International Journal of Emerging Trends in Science and Technology
5 (2), December 2019, 01-03
http://www.publishingindia.com/ijetst

Enhancing the Graphical Password With Sound Signature

S. Ramya[1*], S. Kayathri[2] and S. Meena[3]
[1]Department of MCA, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India.
Email: ramyas.mca@mkce.ac.in
[2]Department of MCA, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India.
Email: kayathris.mca@mkce.ac.in
[3]Department of MCA, M. Kumarasamy College of Engineering, Karur, Tamil Nadu, India.
Email: meenas.mca@mkce.ac.in
*Corresponding Author

Abstract: A graphical password system is based on cued click point. In this scheme contains a cued-recall graphical password technique. Users Click on one pixel per image for a sequence of images. The second image is based on the previous pixel. Compared with other graphical password methods performance and accuracy was very good in terms of speed. Users preferred pixel point to passed click Points. It is easy to remembering only one pixel for one image. Here each picture triggered their memory of where the corresponding pixel was located. Cued Click Point also provides higher security than Pass Points because it increases the workload for attackers.

Keywords: Graphical password, Security, Sound signature.

I. Introduction

Instead of text based password there are various graphical password schemes are available. The experts have shown that the text based password is research and experience have shown that text-based passwords are causing with both usability and security problems that make them less than prudent solutions. Some studies show that, the central organ of human being is recalling the images quickly rather than text. So it helps to reduce the memory and stress in the central organ of human body.

A pixel based graphical password scheme called Pixel Click Points (PCP). Pixel Click Points consist of pixel points, pixel faces and imaginative writing. A password consists of one click-point per image for a sequence of images. The second image is based on the previous pixel point so the user got the quick feedback whether the user is making the login in exact path. The Pixel Click Point provides the higher security and usability.

In Pass Point the user selects multiple click points in a single image. There is a chance to guess the password easily by the hackers. In a proposed system the Pixel Click Points they are having multiple images but the user select single pixel point per image. So the users could quickly generate and re-enter their passwords. One important feature in pixel based click point is the quick feedback telling, that is the whether the user choose the click point correctly entered.

The Pixel Click Point helps to select the single pixel point per image instead of selecting five click points on a single image. It provides the retrieval of memory and preattentive signals to users whether the authorized user only entering the password. Suppose the user may select the wrong pixel point, then go for they leave from which point and it retrieve from the beginning. Hotspot analysis also very difficult activity for made attacks. For every result shows the path of next image as they click on their sequence of points [1]. If the user selects the wrong pixel point it shows the incorrect path. The failure of authentication indicated only after the last selection point. If the users do not like the final images then they create a new password with various images and different click points.

II. Related Work

A. Multiple Password Interference in Text Passwords and Pixel-Based Graphical Passwords

The cardinal issues related with the heterogeneous password is security and usability that is undetermined. However, the users generally having the difficulty to remembering the multiple passwords [1]. Here user reuses the same password in various systems or acknowledge other passwords as they try to log in. The report on a study is related with the graphical password system says that, the comparison of recall multiple image based password is better than recall of multiple text passwords [3]. The analysis report shows that, in a one-hour session, the participants in the text based password condition are not good with graphical password condition. Particularly they identified some errors from recalling passwords; it does not apply to creating passwords with respect to user account names, and does not use same passwords across multiple accounts. After the completion of two weeks, the analysis report shows that,

the participants in text based password condition having lot of recalling error compared with graphical password condition depend on the success rate. In our study, the comparable usability to text password having more vulnerability with pixel-based click graphical passwords.

B. Graphical Passwords: Learning from the First Twelve Years

There are various graphical password schemes are proposed instead of text based password for authentication. The published and research area give the overview of the system evaluation as well as the security and usability aspects [2]. The Graphical User Authentication schemes helps to solve the authorization issue in image based problems. They are increasingly adopted by the researchers with the novel interaction technique. It is having the better usability and security. They identified the graphical password scheme provide the good security and memorability for all kind of users.

C. Exploring Usability Effects of Increasing Security in Pixel-Based Graphical Passwords

The traditional text password having the address known problem. Solving this problem by using the graphical password system. For example, the randomly system assigned password is difficult to remember but the text passwords are selected by the user, it is easy to remember. To increase the security of pixel-based password system by using the system parameters. The usability tests for graphical passwords have used configurations resulting in password spaces smaller than that of common text based passwords. Our study helps to compare the multiple click points, size of the image and the space provided for the image including with the different configuration [2].

Based on our expectation the big image size having the usability advantages, because of more click points. The results suggest promising opportunities for better matching graphical password system configurations to device constraints, or capabilities of individual users, without degrading usability. For example, in smart phone display more click points are used, here big image is not possible. During the password creation the pervasive cued click point design reduces the predictability.

III. Pixel Based Password System

There are eight different user studies including three is based on PCCP, two is based on pass Points, one is based on CCP, and two is based on text passwords. The Pass Points, CCP, and Text Password studies as benchmarks where appropriate. Depend on three methodologies the aim is to assess the different methods of the system. The daily computer users are feel that, text passwords are comfortable to them. No one had before used image based passwords. A part from password tasks the participants are finished the questionnaires related with the demo graphics. The lab and two-week recall studies used standalone J# applications for Windows. 1; 024 x 768 pixels is the resolution of 19-inch screen. The images were 451 x 331 pixels, with tolerance squares 19 x 19 pixels, and passwords of five click-points, yielding a theoretical space of 243 passwords, in earlier studies. The user given passwords were not contains the repeated images. The web-based authentication framework conducted from the web based studies. 451 x 331 pixel images, 19 x 19 tolerance squares, and five click-points were used in the configuration of Pervasive Cued Click Point. The participants were login any location and any kind of resolution of the screen does not controlled. In the real websites asked the user to behave so as to make it appear the passwords were shield the important data, it is gathered from in our studies. This higher value user account password affected the behaviour of the user. Did not allow the user to write the passwords in their presence. There is no way to stop them for doing at home, this issue is real situation. Furthermore, studies are needed to be for conforming the generalizability.

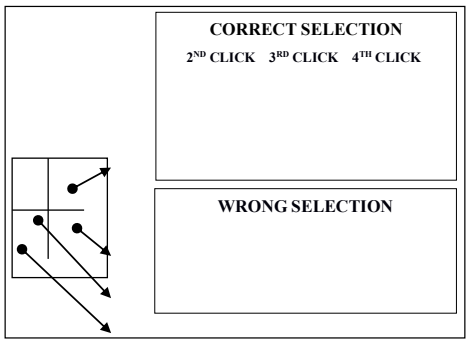

Fig. 1: System Design in CCP

The image based password consist of single click point for one image for a succession images. The second image is based on the previous click point. So the user having the quick response and check whether they go for the exact path or not when they are login. Fig. 1 shows the sequence of pixel point's. Pixel Click Point offers both improved usability and security. Users could quickly create and re-enter their passwords. Another feature of pixel based password is the immediate implicit feedback telling the correct user whether their latest click-point was correctly entered.

IV. User Registration

The password contains sequence of five click points on a defined image. Users may select any pixels in the image as click-points for their password. They repeat the sequence of clicks in exact order within a system defined tolerance square to log in.

A. Hotspots

There will be a difficulty occur for choosing passwords by using five click points. So by include the persuasive characters to improve the user productivity. Here the five click points are the hotspots. Particularly, if the user choose the password it is mildly shaded except view point to avoid guessing of passwords, the hotspots are set randomly instead of setting the known hotspots.

B. Pixel Management

If the user create a password, at that time only the hotspots and shuffle button appears. The user should select within the particular area (view point) then the password will generated. If the user click outside of the view point, then the shuffle button will appear, then the user randomly reposition the view points. At that time the password generation get slow. A time to care late password entry the pictures are displayed with out any change. Then the users may select anywhere on the pictures.

C. Sound Signature

The user select the second pixel point with in the view port on the image and select sound signature. This sound signature taken from the wave file which is already stored.

D. Security

The password creation contains a pixel recall scenario. Here every picture is threaded with the memory of similar click point. The system display one picture at a time. The user should remember the sequence OD click points. The password entry becomes a true cued-recall scenario, wherein each image triggers the memory of a corresponding click-point. If the user gave wrong password for login process, again they need to restart the creation of password. The production failure will occur only based on the final click point.

V. Performance Evaluation

The passwords helps for (a) Security (Provide the effective guardianship) (b) Authorization (Whether the authorized user only entered into the system login) (c) Surveillance (Constraints of permission contains guardianship and authorization). Here a sound signature helps to increase the remembrance of a password. The password consist of a succession of click points, here one picture is based on the previous click point. The user need to select the one pixel point for each picture, then select sound signature for the selected picture. The user should select both the pixel points in the corresponding pictures. This system gives more user friendly, excellent results in speed, performance and the correctness.

A. Illustration

Based on the earth science, gather the grouping of data and arbitrary used to check the two dimensional information. This analysis shows that the statistics of R programming language. This language helps to analyze the statistical computing report and graphical support for computing [4]. Here the statistics of J helps to find the degree of grouping the pixel points within the hotspots.

VI. Simulation Result

In Pervasive cued click point contains the number of click points. The picture having the five click points in a single image, which is selected by the user. Here the view point helps to locate the particular password location [3]. In Pass Points, the passwords contains single click point on a one image. The next image is based on the previous click point. If the user select the right order it will generate the password. Then the user select sound signature with in a tolerance level on a given image. They choose any pixel point, it is depend upon the user. The attacker should not know about the particular pixel point in view area. So there is a less possibility to identify the passwords.

- *Registration:* The user name and the tolerance level between zero to ten is entered by the user.
- *Picture Forum:* The user need to choose any picture from the resource file. User choose first pixel point from the resource file picture. The user selected pixels are passwords. Then choose the sequence of pictures from the resource file.
- *Login:* The registered user id is entered by the user. Once the process completed it will move to the similar page.

VII. Conclusion and Future Work

Generally, the objective of graphical based authentication system is to reduce the password space [4]. This impacts usability when user choice is involved. In Pervasive Cued Click Point's view area should not be abused at the time of attack. If the user forget the view area is difficult to identify the passwords. The response time of the system is slow because of view point. Then set the threshold limit it is simple to identify the passwords. In future we set the tolerance level the user may identify the view area easily. It helps to improve the usability and security for graphical passwords instead of text based passwords. Then the user choose the sound signature from the resource file for the particular picture. This strategy has proven that, make less space in hotspots and the creation of strengthen the graphical password.

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)*, November 2009.

[2] E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring usability effects of increasing security in click-based graphical passwords," *Proc. Ann. Computer Security Applications Conf. (ACSAC),* 2010.

[3] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "User interface design affects security: Patterns in click-based graphical passwords," *International Journal of Information Security*, vol. 8, no. 6, pp. 387-398, 2009.

[4] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys*, vol. 44, no. 4, 2012.