Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.166 – 172

RESEARCH ARTICLE

Cued Click Point Technique for Graphical Password Authentication

Vaibhav Moraskar[1], Sagar Jaikalyani[2], Mujib Saiyyed[3], Jaykumar Gurnani[4], Kalyani Pendke[5]

[1,2,3,4] Department of CSE, Rajiv Gandhi College of Engineering & Research, Nagpur, India

[5] Lecturer, Department of CSE, Rajiv Gandhi College of Engineering & Research, Nagpur, India

[1] vaibhavmoraskar77@gmail.com; [2] sagarjaikalyani@gmail.com;
[3] mujib.saiyyed@gmail.com; [4] a.sunny50@gmail.com, [5] pendke@gmail.com

Abstract— ***In today's world the password security is very important. For password protection various techniques are available. Cued Click Points are a click-based graphical password scheme, a cued-recall graphical password technique. Users Click on one point per image for a sequence of images. The next image is based on the previous click-point. The passwords which are easy to memorize are chosen by the users and it becomes easy for attackers to guess it, but the passwords assigned by the strong system are difficult for users to remember. In this paper, we focus on the evaluation of graphical password authentication system using Cued Click Points, including usability and security. In this authentication system, our usability goal is to support the users in selecting better passwords, thus increases the security by expanding the effective password space. The emergence of hotspots is mainly because of poorly chosen passwords. Thus click-based graphical passwords encourage users to select more random, and hence more complex to guess, click-points.***

Keywords—Cued Click Point (CCP); Graphical passwords; authentication; persuasive technology; usable security; empirical study

I. INTRODUCTION

Authentication is the process of determining whether a user should be allowed to access to a particular system or resource. User can't remember strong password easily and the passwords that can be remembered are easy to guess. A password authentication system should encourage strong and less predictable passwords while maintaining memorability and security. This password authentication system allows user choice while influencing users towards stronger passwords. The task of selecting weak passwords (which are easy for attackers to guess) is more tedious, avoids users from making such choices. In effect, this authentication schemes 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 absent in most schemes.

In this paper, we propose a Cued Click Points (CCP) for graphical password authentication. A password consists of one click-point per image for a sequence of images. The next image displayed is based on the previous click-point so users receive immediate implicit feedback as to whether they are on the correct path when logging in. CCP offers both improved usability and security.

II. BACKGROUND

Various graphical password schemes have been proposed as alternatives to text-based passwords. Research has shown that text-based passwords are filled with both usability and security problems that make them less desirable solutions. Studies revealed that the human brain is better at recognizing and recalling images than text.

Graphical passwords are meant to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by images, more secure passwords can be produced and users will not resort to unsafe practices in order to cope.

Graphical passwords may offer better security than text-based passwords because most of the people, in an attempt to memorize text-based passwords, use plain words (rather than the jumble of characters). A dictionary search can hit on a password and allow a hacker to gain entry into a system in seconds. But if a series of selected images is used on successive screen pages, and if there are many images on each page, a hacker must try every possible combination at random.

III. RELATED WORK

Graphical password schemes can be grouped into three general categories: recognition, recall, and cued recall 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 between these two as it offers a cue which should establish context and trigger the stored memory.

A. Passfaces

Passfaces 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 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.

B. Story

Davis et al proposed an alternative scheme, Story uses everyday images instead of faces, requires that users select their images in the correct order. Users were encouraged for creating a story as a memory aid. It results in somewhat worse than Faces for memorability, but user choices were much less predictable.

C. Passpoint

Fig. 1: Graphical Password Authentication using Passpoint.

Wiedenbeck et al proposed PassPoints, where passwords could be composed of several points anywhere on an image. They also proposed a "robust discretization" schema, with number of overlapping grids, allowing for login attempts that were closely resembling correct to be accepted and converting the entered password into a cryptographic verification key.

D. Cued Click Point

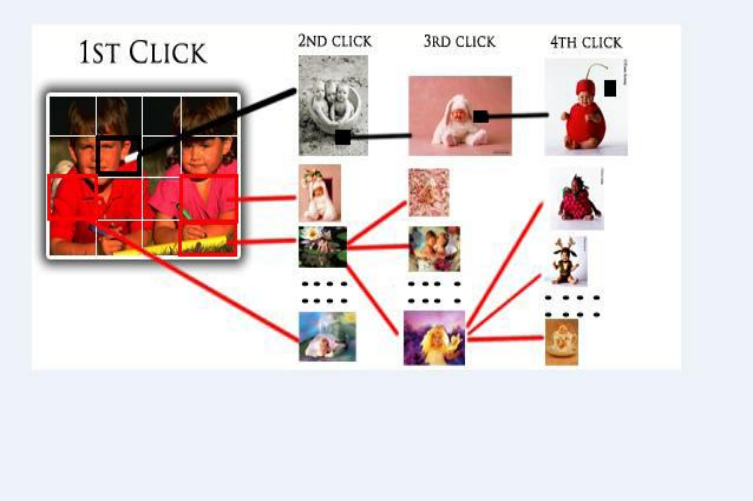

Fig. 2: Graphical Password Authentication using Cued Click Point.

Cued Click Points (CCP) is a proposed alternative to PassPoints. In CCP, users click one point on each image rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point. It also makes attacks based on hotspot analysis more challenging.

IV. BASIC MODEL

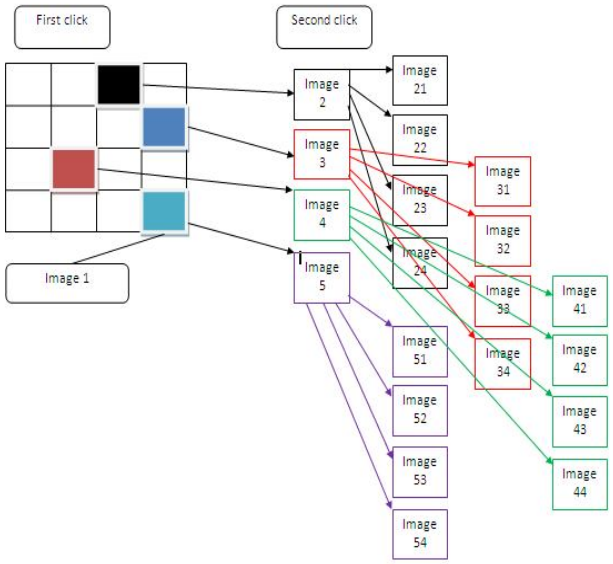

Fig. 3: Basic Model for Graphical Password Authentication.

V. SYSTEM DESIGN

The system designed consists of three modules: user registration module, picture selection module and system login module.

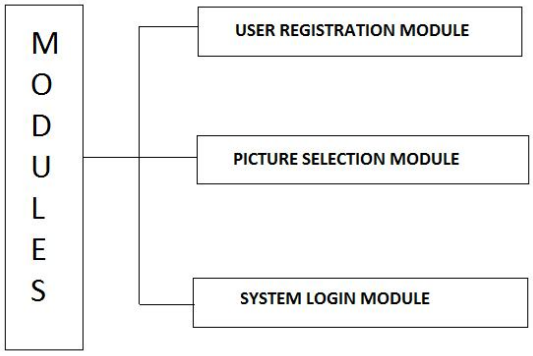

Fig. 4: System Design Modules.

In user registration module user enters the user name in user name. When user entered the all user details in registration phase, this user registration data is stored in data base and used during login phase for verification. In picture selection phase there are two ways for selecting picture password authentication.

1. User defines pictures: Pictures are selected by the user from the hard disk or any other image supported devices.
2. System defines pictures: pictures are selected by the user from the database of the password system.

In picture selection phase user select any image as passwords and consist of a sequence of five click-points on a given image. Users may select any pixels in the image as click-points for their password. Users must select a click-point in the image and proceed on the next image.

During system login process, images are displayed normally, without shading or the viewport, and repeat the sequence of clicks in the correct order, within a system-defined tolerance square of the original click-points.

VI. SCREEN SHOTS

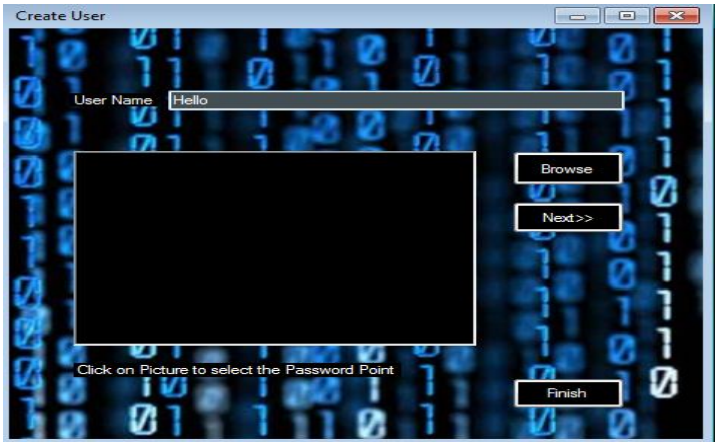

Fig. 5: Create User.

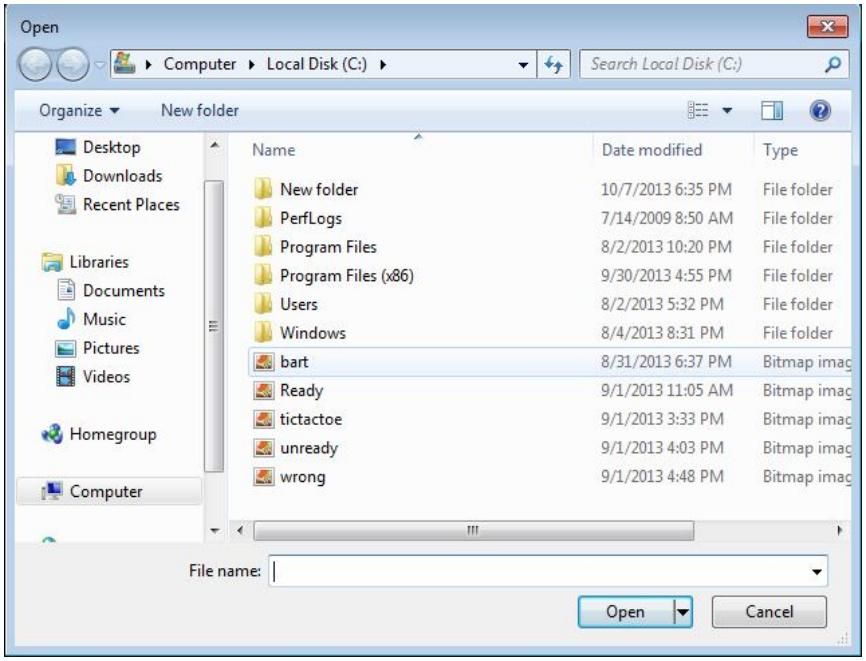

Fig. 6: picture selection.

Fig. 7: picture selected.

Fig. 8: Select password point.

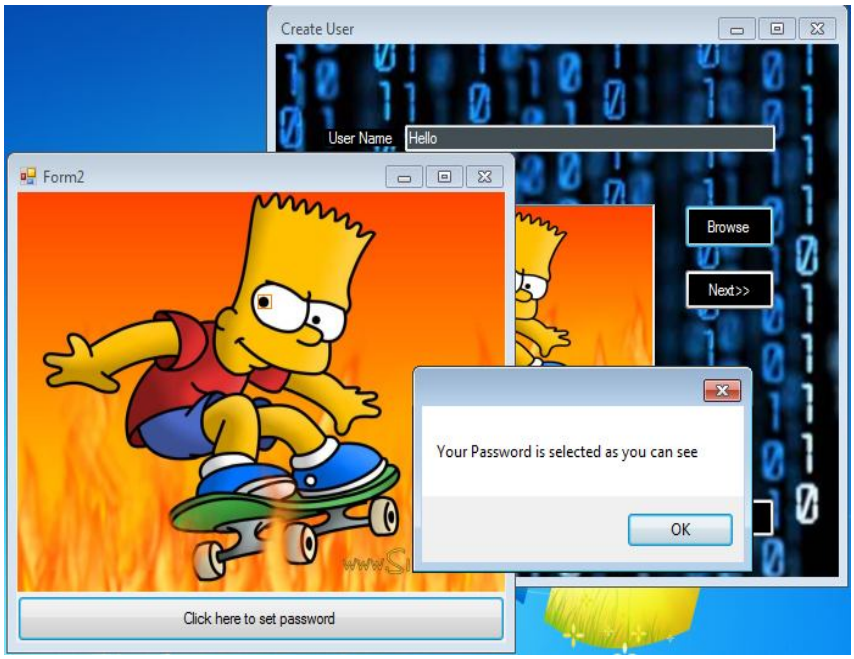

Fig. 9: password selected.

VII. CONCLUSION

The Cued Click-Point method is very usable and provides great security using hotspot technique. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image. Cued Click Point is more secure than the previous graphical authentication methods. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then analyze for hotspot on each of these images. Cued Click-Points method has advantages over other password schemes in terms of usability, security and memorable authentication mechanism.

REFERENCES

[1] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, P. C. van Oorschot, "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism", IEEE Trans, Vol 9, Issue 2.
[2] 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.
[3] A. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," Transactions on Information Forensics and Security (TIFS), vol. 1, no. 2.
[4] D. Nelson, V. Reed, and J. Walling, "Pictorial Superiority Effect," Journal of Experimental Psychology: Human Learning and Memory, vol. 2, no. 5.
[5] 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.
[6] E. Tulving and Z. Pearlstone, "Availability versus accessibility of information in memory for words," Journal of Verbal Learning and Verbal Behavior, vol. 5.
[7] 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.
[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] Dirik, A.E., N. Menon, and J.C Birget. "Modeling user choice in the PassPoints graphical password scheme". ACM SOUPS, 2007.
[10] Thorpe, J. and P.C. van Oorschot. "Human-Seeded Attacks and Exploiting HotSpots in Graphical Passwords." 16th USENIX Security Symposium, 2007.

