Helping Users Protect Themselves from e-Criminals in Click-Based Graphical Passwords

Alain Forget
School of Computer Science
& Human-Oriented Technology Lab
Carleton University
aforget@scs.carleton.ca

Sonia Chiasson
School of Computer Science
& Human-Oriented Technology Lab
Carleton University
chiasson@scs.carleton.ca

Robert Biddle
Human-Oriented Technology Lab
Carleton University
robert_biddle@carleton.ca

ABSTRACT
Click-based graphical passwords, like other user-selected passwords, suffer from predictability problems. With click-based graphical passwords, user click-points form *hotspots*, areas of the image that are more likely to be selected, which e-criminals can predict and use to launch dictionary attacks. Our system, Persuasive Cued Click-Points, helps users select more random click-points and reduces the appearance of hotspots while still maintaining usability.

1. INTRODUCTION
User choice during password selection tends to be predictable. This often occurs in both text and graphical passwords since users want easy-to-remember passwords or they are unsure what would make a good password [7]. In this paper, we present Persuasive Cued Click-Points; a system that aims to convince users to select more random, and hence more secure, click-based graphical passwords while maintaining the usability of initial system. Preliminary results are promising; hotspots (areas of the image that are more likely to be selected) are significantly reduced and login success rates remain high. It appears that our scheme helps users better protect themselves from e-criminals using dictionary attacks.

2. BACKGROUND
Attempts at convincing users to select more secure passwords have focused on text passwords, with only limited success. Strategies include imposing requirements such as including a number in passwords and showing a "strength-meter" that rates the security of passwords based on some arbitrary criteria. While these may produce more secure passwords, the resulting passwords may be more difficult to remember. Another approach tries to improve password memorability by encouraging users to base their passwords on a mnemonic phrase [5]; however it was later shown that users still selected predictable passwords [4,5].

Graphical passwords have been proposed as potentially more secure and usable alternatives to text passwords. Suo et al. [8] provide an overview of several different graphical password schemes. PassPoints [10] is a click-based graphical password system where a user enters a password by clicking on five points on an image in the correct order. This scheme is vulnerable to dictionary attacks since it suffers from hotspots [9]. In a second system, Cued Click-Points (CCP) [2], users instead select one point on a sequence of five images. The next image in the sequence is determined by the coordinates of the preceding click-point. While improving usability, CCP makes it more difficult for attackers to take advantage of hotspots by requiring more effort to mount an attack.

Visual attention research [11] shows that humans are attracted to the same predictable areas when looking at an image. This suggests that if users select their own click-based graphical passwords without guidance, hotspots will likely remain an issue. So far, little research exists on helping users avoid hotspots during password creation.

3. PCCP
Our system aims to reduce hotspots by encouraging users to select more random passwords. We have currently implemented it for CCP, but the technique could be applied to any click-based graphical password scheme.

When creating a password, Persuasive Cued Click Points (PCCP) helps users select their click-point by lightly shading the entire image, except for small area, known as the *viewport* (see Figure 1). Users can only click within this randomly positioned viewport. If they are unable to find a suitable click-point, they can press the "shuffle" button to randomly reposition the viewport. The most straightforward and quickest action is to select a click-point from the first viewport. However, someone determined to reach a specific click-point can repeatedly shuffle until the viewport reaches that area. Other than the modified password creation process, the system operates the same as the original CCP system.

3.1 User Study
To test PCCP, we conducted an in-lab user study with 24 participants. Each completed a one-hour session in the lab, creating and logging in with up to ten PCCP passwords. In total, 224 trials were completed.

For each trial, users created a password by selecting a click-point on each of five images, confirmed the password by re-entering their click-points, performed a distraction task, and then logged in by re-entering the password one last time, to show the password had been successfully memorised.

A set of 330 images was used, but the system ensured that 17 core images were seen by all participants in order to gather sufficient click-point data on these images. Consistent with previous

Anti-Phishing Working Group eCrime Researchers Summit, October 4-5, 2007, Pittsburgh, PA, USA.

PassPoints and CCP studies [1,2,10], the image dimensions were 451x331 pixels and were displayed on a 1064x768 screen.

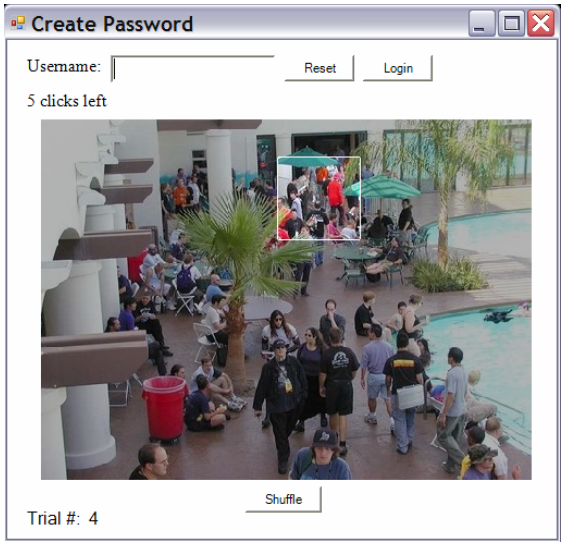

Figure 1: Screenshot of the PCCP Create Password interface with the viewport highlighting a portion of the image [6].

As shown in Table 1, participants were able to successfully use PCCP. Success rates were calculated as the number of trials completed without errors or restarts over all trials. As in earlier studies with click-based graphical passwords [1,2], participants had some difficulty during confirmation as they were learning their password, but had no problem logging on afterwards.

Table 1: Success rates and completion times out of 224 trials

	Create	Confirm	Login
Success rate	223 (99%)	163 (73%)	212 (95%)
Median Time (sec)	44.1	18.0	14.0

Most participants used the shuffle button sparingly; the median number of shuffles per trial was 0. In these cases, the viewport remained in its initial random position, lowering the chance of participants selecting hotspots as their click-points. We compared the PCCP click-points to those collected from our earlier PassPoints [1] and CCP studies [2], and found that click-points for PCCP were much more uniformly distributed and evaded hotspots (Figure 2).

4. DISCUSSION AND CONCLUSION

PCCP helps users create more random passwords, forcing attackers to use larger click-point dictionaries to be successful. Users were able to remember and accurately log in using their passwords, suggesting that the randomness had little impact on usability once participants learned their password. We further hypothesise that PCCP helps users form more accurate mental models of creating a secure click-based graphical password, teaching them that randomness equates to greater security.

Click-based graphical passwords, like all user-selected passwords, suffer from predictability problems. This is worrisome from a security perspective since it can be exploited by attackers. Persuasive Cued Click-Points addresses the issue of hotspots by assisting users during the password creation process and encouraging them to select more random passwords. Results of our user study show that hotspots are significantly less likely to occur with PCCP than with other click-based graphical password systems while still maintaining the usability of the system. Although preventing all password attacks may not be possible, PCCP helps users create more secure passwords, forcing attackers to commit more resources to exhaustively search a much larger click-point space, rather than a small number of hotspots. Furthermore, our viewport technique can be applied to any click-based graphical password scheme to minimise hotspots.

Figure 2: Aggregated hotspots from previous studies (red & green) compared to PCCP user click-points (black circles) [6].

REFERENCES

[1] Chiasson, S., Biddle, R., van Oorschot, P.C. A Second Look at the Usability of Click-based Graphical Passwords. SOUPS 2007.

[2] Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007.

[3] Davis, D., Monrose, F., Reiter, M.K. On User Choice in Graphical Password Schemes. USENIX Security 2004.

[4] Forget, A., Chiasson, S., Biddle, R. Helping Users Create Better Passwords: Is this the right approach? SOUPS 2007.

[5] Kuo, C., et al. Human Selection of Mnemonic Phrase-based Passwords, SOUPS 2006.

[6] PD Photo. http://pdphoto.org Accessed August 2007.

[7] Sasse, M.A., Brostoff, S., Weirich, D. Transforming the 'weakest link': a human/computer interaction approach to usable and effective security. BT Technology Journal 19(3), 122-131, 2001.

[8] Suo, X., Zhu, Y., and Owen, G.S. Graphical Passwords: A Survey. ACSAC 2005.

[9] Thorpe, J. and van Oorschot, P.C. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security 2007.

[10] Wiedenbeck, S., et al. PassPoints: Design and longitudinal evaluation of a graphical password system. International Journal of Human-Computer Studies 63, 102-127, 2005.

[11] Wolf, J. Visual Attention. In Seeing, 2nd edition. K.K. De Valois (ed.). Academic Press, 2000, 335-386.