AN EFFECTIVE USER AUTHENTICATION METHOD USING PERSUASIVE CUED CLICK POINTS

Anusha Bellam
SE, M.Tech, SNIST, Hyderabad, Andhra Pradesh, India
bellamanu.203@gmail.com

ABSTRACT

It is an evolution of Persuasive Cued Click Points graphical password scheme which includes usability and security evaluations. This paper includes the persuasion to influence user choice in click based graphical passwords, so that users select more random and more difficult to guess the passwords. In this paper, in order to increase the security, the process of click points is done for 5 number of images. It also encourages user to select less predictable passwords, and hence it supports the user in selecting passwords of higher security.

KEYWORDS: Authentication, Graphical Passwords, Usability, Security.

1. INTRODUCTION

The most common computer authentication method is to use text-based passwords. This method has been shown to have significant drawbacks. For example, users choose the passwords that can be easily remembered and hence the attackers can easily guess the password. If the user choose the password which is hard to guess, then it is hard for user to remember for long time. To solve this problem, an authentication method that uses pictures as password has developed. A password authentication system should encourage strong passwords while maintaining memorability.We propose the authentication system so that it allows the user to select the strong password. In our system, the task of selecting weak passwords which are easy for attackers to predict is more tedious. In effect, this approach makes choosing a more secure password the path-of-least-resistance. Than increasing burden on users, it is easier to follow the system suggestions for a secure password.

Authentication is the process of determining whether a user should be allowed access to a particular system. We use persuasive click based graphical password system evaluating usability and security. It provides new evaluation of password distributions, extends security analysis. This systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues. We compare PCCP to text passwords, the results show that PCCP is effective at reducing hotspots (areas of the image where users are more likely to select click-points) and avoiding patterns formed by click-points within a password. The system could influence users to select more random click-points while maintaining usability. The main goal was to encourage more secure behaviour by making less secure choices. Behaving securely became the safe path-of-least-resistance.

By adding persuasive feature to CCP, PCCP encourages users to select less predictable passwords, and makes it more difficult to select the passwords where all five click points are hotspots. When user creates a password, the viewport is displayed. The viewport is positioned randomly, rather than specifically to avoid the known hotspots. Users must select a click-point within this viewport and cannot click outside the viewport, unless they press the shuffle button to randomly reposition the viewport. The viewport and shuffle button appear only during password creation. During later password entry, the images are displayed normally and users may click anywhere on the images. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. Keeping in mind about the usability and security evaluations, the process of selecting the click point is very important. The user feels comfortable with this type of graphical passwords when compared with text passwords. Humans are very good at recognising than recalling.

2. PROPOSED SCHEME

Persuasive technology is to motivate and influence people to behave in a desired manner. An authentication system which applies persuasive technology should guide and encourage users to select stronger passwords, but not impose the system generated passwords. The users must not ignore the persuasive elements and the resulting password must be memorable. The path-of-least-resistance for users is to select a stronger password. The formation of hotspots is minimized since click points are more randomly distributed.

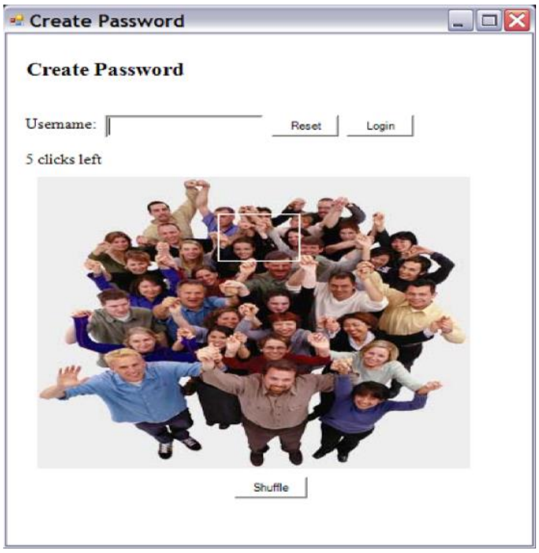

Fig.1. Creating password in Registration process

A. Registration Process:

User must enter the unique user name. Now for entering the password, he must browse the image. Place the viewport and within that viewport only select the click point. The viewport is highlighted only at registration process shown Fig.1. The viewport is positioned randomly, rather than specifically to avoid the known hotspots, since such information might allow the attackers to improve guesses and could lead to the formation of new hotspots. This process is repeated for 5 number of images. To increase the complexity, the number of images is 5 to be selected and given a click point as password.

B. Login Process:

During login, the user must enter the user name, if it exists then only he can able to select the image. The viewport will not display at the time of entering the password in login process. Now he must select the same sequence of images which he selected during registration process. If first click point is correct then only he can able to see the next image, if not he’ll be given two more chances and then quit. The shuffle button will not be displayed at login time. With this sequence, the process is done for 5 images.

3. CONCLUSION

The users are flexible in recognising the images which they provided at the time of registration. Users can easily recognise the image when compared to recalling the text password. Humans are very good at recognising so they can remember te password for a long time when compared to te text based password. The main security goal in password-based authentication system is to maximize the effective password space. The tools such as PCCP’s viewport cannot be exploited during an attack. Best user interface design can influence the users to select the strong passwords. The key feature of PCCP is to select the password which is hard to guess is path-of-least-resistance, making it more effective where security is provided. This approach proves that it is effective at reducing the formation of hotspots and patterns, therefore it increases the effective password space. So, it is the better user authentication method by solving usability and security issues.

Viewport:

A viewport is a 2D rectangle that defines the size of the rendering surface onto which a 3D scene is projected. The viewport is visible during password creation which must be large enough to allow the user choice but small enough to have its intended effect of distributing click-points across the image.

Hotspot:

It is an area of the image where users are likely to select as password click points. Attackers who have knowledge on these hotspots through harvesting the sample passwords can build attack dictionaries and more successfully guess the passwords. To avoid this kind of situation, user must give the password which is hard to guess for attacker.

REFERENCES

[1] Sonia Chiasson, "Usable Authentication and click-based graphical passwords," December 2008.

[2] K. Renaud, "Evaluating authentication mechanism in Security and Usability," pp. 103-128, 2005.

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

[4] S. Chaisson, P. van Oorschot and R. Biddle, "Graphical password authentication using Cued Click Points," pp. 359-374, September2007.

[5] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon, "Authentication using Graphical passwords-Effects of Tolerance and Image Choice," 2005.

[6] Sonia Chiasson, P.C. van Oorschot, Robert Biddle, "Modeling user choice in the PassPoints Graphical password scheme," 2007.

[7] S.Chaisson, E. Stobert, A. Forget, R. Biddle, P. Van Oorschot, "Persuasive cued click-points: Design, implementation and evaluation of a knowledge-based authentication mechanism," vol. 19, no. 4, pp. 669-702, 2011.

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