Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

ECCP: Enhanced Cued Click Point Method for Graphical Password Authentication

Lavanya Reddy L*
Department of CSE
Sri Venkateswara College of Engineering, India

K.Alluraiah
Department of CSE
Sri Venkateswara College of Engineering, India

Abstract: More often the computer systems are access based on alphanumeric passwords. However users are difficult to remember long and randomized passwords, so that they create simple, short and insecure password. Graphical passwords have been designed for more secure and that to make passwords more memorable and easy to use by the people. Using this technique user's click on the images rather than typing alphanumeric passwords. This paper present and examine usability and security Enhanced cued click point method for authentication using graphical passwords. In this paper we describe the Enhanced cued click point method, its characteristics for security and performed empirical study comparing cued click point method and alphanumeric passwords. The results shows graphical passwords are more secure which is difficult to guess the click points.

Keywords: Graphical Password, Authentication, Empirical Study, Usability, Security.

1. INTRODUCTION

Traditionally, alphanumeric passwords have been used for authentication, but they are known to have security and usability problems. We refer to the security and usability problems associated with alphanumeric passwords as "the password problem". The problem arises because passwords are expected to comply with two fundamentally conflicting requirements: the password should be secure and easy to remember. Satisfying these requirements is virtually impossible for users. Consequently, users ignore the requirements, leading to poor password practices. This problem has led to innovations to improve passwords. One innovation is graphical passwords, i.e., passwords that are based on images rather than alphanumeric strings. The basic idea is that using images will lead to greater memorability and decrease the tendency to choose insecure passwords. This, in turn, should increase overall password security. In this paper, we propose an Enhanced Cued Click Points (ECCP) 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. ECCP offers both improved usability and security.

In order to evaluate the usability of the system, we conducted an empirical study with 24 users and a total of 257 trails. During evaluation users could create and re-enter their passwords very quickly. The result of the empirical study shows that users had high success rate and get very accurate when entering their click-points. They also said that they appreciated the immediate implicit feedback telling them whether their latest click-point was correctly entered.

In order to improve the security, we introduce hotspots in this paper. Hotspots (i.e., areas of the image that users are more likely to select) are a concern in click-based passwords, so ECCP uses a large set of images that will be difficult for attackers to obtain. For our proposed system, hotspot analysis requires proportionally more effort by attackers, as each image must be collected and analyzed individually. ECCP appears to allow greater security than previous graphical password methods.

The rest of this paper is organized as follows: Section 2 presents background material and related work on Graphical password scheme. Section 3 introduces the Enhanced Cued Click point for graphical authentication scheme. Section 4 describes empirical study on ECCP. Section 5 shows the results of empirical study while section 6 concludes.

2. BACKGROUND AND RELATED WORK

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 [3]. 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 [4]. A comprehensive review of graphical passwords is available elsewhere. Of interest herein are cued-recall click-based graphical passwords (also known as locimetric [5]). In such systems, users identify and target previously selected locations within one or more images. The images act as memory cues [6] to aid recall. Example systems include PassPoints [7], Cued Click-Points [2] and Persuasive Cued Click-Points [1].

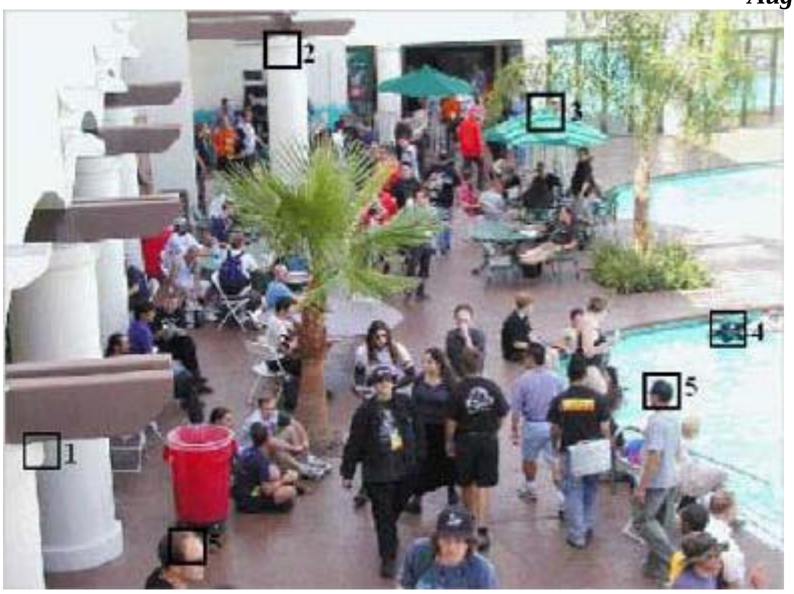


Fig. 1 Graphical Password Authentication using Passpoint

In PassPoints [7], passwords 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. To log in, they repeat the sequence of clicks in the correct order (Shown in figure 1), within a system-defined tolerance square of the original click-points. Although PassPoints is relatively usable security weaknesses make passwords easier for attackers to predict. Cued Click-Points [2] uses one click-point on five different images in sequence rather than 5 clicks in single image. The next image displayed is based on the location of the previously entered click-point, 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-points results in a different image sequence. User testing and analysis showed no evidence of patterns in CCP, so pattern-based attacks seem ineffective. Persuasive Cued Click-Point [1] also uses the same technique that uses Cued-Click point but it provides more security than the CCP. Sonia Chiasson et., al. investigated whether the system could influence users to select more random click-points while maintaining usability. Their goal was to encourage more secure behavior by making less secure choices (i.e., choosing poor or weak passwords) more time consuming and awkward. In effect, behaving securely became the safe path-of-least-resistance. We proposed Enhanced Cued Click-Point in which 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. ECCP offers both improved usability and security.

3. Enhanced Cued Click Point

Enhanced Cued Click Points (ECCP) is a proposed alternative to Cued Click Points. In ECCP, users click one point on each of c = 5 images 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 (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging, as we discuss later. As shown in Figure 2, each click results in showing a next-image, in effect leading users down a “path” as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image. If they dislike the resulting images, they could create a new password involving different click-points to get different images.

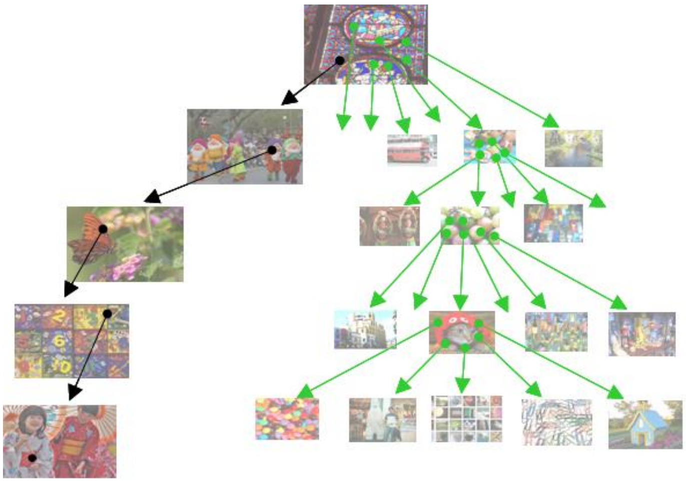


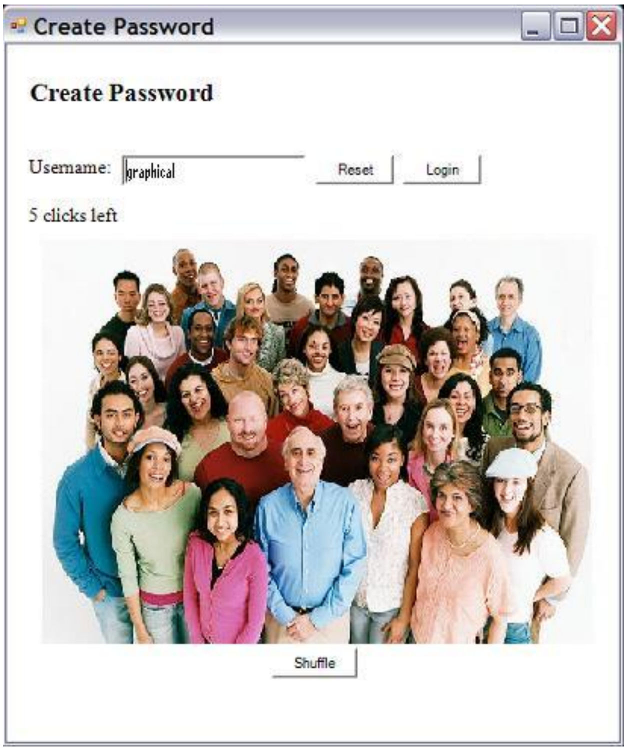
Fig. 2 Enhanced Cued Click-Points Method of Graphical Password Authentication

For implementation, ECCP initially functions like Cued Click Points. During password creation, a discretization method [8] is used to determine a click-point's tolerance square and corresponding grid. For each click-point in a subsequent login attempt, this grid is retrieved and used to determine whether the click-point falls within tolerance of the original point. With ECCP, we further need to determine which next-image to display. A user's initial image is selected by the system based on some user characteristic (as an argument to f above; we used username). The sequence is re-generated on-the-fly from the function each time a user enters the password. If a user enters an incorrect click-point, then the sequence of images from that point onwards will be incorrect and thus the login attempt will fail. For an attacker who does not know the correct sequence of images, this cue will not be helpful. We expect that hotspots [9, 10] will appear as in Cued Click Points, but since the number of images is significantly increased, analysis will require more effort which increases proportionally with the configurable number of images in the system. For example, if attackers identify thirty likely click-points on the first image, they then need to analyze the thirty corresponding second images (once they determine both the indices of these images and get access to the images themselves), and so on, growing exponentially.

A major usability improvement over Cued Click Points [2] is the fact that legitimate users get immediate feedback about an error when trying to log in. When they see an incorrect image, they know that the latest click-point was incorrect and can immediately cancel this attempt and try again from the beginning. The visual cue does not explicitly reveal "right" or "wrong" but is evident using knowledge only the legitimate user should possess. As with text passwords, Cued Click Points can only safely provide feedback at the end and cannot reveal the cause of error. Providing explicit feedback in Cued Click Points before the final click-point could allow Cued Click Points attackers to mount an online attack to prune potential password subspaces, where as ECCP's visual cues should not help attackers in this way. Another usability improvement is that being cued to recall one point on each of five images appears easier than remembering an ordered sequence of five points on one image.

4. Empirical Study

We conducted an in-lab user study of ECCP with 24 participants. Participants completed two practice trials followed by at most 12 real trials. In total, 257 real CCP trials were completed. Create password user interface (shown in figure 3) which the participants are practiced.



Create Password

Username: graphical

5 clicks left

Fig 3. ECCP Create Password User Interface

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 [10]. 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). 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.

5. COLLECTED RESULTS

*A. Usability:*Participants used the reset button as soon as they saw an incorrect image and realized they were on the wrong path. This effectively cancelled the current attempt and returned them to the first image where they could start entering their password again. A few times, participants restarted even when they saw the correct image because they had forgotten the image. Failed login attempts (where users pressed the login button and were explicitly told that their password was incorrect) occurred only when users clicked on the wrong point for the last image since they did not receive any implicit feedback for that click-point. Because these were so few, failed login attempts are included in the restart counts. Participants said that confirming the password helped them to remember it. Once they had successfully confirmed the password, logging on even after the distraction task was relatively easy.

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%)

Four participants completed all their trials without any restarts, i.e., they made no errors during the entire session. In total, 209 of 257 trials (81%) were completed without restarts in any phase. The success rates were high for all phases, as shown in Table 1. Success rates were calculated as the number of trials completed without errors or restarts over the total number of trials.

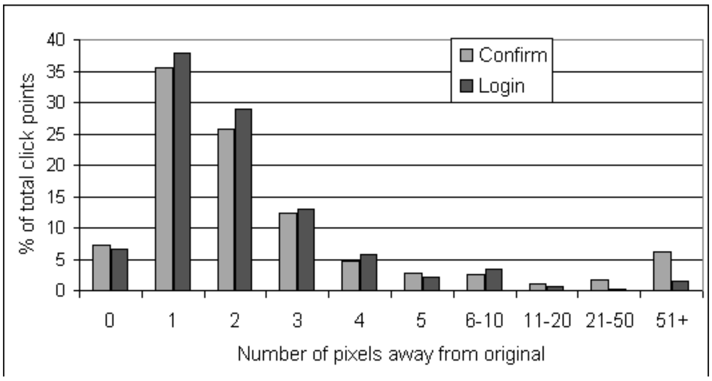


Fig. 4 Accuracy for each phase

B. Accuracy: Participants were extremely accurate in re-entering their passwords. As a measure of accuracy, all individual click-points in the Confirm and Login phases were evaluated. This totalled 1569 click-points for the Confirm phase and 1325 click-points for the Login phase. For each point, the accuracy was computed as the maximum of $|x_{original} - x_{current}|$ and $|y_{original} - y_{current}|$. All click-points were considered in the analysis, even those that were unsuccessful. A few times, participants reached an incorrect image and still proceeded to click on a point. These were included in the 51+ category since the point was obviously forgotten. As indicated in Figure 4, 86% of points were within 4 pixels of the original click-point for the Confirm phase compared to 92% for the Login phase. Falling within 4 pixels of the original point means that these click-points would have been accepted within a tolerance square of 9x9 pixels.

C. Security: Hotspots are specific areas in the image that have a higher probability of being selected by users as part of their passwords. If attackers can accurately predict the hotspots in an image, then a dictionary of passwords containing combinations of these hotspots can be built. Hotspots are known to be problematic for Cued Click Points; further analysis is needed to determine whether precautions such as carefully selecting images can minimize this threat.

A key advantage of ECCP over Cued Click-Points is that attackers need to analyze hotspots on a large set of images rather than only one image since they do not know the sequence of images used for a given password. Secondly, using different subsets of images for different users means that an attacker must somehow gather information about the specific subset assigned to the current user.

6. Conclusions

The proposed Enhanced Cued Click-Points method shows promise as a usable and provides great security using hotspot technique. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image. ECCP provides greater security than the previous graphical authentication methods. ECCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. Enhanced Cued Click-Points method has advantages over Cued Click-Point 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, pp. 359–374.

[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, pp. 125–143, 2006.

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

[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, no. 1-2, pp. 128–152, 2005.

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

[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, no. 1-2, pp. 102–127, 2005.

[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.