A Graphical Password Scheme using Persuasive Cued Click Points

Moulisai Rachagundla[1], Syed Gulam Gouse[2]
[1]M.Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.
[2]Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.

ABSTRACT: *Despite the ubiquity of password systems, knowledge-based authentication mechanism remains an important and active research area. Many current systems have low level security, and even then users often devise insecure coping strategies in order to compensate for memorability and usability problems. Alternatives such as tokens or biometrics raise other issues such as privacy and loss. Various graphical password mechanisms have received considerable attention in response. A systematic review of the literature on graphical passwords shows no consistency in the usability and security evaluation of various schemes. The situation is similar for text passwords, making fair comparison between methods nearly impossible. This paper presents a graphical password scheme using persuasive cued click points. This method is based on knowledge based authentication.*

Keywords: *Authentication, Cued click points, Graphical password, Persuasive technology.*

I. INTRODUCTION

To validate the end user for authentication, we usually prefer to adopt the knowledge-based authentication mechanism, which involves text based passwords. The text based passwords [1] are vulnerable to be hacked. The hackers 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 hacker cannot guess. But the system assigned passwords are very difficult to memorize and also remembered by the user. The study on the graphical password mechanisms 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 scheme while maintaining the memorability of the user. This paper proposes the idea of persuasive technology [2] cued click point authentication with dynamic user blocks.

This mechanism 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 the internet. But the existing system provides a concrete security level, which is same for all users and the applications. It sets the threshold value as a fixed one whose size cannot be changed. In the proposed system the size of the threshold value 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 clip. So that legitimate user can be alarmed for wrong clicks.

II. LITERATURE SURVEY

A. Token based Methods

The traditional user name /password or personal identification number (PIN) based authentication scheme is an example of the Token Based. It is based on “something You possess”. For example, Smart Cards, a driver's license, credit card, a university ID card etc. It allows users to enter their user name/ password in order to obtain a token which allows them to fetch a specific resource- without using their user name and password. Once their token has been obtained, then the user can offer the token-which offers access to a specific resource for a time period- to the remote site[3].

B. Biometrics

Biometrics is the study of automated methods for uniquely recognizing human beings based upon one or more intrinsic physical or behavioral traits. It is based on “something you are”. It uses physiological or behavioral characteristics like facial or fingerprint scans and iris or voice recognition to identify users[4].

C. Knowledge based Authentication

Knowledge based authentication are the most extensively used authentication techniques and include both text based and picture based passwords KBA is based on “something You Know to identify you”. The major drawback of token-based and biometric- based authentication methods are expensive and requires special devices. Graphical- based password methods have been proposed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text Psychologists have confirmed that in both recognition and recall scenarios, the images are more memorable than text. Therefore, graphical- based authentication mechanisms have higher usability than other authentication techniques In general, the graphical password methods can be classified into two categories: Recognition-based[5] and Recall- based graphical techniques [6].

D. Click based Graphical Password

Graphical password mechanisms are a type of knowledge-based authentication that attempts to leverage the human memory for visual information. A precursor to Persuasive cued click points(PCCP) was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Rather than five click- points on one image, CCP uses one click-point on five different images shown in the sequence[7].The next image displayed is based on the location of the previously entered cued click-point (Figure. 1), creating a path through an image set. Users select their images only to the extent that their cued click-point determines the next image. Creating a new password with different cued click-points results in a different image sequence[8].

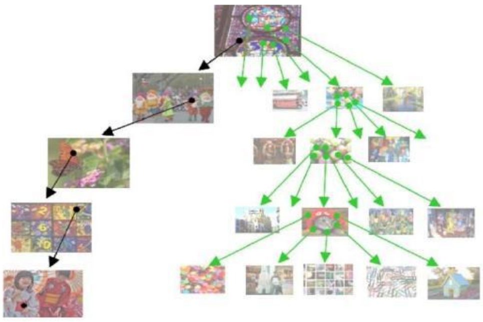


Figure 1: A user navigates through images to form a CCP password

E. Persuasive Technology

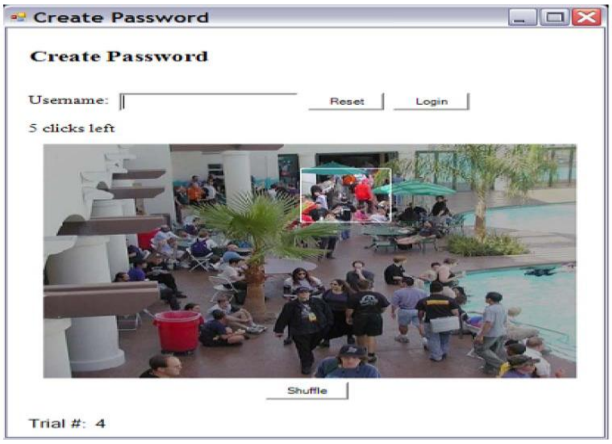
Persuasive Technology is a technology to motivate and influence people to behave in a desired manner. An authentication method which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive technology elements and the resulting passwords must be memorable. As detailed below, PCCP accomplishes this by making the task of selecting a low level(weak) password more tedious and time consuming [7]. The path of least resistance for users is to select a strong password (not comprised entirely of known hotspots or following a predictable pattern).The formation of hotspots across various users is minimized since click-points are more randomly distributed.

III. PERSUASIVE CUED CLICK POINT MECHANISM

Using a skewed password distribution the hackers can guess the password in the previous graphical password schemes. Without the system guidance most of the users clicks on the hotspot in each selected image. In this method the system influence the user to select more random clicks, and also maintains the memorability of the user. In this method 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 of the image. This is how the PCCP influence the user to select the position of the cued click point. The view ports of the image are selected by the system randomly for each image to create a graphical password. It will be very hard for the hackers to guess the click point in all the images.

The users are allowed to click anywhere in the view port of the image. There is an option for changing the viewport (Figure 2) position also. This option is called as “Shuffle”. There is a limit on the number of times the shuffle option to be used by the user. While users may shuffle as often as desired, this significantly slows down the password creation. The viewport and shuffle button appear only during password creation process. During later password entry, the images are displayed normally, without shading or the view port, and the users may click anywhere on the images. Like Pass Points and CCP, login click-points must be within the defined tolerance squares of the original points in the image. The theoretical password space for a password system is the total number of unique passwords that could be generated according to the given system specifications.

Ideally, a larger theoretical password space would 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, therefore PCCP is specifically designed to significantly reduce such skews. The recall studies of the PCCP approach proved that remembrance of the graphical password methods is much better than the text-based passwords.



Create Password

Create Password

Username:

5 clicks left

Trial #: 4

Figure 2: PCCP Create Password interface. The viewport highlights part of the image

IV. USABILITY EVALUATION AND SECURITY ANALYSIS

A. Usability of PCCP

PCCP has similar success rates to the other authentication mechanisms evaluated (CCP, PassPoints, and text). PCCP password entry takes a similar time to the other mechanisms in the initial lab sessions, but the results indicate longer recall times for PCCP when recalling passwords beyond the initial session. Users who shuffled more had significantly higher success rates in the PCCP Lab study, but the difference in success rates between high and low shufflers was not statistically significant for the two week or the web studies. Furthermore, users reported favorable opinions of PCCP in the post-task questionnaires; a general trend indicates that larger images or more click- points negatively impacts the password entry time. No clear pattern emerges between the 6 conditions for success rates, providing no evidence that either manipulation affects success rates in a consistent manner.

B. Security of PCCP

Given that click-point clustering and hotspots are significantly less prominent for PCCP than for CCP and PassPoints, guessing attacks based on these characteristics are less likely to succeed. Taking into account PCCP's sequence of images rather than a single image offers further reduction in the efficiency of the guessing attacks. For capture attacks, PCCP is susceptible to shoulder surfing and malware capturing user input during the password entry. However, we expect social engineering and phishing to be more difficult than for other cued recall graphical password methods due to PCCP's multiple images.

V. CONCLUSION

Graphical password schemes essentially use images or representation of images as passwords. Human brain is good in remembering images (pictures) than textual character. There are various graphical password methods or graphical password software's are available in the market. Therefore, this paper work merges persuasive cued click points and the password guessing resistant protocol. 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 by attackers. Well known security threats like brute force attacks and the dictionary attacks can be successfully abolished using this method.

REFERENCES

[1] 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.

[2] A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Improving Text Passwords through Persuasion," Proc. Fourth Symp. Usable Privacy and Security (SOUPS), July 2008.

[3] Wazir Zada Khan, Mohammed Y. Aalsalem and Yang Xiang ―A Graphical Password Based Systems for Small Mobile Devices, IJCS Issues, vol 8,Issue 5, No. 2, September 2011.

[4] Neil Yager and Ted Dunstone ―The Biometric Menagerie‖ IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 32, No. 2 February 2010.

[5] Sadiq Almuairrfi, Prakash Veeraraghavan and Naveen Chilamkurti ―Implicit Password Authentication System ― 2011 Workshops of International Conference on Advanced Information Networking and Applications.

[6] Xiaoyuan Suo Ying Zhu and G. Scott. Owen ―Graphical Passwords : A Survey.

[7] 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.

[8] X.S. Zhou and T.S. Huang, ― Relevance feedback For Image Retrieval: A Comprehensive Review,Multimedia systems, vol.8, no. 6 Apr. 2003.