ijournals International Journal of Software & Hardware Research in Engineering
ISSN No: 2347-4890 Volume 2 Issue 3, March 2014

IMAGE BASED AUTHENTICATION USING PERSUASIVE CUED-CLICK POINT TECHNIQUE

Snehal Ambade [1]; Shubham Bhivgade [2]; Saurabh Trivedi [3]; S. B. Lanjewar[4]

[1,2,3] UG Students, [4] Assistant Professor Department of CSE Dr. Babasaheb Ambedkar College of Engineering & Research, Nagpur, India

ABSTRACT

It is an advancement of Persuasive Cued-Click Point graphical password technique 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, the process of click points is done for 5 numbers of images, in order to increase the security. It also encourages user to select less predictable passwords by reducing hotspot, and hence it supports the user in selecting password of higher security.

Keywords

Authentication, Graphical Passwords, Persuasive technology, Security.

1. INTRODUCTION

The problems of text-based passwords are well known to us. User often creates memorable passwords that are easy for any unauthorized person to guess, but strong system-assigned passwords are difficult for users to remember [11].

A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication in which the system allows user choice while influencing user towards stronger and secure passwords. In our system, the task of selecting weak passwords (which are easy for unauthorized one to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes user to choose a more secure password the path-of-least-resistance. 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 of the schemes. We applied this approach to create the persuasive click-based graphical password system and compared PCCP scheme to text passwords and two related graphical password systems. 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, while still maintaining usability.

2. BACKGROUND

Text passwords are the most popular user authentication method, but have certain security and usability problems. Replacements such as biometric systems and tokens have their own drawbacks [5]–[12]. In general, graphical passwords techniques are mainly classified into two main categories (figure.1): recognition-based technique and recall based technique. In recognition based, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he selected earlier during the registration stage. In recall based graphical password, a user is asked to reproduce something that he created or selected earlier during the registration stage. Graphical passwords offer another replacement, and are the point of focus in this paper.

2.1Click-Based Graphical Passwords

Graphical password systems are the types of knowledge-based authentication that attempt to leverage the human memory for visual information [4]. A user navigates through images to form a CCP password. Each click determines the next image of graphical passwords is available elsewhere [13]. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric). In such systems, users identify and target previously selected locations within one or more images.

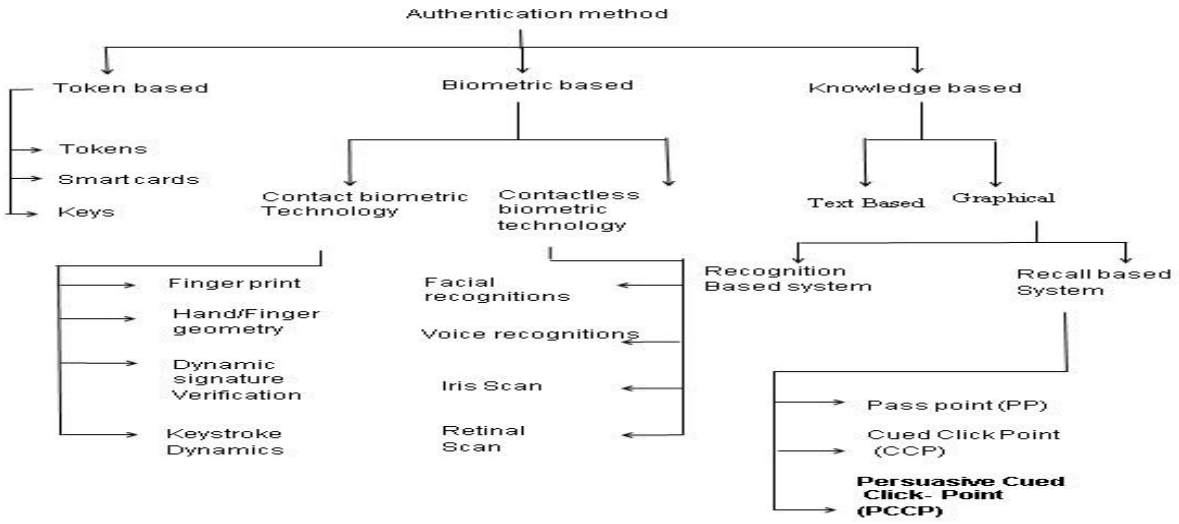

Fig.1.Classification of Authentication Techniques

The images act as memory [14] cues to aid recall. Example systems include Pass Points and Cued Click-Points (CCP).

2.1.1 Pass Point (PP):

In Pass Points, passwords consist of a sequence of five click-points on an image. Users may select any pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points. Although Pass Points is relatively usable [1], [15], [16] security weaknesses make passwords easier for attackers to guess. Hotspots [7]–[8] are areas of the image that have higher likelihood of being selected by users as password click-points. Attackers who gain knowledge of these hotspots through harvesting sample passwords can build attack dictionaries and more successfully predict Pass point passwords [6] - [17].

Fig.2.Pass Point

Predictable patterns [3], [8] which can also be exploited by attackers even without knowledge of the background image; indeed, purely automated attacks against Pass Point based on image processing techniques and spatial patterns are a threat [10].

2.1.2 Cued Click-Points (CCP):

A precursor to PCCP, Cued Click-Points (CCP) [9] 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 sequence. The next image displayed is based on the location of the previously selected click-point (figure.3), creating a path through an image set. Users select their images only to the extent that their click-point determines the next image. Creating a new password with different click - point results in a different image sequence.

The claimed advantages are that password entry becomes a true cued-recall scenario based, where in each image triggers the memory of a corresponding click point. Remembering the order of the click-points is no longer a requirement on users, as the system presents the images one at a time. CCP also provides implicit feedback claimed to be useful only to legitimate users. When logging on, seeing an image they do not recognize alerts users that their previous click-point was incorrect and users may restart password entry. Explicit indication of authentication failure is only provided after the final click-point, to protect against incremental guessing attacks. User testing and analysis showed no evidence of patterns in CCP [3], so pattern-based attacks seem ineffective. Although attackers must perform proportionally

more work to exploit hotspots, results showed that hotspots remained a problem [2].

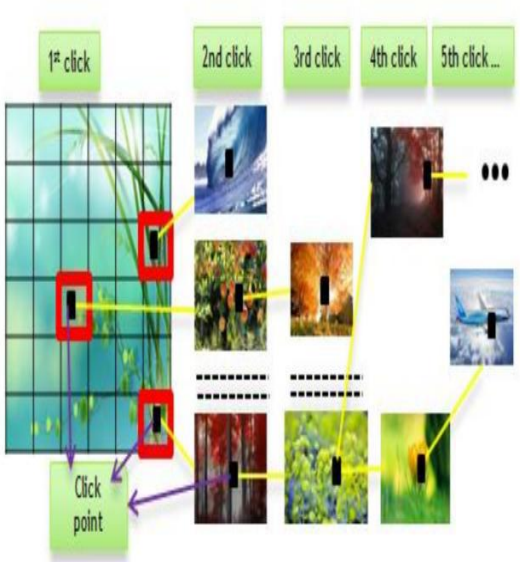

Fig.3.Cued Click Point

2.2 Persuasive Technology

Persuasive Technology was first articulated by Fogg [18] as using technology to motivate and influence the people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select less predicted and stronger passwords, but not impose system-generated passwords. To be effective, the users must not ignore the persuasive elements and the resulting passwords must be memorable. 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 (not comprised entirely of known hotspots or following a predictable pattern).The formation of hotspots across users is minimized since click-points are more randomly distributed. PCCP's design follows Fogg's Principle of Reduction by making the desired task of choosing a strong password easiest and the Principle of Suggestion by embedding suggestions for a strong password directly within the process of choosing a password.

3. PROPOSED SYSTEM

Previous work showed that hotspots and patterns formed by click-points reduce the security of click-based graphical passwords, as attackers can use skewed password distributions to guess and prioritize higher probability passwords for more successful guessing attacks. Visual attention [19] research shows that different people are attracted to the same predictable areas on an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will remain a problem. Davis et al. [28] suggest that user choice in all types of graphical passwords is inadvisable due to predictability. We investigated whether the system could influence users to select more random click-points while maintaining usability [2] - [3].

The goal was to encourage more secure behavior by making less secure choices more time consuming and awkward. The viewport is the highlighted part of the image. By adding a persuasive feature to CCP encourages users to select less predictable passwords and makes it more difficult to select passwords where all five click-points are hotspots. Specifically, when users create a password, the images are slightly shaded except for a viewport (figure.3 and 4). The viewport is positioned randomly in image, 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 viewport's size is intended to offer a variety of distinct points but still cover only an acceptably small fraction of all possible points. Users must select a click-point within this highlighted viewport, unless they press the shuffle button to randomly reposition the viewport. While users may shuffle as often as required, this significantly slows password creation. The viewport and shuffle button appear only during password creation and cannot appear during login. During Login process, the images are displayed normally, without shading or the viewport, and users may click anywhere on the images. Like Pass Point and CCP schemes, Login click-points must be within the defined tolerance squares of the original points.

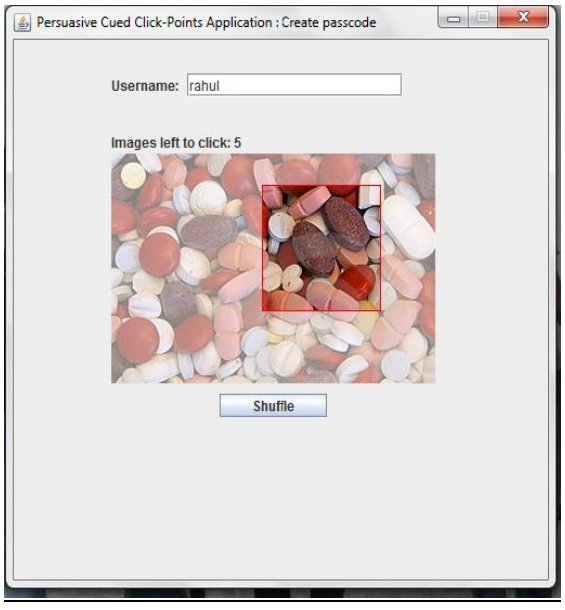

Fig.4. PCCP Create Password interface.

The theoretical password space for a password system is the total number of unique passwords that could be generated according to the system specifications. Ideally, a larger theoretical password space lowers the likelihood that any particular guess is correct for a given password. For PCCP, the theoretical password space is $((w * h)/t^2)^c$, where the size of the image in pixels (w * h) is divided by the size of a tolerance square (t^2) , to get the total number of tolerance squares per image, raised to the power of the number of click-points in a password (c is number of images = 5). Florencio and Herley [20] suggest that theoretical password spaces of 220 suffice to withstand online attacks. Whereas text passwords have very skewed distributions [21], resulting in an effective password space much smaller than the theoretical space, PCCP is specifically designed to significantly reduce such skews.

4. MODULE DESCRIPTION

There are two modules in our project:

4.1 Creation Module

PCCP encourages user to select less predictable password, where all five click points are memorable to user specifically when create a password, the images are slightly shaded accept for a viewport. The viewport is positioned randomly, rather than specifically to avoid known hotspot. User must select a click point within the viewport and cannot click outside of the viewport, unless the press the shuffle button to randomly reposition the viewport. The viewport and shuffle button appears only during password creation.

4.2 Login Module

While login, the user must enter the username and click within the defined tolerance squares of the original points on the image. After clicking on the image the next image is open which is stored on that click point. The user must click on tolerance squares of the original point for all the five images.

5. FLOW DIAGRAM

Registration procedure includes both registration (username) and picture selection. The process flow starts from registering username and tolerance value. Once user enters the username then precede to next stage, which is selecting click points on generated images. After done with all these above procedure, user profile data will be created.

In login procedure (see figure below), first user enters the unique username as same as entered during registration. Then images are displayed normally without shading and the viewport, use have to repeat the sequence of clicks in the correct order, within a tolerance square of the original click-points. After done with all these procedure, user profile data will be opened.

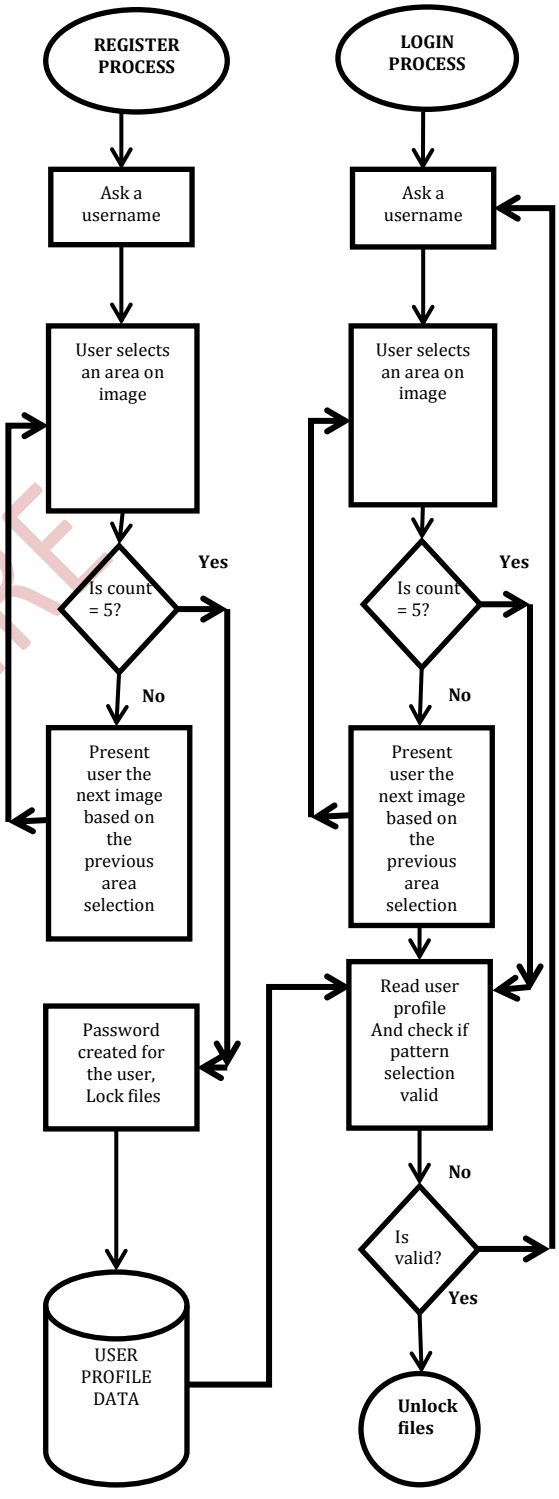

Fig.5. Registration and login procedure

6. CONCLUSION

In this paper the Persuasive Cued-Click Point graphical password technique is mainly useful for authentication purpose. The advantages of this technique are increasing usability and security by providing password of higher security. The goal of Persuasive cued click point is to encourage and guide user to select better password while still maintaining memorability. Persuasive cued click points increases the workload for attackers and the system's flexibility to increase the overall number of images in the system that allows us to arbitrarily increase this workload. The approach has proven effective at reducing the formation of hotspots, avoiding pattern formations and also provides high security.

7. ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lecturers who helped us to understand the importance of knowledge and show us the best way to gain it.

8. REFERENCES

[1] S. Chiasson, R. Biddle, and P. van Oorschot,"A Second Look at the Usability of Click-Based Graphical Passwords," Proc. ACM Symp.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 ClickPoints,"Proc.British HCI Group Ann. Conf. People and Computers: Culture,Creativity, Interaction,Sept. 2008.

[3] S. Chiasson, A. Forget, R. Biddle, and P.C. van Oorschot, "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords,"Int'l J. Information Security, vol. 8, no. 6, pp. 387-398,2009.

[4] D. Nelson, V. Reed, and J. Walling, "Pictorial SuperiorityEffect," Journal of Experimental Psychology: Human Learning andMemory, vol. 2, no.5, pp. 523–528, 1976.

[5]L.Jones, A. Anton, and J. Earp, "Towards understanding userperceptions of authentication technologies," in ACM Workshopon Privacy in Electronic Society, 2007.

[6] Dirik, N. Menon, and J. Birget, "Modeling User Choice in the Passpoints Graphical Password Scheme," Proc. Third ACM Symp. Usable Privacy and Security (SOUPS), July 2007.

[7] K. Golofit, "Click Passwords under Investigation," Proc.12th European Symp. Research in Computer Security (ESORICS), Sept. 2007.

[8] A. Salehi-Abari, J. Thorpe, and P. van Oorschot, "On Purely Automated Attacks and Click-Based Graphical Passwords," Proc. Ann. Computer Security Applications Conf. (ACSAC), 2008.

[9] S. Chiasson, P. van Oorschot, and R. Biddle, "Graphical Password Authentication Using Cued Click Points," Proc. European Symp. Research in Computer Security (ESORICS), pp. 359-374, Sept. 2007.

[10]P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on PassPoints-Style graphical passwords," IEEE Trans. Info. Forensics and Security, vol. 5, no. 3, pp. 393–405, 2010.

[11] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "The Memorability and Security of Passwords," Security and Usability: Designing Secure Systems That People Can Use, L. Cranor and S. Garfinkel, eds., ch. 7, pp. 129-142, O'Reilly Media, 2005.

[12] A. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool forinformation security," Transactions on Information Forensics andSecurity (TIFS), vol. 1, no. 2, pp. 125–143, 2006.

[13] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM ComputingSurveys (to appear), vol. 44, no. 4, 2012.

[14]E. Tulving and Z. Pearlstone, "Availability versus accessibilityof information in memory for words," Journal of Verbal Learningand Verbal Behavior, vol. 5, pp. 381–391, 1966.

[15] S.Wiedenbeck, J.Waters, J. Birget, A. Brodskiy, and N. Memon,"PassPoints: Design and longitudinal evaluation of a graphicalpassword system," International Journal of Human-ComputerStudies, vol. 63, no. 1-2, pp. 102–127, 2005.

[16] ——, "Authentication using graphical passwords: Effects oftolerance and image choice," in 1stSymposium on UsablePrivacy and Security (SOUPS), July 2005.

[17] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks andexploiting hot-spots in graphical passwords," in 16th USENIXSecurity Symposium, August 2007.

[18] B. Fogg Persuasive Technologies: Using Computers to Change What We Think and Do. Morgan Kaufmann Publishers, San Francisco, CA, 2003.

[19] J. Wolf, "Visual Attention," in Seeing, K. De Valois, Ed. AcademicPress, 2000, pp. 335–386.

[20] D. Florencio and C. Herley, "Where do security

policies comefrom?" in Symposium on Usable Privacy and Security, 2010.

[21] M. Weir, S. Aggarwal, M. Collins, and H. Stern, "Testing metricsfor password creation policies by attacking large sets ofrevealed passwords," in Computer and Communications Security(CCS), 2010.

AUTHORS BIOGRAPHIES

Mr. Snehal T. Ambade

Pursuing BE (Computer Science & Engineering) in Dr. Babasaheb Ambedkar College of Engineering & Research, Nagpur.

Mr. Shubham Y. Bhivgade

Pursuing BE (Computer Science & Engineering) in Dr. Babasaheb Ambedkar College of Engineering & Research, Nagpur.

Mr. Saurabh Trivedi

Pursuing BE (Computer Science & Engineering) in Dr. Babasaheb Ambedkar College of Engineering & Research,Nagpur.

Mr. S. B. Lanjewar

Lecturer, (Computer Science & Engineering) in Dr. Babasaheb Ambedkar College of Engineering & Research,Nagpur,MS,INDIA.