User interface design affects security: Patterns in click-based graphical passwords*

Sonia Chiasson[1,2], Alain Forget[1,2], Robert Biddle[2], P.C. van Oorschot[1]
[1]School of Computer Science & [2]Human Oriented Technology Lab
Carleton University
Ottawa Canada
{chiasson, aforget, paulv}@scs.carleton.ca, robert_biddle@carleton.ca

ABSTRACT
Design of the user interface influences users and may encourage either secure or insecure behaviour. Using data from four different but closely related click-based graphical password studies, we show that user-selected passwords vary considerably in their predictability. Our analysis looks at click-point patterns within passwords and shows that PassPoints passwords follow distinct patterns. Surprisingly, these patterns occur *independently of the background image*. Conversely, CCP and PCCP passwords are nearly indistinguishable from those of a random dataset. These results provide insight on modeling effective password spaces and on how user interface characteristics lead to more (or less) secure user behaviour.

Categories and Subject Descriptors
K.6.5 [**Management of computing and information systems**]: Security and protection: Authentication

General Terms
Security, Human Factors

Keywords
Usable security, Graphical passwords, Authentication

1. INTRODUCTION
Users tend to select predictable passwords and tend to re-use passwords across different accounts. This occurs partially because users are unaware of what makes a secure password and partially as a coping strategy since users must remember an ever-increasing number of passwords. Studies have shown that most user-selected passwords suffer from this problem, including text passwords created with different strategies [9, 14, 18] and various graphical password schemes [6, 8, 19, 21].

A password scheme has both a full theoretical password space and an effective password space. The full theoretical password space includes all possible passwords, while the effective password space includes only the subset of passwords likely chosen by users of the system. Ideally, we want the effective password space to be as close as possible to the full theoretical password space.

To better understand effective password spaces and the characteristics of user interfaces that can influence users towards more secure behaviour, we analyzed datasets collected through user studies of three different variants of click-based graphical passwords and compared them to a random dataset. The random dataset simulates passwords that would occur if all passwords were equally likely and thus used the full theoretical password space. We chose to examine click-based graphical passwords because they allow for clear comparisons of user choice, and can provide a simple platform on which to test novel design ideas. Our goal is not to criticize or advocate for specific click-based password schemes, but to use them as an investigative tool. Our findings can inform the design of other authentication systems, such as applying them to text passwords.

In this paper, we take a closer look at the types of patterns that occur in click-based graphical passwords and show that in some cases, these occur regardless of the background image. Obviously, such patterns in user choice reduce the effective password space. We show that the design of the interface impacts whether users select their click-points in predictable patterns and that the security of passwords can be improved through interface design choices. In fact, we show that for user-selected click-points in Cued Click-Points [4] and Persuasive Cued Click-Points [2], the click-point patterns are nearly indistinguishable from randomly selected click-points with respect to the metrics examined in this paper. We suspect that the differences compared to PassPoints [22, 23] are due to design choices such as providing one-to-one cued recall to aid in memorability and dividing the password selection process into several independent tasks.

From our results, we note that design choices which subtly alter user selection of passwords cannot be made naively because they may weaken security by leading users to employ coping mechanisms, by making it too easy to make insecure choices, or by making the insecure option most logical or most convenient from a user's perspective.

The remainder of the paper is organized as follows. Sec-

*version: March 6, 2008

tions 2 and 3 provide background on user-selected passwords and introduce the click-based graphical passwords systems corresponding to the datasets analyzed in this paper. Our data analysis is described in Section 4. The paper concludes with discussion of how the design of the user interface can impact both usability and security of the password scheme.

2. BACKGROUND

In investigating the security of an authentication system, its usability must also be evaluated since it can significantly impact the real-world security of the system. User interface design decisions may sway user behaviour, often towards less secure behaviour. This may be a direct result of the particular interface, or may compounded by external influences. Often, the easiest way of using a system is also the least secure way, for example, choosing very short, simple text passwords as opposed to longer, more complex sequences of characters.

Users must select and remember passwords to protect an ever-increasing number of accounts. Systems sometimes provide on-screen advice on how to create more secure passwords (e.g., select something memorable that would be difficult for others to guess), give feedback about password choice (e.g., with a password strength meter), or force users create passwords that comply with specific system-defined rules (e.g., the password must include both letters and numbers). Despite these strategies, users often select weak passwords. This occurs partially because users misunderstand the advice or requirements, underestimate the risks, and because limitations of human memory mean that they must employ coping mechanisms in order to reduce the burden of remembering so many passwords. These coping mechanisms may include reusing passwords across several accounts, using predictable alphanumeric combinations, or storing passwords in an easily accessible, insecure location.

Alternatives to text password systems have also been shown to result in predictable passwords. Davis et al.'s PassFaces [6, 15] study revealed that when given the task of selecting a set of facial images for their password, user choices followed obvious patterns (e.g., attractive females of their own race). Draw-A-Secret (DAS) [13] passwords consist of drawing a free-form picture onto a grid. Users of DAS favoured symmetrical sketches in several user studies [8, 19, 21]. A modification named BDAS [8] introduces a background image to a DAS system and early results show that this may lead to less symmetrical passwords; a closer look at patterns remains to be undertaken.

3. CLICK-BASED GRAPHICAL PASSWORDS

PassPoints (PP) [22, 23] is a click-based graphical password system where a password consists of an ordered sequence of 5 click-points on a pixel-based image (Figure 1). To log in, a user must click within some system-defined tolerance region for each click-point. The image acts as a cue to help users remember their password click-points. Earlier studies [3, 22, 23] show that PassPoints is usable both in lab and field settings. However, it has also been shown [3, 7, 11, 20] that some areas of the images were more popular among users, forming hotspots (areas of the image more likely to be selected by users for their click-points). Attackers can determine likely hotspots by gathering sample passwords on an image or through automated image processing techniques, and then use these to build an attack dictionary of likely passwords. Both these methods have had success at cracking some passwords [7, 20]. Furthermore, Golofit [11] manually categorized different areas of three images based on prominent features (e.g., flat, structural, commonplace, block edges) and shows that user-selected click-points cluster within the areas of the images categorized as "commonplace" or "block edge" based on his classification scheme.

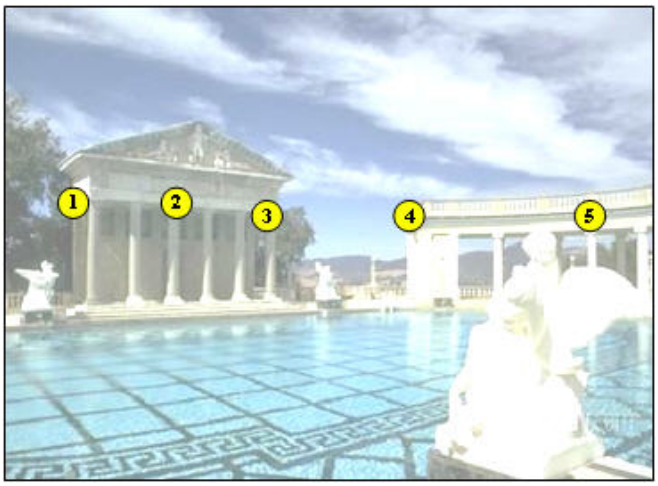

Figure 1: On PassPoints, a password consists of 5 ordered click-points on the image. Background image reprinted from [10].

Since PassPoints showed promise as usable system, we decided to further explore the area.Cued Click-Points (CCP) [4] was developed as an alternative click-based graphical password scheme where users also select 5 click-points, however CCP users select one point per image for 5 images (Figure 2). The interface is similar to PassPoints, displaying only one image at a time. The system determines the next image to display based on the user's current click-point. This modified design has several security and usability implications. It now presents a one-to-one cued recall scenario where each image triggers the user's memory of the one click-point on that image. Secondly, if a user enters an incorrect click-point during login, the next image displayed will also be incorrect. Legitimate users who see an unrecognized image know that they made an error with their previous click-point. Conversely, this implicit feedback is not helpful to an attacker who does not know the expected sequence of images. A lab study [4] showed that hotspots are slightly less likely to occur in CCP than PassPoints, but they do still occur. The advantage is that there are now hundreds/thousands (depending on system configuration) of images that attackers must first acquire and analyze individually as they do not know which images belong to a user password, increasing the amount of work to mount an attack compared to one image for PassPoints.

To address the issue of hotspots, Persuasive Cued Click-Points (PCCP) was proposed [2]. As with CCP, a password consists of 5 click-points, one on each of 5 images. During password creation, most of the image is dimmed except for

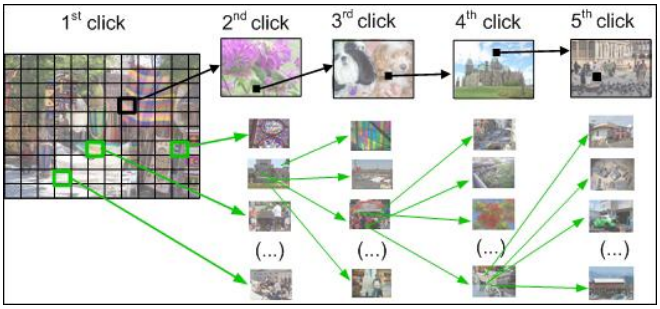

Figure 2: With CCP, users select one click-point per image. The next image displayed is determined by the current click-point.

a small viewport window that is randomly positioned on the image (Figure 3). Users must select a click-point within the viewport. If they are unable or unwilling to select a point in the current viewport, they may press the Shuffle button to randomly reposition the viewport. The viewport guides users to selecting more random passwords that are less likely to include hotspots. A user that is determined to reach a certain click-point may still shuffle until the viewport moves to the specific location, however this is a time-consuming and more tedious process. In effect, PCCP makes selecting a stronger password the "path-of-least-resistance" because choosing from the first offered viewport is quickest and simplest. The system does not rigorously constrain user choice, but makes it more difficult to behave insecurely. The viewport is only applied during password creation; subsequent logins operate the same as CCP.

3.1 Data Collection

In separately reported work, we conducted user studies on each of the click-based graphical passwords discussed above. Lab studies using identical methodology were done for all three systems [2, 3, 4].

The lab studies focused on a core set of 17 images. CCP and PCCP required a larger pool of images so a set of 330 images was used, which included the 17 from the core set. We also manipulated the selection algorithm so that users saw all 17 core images.[1] To be consistent with the original PassPoints user studies [22, 23], the images were of size 451x331 pixels and the tolerance region around click-points was 19x19 pixels.

Users came to the lab for individual 1-hour sessions during which they completed as many trials as time permitted. A trial involved creating, confirming, and logging on with a new password; it consisted of the following steps:

1. Create: Users created a password by clicking on 5 click-points. With PassPoints, these click-points were on one image; with CCP and PCCP, users saw a sequence of 5 images.

[1]This weighted image selection algorithm was not in place for the first few CCP participants. The system displayed random images and users may not have seen all 17 core images. This was modified for later participants of CCP and was in place for all of PCCP participants.

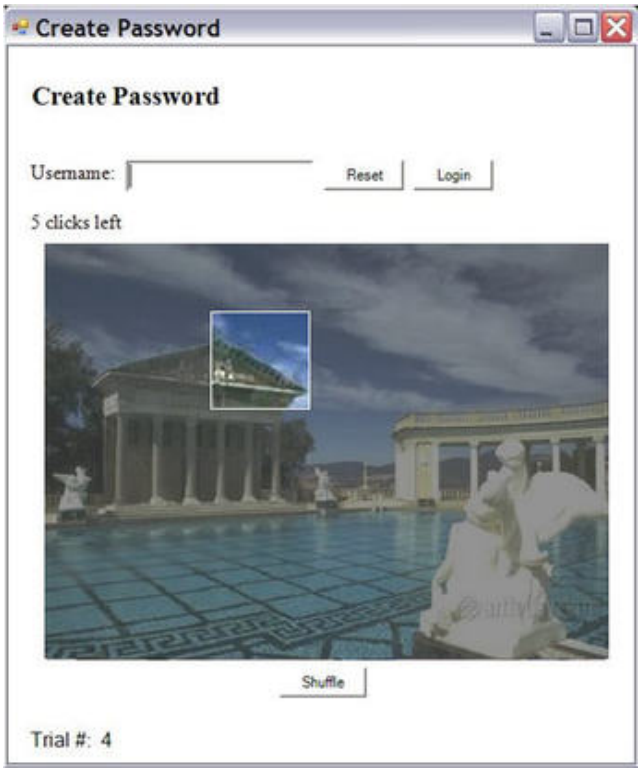

Figure 3: The PCCP password creation interface. Users must select a click-point from the randomly-positioned highlighted viewport or press the Shuffle button to randomly reposition the viewport.

2. Confirm: Users confirmed their password by re-entering their 5 click-points. If they made a mistake, they could re-try as many times as they wished, they could reset their password (returning to step 1), or they could skip this trial.

3. Questionnaire: Users answered two questions pertaining to their newly created password, giving their opinion of how easy this password would be to remember in a week and how easy it was to create the password.

4. Distraction task: To simulate the passage of time and to clear working memory, users spent at least thirty seconds completing an MRT puzzle [16].

5. Login: Users re-entered their password. They could retry if they made mistakes, they could reset their password (return to step 1), or skip the trial if they were unable to remember their password.

Table 1 shows the number of participants, passwords, and individual click-points collected. More points per image were collected for PassPoints since each user password gave 5 click-points on an image whereas for CCP and PCCP, there was only one click-point per image.

For PassPoints, we also previously conducted a field study [3] where 191 participants used a web-based PassPoints system for accessing their class notes for 7-9 weeks. Two images,

Table 1: Number of participants, click-points, and passwords for each lab study and the random dataset. Note that only passwords where users were successfully able to confirm and login are used in our analysis and included in this table.

Study	Number of participants	Total number of click-points	Total number of passwords
PassPoints (PP)	43	2800	560
CCP	57	2520	504
PCCP	39	1500	300
Random dataset	–	5000	1000

Pool and Cars (Figures 12 and 13), were selected from the core set for use in the field study because they had performed well during lab testing. We collected 116 passwords (580 click-points) on the Pool image and 109 passwords (545 click-points) on the Cars image.

We generated a random dataset to act as a control. This random dataset approximates passwords taken from the full theoretical password space, where all passwords are equally probable. It was generated using R's [12] random number generator function for uniform distributions (*runif()*). The dataset contains 1000 random passwords. Each password consists of 5 pairs of (x,y) coordinates, corresponding to 5 click-points.

In the present paper, we are using these datasets to explore a new question: *how does user interface design affect security in these similar graphical password schemes, and what patterns of user choice emerge as a result of the different interfaces?*

4. ANALYSIS OF USER CHOICE

Any patterns in user choice reduce the effective password space and are advantageous to attackers who can use this knowledge to modify their attack strategy and increase the likelihood of success. Previous studies [2, 7, 11, 20] show that when attackers know the images used to create passwords, they can determine likely hotspots and use this information to successfully attack PassPoints and CCP passwords. In the following sections we show that, surprisingly, patterns emerge even without knowing the images. We look at several different password characteristics to see which ones reveal patterns that could help attackers fine tune their attack strategy.

We focus mainly on data from the lab studies because the methodologies are the same and the studies cover a wide range of images, eliminating the risk of getting results that are an artifact of a particular image. In the following analysis, data from the three lab studies (PassPoints, CCP, and PCCP) are examined and compared against the randomly-generated dataset. The number of passwords and individual click-points for each dataset is available in Table 1. Unless otherwise indicated, all analyses of PassPoints refers to the dataset from the lab study (not the field study also mentioned in Section 3.1).

4.1 Click-point distribution

Independent of the background image, are click-points distributed in some recognizable manner? We found that when selecting 5 click-points on a single image (as in PassPoints), users tend to select their first point towards the top-left of the image and progressively move towards the bottom left with each subsequent click-point. This was not the case when users only selected one click-point per image (as per CCP and PCCP).

Figure 4 shows the distribution of click-points along the x-axis of the image.[2] The origin (0,0) is at the bottom-left of the image. With PassPoints, there is a clear progression from the left side of the image for the first click-point towards the right for fifth click-point. The same occurs for the y-axis, as demonstrated in Figure 5; PassPoints click-points progress from the top of the image towards the bottom. Note that our participants were biased towards Western culture; we suspect that a tendency towards right-to-left or other distributions may be evident in other cultures. With CCP, PCCP, and the random dataset, the click-points are quite evenly distributed along both the x- and y-axes, regardless of the click-point number, as also illustrated on Figures 4 and 5.

Regression analysis shows that for PassPoints, there exists a strong relationship between the click-point number and its position on the x- and y-axes.[3] For the x-axis, $F(1,2798)=483.9$ and $p<.0001$, and $F(1,2798)=118.9$ and $p<.0001$ for the y-axis. No such relationship exists for CCP, PCCP, or the random datasets.

With PassPoints, it is possible to determine which areas of the image are more likely to contain click-points based entirely on the click-point number, without knowledge of the image used. For example, looking at Figure 4 we see that 75% of the first click-points fall within the first 200 pixels (out of 451 pixels) on the x-axis. Contrarily, CCP and PCCP are indistinguishable from the random dataset; click-point number is not a predictor of click-point location.

4.2 Segment lengths

[2]Notched box-and-whisker graphs can be interpreted as follows. The thick line in the narrowest part of the box represents the median. The box represents the center quartiles (25th to 75th percentile). The dashed lines (whiskers) represent the lowest and uppermost quartiles respectively. The notches surrounding the median represent the confidence intervals. If the notches of two boxes do not overlap, then they are significantly different from each other at $p<0.5$.

[3]For these and subsequent tests of statistical significance used in this paper, $p < .05$ signifies that the relationship did not occur as a result of chance with at least 95% probability.

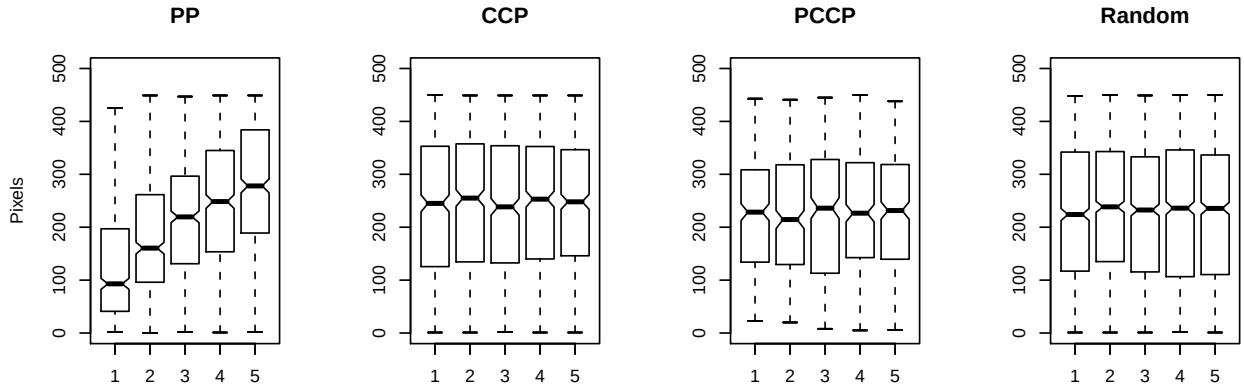

Figure 4: The distribution of click-points along the x-axis of the image, grouped and ordered by click-point number. The image dimensions were 451x331, therefore 451 is the maximum possible x-coordinate.

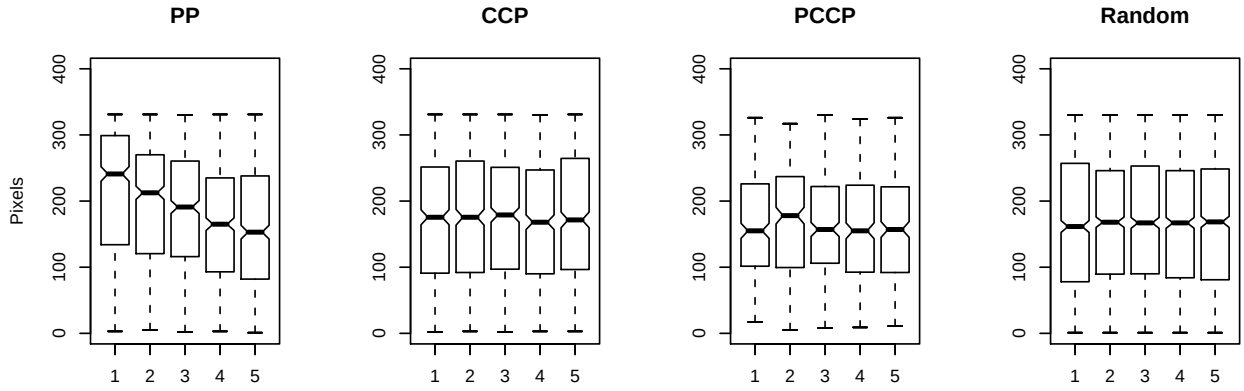

Figure 5: The distribution of click-points along the y-axis of the image, grouped and ordered by click-point number. The image dimensions were 451x331, therefore 331 is the maximum possible y-coordinate.

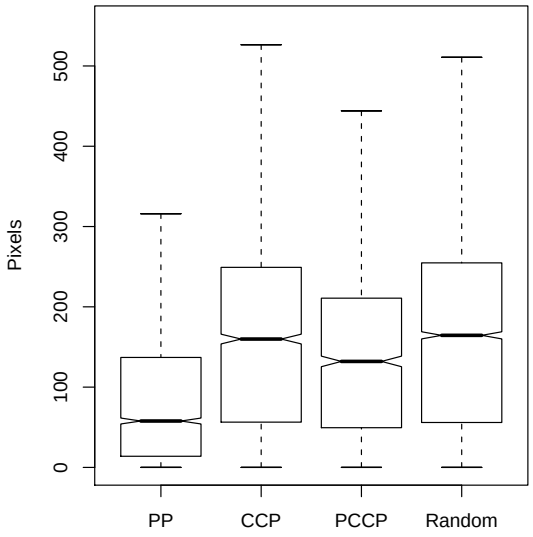

Figure 6: The distance in pixels between two adjacent click-points in a password (segment length).

We next looked at the length of the segments formed between two adjacent click-points. If attackers can predict the likely distance between click-points, they could prioritize guesses containing click-points that are approximately that distance apart.

Figure 6 illustrates the distance in pixels between adjacent click-points in each dataset. For example, in PassPoints, the median segment length is 58 pixels while the median for CCP is 160 pixels. Adjacent click-points in PassPoints are more closely positioned, with very few individual segments spanning the entire image. This distribution is statistically different from the random dataset ($t(4778)= 35.08$, $p<.0001$)). An attacker may be able to use this information to predict higher probability click-point combinations, again even without knowledge of the specific image.

On the other hand, CCP segment lengths are more evenly distributed and are indistinguishable from those of the random dataset. The PCCP dataset appears distinct from the random dataset for segment lengths ($t(2238)=11.48$, $p<.0001$). Figure 6 confirms that PCCP segments are shorter than those of the random set. We were surprised by this result and will be investigating whether it may have occurred as a side-effect of the viewport positioning algorithm.

We also examined whether the segment number had any effect on segment length. Segment lengths appear consistent regardless of their position within the password (Figure 7). T-tests confirmed that there were no statistically significant relationships between segment number and segment length for any of the datasets.

4.3 Angles and slopes

Users of PassPoints tend to create a straight line with their click-points, as evidenced in Figure 8.[4] The PassPoints diagram shows that the most common angles formed between two line segments are near 0 degrees, indicating that the users often selected click-points in a straight line, heading in the same direction. In comparison, CCP, PCCP, and the random dataset favour large angles resulting from back and forth motion between click-points.

The distribution of segment slopes relative to the x-axis in PassPoints (Figure 9) shows that users strongly favour horizontal lines (0 degree slopes), followed by vertical segments in the downward direction (270 degree slopes). The slopes for the CCP and PCCP datasets are quite evenly distributed, which matches the slopes from the random dataset. In fact, the three are statistically indistinguishable from each other ($F(2, 7213)=.067$, $p=.936$), while PassPoints is distinct ($F(3, 9452)=19.17$, $p<.0001$).

We further investigated whether angle number or slope number had any effect on the angle or slope respectively. We found no evidence of such interaction. In other words, the likelihood of finding a given angle (or slope) was not impacted by its ordinal position within the password.

4.4 Shapes

We further looked at shapes formed by all 5 click-points and the line segments between adjacent points. Our classification scheme identified 5 different categories of patterns, as detailed in Table 2 and Figure 10. For example, click-points may form a W pattern. A password was classified into this category if the line segments formed this particular pattern, regardless of orientation; a sideways W was still considered a W, as illustrated in Figure 10.

Once again, we found that the PassPoints dataset was easily distinguishable from the random dataset ($\chi^2(5,1560)=266$, $p<.0001$). PassPoints includes simpler shapes, with far more passwords forming lines and V-shape patterns. Figure 11 reveals how PassPoints is distinguishable from CCP, PCCP, and the random dataset. The CCP and PCCP patterns are indistinguishable from random ($\chi^2(10,1804)=13.1$, $p=.220$).

4.5 Our PassPoints field study (PPField)

The PassPoints field study [3], as previously mentioned, offers an opportunity to look at "real-world" passwords used over an extended period of time. It provides evidence of the types of passwords that one may expect to see if such a system was deployed. However since only two images were used, the patterns may be a direct result of the Pool (Figure 12) and Cars (Figure 13) images. We present the patterns found, but caution that further work is required to determine whether these occur across different images as well.

Figure 14 reveals that in the PassPoints field study, the click-point number has an effect on the x-coordinates of the click-points but not on the y-coordinates. The lack of in-

[4]Figures 8, 9, and 17 use rose diagrams to summarize angle data. These can be interpreted as circular frequency distribution diagrams.

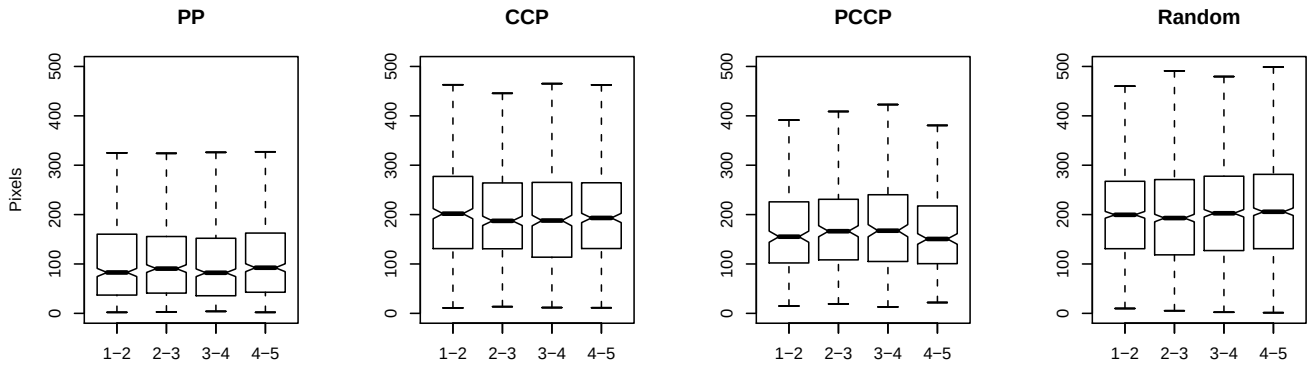

Figure 7: Segment lengths grouped by segment number.

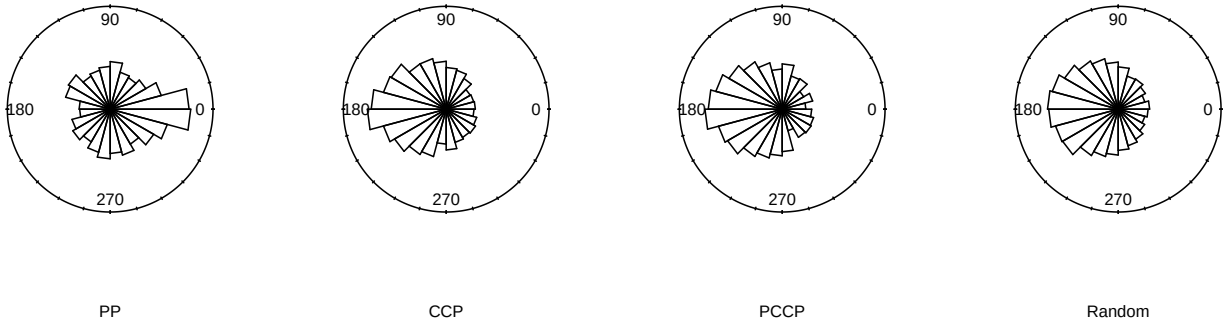

Figure 8: Normalized frequency distribution of the angle (in degrees) formed between two adjacent line segments. These line segments are formed by joining two consecutive click-points in a password.

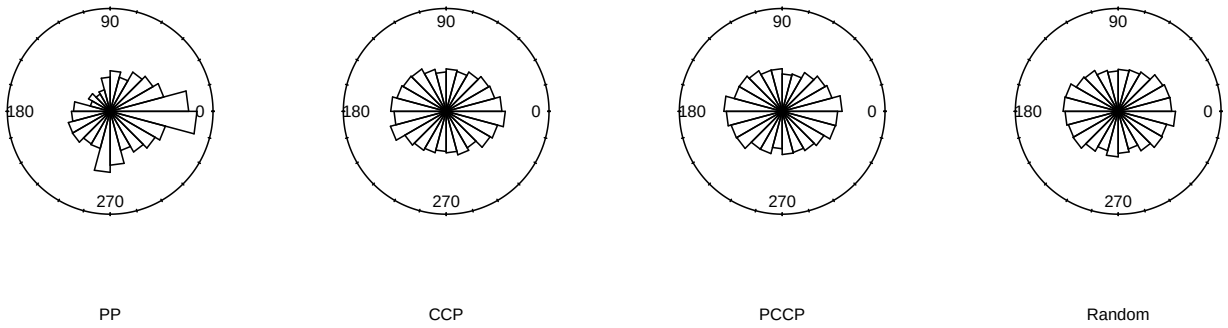

Figure 9: Normalized frequency distribution of the angle (in degrees) of the slope of each line segment, relative to the x-axis. Line segments are formed by joining two consecutive click-points in a password.

Table 2: Shape classification scheme

Shape	Description
Line	The sum of the absolute values for all 3 angles is less than 15 degrees.
W	Angle 1 and angle 3 have the same sign (turn in the same direction) and angle 2 has the opposite sign.
Z	Two of the angles have opposite signs (turn in opposite directions) and the third angle is less than 15 degrees (forms a straight line).
V	Two of the angles are less than 15 degrees and the third angle is greater than 15 degrees.
C	All 3 angles have the same sign (turn in the same direction) and the sum of the absolute values for all 3 angles is greater than 180.
Other	Anything that does not fall into another pattern category, "no pattern".

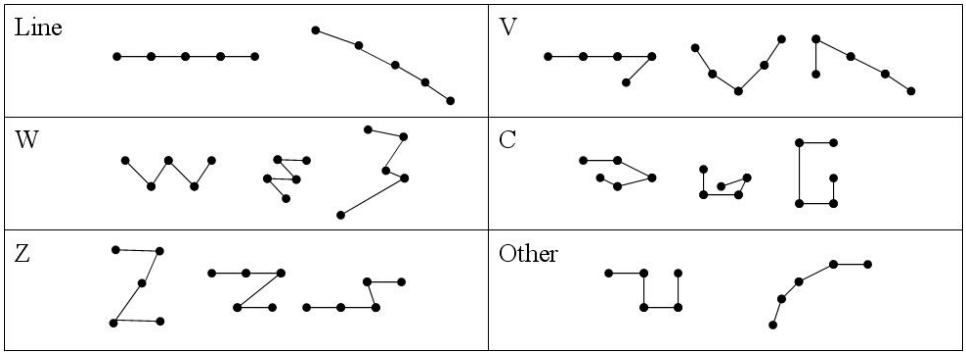

Figure 10: Examples of the click-point patterns for each category.

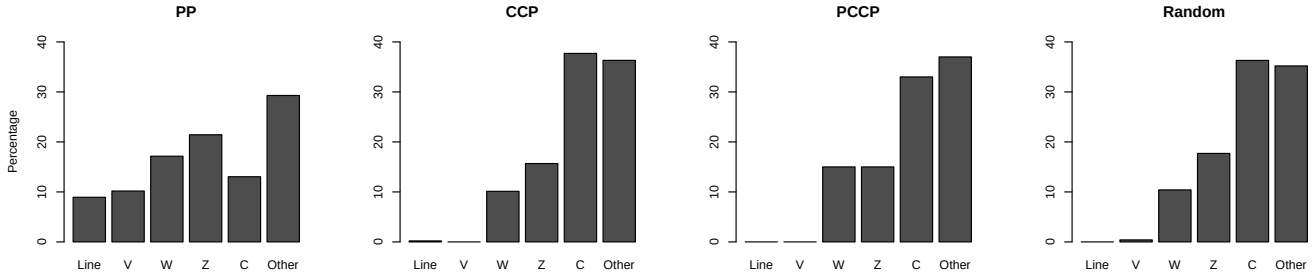

Figure 11: Percentage of passwords that fall into each shape category

Figure 12: The Pool image [17] used in the PassPoints field study.

Figure 13: The Cars image [1] used in the PassPoints field study.

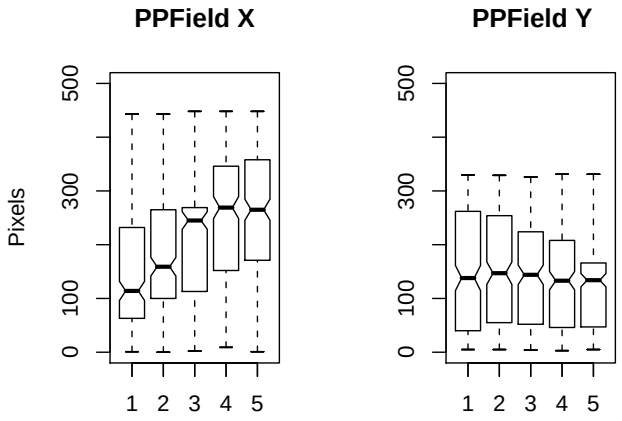

Figure 14: The distribution of click-points for the PassPoints field study along the x- and y-axes of the image, grouped and ordered by click-point number. The image dimensions were 451x331, therefore 451 is the maximum possible x-value and 331 is the maximum y-value.

teraction for the y-axis is likely a result of the Cars image since users frequently selected their click-points in a horizontal line across a row of cars. This is further supported by Figure 15 which shows that 24% of passwords followed a straight line. A further 17% had only one bend, forming a V-shape. Figure 17 also shows users' preference for straight lines since the most popular angles and slopes are very near 0 degrees. The slopes diagram further highlights that users preferred horizontal or vertical directions, with peaks near 0, 90, 180, and 270 degrees.

The median segment length for the PassPoints field study matches the median for the PassPoints lab study (Figure 16). This shows that even in the field study, users still tended to select adjacent click-points in close proximity to each other.

The PassPoints field data certainly exhibits click-point patterns; although some of these are likely side-effects of the Pool and Cars images. However, we suspect that they may also be partially attributed to users trying to select more memorable and simple passwords since they had to remember passwords over a longer period of time and because they had to actually use their passwords on a regular basis to access their class notes. This serves as further cautionary evidence that user behaviour tends towards the easiest path when using these systems in a practical setting.

5. DISCUSSION AND CONCLUSION

Previous studies [3, 7, 11, 20] have shown that hotspots occurred in PassPoints and provide mild evidence of click-point patterns. Our present analysis provides considerably more evidence of click-point patterns. Our analysis revealed that click-point coordinates, segment lengths, angles between segments, segment slopes, and shapes formed by click-points can all be used to identify patterns in user passwords when

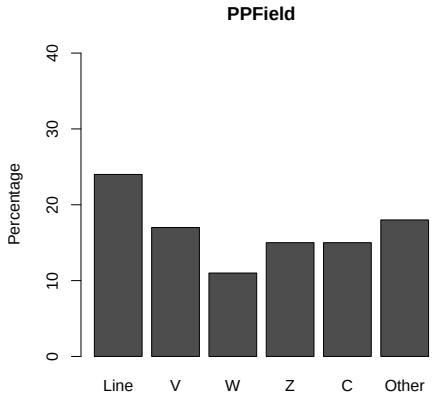

Figure 15: Percentage of passwords that fall into each shape category.

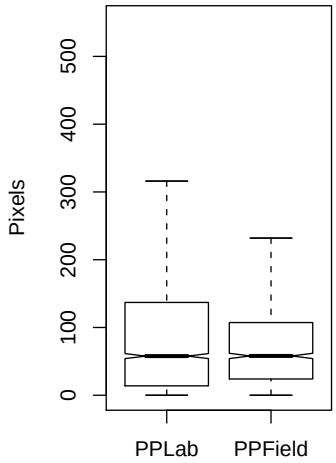

Figure 16: Comparison of the line segment lengths for the PassPoints lab (PPLab) and PassPoints field (PPField) studies. Line segments are formed by joining two consecutive click-points in a password.

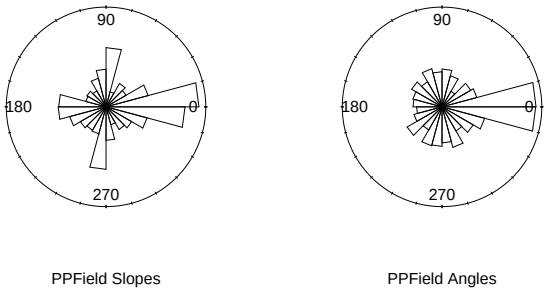

Figure 17: Normalized frequency distributions of angles between segments and segment slopes for the PassPoints field study.

all click-points are on a single image. Interestingly, these same patterns were not apparent when click-points within a password were based on separate images. For example, users of PassPoints prefer straight lines, with click-points that are roughly evenly spaced across the image, starting from left to right, and either completely horizontal or sloping from top to bottom. These patterns were apparent independent of the specific image used. Conversely, CCP and PCCP do not display these same patterns and are very similar to the randomly generated dataset based on the pattern characteristics analysed in this paper.

In click-based graphical passwords, hotspot information may be combined with knowledge of common click-point patterns. We expect that knowledge of likely patterns could be effectively used to prioritize a dictionary of hotspots or even to make educated guesses without knowledge of the particular image.

All three schemes (PassPoints, CCP, and PCCP) are based on the same fundamental idea that a password consists of 5 ordered click-points while the image (or images) acts as a cue to remember the click-points. Nonetheless, our results indicate important differences in usage which lead to differences in security.

With PassPoints, users receive one image as a cue and must recall 5 click-points. This may be a more challenging cognitive task and users resort to click-point patterns in effort to cope. Alternatively, asking users to select 5 click-points on one image may simply afford the creation of patterns because it is the easiest or most logical strategy. If this is the case, the mere fact that a password consists of 5 clicks on one image leads to insecure behaviour and design choices such as "what type of images" become less significant, since the system is inherently less secure.

With CCP and PCCP, each image provides a cue for the corresponding click-point. The one-to-one relationship may be easier for users to remember, therefore reducing the tendency towards selecting an overall geometric pattern formed by the click-points. Also, as each image appears on the screen, it forces users to refocus and take in the new stim-

ulus which may interrupt the thought process for forming a pattern. PCCP further tries to persuade users to select more random points through the viewport, making it much less convenient to select hotspots. Consequently, the easiest path is most secure.

Overall, we note that the implications of design choices need to be carefully considered when making security-related modifications to a graphical password design or user interface. For example, adding a sixth click-point to PassPoints will provide less of a security improvement than adding a click-point to PCCP. With PassPoints, our results suggest that an extra click-point is likely to extend an existing click-point pattern, whereas in PCCP the extra click-point would add considerably more randomness to the password.

User choice is heavily influenced by design of the system. Previous work focused on how the choice of image led to the formation of hotspots, but images appear to play a further role as well. We show that relatively minor changes in how images are used for cueing and feedback can lead to a significant reduction in the occurrence of patterns. In the case of click-based graphical passwords, it appears that having multiple images within a password is a main factor in reducing patterns in user-selected passwords. We are currently investigating what parallels exist with text-passwords and hope that the insight gained from graphical passwords can be applied to other types of passwords or usable security systems in general.

6. REFERENCES

[1] Britton, Ian. http://freefoto.com Last accessed Feb. 2007.

[2] Chiasson, S., A. Forget, R. Biddle, P.C. van Oorschot. Influencing Users Towards Better Passwords: Persuasive Cued Click-Points. HCI 2008. British Computer Society. September 2008.

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

[4] Chiasson, S., P.C. van Oorschot, R. Biddle. Graphical Password Authentication Using Cued Click Points. ESORICS 2007, LNCS 4734, pp.359-374, 2007.

[5] Cranor, L.F., S. Garfinkel. *Security and Usability.* O'Reilly Media, 2005.

[6] Davis, D., F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. 13th USENIX Security Symposium, 2004.

[7] Dirik, A.E., N. Menon, and J.C Birget. Modeling user choice in the PassPoints graphical password scheme. ACM SOUPS, 2007.

[8] Dunphy, P., Yan, J. Do Background Images Improve "Draw a Secret" Graphical Passwords? ACM CCS'07, 2007.

[9] Florencio, D. and Herley, C. A Large-Scale Study of Web Password Habits. ACM WWW 2007, 657-666, 2007.

[10] FreeImages.com. http://www.freeimages.com Last accessed: February 2008.

[11] Golofit, K. Click Passwords Under Investigation. ESORICS 2007, LNCS 4734, 343-358, 2007.

[12] Ihaka, R., Gentleman, R. R: A Language for Data Analysis and Graphics. *Journal of Computational and Graphical Statistics*, 5(3), 299-314, 1996.

[13] Jermyn, I., A. Mayer, F. Monrose, M.K. Reiter, and A.D. Rubin. The Design and Analysis of Graphical Passwords. 8th USENIX Security Symposium, 1999.

[14] Kuo, C., Romanosky, S., and Cranor, L.F. Human. Selection of Mnemonic Phrase-based Passwords. ACM SOUPS, 2006.

[15] Passfaces. http://www.realuser.com Last accessed: December 1, 2006.

[16] Peters, M. Revised Vandenberg & Kuse Mental Rotations Tests: forms MRT-A to MRT-D. Technical Report, Department of Psychology, University of Guelph, 1995.

[17] PD Photo. http://pdphoto.org/ Last accessed August 2007.

[18] St. Clair, L., Johansen, L., Enck, W., Pirretti, M., Traynor, P., McDaniel, P., and Jaeger, T. Password Exhaustion: Predicting the End of Password Usefulness. ICISS 2006, Springer-Verlag, 37-55, 2006.

[19] Tao, H. Pass-Go, a New Graphical Password Scheme. M.S. thesis, School of Information Technology and Engineering, University of Ottawa, Canada, 2006.

[20] Thorpe, J. and P.C. van Oorschot. Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. 16th USENIX Security Symposium, 2007.

[21] van Oorschot, P.C., Thorpe, J. On Predictive Models and User-Drawn Graphical Passwords. ACM TISSEC, 10(4), Article 17, 1-33, Nov. 2007/Jan. 2008.

[22] Wiedenbeck, S., J.C. Birget, A. Brodskiy, and N. Memon. Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice. ACM SOUPS, 2005.

[23] Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies* 63, 102-127, 2005.