ISSN : 2231-0711

Security of Graphical Passwords Using PCCP

Sarika Choudhary
M.tech (Network Security)
School of Engineering and Sciences
BPS Mahila Vishwavidyalaya
Khanpur Kalan, Sonepat, Haryana, India

Dr. Ajit Singh
Dean, Department of CSE & IT
BPS Mahila Vishwavidyalaya
Khanpur Kalan, Sonepat
Haryana, India

Abstract: **We are well aware about problems persists in typically text-based passwords. Users generally choose memorable passwords, that are easy for attackers to guess, but the strong system generated passwords are difficult to remember. So a password authentication system should emphasis on maintaining high password strength on one hand and memorability on other. In this paper we'll discuss about Persuasive Cued Click-Points i.e. persuasive click based graphical password system, which provide password strong password along with memorability. In this paper we'll present perspective view of graphical passwords for authentication. In this work we will also conduct comprehensive analysis of the existing image based password techniques. We'll discuss strengths and limitations of each method.**

Keywords: **authentication, guessing attacks, graphical passwords, PCCP, CCP.**

I. Introduction

Passwords are the most commonly used method for authentication in computer and over communication channel. The most commonly used passwords are strings of letters and digits i.e. called text passwords. There are many things that are well known about passwords; such as that users are not able to remember strong password and that the passwords they can remember are easy to guess. The task of selecting weak passwords is more monotonous, avoids users from making such choices. In effect, this authentication schemes makes choosing a more secure password the path-of-least-resistance. Rather than it is easier to follow the system's suggestions for a secure password. We are not arguing that graphical passwords are the best appear for authentication; we find that they offer a brilliant environment for helping user's select better passwords since it is easy to compare user choices. Indeed, we also talk about how our approach might be made to order to text-based passwords.

II. Existing Techniques

Even though text passwords are the most popular user authentication method, they have security and usability problems. The alternatives for text based passwords such as biometric systems and tokens have their own drawbacks [9],[10],[11]. Graphical passwords were originally defined by Blonder (1996). A graphical password scheme using click point offers the best substitute for the text password, and is discussed in this paper.

A. *Pass Points (PP):*

In this system an image is picked from set of images and user is shown the image. Task of user is to click N points. As user clicks on the points, features from points are stored and not the point itself. Because storing points directly reduces the security of the technique. As it is very difficult to memorize the random points, user chooses to select points on images that can be easily accepted in the image i.e. called Hot Spot [10]-[13]. Advantage of this is simplicity of execution and drawback is low protection.

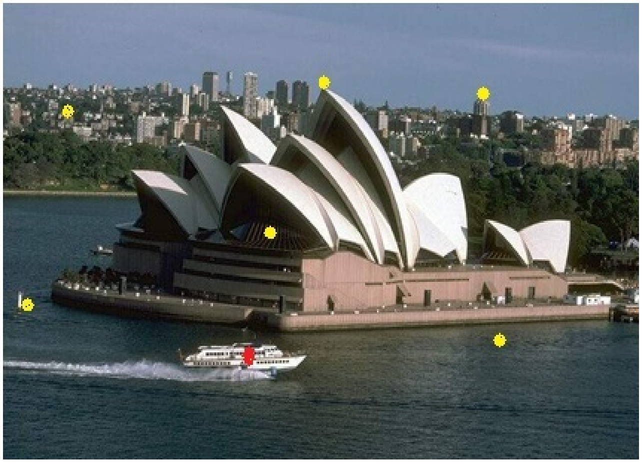

Fig.1: Pass Points (PP)

B. *Cued Click-Point (CCP):*

To increase the security ambiguities mentioned in pass points system, this password distribution scheme is developed. The cued click point method uses a series of images for click point password creation. Here user is obtainable with N random different images and user has to click one point at every image. The place of the click point on the previous image decides the next image to become visible. Based on selected click point of existing image, next image is displayed arbitrarily by the system.

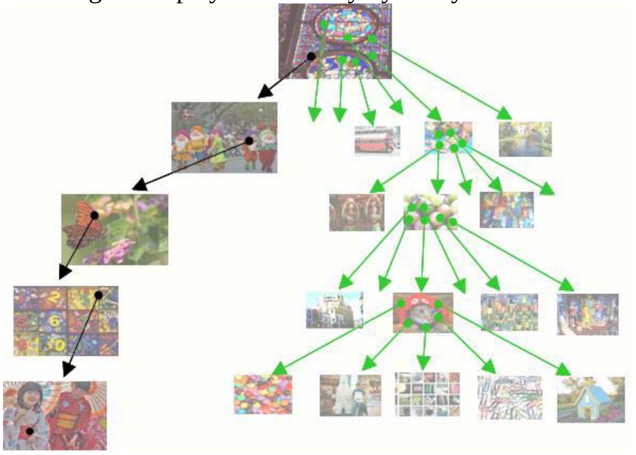

Fig.2: Cued Click-Points (CCP)

III. PERSUASIVE CUED CLICK POINTS (PCCP)

It refers to using technology persuade, motivate and persuade people to behave in desired manner. An authentication method based on persuasive technology, encourage user to select stronger password, but not impose system generated password. According to the Visual attention research, different people are attracted to the same predictable areas on an image. So if users select their own click-based passwords without guidance, this will lead to formation of hotspot which enables attacker to easy to crack the passwords.

In PCCP, the user is encouraged to select less expected passwords and make it more difficult to select passwords where all three click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport. The view-port is positioned randomly, rather than specifically to avoid known hotspots, since such information might allow attackers to improve guesses and could lead to the formation of new hotspots.

The theoretical password space for a password system is the total number of unique password that can be generated according to the system specifications. Ideally a larger theoretical password space lowers the, likelihood to guess a particular password. For a text password the theoretical password space is 95^n, where 95 is the number of type-able character. In PCCP, the theoretical password space is calculated as: $((w \times h)/t^2)^c)$, where the size of the image in pixels ($w \times h$) is divided by the size of a tolerance square (t^2, typically 75), to get the total number of tolerance squares per image, then is raised to the power of the number of click-points (c) i.e. number of images. So an 8-character text password has approximately the same password space (253 or 53 bits) as a PCCP password with a small image size (451 × 331 pixels) and 6 click-points, or a large image size (800×600 pixels) and 5 click-points. PCCP password effectively provides equal security as of text password or we can say better than text passwords.

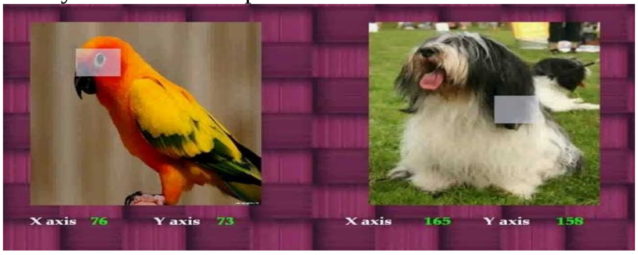

Fig.3: Sample PCCP, The viewport highlights part of the image.

IV. SUMMARIZED VIEW OF SECURIY ANALYSIS

Given that hotspots and click-point clustering are significantly less prominent for PCCP than for CCP and Pass Points, 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 guessing attacks. For capture attacks, PCCP is susceptible to shoulder surfing and malware capturing user input during password entry. However, we expect social engineering and phishing to be more difficult than for other cued-recall graphical password schemes due to PCCP's multiple images.

V. CONCLUSION

The major advantage of persuasive cued click point scheme is its large password space since entire image is used for generating the password and it helps in plummeting number of hotspots in the image compared to existing click based graphical password systems. Therefore it provides better security. Arbitrariness of the system is very high in comparison to both single-image multi-point based technique and multi-image single-point based techniques. The graphical click point passwords are more random and strong, so that no hacker can guess it. Thus physical password does not store the image points. Thus system is better equipped to deal with false acceptance attacks. The security strength is decided by the user himself, depending upon the requirement. This paper gives an idea of having an effective authentication system, which provides strong and easily remembered graphical passwords with dynamic security level. This work can be improved by using more complex images and with more bright colors.

REFERENCES

[1] S. Chiasson, R. Biddle, and P.van Oorschot, "A second look at the usability of click-based graphical passwords," in ACM Symposium on Usable Privacy and Security (SOUPS), July 2007.

[2] S. Chiasson, A. Forget, R. Biddle, and P. van Oorschot, "Influencing users towards better passwords: Persuasive Cued Click-Points," in Human Computer Interaction (HCI), The British Computer Society, September 2008.

[3] S. Chiasson, A. Forget, E. Stobert, P. van Oorschot, and R. Biddle, "Multiple password interference in text and click-based graphical passwords." in ACM Computer and Communications Security (CCS), November 2009.

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

[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The memorability and security of passwords," in Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, Eds. O'Reilly Media, 2005, ch. 7,pp. 129–142.

[6] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical password authentication using Cued Click Points," in European Symposium On Research In Computer Security (ESORICS), LNCS 4734, September 2007, pp. 359–374.

[7] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[8] E. Tulving and Z. Pearlstone, "Availability versus accessibility of information in memory for wor ds," Journal of Verbal Learning and Verbal Behavior, vol. 5, pp. 381–391, 1966.

[9] 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.

[10] K. Golofit, "Click passwords under investigation," in 12th European Symposium on Research in Computer Security (ESORICS), LNCS 4734, September 2007.

[11] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Trans. Information Forensics and Security (TIFS), vol. 1, no. 2, pp. 125-143, June 2006.

[12] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," Proc. First Symp. Usable Privacy and Security (SOUPS), July 2005.

[13] Whitten, A. and Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. 8th USENIX Security Symp. 1999.