User-Choice Patterns in PassTiles Graphical Passwords

Elizabeth Stobert
Department of Psychology
Carleton University
Ottawa, Canada
estobert@connect.carleton.ca

Sonia Chiasson
School of Computer Science
Carleton University
Ottawa, Canada
chiasson@scs.carleton.ca

Robert Biddle
School of Computer Science
Carleton University
Ottawa, Canada
robert_biddle@carleton.ca

ABSTRACT

Graphical passwords are an alternative to text passwords, with advantages to both usability and security. We investigate PassTiles, a research graphical password system, and look specifically at user-chosen PassTiles passwords. We examine whether having a blank background or a background image affects patterns and hot-spots. We found reduced entropy in both conditions due to patterns, which weakens the scheme against guessing attacks, and suggests that different approaches to memorability might be more appropriate.

1. BACKGROUND

Graphical passwords are a form of knowledge-based authentication that use images instead of text. They leverage the *pictorial superiority effect* [5], or the human ability to better remember images than text. A comprehensive summary of graphical passwords is available elsewhere [1].

Password security is often measured by the *theoretical password space*, or the total number of passwords that can be created with a given system configuration. The theoretical password space estimates the difficulty of mounting a brute-force attack. The *effective password space* represents the set of passwords likely to be chosen by users. These are considerably more difficult to estimate, since user choice is based on personal preference. However, users often choose passwords with easily identifiable patterns, reducing the effective password space. While larger password spaces are generally more secure, Florencio and Herley [4] suggest that a space of 2^{20} is sufficient for most websites.

The threat exacerbated by patterns in user-chosen passwords is that of a dictionary attack, where an attacker prioritizes password guesses according to more frequently chosen patterns. Studies of graphical passwords have showed that users tend to follow exploitable patterns when selecting passwords. In studies of PassPoints [2], users tended to choose similar click-points to other users, allowing 23% of passwords in the study to be easily guessed. Van Oorschot and Thorpe [6] showed that characteristics such as mirror symmetry in Draw-a-Secret (DAS) passwords significantly reduced the effective password space. Dunphy and Yan [3] introduced a background image to DAS, and found that it increased password complexity and reduced symmetry.

PassTiles is a new graphical password scheme, developed to represent the strengths of existing graphical passwords while serving as a tool for research. In this study, PassTiles presented the user with a 6×8 grid of password "tiles" and the password consisted of 5 of those tiles. To log in, users had to click on the correct tiles (in any order). In this setup, PassTiles has a theoretical password space of 21 bits.

2. USER STUDY

Our study investigated the effect of background images on the predictability of user-chosen PassTiles passwords. We had two study conditions: *image*, with a background image and *blank*, with a blank background. We hypothesized that having a background image would lead to fewer patterns in passwords, and thus, increased security.

Participants created PassTiles passwords for two websites, then used those passwords to log in and complete short tasks on the websites. The study used a within-subjects design, and each participant created two PassTiles passwords: one with a background image and one without. 33 people (22 female) participated in the study and most were undergraduate students. Participants ranged from 18 to 50 years of age. No participants had ever used graphical passwords.

3. PATTERNS

We identified five patterns to analyse PassTiles passwords.

Rectangle: A password contained a rectangle pattern if it contained four tiles aligned in the same rows and columns.

Line: A password contained a line pattern if all password tiles fell in the same row or the same column.

Corner: A password contained a corner pattern if any password tiles fell in the corners of the grid.

Diagonal: A password contained a diagonal pattern if all password tiles fell in the same diagonal line of tiles.

Proximity: A password contained a proximity pattern if all password tiles could be enclosed in a 5×5 grid.

Passwords were visually inspected for the above patterns. Patterns were not mutually exclusive; a password could (and many passwords did) contain more than one pattern. Some passwords did not contain any patterns.

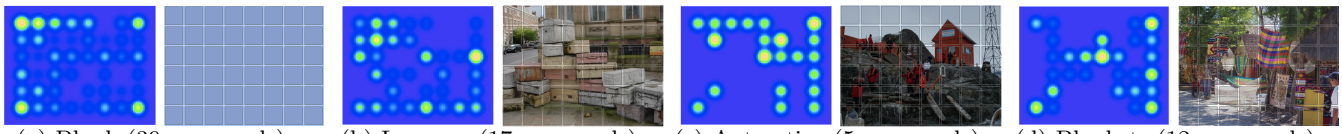
4. RESULTS

Patterns: Table 1 shows the frequency counts for each pattern. Participants could reset forgotten passwords, and these extra passwords were included in the data set, for a total of 73 passwords (34 in *image*, 39 in *blank*). The most common pattern was corners, with 68% of all passwords hav-

ACSAC '11 Orlando, Florida USA

Pattern	Blank	% of Blank (39 pwds)	Image	% of Image (34 pwds)	Total	% of Total (73 pwds)	χ^2	df	p	# of Possible Passwords	Password Space
Rectangle	10	26 %	7	21%	17	23%	0	1	0.99	18,480	2^{14}
Line	10	26 %	10	29%	20	27%	0.016	1	0.90	384	2^{9}
Corner	30	77 %	20	59%	50	68%	0.254	1	0.61	626,296	2^{19}
Diagonal	2	5%	1	3%	3	4%	0.241	1	0.62	38	2^{5}
Proximity	20	51 %	16	47%	36	49%	0.0004	1	0.99	425,040	2^{18}

Table 1: Pattern count data by password type.



(a) Blank (39 passwords) (b) Luggage (17 passwords) (c) Antarctica (5 passwords) (d) Blankets (12 passwords)

Figure 1: Hot-spot graphs for each of the four background images used in the study.

ing at least one corner tile. Diagonal was the least seen pattern and it occurred in only 4% of passwords.

Table 1 shows results of Chi-squared tests to look for differences in pattern frequency between the *image* and *blank* conditions. Contrary to our expectations, no statistically significant differences were seen between *image* and *blank* for any of the five patterns. Twelve passwords had no pattern occurrences, 7 in *image*, and 5 in *blank*, but this difference was not statistically significant ($\chi^2_{(1)} = 0.021, p = 0.882$).

Usability: PassTiles passwords were memorable for users. The median number of password resets was 0, indicating that most users were able to remember the same password without difficulties for the week. PassTiles passwords were also quick for users to create (med = 41 seconds) and login (med = 5 seconds). A t-test showed that the password creation time was significantly longer for *image* than for *blank* ($t_{(63)} = -2.93, p = 0.005$).

Hot-spots: Hot-spots, or particular grid tiles often chosen as part of passwords, can also make passwords more susceptible to attack. Figure 1 displays heatmaps of chosen grid tiles for the four backgrounds used in the study. Paler colours indicate higher popularity. For easier comparison, each heat-map is displayed with its corresponding image.

The heat-map for the blank background (Figure 1(a)) showed that the four corners were popular tile choices, especially the top left corner. Tile choices were skewed toward the top and left sides of the grid (perhaps due to western reading order). Figures 1(b) – 1(d) show the heat-maps for the three image backgrounds. Higher concentration areas in the heatmaps clearly correspond to points of visual interest in the images.

Security Analysis: Based on the data collected in the user study and the pattern analysis from above, we attempted to estimate the effective password space for PassTiles. Thorpe and van Oorschot [6] introduce *weak password spaces*, or subsets of the password space with an increased likelihood of password choices. We speculate that the patterns identified in the previous section are candidate weak password spaces, since they are generable, contain an increased likelihood of passwords, and are small enough to be exhaustively searched. Table 1 shows the total number of possible PassTiles passwords containing each pattern, and the corresponding theoretical password space. Since we did not see any significant differences between the *image* and *blank* conditions, we assume that the effective password space is the same over both study conditions.

5. DISCUSSION AND CONCLUSION

The results of the study showed no evidence of differences between the frequency of patterns in passwords with background images and passwords with blank backgrounds, and pattern frequency was high for both conditions. These patterns correspond to small password spaces which limit the effective password space of the system. We also found hot-spots, located in easily identified grid tiles on the blank background, and corresponding to points of visual interest in the image backgrounds. This showed that users did take the image into account when choosing passwords. However, background images did not discourage users from choosing passwords with patterns.

Given that users do seem to choose their passwords in various patterns, some techniques might help prevent users from picking potentially weak passwords. One way to do this could be to write a password policy that disallowed users from picking passwords with specific patterns, similar to text password policies. This policy might prevent users from picking passwords with more than one corner tile, or from choosing all of their password tiles in the same line.

This study found that user choice promotes memorability of passwords, but if it also reduces security, perhaps we should look at other approaches to memorability.

6. REFERENCES

[1] R. Biddle, S. Chiasson, and P. van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4), in press.

[2] S. Chiasson, R. Biddle, and P. C. van Oorschot. A second look at the usability of click-based graphical passwords. In *SOUPS*. ACM, 2007.

[3] P. Dunphy and J. Yan. Do Background Images Improve "Draw a Secret" Graphical Passwords. In *CCS '07*. ACM, 2007.

[4] D. Florencio and C. Herley. Where Do Security Policies Come From? In *SOUPS*. ACM, 2010.

[5] D. Nelson, V. Reed, and J. Walling. Pictorial superiority effect. *Journal of Experimental Psychology: Human Learning and Memory*, 2(5):523 – 528, 1976.

[6] P. C. van Oorschot and J. Thorpe. On Predictive Models and User-Drawn Graphical Passwords. *ACM Transactions on Information and System Security*, 10(4), 2008.