The Presentation Effect on Graphical Passwords

Julie Thorpe
University of Ontario
Institute of Technology
julie.thorpe@uoit.ca

Muath Al-Badawi
University of Ontario
Institute of Technology
muath.albadawi@uoit.net

Brent MacRae
University of Ontario
Institute of Technology
brent.macrae@uoit.ca

Amirali Salehi-Abari
University of Toronto
Dept. of Computer Science
abari@cs.toronto.edu

ABSTRACT
We provide a simple yet powerful demonstration of how an unobtrusive change to a graphical password interface can modify the distribution of user chosen passwords, and thus possibly the security it provides. The only change to the interface is how the background image is presented to the user in the password creation phase—we call the effect of this change the "presentation effect". We demonstrate the presentation effect by performing a comparative user study of two groups using the same background image, where the image is presented in two different ways prior to password creation. Our results show a statistically different distribution of user's graphical passwords, with no observed usability consequences.

Author Keywords
user authentication; passwords; graphical passwords

ACM Classification Keywords
H.5.2. Information Interfaces and Presentation; K.6.5 Management of Computing and Information Systems: Security and Protection

INTRODUCTION
Graphical passwords [1] are an alternative to traditional text passwords where users choose an image (or some of its parts) instead of a word. Many graphical password schemes have been proposed; unfortunately, many studies have shown that users often create graphical passwords with similar properties that make them easy for attackers to guess [4, 9, 10]. Surprisingly, little attention has been given to understanding how the user interfaces of these systems impact their security.

Motivated by this, we study graphical passwords under what we call the *presentation effect* – the effect that presenting an object's informative components in a different order has on the viewer's perception and decision making processes. Consider the presentation effect upon entering a hotel for the first time; you enter through the main door, then walk through the lobby, and finally each hallway. Now again consider entering the same hotel for the first time, but instead you take a different path, entering through the emergency side door, walking through each hallway, and finally going to the lobby. Are your perceptions of the hotel the same in each case? If you plan to visit the hotel again at a later time, are you more inclined to take the same path? We aim to study the presentation effect on the creation of graphical passwords, how it alters the distribution of user choice, and whether it impacts usability.

We focus on a form of graphical password known as *PassPoints* [14] as it is known to suffer from patterns in the distribution of user choice [10]. In PassPoints, a user is shown a background image and then asked to select a sequence of 5 *click-points* as his/her password. This style of graphical password can be input using a mouse or a finger (on a touch screen), but to reduce its vulnerability to observation attacks it can be input using an eye tracker as in other systems [6, 2].

We studied a variant of PassPoints with two different image presentations in the password creation phase: the image is initially covered with a white foreground (a *curtain*), and the curtain is drawn from either right-to-left (RTL) or left-to-right (LTR), gradually revealing the image beneath. The users watch the image reveal completely before creating their graphical password, thus any effect we observe is not due to users desire to choose a password quickly. The image presentations are only used just before password creation; all other interactions with the system display the full background image to the user (as in the original version of PassPoints).

Our results demonstrate a statistically significant difference in the distribution of the first click-points of users in the RTL vs. LTR groups, with no observed negative usability consequences. We discuss the security and usability implications of these findings and some exciting possibilities for future work.

RELATED WORK
The literature on graphical passwords is rich (see a recent survey [1] for an exposition). The present research is based on a "cued-recall" scheme called PassPoints [14], in which a pass-

CHI 2014, April 26 - May 01 2014, Toronto, ON, Canada.

http://dx.doi.org/10.1145/2556288.2557212

word is a sequence of 5 (x, y) *click-points* on a background image. The user logs in by clicking on the same sequence of 5 points, in the same order. A small amount of error tolerance is permitted upon re-entering these click-points, e.g., other studies have allowed up to 7-10 pixels for each click-point.

PassPoints suffer from security problems caused by users choosing popular points [10] which help the success of automated attacks [4, 9]. To counter these vulnerabilities, some persuasive techniques have been proposed that limit user's choice at the password creation phase to deter users from choosing popular points. One approach, Persuasive Cued Click Points [3], is based on a different cued-recall variant, and uses a randomly placed viewport containing a small region of the image where the user can choose his/her point. Another approach [2] uses saliency masks to reduce interest in the salient and presumably more attractive parts of the image. Our approach in this paper does not limit user's choices by making parts of the background image unavailable, but rather aims to influence user's choices in an unobtrusive way.

SYSTEM AND IMAGE PRESENTATION STYLES

The purpose of this study was to determine whether different background image presentations can influence user choice in PassPoints graphical passwords. We focus on one presentation style that we call *drawing the curtain*, where the image is first covered with a white foreground (a *curtain*) and then the curtain is drawn from either right-to-left (RTL) or left-to-right (LTR), gradually revealing the image beneath. The image presentations are only used immediately before password creation; all other interactions with the system display the full background image to the user. In our experiments, users must watch the image reveal before creating their graphical password. In both presentations, it takes 20 seconds for the image to be revealed at a constant rate. Figure 1 illustrates the curtain effect in the RTL group. The background image used (see Figure 2) was 640×480 pixels. We used an error tolerance of 10 pixels in each direction (consistent with other studies).

(a) $t = 0$ (b) $t = 7$ (c) $t = 20$

Figure 1. Snapshots of *drawing the curtain* from right-to-left (RTL). The time t is the number of seconds since the curtain started being drawn.

For a field implementation, the system can allow users to select their passwords on the portion of the image revealed while the presentation is taking place. If users select their first points during the presentation, their choices will naturally be biased toward the first parts revealed, due to limited options. However, users may still select their first points *after* the presentation completes; this scenario motivates our experiments.

USER STUDY

We conducted a user study with our system involving three sessions over 8 days. Two of the sessions were held *in lab*, in an isolated room on a university campus. These sessions were completed in a desktop environment with a 24-inch monitor.

Figure 2. Background image used in both groups, ©Kee Song Yeoh [11].

1. Day 1 (in lab). In session one, participants were evenly assigned to one of the two groups. They were shown a demo video, then practiced creating and confirming a graphical password on a different background image. Next, they created and confirmed their password for the duration of the study on the background image shown in Figure 2. The user was then distracted for 10-15 minutes with a background questionnaire. At the end of the session, they were asked to login. 35 participants completed this session.
2. Day 2 (online). Session two was held approximately one day (24-48 hours) after session one. This timing was chosen to model user's self-reported frequency of logging on to email accounts (avg. 0.9 times/day[7]). Participants remotely logged in to our online system. 34/35 participants completed this session.
3. Day 8 (in lab). Session three was arranged seven days after session one. This timing was chosen to model user's self-reported frequency of logging on to financial accounts (avg. 1.3 times/week [7]). Participants returned to the lab, logged in, and completed a feedback questionnaire. 34/35 participants completed this session.

Participants. Thirty-five participants were recruited from the UOIT campus. Only 34 completed all sessions: 17 in each group (RTL and LTR), each with 10 males and 7 females. All participants were between the ages of 18 and 30. None were enrolled in a computer/IT security program and only one reported using a graphical password before.

Limitations. Our participants are university students and may have better spatial memory than average, which could positively influence our usability results. As participant's data was collected individually in a lab setting, we only had 34 participants; with a larger population we might be able to observe further patterns. However, the purpose of this study was to observe whether the presentation effect had an impact on the distribution of user choice, which we found was statistically significant even with this small sample size. Our study does not include a control group without a presentation effect, thus our usability comparisons to PassPoints are informal. Note that we do not perform a multiple-comparison correction on our results.

RESULTS

We report on how the image presentations used influenced user's graphical password selections, user perceptions of their selection strategies, and usability. Data is reported from the 34 participants who completed the study.

Effect on Password Selections

We highlight that users only began creating their graphical passwords after the image was fully revealed, thus any effect demonstrated is not due to users aiming to choose a password faster. We analyze the effect of *drawing the curtain left-to-right (LTR)* and *right-to-left (RTL)* on users' graphical password selections. Recall that a graphical password, for both LTR and RTL groups, is a sequence of 5 (x, y) click-points.

Of special interest to us is the question of whether the two experimental groups exhibit the same distribution over the i^{th} click points. As our study has tested drawing the curtain in two horizontal directions, we are interested to see the effect on the distribution of click-points over the x axis (i.e., along the image width). We let $x_{ij}^{(l)}$ and $x_{ij}^{(r)}$ denote the x coordinate of the i^{th} click point, associated with subject j in LTR and RTL experimental groups, respectively. We formulate five null hypotheses in the form of

H_0^i*: the two samples* $\left(x_{i1}^{(l)}, \cdots, x_{in}^{(l)}\right)$ *and* $\left(x_{i1}^{(r)}, \cdots, x_{in}^{(r)}\right)$ *come from the same distribution,*

where H_0^i refers to the distribution of the x coordinates of the i^{th} click-points for our two experimental groups, $i \in \{1, \cdots, 5\}$, and $n = 17$ in our study.

We ran the *two-tailed Mann-Whitney U* test for each of these five null hypotheses. We found that the test rejects H_0^1 with $p = 0.019$ (U score=76), implying that the distribution of the first click-point's x coordinates are statistically different between the two groups. The effect size is $|r| = 0.405$, which is medium-large by Cohen's convention. The test fails to reject H_0^i for $i \geq 2$, suggesting that the 2^{nd}, 3^{rd}, 4^{th}, and 5^{th} click-point distributions are not statistically different. Note the p-value above does not include a multiple-test correction (e.g., Bonferroni, which would more conservatively suggest that $p = 0.091$). Finally, we visualize these first click-points in Figure 3. In the RTL group, 14/17 chose their points in the 5 rightmost columns of the image, and in the LTR group, 13/17 chose their points in the 5 leftmost columns of the image. Interestingly, the remaining 3 and 4 in each group chose their first click-point in the last two columns revealed.

User Perception of Password Selections

Although the data analysis in the last section shows that approximately 80% of users chose their first point from the first 5 columns of the image revealed, only 38% (13/34) users agreed or strongly agreed with the statement that their strategy for choosing a graphical password involved the first object that drew their attention. This suggests that although the image presentations influenced their first click-point choices, users may not have been aware of this influence. We surveyed user's self-reported password creation strategies and found that most users 85% (29/34) agree or strongly agree that they used colours, shapes, patterns, and/or letters for selecting their password points. We hypothesize that the remaining points are chosen based on similarity of shapes, colours, or patterns; we leave testing this hypothesis as future work.

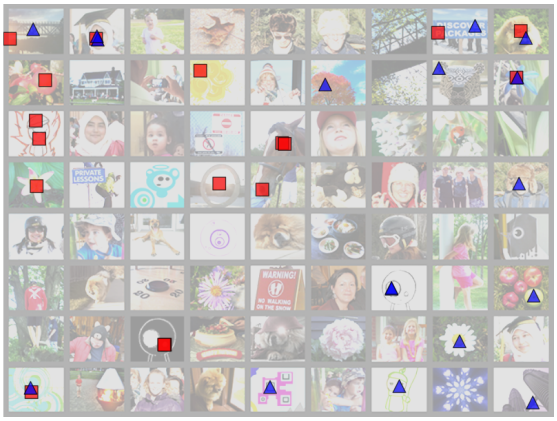

Figure 3. The first click-points for all users, with background image faded to show points more clearly (squares for LTR, triangles for RTL).

Usability

We evaluate the usability of the system in terms of login times, memorability, and user acceptance, finding that the image presentation did not have a negative impact when informally compared to other PassPoints studies [14].

Login Time. The mean login time for sessions 1, 2, and 3 were 23, 25, and 22 seconds respectively. These login times (measured from image display until login success) appear comparable to the mean login time of 24 seconds found in previous PassPoints studies [14]. The mean time to create a graphical password was 75 seconds, which is a bit higher than previous studies on PassPoints that found a mean creation time of 64 seconds [14]. This may be because the creation time recorded includes the time the user is watching the image being revealed, which takes 20 seconds.

Memorability. The memorability of the system was very good; only one password reset occurred. Only 3% (1/34) of users had more than 2 login failures one week after password creation, which is a better result than in previous PassPoints studies [14], where 30% (6/20) had more than 5 login failures.

Acceptability. We asked the participants about their opinion regarding the way the background image was shown. The majority (80%) of participants had no problem with the image presentation. Only 3% did not like it, and 12% indicated that they did not like it at the time but are OK with it now (remaining 5% with no opinion).

DISCUSSION OF SECURITY IMPLICATIONS

Our simple modification to the PassPoints user interface resulted in different distributions of user's first click-points on the same background image. Since different first click-points result in different graphical passwords, we have modified the password distribution for a given background image, simply by presenting it differently to the user upon password creation. The image presentations used in password creation is unknown to an adversary, and provided there are enough presentations possible to be used, it complicates hot-spot analyses that could be used to inform guessing attacks. Password

system designers can make use of our findings by implementing a set of presentation styles to complicate password prediction and consequently increase the system's effective security.

For the purpose of demonstration, the present study only focuses on two opposite image presentations, but one can imagine many different presentations that might produce similar results. If we only consider curtain presentations as in the present study, there are 8 possible when we consider pulling curtains in 2 vertical, 2 horizontal, and 4 diagonal directions. We can also consider *growing style* presentations that start by revealing a small circle in a randomly placed position on the background image, and as the circle grows, it slowly reveals the entire image. Another alternative is a *pop-up style* presentation where the image is decomposed into different chunks and the chunks appear in random order.

The risk of shoulder-surfing a users' presentation style during password creation can be mitigated by using LCD screens with concurrent dual views [8]. Even if an adversary observes or somehow determines a user's presentation style, it may help them predict the first click-points but not the remaining four. Based on our collected data (see Figure 3), about 80% of first click-points can be found in the first-revealed half of the image (vs. the whole image).

Of interest is that the presentation effect seems to influence the first click-point, but apparently not the remaining points. For security, this is likely a good thing; if the remaining points were to have a predictable pattern conditional on the presentation style, then the adversary could easily compile a list of highly probable passwords for each possible presentation style that a target system offers. However, to determine the security that the presentation effect will offer in practice, we need to run larger scale studies, which is future work.

The presentation effect can possibly enhance the security of PassPoints by an order of the number of presentation styles. However, one might also use this technique beyond the first click-point. For example, it could be applied before each possible click-point in PassPoints, or for every image of multi-image graphical passwords (e.g., CCP [3]). The presentation effect may also be useful in other knowledge-based schemes.

CONCLUDING REMARKS AND FUTURE WORK

We have demonstrated that the presentation effect is a simple, unobtrusive, and acceptable way to modify the distribution of user choice in graphical passwords. We found that image presentations significantly modified the distribution of user's first click-points, which adds an unknown element for an adversary attempting to discover the distribution of popular points for a target user's background image. The results of our user study indicate that using the presentation effect from horizontally *drawing the curtain* does not have negative usability consequences. We also found that the system is acceptable to users, which is sensible given that it does not limit allowable click-points on the background image.

The positive findings of our study raise the question of whether the presentation effect might be useful for influencing users to create secure choices in other password schemes. For example, the distribution of text passwords might benefit from presenting a word cloud or a scrabble board containing different concepts immediately before password creation. Future work includes investigation of such presentation effects in text passwords, CCP [3], Background Draw-A-Secret [5], map-based authentication systems [12], video-passwords [13], and text passwords. Investigation of more diverse presentation styles, faster presentations ($<$ 20 sec.), and understanding their security/usability impact is also of interest.

ACKNOWLEDGMENTS

We thank our user study participants. This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

1. Biddle, R., Chiasson, S., and Oorschot, P. C. van. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys 44(4)* (2012).
2. Bulling, A., Alt, F., and Schmidt, A. Increasing the Security of Gaze-based Cued-recall Graphical Passwords Using Saliency Masks. In *CHI* (2012).
3. Chiasson, S., Stobert, E., Forget, A., Biddle, R., and Oorschot, P. C. van. Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism. *IEEE TDSC 9(2)* (2011), 222–235.
4. Dirik, A., Memon, N., and Birget, J.-C. Modeling User Choice in the PassPoints Graphical Password Scheme. In *SOUPS* (2007).
5. Dunphy, P., and Yan, J. Do Background Images Improve Draw-A-Secret Graphical Passwords? In *ACM CCS* (2007).
6. Forget, A., Chiasson, S., and Biddle, R. Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. In *CHI* (2010).
7. Hayashi, E., and Hong, J. A Diary Study of Password Usage in Daily Life. In *CHI* (2011).
8. Kim, S., Cao, X., Zhang, H., and Tan, D. Enabling Concurrent Dual Views on Common LCD Screens. In *CHI* (2012).
9. Oorschot, P. C. van, Salehi-Abari, A., and Thorpe, J. Purely Automated Attacks on Passpoints-Style Graphical Passwords. *IEEE TIFS 5*, 3 (2010), 393–405.
10. Oorschot, P. C. van, and Thorpe, J. Exploiting Predictability in Click-Based Graphical Passwords. *JCS 19*, 4 (2011), 669–702.
11. Song Yeoh, K. (Photograph Courtesy of), 2013.
12. Thorpe, J., MacRae, B., and Salehi-Abari, A. Usability and Security Evaluation of GeoPass: a Geographic Location-Password Scheme. In *SOUPS* (2013).
13. Thorpe, J., Salehi-Abari, A., and Burden, R. Video-passwords: Advertising while authenticating. In *NSPW* (2012).
14. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., and Memon, N. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *Int. J. of Human-Computer Studies 63*, 1-2 (2005), 102–127.