IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-9 E-ISSN: 2347-2693

Implementation of Persuasive Cued Click Points (PCCP) with the Integration of CAPTCHA and Sound Signature

Anjumol P S[1*] and Amina Beevi A[2]

[1*,2] *Department of Computer Science and Engineering, MG University, Kerala, India*

www.ijcseonline.org

Received: Sep /03/2015 Revised: Sep/10/2015 Accepted: Sep/24/2015 Published: Sep/30/ 2015

***Abstract*—** Various graphical password schemes have been proposed as an alternative to text-based passwords. We propose and examine the usability and security of Persuasive Cued Click Points (PCCP) with a supportive sound signature, a cued-recall graphical password technique. Users click on one point per image for a sequence of images and they are asked to select a sound signature corresponding to each click-point. In PCCP, the next image will be based on the previous click-point. PCCP provides greater security than Pass Points because the number of images increases the workload for attackers. The cued-click point application in this project can be used to enter into a private SMS area, where the SMSs from specified numbers are kept hidden from the Inbox of the ANDROID mobile. As the solution to image gallery attacks digital watermarking is used in the images. In addition to these, we propose to implement a CAPTCHA which ensures the user to be a human and not any machine. Thus additional security to spambot can be ensured.

***Keywords*—** Graphical Password; Persuasive Cued Click Points; Cued Click Point; Sound Signature; Digital Signature; CAPTCHA; ANDROID; SMS; Spambot.

I. INTRODUCTION

A password authentication system should encourage strong passwords while maintaining memorability. We propose that authentication schemes allow user choice while influencing users toward stronger passwords. In our system, the task of selecting weak passwords (which are easy for attackers to predict) is more tedious, discouraging users from making such choices. In effect, this approach makes choosing 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 schemes.

We applied this approach to create the first persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) [2], [3], and conducted user studies evaluating usability and security. This paper presents a consistent assimilation of earlier work [1], [2], [3], [4], [5] and two unpublished web studies, reinterprets and updates statistical analysis incorporating larger data sets, provides new evaluation of password distributions, extends security analysis including relevant recent attacks, and presents important implementation details. This systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issues, to advance understanding as is prudent before practical deployment of new security mechanisms. Through eight user studies [1], [2], [3], [4], [6], we compared PCCP 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.

CAPTCHA (Completely Automated Public Turing tests to tell Computers and Humans Apart) is a program that generates and grades tests that are human solvable, but beyond the capabilities of current computer programs [7]. The robustness of CAPTCHA is found in its strength in resisting automatic adversarial attacks, automatic adversarial attacks, and it has many applications for practical security, including online polls, free email services, search engine bots, worms and spam, and preventing dictionary attacks [7]. Our proposal creates an innovative use of CAPTCHA in the context of graphical passwords to provide better password protection against spyware attacks. In this paper, we have proposed a new authentication scheme combining graphical passwords with text-based CAPTCHA. The scheme is easy for humans but makes it almost impossible for automated programs to harvest passwords. The novel scheme is friendly for legitimate users, while simultaneously raising the time and computer capacity cost to adversaries by several orders of magnitude. Experiments showed its effectiveness, but also indicated further research would improve its usability.

II. RELATED WORK

Graphical password schemes can be grouped into three general categories based on the type of cognitive activity required to remember the password: recognition, recall, and cued recall [10,12]. Recognition is the easiest for human memory whereas pure recall is most difficult since the information must be accessed from memory with no triggers. Cued recall falls somewhere between these two as it offers a cue which should establish context and trigger the stored memory [12]. Among existing graphical passwords, PCCP most closely resembles aspects of Passfaces [11], Story [10], and PassPoint [14,15]. Therefore these graphical password schemes are presented in more detail. Conceptually, PCCP is a blend of the three; in terms of implementation, it is most similar to PassPoint. It also avoids the complex user training requirements found in a number of graphical password proposals, such as that of Weinshall [13]. Passfaces [11] is a graphical password scheme based primarily on recognizing human faces. During password creation, users select a number of images from a larger set. To log in, users must identify one of their pre-selected images from amongst several decoys. Users must correctly respond to a number of these challenges for each login. Davis et al. [10] implemented their own version called Faces and conducted a long-term user study. Results showed that users could accurately remember their images but that user-chosen passwords were predictable to the point of being insecure. Davis et al. [10] proposed an alternative scheme, Story, which used everyday images instead of faces and required that users select their images in the correct order. Users were encouraged to create a story as a memory aid. It fared somewhat worse than Faces for memorability [10], but user choices were much less predictable. The idea of click-based graphical passwords originated with Blonder [9] who proposed a scheme where a password consisted of a series of clicks on predefined regions of an image. Later, Wiedenbeck et al. [14,15] proposed PassPoint, wherein passwords could be composed of several points anywhere on an image. They also proposed a "robust discretization" scheme [8], with three over- lapping grids, allowing for login attempts that were approximately correct to be accepted and converting the entered password into a cryptographic verification key.

III. PROPOSED SYSTEM

Persuasive cued click points

Visual attention research [16] 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 an issue. Davis et al. [10] 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], [4], [5].The goal was to encourage more secure behaviour by making less secure choices (choosing poor or weak passwords)more time consuming and awkward. In effect, behaving securely became the safe path of least resistance [2].

Sound signature

It is a method in which the images are integrated with sound to enhance recalling capability. In daily life we see various examples of recalling an object by the sound related to that object. Our idea is inspired by this novel human ability.

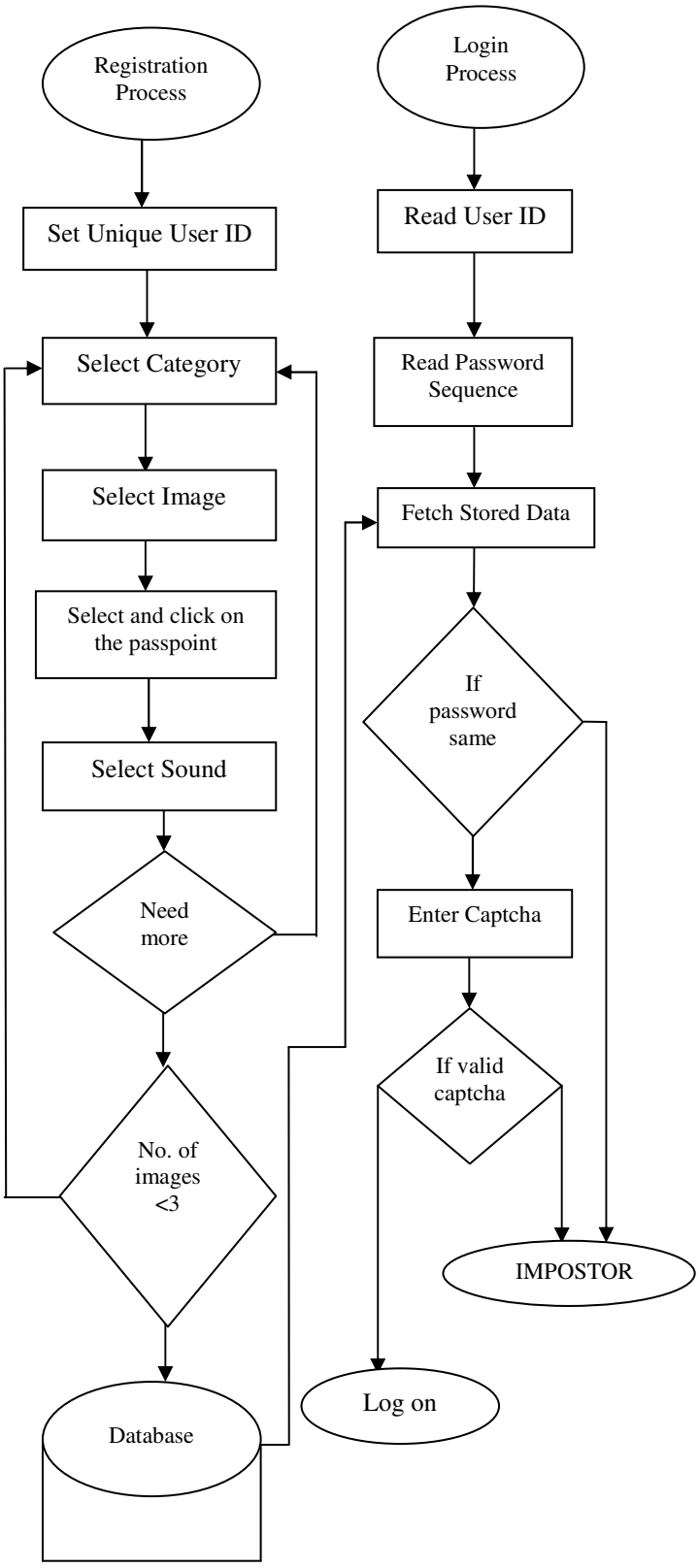
Digital Watermarking

The digital watermarking or digital signature can be done by associating a text with each of the images used in the application. The text can be verified with the images during the login section. This provides security to the images included in the application from gallery attacks.

Our proposed scheme comprises of mainly two phases: *registration and login.* The application of the PCCP in a mobile can be SMS hiding. In our system the user is provided with a set of images from different category. During the registration phase, the user can select images from any category of his choice. Then he can select any point from the image selected and each pixel value selected is associated with a sound signature. A minimum of three pixel values are selected to ensure security. During the login phase, the user is required to correctly enter the pixel values and also the sound signature associated with it. A tolerance value is provided for each point. As an additional security measure a number *captcha* is also added. After the successful entry of PassPoint the user needs to enter the captcha to complete the login phase.

During registration phase the selected image id along with the pixel values and the corresponding sound signature id are stored into the database. During the login phase while re-entering the click points each value is compared with the corresponding value stored in the database. A tolerance is allowed to increase the easiness of the user.

IV. SYSTEM FLOW DIAGRAM



Applications

The proposed system can be applied in mobile phones to create a private message area to store the private messages. Here the messages from certain selected numbers are hidden if the application is on. The hidden messages are directed to a private message inbox and login to the inbox can be done using the proposed scheme. PCCP can also implement to make call blocking, application locking applications. Manufactures of smartphones or tablets can make power on password using PCCP. Operating systems like Windows 8 uses PassPoint authentication and this can be altered with the proposed system PCCP since it is more secure than PassPoint. This can also implement in web based applications or websites which are specially designed for touch based devices.

V. CONCLUSION

We have proposed a novel approach which uses sound signature to recall graphical password click points. No previously developed system used this approach this system is helpful when user is logging after a long time. In future systems other patterns may be used for recalling purpose like touch of smells, study shows that these patterns are very useful in recalling the associated objects like images or text. It is also possible to use audio capturing devices for capturing the input directly from the user at the time of sign up .A common security goal in password-based authentication systems is to maximize the effective password space. This impacts usability when user choice is involved. We have shown that it is possible to allow user choice while still increasing the effective password space. In PCCP, creating a less guessable password (by selecting a click-point within the first few system-suggested viewport positions) is the easiest course of action. Users still make a choice but are constrained in their selection. The image is water marked to provide additional security and usage of captcha helps in distinguishing human and spambot. There are broad applications of PCCP in touch based devices like smartphones and tablets. For smartphones this system can be used to make mobile applications aiming SMS security, call blocking, application locking etc. Most of the websites sends one time passwords and verification codes to mobile phone. So SMS security can be extended to such secret messages too.

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 Click-Points," Proc. British HCI Group Ann. Conf. People and Computers: Culture, Creativity, Interaction, Sept. **2008**.

[3] 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), Nov. **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," Proc. Ann. Computer Security Applications Conf. (ACSAC), **2010**.

[5] 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**.

[6] 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**.

[7] L. von Ahn, M. Blum, and J. Langford. Telling Humans and Computer Apart Automatically. Communications of the ACM, **2004**, 47(2), pp.57-60.

[8] Birget, J.C., D. Hong, and N. Memon. Graphical Passwords Based on Robust Discretization. IEEE Trans. Info. Forensics and Security, 1(3), September **2006**.

[9] Blonder, G.E. Graphical Passwords. United States Patent 5,559,961, **1996**.

[10] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, **2004**.

[11] Passfaces. http://www.realuser.com Last accessed: December 1, **2006**.

[12] Renaud, K. Evaluating Authentication Mechanisms. Chapter 6 in [4].

[13] Weinshall, D. Cognitive Authentication Schemes Safe Against Spyware (Short Paper). IEEE Symposium on Security and Privacy, **2006**.

[14] Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, **2005**.

[15] Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, 102-127, **2005**.

[16] J. Wolf, "Visual Attention," Seeing, K. De Valois, ed., pp. 335-386, Academic Press, **2000**.