects a click point.The system determines the next image to display based on the user's click-point on the current image. It now presents a one to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect.

Sound Signature:

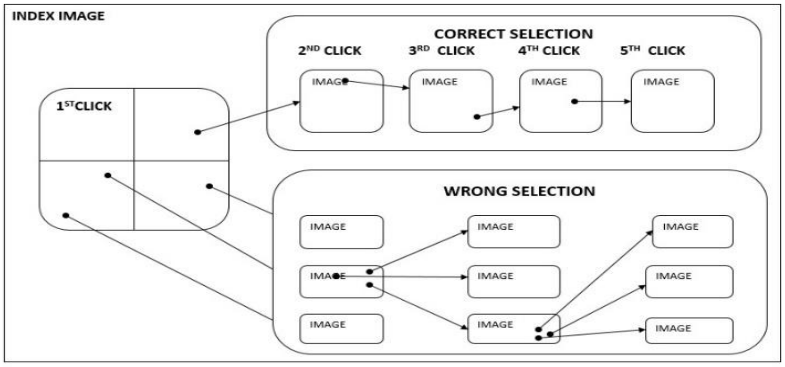
It Produce the Cude click point in Adding Sound Value In Identifying Correct Pixel In Password.

4. FUNCTIONAL RIDE:

CCP is a click-based graphical password scheme, a cued-recall graphical password technique. Various graphical password schemes have been proposed as alternatives to text-based passwords .It can be used as password for folder lock, web-driven applications, desktop lock etc. In this system user can choose the existing images from the database with almost any form (ie. Jpeg, png etc.). User can also able to upload own images while during run-time to register. Those images store in database. At the time of authentication those images appears for click for user to click. The security of click-based graphical passwords, as attackers can use skewed password distributions to predict and prioritize higher probability passwords for more successful guessing attacks. Visual attention research shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain an issue. Suggest that user choice in all types of graphical passwords is inadvisable due to predictability. We investigated whether the system

could influence users to select more random click-points while maintaining usability. The goal was to encourage more secure behavior by making less secure choices (i.e., choosing poor or weak passwords) more time consuming and awkward. In effect, behaving securely became the safe path-of-least-resistance.

5. CUED POINT SELECTION:



CONCLUSION:

A common security goal in password-based authentication systems is to maximize the effective password space. This impacts usability when user choice is involved. We have shown that it is possible to allow user choice while still increasing the effective password space. Furthermore, tools such as PCCP's viewport (used during password creation) cannot be exploited during an attack. Users could be further deterred (at some cost in usability) from selecting obvious click-points by limiting the number of shuffles allowed during password creation or by progressively slowing system response in repositioning the viewport with every shuffle past a certain threshold. The approaches discussed in this paper present a middle ground between insecure but memorable user-chosen passwords and secure system- generated random passwords that are difficult to remember. Providing instructions on creating secure passwords, using password managers, or providing tools such as strengthmeters for passwords have had only limited success. The problem with such tools is that they require additional effort on the part of users creating passwords and often provide little useful feedback to guide users' actions. In PCCP, creating a less guessable password (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action. Users still make a choice but are constrained in their selection.

SCOPE FOR FUTURE ENHANCEMENT

Another often cited goal of usable security is helping users from accurate mental models of security. Through our questionnaires and conversations with participants in authentication usability studies, it is

apparent that in general, users have little understanding of what makes a good password and how to best protect themselves online. Furthermore, even those who are more knowledgeable usually admit to behaving insecurely (such as reusing passwords or providing personal information online even when unsure about the security of a website) because it is more convenient and because they do not fully understand the possible consequences of their actions. To adding file system and document locking Encryption and decryption.

BIBLIOGRAPHY

[1] P. Golle and D. Wagner. Cryptanalysis of a cognitive authentication scheme. In Security and Privacy, 2007. SP'07. IEEE Symposium on, pp. 66-70. 2007.

[2] T. Grüter, M. Grüter, C.C. Carbon: Neural and genetic foundations of face recognition and prosopagnosia. In Journal of Neuropsychology, Vol 2(1), pp. 79-97. 2008

[3] N. Hopper and M. Blum. Secure human identification protocols. Advances in cryptology ASIACRYPT 2001 (2001): 52-66.

[4] D. Kim, P. Dunphy, P. Briggs, J. Hook, J.W. Nicholson, J. Nicholson, and P. Olivier. Multi-touch authentication on tabletops. In Proceedings of the 28th international conference on Human factors in computing systems (pp. 1093-1102). 2010

[5] S. Li and H.Y. Shum. Secure human-computer identification (interface) systems against peeping attacks: SecHCI. IACR's Cryptology ePrint Archive: Report 268, 2005.

[6] Xiang-Yang Li and Shang-Hua Teng. Practical human-machine identification over insecure channels. Journal of Combinatorial Optimization 3.4 (1999): 347-361.

[7] Z. Li, Q. Sun, Y. Lian, and D.D. Giusto. An association-based graphical password design resistant to shoulder-surfing attack. In Proceedings, Multimedia and Expo, 2005. ICME 2005.

[8] T. Matsumoto. Human-computer cryptography: An attempt. Proceedings of the 3rd ACM conference on Computer and communications security. 1996.

[9] T. Matsumoto and I. Hideki. Human identification through insecure channel. Advances in Cryptology—EUROCRYPT'91. Springer Berlin/Heidelberg, 1991.

[10] V. Roth, K. Richter, and R. Freidinger. "A PIN-entry method resilient against shoulder surfing." Proceedings of the 11th ACM conference on Computer and communications security. 2004.