IJDCST @Jan Issue- V-2, I-1, SW-16
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Dynamic Authentication over Persuasive Cued Click Points

[1] Amudalapalli Brahmaiah,[2] Dr Samidha Dwivedi Sharma
[1] NRI Institute of Technology & Science,Bhopal M.P.INDIA
[2] HOD IT & MCA, NRI Institute of Technology & Science,Bhopal M.P.INDIA

ABSTRACT: Nowadays, graphical password is being regarded as a promising alternative in network security to replace traditional text-based password in which users interact with images for authentication rather than input alphanumeric stings. Traditionally researchers develop a a click-draw based graphical password scheme (CD-GPS) with the purpose of improving the image-based authentication in both security and usability by combining the above three techniques. An initial user study which shows positive results that our scheme is good at both security and usability, and subsequently give a preliminary security analysis of our scheme against several well-known attacks (e.g., dictionary attack). But this application is not suitable for sufficient security considerations in large applications. Due to this problem of large site application development security, in this paper we proposed to develop an application is Persuasive Cued Click Points graphical password schema. An important usability goal for knowledge based authentication system is to support evaluations, and implementation considerations. Our experimental result shows multi image security using cued click points in sufficient large applications effectively.

Index Terms: Usable security, Authentication, graphical passwords, Sound Signature.

I. INTRODUCTION

User authentication is an important factor in computer and network security. Currently, the most commonly used method in the computer authentication is called text-based password in which users have to input their user names and text passwords for authentication. But previous research work has shown that the text-based passwords are suffered from both security and usability problems (i.e., users are likely to choose short and simple strings for easy memorization). To mitigate the drawbacks of traditional text-based authentication, graphical password schemes have been proposed as an alternative to text- based passwords according to the psychology studies that human brain is better at remembering and recognizing images than text (e.g., digital strings). An assumption here is that by reducing the memory burden, users can produce more secure passwords through using images (i.e., offering larger password space) than text-based password schemes.

In general, graphical password schemes can be divided into three categories1: click-based graphical password, choice based graphical password and draw-based graphical password. For the authentication, the click-based scheme requires users to click on the provided image(s) (i.e., choosing an object in an image), the choice-based scheme requires users to select a sequence of images (i.e., choosing images in a fixed sequence) while the draw-based scheme requires users to

draw some secrets (i.e., drawing a user signature). Previous studies and investigations have reported positive results by using image-based authentication (i.e., participants can remember their graphical passwords accurately after a long time). However, each category of the above graphical password schemes is suffered from some intrinsic limitations.

User authentication is a main component of almost all security applications. The weaknesses of using text based passwords for authentication are well known and there is a significant body of recent research exploring the feasibility of graphical approaches to provide a more secure and usable alternative. Based on the studies showing that human brain is best at recalling images than text, graphical positive identifications are to resolve memory burden and little password area problem of classical passwords. Another solution to generate strong passwords is password managers. These manager programs can be implemented as plug-ins to web browsers and they translate easy to remember and low-entropy passwords into stronger passwords, which are immune to dictionary, attacks. For maintaining the memorability, the password authentication system should encourage strong passwords. We propose that authentication schemes which, allows the user choice to influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to Predict) is more tedious, prostate users from making such choices. Moreover, in the effect of this approach makes choosing a more secure password the path-of- least-resistance. It is easier to follow the system's suggestions for a secure password a feature lacking in most schemes rather than increasing the burden on users. Using above process in graphical password interaction we will introduce the first Persuasive Cued Click Points and conducted user studies evaluating usability and security. This analytical examination provides a comprehensive and integrated evaluation of PCCP covering each usability and security issues, to prior understanding as is prudent before practical readying of new security mechanisms. Through eight user studies. In this paper we are introduce the specialized technique for protecting user data. By controlling the pattern design in data representation using hotspots for increasing the usability in data retrieval. In the proposed work we have integrated sound signature to help in recalling the password. No system has been devolved so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter. To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice. Profile vector is created.

II. RELATED WORK

Traditionally, a secure text-based password should be 8 characters or longer, random with upper-case, lower-case and special characters.

Such password is meaningless and can only be remembered by rote memorization. Therefore, it is hard for users to handle these alphanumeric passwords due to long-term memory limitations that users have difficulty in remembering complex, random passwords over time. In this case, many users choose to use short, simple passwords (i.e., even using the word "password" as their personal password [16]) for easy memorization while these simple passwords are vulnerable to kinds of attacks (e.g., brute-force attack, dictionary attack. Even worse, some users are likely to write down their pass words in a paper to help them remember their secrets, however, such behavior must bear a very high risk of leakage.

Therefore, a lot of graphical password schemes have been developed to reduce the memory burden on users and aims to replace the text-based passwords. For the click-based scheme, Blonder first designed a graphical password scheme that users could click on several pre-defined locations on an image. Wiedenbeck et al. extended Blonder's idea and proposed a PassPoints system that users could click on any place on an image to create their passwords based on the technique of "Robust Discretization" . They also analyzed the effect of pixel tolerance (i.e., determining the minimum size of tolerance square) . Chiasson et al. proposed a scheme of Cued Click Points (CCP) afterwards that users clicked on one point per image for a sequence of images. In the scheme of CCP, the next image was based on previous click-point. Their analysis showed that CCP was more secure than PassPoints by increasing the number of images.

Our proposed scheme of CD-GPS can be partly treated as an improvement for DAS scheme since drawing a secret is the main step in our scheme, but our scheme is different from DAS scheme and other draw-based graphical schemes in that our scheme consists of two steps: image selection and secret drawing. The step of image selection involves the technique in choose-based schemes that users should select their images in an ordered sequence and remember this order like a story.The step of secret drawing combines the techniques in both click-based and draw-based schemes in which users have to draw their secrets (e.g., a number) by using series of clicks. In addition, the proposed action of click-draw in our scheme makes the drawing trajectory either continuous or discontinuous (i.e., users can click on any coordinates to finally construct their secrets), whereas the drawing trajectory in a typical draw based scheme is continuous. Therefore, our scheme of CD- GPS is overall a combination of current graphical password techniques more than a pure draw-based scheme.

Text passwords are the most popular user authentication method even though it has security and usability problems. Preference such as biometric systems and tokens has their own drawbacks. The extension implemented is user-friendly and provides a more secure user experience. Consider for an instance in our system it is obvious when the plug-in has been activated and is awaiting input and thus the solution alleviates the problems associated with incorrectly assumed state of the system. With any authentication, system there is a risk of

memory interference, where users are expected to recall information to log in. Multiple password interference occurs when users must remember passwords for many systems and the memories of the different passwords interfere with each other. Studies have shown that users typically create easy-to-guess text passwords and reuse these passwords across several accounts.

We are interested in the graphical password approach. It has been suggested that graphical passwords may be less susceptible to multiple password interference since humans have better memory for recognizing and recalling images than text.

Cued-recall: Users identify and target previously selected locations within one or more images. PCCP is stronger against password-guessing attacks than other click-based password systems and maintains login times and success rates comparable to text passwords.

Persuasive Technology: Persuasive Technology was first articulated by Fogg as using technology to motivate and influence people to behave in a desired manner. Persuasive Technology should guide and encourage users to select stronger passwords i.e. an authentication system, but not impose system- generated passwords. To adequate, the users must not ignore the persuasive elements and the resulting passwords must be memorable. As mentioned, the PCCP accomplishes this by making the task of selecting a weak password more tedious and time consuming. The path-of-least resistance for users is to select a stronger password.

III. EXISTING APPROACH

Click-Draw Based Graphical Password Scheme:

The purpose of our proposed click-draw based graphical password scheme (CD-GPS) is to enhance the image-based authentication in both security and usability. The security and usability improvements will be discussed later. In particular, there are mainly two operational steps in our scheme: namely, image selection and secret drawing.

Image Selection:

In CD-GPS, the first step is image selection in which users are required to select several images from an image pool. Suppose there are N1 images in the image pool, users should first select $n \in N1$ images from the pool in a fixed order and remember this order of images like a story. The function of using story memorization is the same as the scheme of Story in that users can better remember their selected images and the image orders. The images in the pool are everyday images with different topics (e.g., images of cartoon characters, images of landscape). Subsequently, users should further choose $k \in n$ images from the above selected n images which will be used in the next step.

In our example system which was implemented in our user study, we set N1 = 10 and users should first select n = 4 images out of the image pool and organize these images in a story order. Then, users have to further select k = 1 image for click-drawing their secrets. During the authentication, users should re-select the same n = 4 images in the correct ordered sequence and

further select the right k = 1 image for click drawing their secrets. In Fig. 1, we give a case to illustrate the step of image selection in our implemented example system.

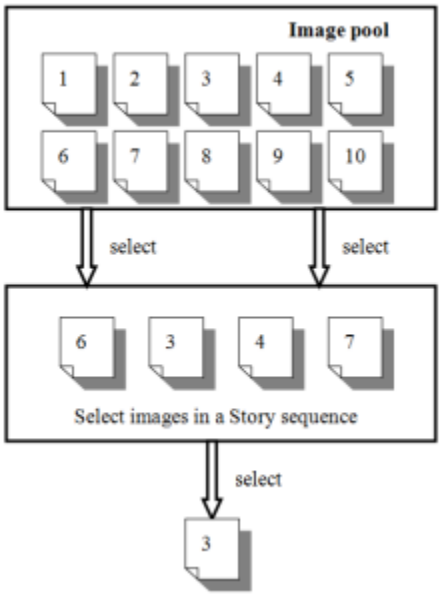


Fig. 1. A case: the step of image selection in our example system.

Persuasive Cued Click-Points (PCCP): 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 firmly became the safe path-of-least-resistance. The viewport is positioned indiscriminately, instead of specifically to avoid far-famed hotspots, since such info may allow attackers to improve guesses and could cause the formation of recent hotspots. We evaluated the usability of PCCP through several performance measures. We compared PCCP, the results in context, to the other authentication schemes tested under similar conditions. Statistical analysis was used to determine whether differences in the data reflected actual differences between conditions or might reasonably have occurred by chance.

IV. PROPOSED APPROCH

A password authentication system should encourage strong passwords while maintaining memorability. The proposed authentication schemes allow user choice while influencing users toward stronger passwords. Our scenario says the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, prostate users from making such choices. Moreover, in the effect of this approach makes choosing a more secure password the path-of-least- resistance. It is easier to follow the system's suggestions for a secure password a feature lacking in most schemes rather than increasing the burden on users. Rather than increasing the burden on users. It is easier to follow the system's suggestions for a secure password—a feature lacking in most schemes. The PCCP approach is to create the first persuasive click- based graphical password system, Persuasive Cued Click-Points (PCCP).

Shuffles:

During password creation, PCCP users may press the shuffle button to randomly reposition

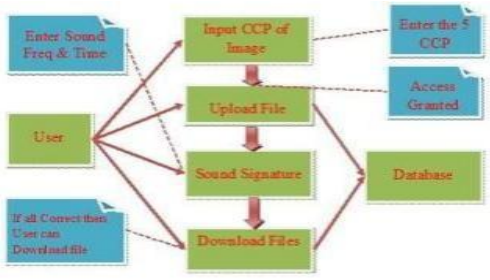
the viewport. For click-points across users, fewer shuffles lead to more randomization. The shuffle button was used moderately. Consider the example since PCCP Lab passwords involved five images and the mean number of shuffles per password would be 3 < 5 =PCCP Lab study users who shuffled a lot had higher login success rates than those who shuffled little and the result was statistically significant.

Varying System Parameters: Mean times for each condition are generally elevated compared to times in the studies with smaller theoretical password spaces. In time taken, to create a password, there is no clear pattern emerges. A general increase in times can be seen in both the login and recall phases as more click points or larger images are used. The participants took much longer to reenter their passwords after two weeks (recall) as expected, reflecting the difficulty of the task.

Usability Results: Overall, PCCP has similar success rates to the other authentication schemes evaluated (CCP, Pass Points, and text). PCCP password entry takes a similar time to the other schemes in the initial lab sessions. The results indicate longer recall times for PCCP when recalling passwords beyond the initial session. The more shuffled users had significantly higher success rates in the PCCP Lab study. However the difference in success rates between high and low shufflers was not statistically significant for the two-week or web studies. In additional, users reported favorable opinions of PCCP in post-task questionnaires.

Pattern-based attack: The proposed attacks on Pass Points is an automated pattern based dictionary attack that prioritizes passwords consisting of click-points ordered in a consistent horizontal and vertical direction (including straight lines in any direction, arcs, and step patterns), but ignores any image- specific features such as hotspots.

Sound Signature Patterns: We have integrated sound signature to help with the password. No system has been devolved so far which uses sound signature and graphical password authentication. Study says that sound signature or tone can be used to add facts like images, text etc. Our idea is inspired by this novel human ability. Research says that human can remember images as well as sound tone easily; by applying this method we design our project so it will provide more security. Observed that all student who were registered entered their graphical password and video sound clip and it will be more secured from their point of view it is very good for Graphical and sound clip password authentication system.



System Architecture

Firstly we need to enter the CCP of image. If entered CCP's are correct then system will allows user for next level of logging. In next level user required to enter the volume level, if volume level is correct system will allows for next authentication level. In last stage of logging user need to enter correct video timing. If any of them (CCP's, Volume level, Video timing) are incorrect then system will go in halt state for next 12 hours. After completion of 12 hours reboot again and user can try for uploading and downloading of data by entering correct password for all stages.

V. CONCLUSION

Better user interface design can influence users to select stronger passwords. The main objective in PCCP is that creating a harder to guess password is the path- of-least-resistance likely to make it more effective than schemes where secure behavior adds an extra burden on users. The schema has proven effective at reducing the formation of hotspots and patterns and increasing the effective password space. In our approach makes choosing a more and secure password the path of least resistance. Moreover increase in the burden on users and it is getting easier to follow the system's suggestions for a secure password.

VI. REFERENCES

1) Emerald Assessing Image Based Authentication Techniques In A Web (www.Emraldinsight.Com).

2) Sonia Chiasson, Member, IEEE journal, Alain Forget, Elizabeth Stobert, Robert Biddle, Member, IEEE, And P. C. Van Oorschot, Member in IEEE journal, "Persuasive Cued Click-Points: Design, Implementation, And Evaluation Of A Knowledge- Based Authentication Mechanism", Edition: Oct, 2011.

3) Kemal Bicakci, Mustafa Yuceel, Burak Erdeniz," Graphical Passwords As Browser Extension: Implementation And Usability Study", By K Bicakci- 2009.

4) Sonia Chiasson, Alain Forget, Elizabeth Stobert "Multiple Password Interference in Text Passwords and Click-Based Graphical Passwords", the definitive version was published in ACM CCS'09 November 9–13, 2009.

5) Elizabeth Stobert, Alain Forget, Sonia Chiasson, **"**Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords", ACSAC '10 Dec. 6- 10, 2010, Texas, USA.

6) S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

7) "Authentication using graphical passwords: Effects of tolerance and image choice," in 1st Symposium on Usable Privacy and Security (SOUPS), July 2005.

8) K. Golofit, "Click passwords under investigation," in 12th European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007.

9) Designing Click-Draw Based Graphical Password Scheme for Better Authentication by Yuxin Meng.