Click-Based Graphical Password Scheme Using Cued Clicks

S.Geetha[#], V.Ranjani[*], S.Gowthami[#], R.Selvarathi[#]
[#]*CSE, Saranathan College of Engineering*

***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*— Authentication, Cued Click Point (CCP), Graphical passwords, Pass faces, Pass points**

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.

A. Graphical Passwords

Graphical passwords refer to using pictures (also drawings) as passwords. In theory, graphical passwords are easier to remember, since humans remember pictures better than words . Also, they should be more resistant to bruteforce attacks, since the search space is practically infinite.

In general, graphical passwords techniques are classified into two main categories: recognition-based and recallbased graphical techniques. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Passfaces is a recognition-based technique, where a user is authenticated by challenging him/her into recognizing human faces. An early recall-based graphical password approach was introduced by Greg Blonder in 1996 .

In this approach, a user create a password by clicking on several locations on an image. During authentication, the user must click on those locations. PassPoints builds on Blonders idea, and overcomes some of the limitations of his scheme.

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

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.

Text based passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks . Graphical passwords offer another alternative, and are the focus of this paper. Click-based graphical passwords: Graphical password systems are a type of knowledge-based authentication that attempt to leverage the human memory for visual information . A comprehensive review of graphical passwords is available elsewhere. 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. The images act as memory cues to aid recall. Example systems include PassPoints , Cued Click-Points and Persuasive Cued Click-Points.

C. Pass Point

Fig. 1 Graphical Password Authentication using Passpoint.

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

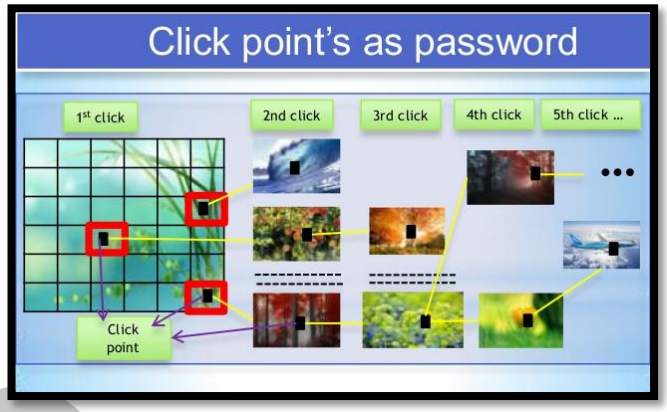

Fig. 2 Graphical Password Authentication using Cued Click Point.

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

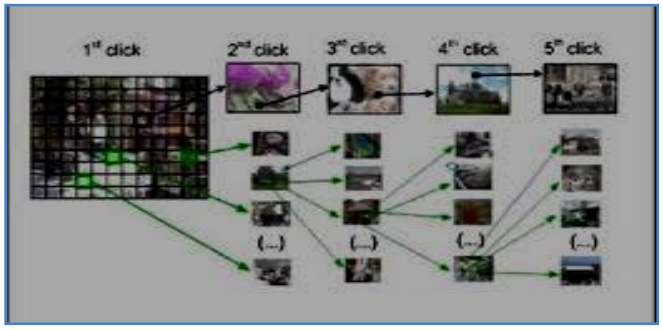

Fig. 3 Basic Model for Graphical Password Authentication.

V. RELATED WORK

A trial consisted of the following steps. The phases indicated in steps 1, 2, and 5 represent the password phases used in later analysis.

1) *Create Phase:* Create a password by clicking on one point in each of five system-selected images presented in sequence.

2) *Confirm Phase:* Confirm this password by re-entering it correctly. Users incorrectly confirming their password could retry the confirmation or return to Step 1. A new password started with the same initial image, but generally included different images thereafter, depending on the click-points.
3) *Two Questions:* Answer two 10-point Likert-scale questions on the computer about their current password's ease of creation and predicted memorability. Likert-scale questions ask respondents to indicate their level of agreement with the given statement on a scale ranging from strongly agree to strongly disagree.
4) *MRT:* Complete a Mental Rotations Test (MRT) puzzle. This paper-based task was used to distract users for a minimum of 30 seconds by giving them a visual task to complete in order to clear their working memory.
5) *Login Phase:* Log in with their current password. If users noticed an error during login, they could cancel their login attempt and try again. Alternatively, if they did not know their password, they could create a new password, effectively returning to Step 1 of the trial with the same initial image as a starting point. If users felt too frustrated with the particular images to try again, they could skip this trial and move on to the next trial.

Participants completed as many trials as they wished in the one-hour session, to a maximum of 14 (2 practice + 12 real trials). trials). At the midpoint, participants took a break and completed a demographics questionnaire. The last ten minutes of the session were devoted to completing a Likert-scale and open-ended questionnaire about their perceptions and opinions of these graphical passwords. For each participant, data from the two practice trials were discarded, so all results reported in this paper are based on data from the subsequent trials.

TABLE 1
TOTAL NUMBER OF RESTARTS, SUCCESS RATES OF CREATE, CONFIRM AND LOGIN PHASES

	Create	Confirm	Login
Total Number of Restarts	7	101	14
Success rates	251/257 (98%)	213/257 (83%)	246/257 (96%)

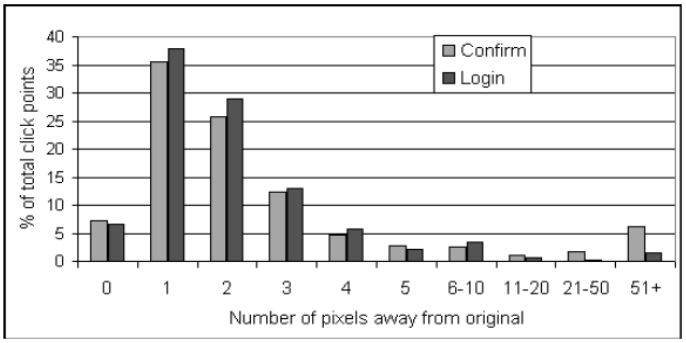

Fig. 4 Accuracy for each phase

VI. 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.