Analyzing User Choice in Graphical Passwords

Deholo Nali* Julie Thorpe†
deholo@site.uottawa.ca, jthorpe@scs.carleton.ca

May 27, 2004

Abstract

In ubiquitous textual password schemes, users choose passwords that contain predictable characteristics that are roughly equated with what users find easy to recall. This motivates us to examine user choice in graphical passwords to determine whether predictable characteristics exist that may reduce the entropy of the password space. We present an informal user study of the scheme proposed by Jermyn et al. (1999), and the results, both in context of the study's goals and a separate analysis of the results performed at a later date. Our results support that user drawings contain the predictable characteristics relating to symmetry, number of composite strokes, and centering within the grid. Our results also highlight a usability challenge with the DAS scheme.

1 Introduction

Graphical password schemes (e.g. [6, 1, 4]) have been gaining popularity as a plausible alternative to ubiquitous textual password schemes. The appeal of graphical passwords is primarily due to people's remarkable memory for pictures over words [7, 2, 8]. If user's memory capabilities can be effectively utilized in a graphical password scheme, the variety of passwords that people can easily recall (and thus presumably choose) may be improved over that of textual passwords. It is desirable to have a larger variety of passwords chosen by users, as the known threat of a *dictionary attack* is more computationally expensive. A dictionary attack is a brute-force guessing attack where the guesses are drawn from a dictionary composed of "likely" passwords (roughly based on those users easily recall). Such dictionaries are normally ordered from most to least probable. If the probability distribution of the passwords is known to be non-uniform, the entropy of the password scheme is reduced.

One particular graphical password scheme, called "Draw-A-Secret" (DAS) by Jermyn et al. [6] (see §3.1) appears particularly promising given its large total number of possible passwords (the *full password space*). This motivated an informal user study in which users were asked to draw a DAS password on paper in order to determine if there are predictable characteristics in the graphical passwords that people choose. This user study, performed by the first author, aimed to determine if users tend to draw strokes starting or ending at certain points on a grid and what sort of graphical passwords they choose. The study did not find any predictability in the start and end points for DAS password strokes, but found that certain symmetries (e.g. crosses and rectangles), letters, and numbers were common.

An analysis is performed by the second author to determine how often the user study's passwords exhibit reflective symmetry, a small number of composite strokes, or centering within the grid. These characteristics, used in a separate analysis [11], are based on a collection of psychological studies on visual memory and the assumption that users are likely to choose easily remembered passwords. If these characteristics are likely, and describe a small subset of the full DAS password space, the entropy of the DAS password scheme may be reduced. Our analysis aims to determine the frequency of these characteristics in the user study's passwords, and found that: 45% were symmetric ($\frac{2}{3}$ of which were reflective), 80% were composed of 1-3 strokes, and 86% were centered or approximately centered within the grid. We also examined the validity of the passwords according to the DAS scheme, since certain passwords are invalid and rejected if considered

*School of Information Technology and Engineering, University of Ottawa, Canada
†School of Computer Science, Carleton University, Canada

difficult to repeat exactly (as defined in DAS; see §3.1). 29% of passwords drawn in this study were found to be invalid as they followed grid lines or crossed through cell corners. The apparent frequency of invalid DAS passwords indicates a likely usability challenge.

The sequel is organized as follows. §2 discusses related work. §3 provides the relevant background, population, methodology, and results for the user study. §4 analyzes the user study results in terms of some password characteristics. Finally, concluding remarks are made and future work is discussed in §5.

2 Related Work

In the last five years, there have been a few graphical password schemes proposed. One using hash visualization [10] was implemented in a program called Déjà Vu [4], where a user has a portfolio of pictures of cardinality F that they must be able to distinguish within a group of presented pictures of cardinality T. This scheme requires the user to recognize, not recall, the group of pictures that comprise his/her password.

Alternatively, a couple of recall-based schemes have been proposed that require "exact repetition". Exact repetition maps an area to the same encoded point for the purpose of permitting some degree of user input error; it allows for the password to be stored as the output of a one-way function, or used to generate cryptographic keys. Birget et al. [1] propose a scheme that requires a user to click on several points on a background picture. A small amount of error is permitted in the area that they click on using *robust discretization* to allow exact repetition. The DAS scheme [6] uses user-defined drawings as graphical passwords. These drawings are exactly repeatable as defined within the DAS scheme (see §3.1). Given reasonable-length passwords in a 5×5 grid, Jermyn et al. show that the full password space of DAS is larger than that of the full textual password space. This study assumes DAS as the underlying scheme for encoding graphical passwords.

There have been a number of analyses of graphical passwords in terms of their memorability. Davis et al. [3] examine user choice in graphical password schemes. Particular to the DAS scheme, Goldberg et al. [5] showed that people are less likely to recall the order in which they drew a DAS password than the resulting image. Jermyn et al. [6] argue that the DAS scheme has a large memorable password space by modeling user choice. Thorpe et al. [11] propose a memorable class of graphical passwords based on psychological studies on visual memory; an understanding of how their proposed class and related assumptions hold motivates our secondary analysis.

3 User Study Details

The first author conducted a study, detailed in this section, of user-drawn graphical passwords. The graphical passwords under consideration belong to the DAS scheme proposed by Jermyn et al. [6] (see §3.1). The purpose of the study was to determine the following:

- User's understanding of the instructions.
- User's choice of a start and end point.
- User's choice of doodles (DAS graphical passwords).

The study's population, methodology, and results are respectively provided in §3.2, §3.3, and §3.4.

3.1 Review of DAS Scheme

The DAS scheme [6, 9] decouples the position of the input from the temporal order, producing a larger password space than textual password schemes with keyboard input (where the order in which characters are typed predetermines their position).

A DAS password is a simple picture drawn on a $G \times G$ grid. Each grid cell is denoted by two-dimensional coordinates $(x, y) \in [1 \dots G] \times [1 \dots G]$. A completed drawing is encoded as a sequence of coordinate pairs by listing the cells through which the drawing passes, in the order in which it passes through them. Each time the pen is lifted from the grid surface, this "pen-up" event is represented by the distinguished coordinate

pair $(G+1, G+1)$. Two drawings having the same encoding (i.e. crossing the same sequence of grid cells with pen-up events in the same places in the sequence) are considered equivalent. Drawings are divided into equivalence classes in this manner.

DAS disallows passwords considered difficult to repeat exactly (e.g. passwords involving pieces lying close to a grid boundary). The definition of "close to a grid boundary" is unclear [6]; we define it as any part of a stroke that is indiscernible as to which cell it lies within. Any stroke is invalid if it touches an indiscernible part of the grid at any point. We reuse the following terminology.

- The *neighbours* $N_{(x,y)}$ of cell (x, y) are $(x-1, y), (x+1, y), (x, y-1)$ and $(x, y+1)$.
- A *stroke* is a sequence of cells $\{c_i\}$, in which $c_i \in N_{c_{i-1}}$ and which is void of a pen-up.
- A *password* is a sequence of strokes separated by pen-ups.
- The *length of a stroke* is the number of coordinate pairs it contains.
- The *length of a password* is the sum of the lengths of its strokes (excluding pen-ups).

Jermyn et al. [6] recursively compute the (full) password space size, i.e. the number of distinct representations of graphical passwords in the DAS scheme. This gives an upper bound on the memorable password space and thus on the security of the scheme. It is assumed that all passwords of total length greater than some fixed value have probability zero. They compute the full password space size for passwords of total length at most L_{max}. For $L_{max} = 12$ and a 5×5 grid, this is 2^{58}, exceeding the number of textual passwords of 8 characters or less constructed from the printable ASCII codes ($\sum_{i=1}^{8} 95^i < 2^{53}$).

3.2 Population

There were 16 computer science and engineering undergraduate students surveyed, 2 of which were known to have some computer security background. Of the subjects chosen, 10 were men and 6 were women. At least 10 subjects were raised in the Middle east or Asia, with English as a second language; we note that since the instructions were only provided in English, this may have affected the results.

3.3 Methodology

The survey consisted of two sections:

1. The first section included four 6×6 grids, which the subjects were asked to fill using the following instructions:
   a. Please draw four doodles by joining grid cell centers in a specific memorable way.
   b. Locate your start point with a bold dot and your end point with a square dot.
2. The second section included four 6×6 grids, which the subjects were asked to fill using the following instructions:
   a. Please draw a logo by joining grid cell centers.
   b. Logos may include shapes, numbers and letters of various sizes and fonts.

An example was provided for each section on a fifth 6×6 grid; for section 1, the example was at least of length 8 and included an intersection of strokes, whereas for section 2, the example depicted a digit and 5 letters of various sizes and fonts.

Subjects were provided as much time as needed to answer the survey questions and encouraged to ask for clarifications if the instructions were unclear. The purpose of the survey was presented after the subjects had answered both questions.

3.4 Results

The instructions were found to be well understood, except the word "doodle" (possibly due to the fact that English is many of the subject's second language). The location of start and end points for each stroke were found to be scattered rather uniformly across the grid. Finally, the study demonstrated that many subjects drew symmetric shapes (e.g. crosses and rectangles) and many people drew letters and numbers (probably influenced by the instructions).

4 Analysis of Results

For the purpose of testing the theories presented in another analysis [11], the second author performed an analysis of the user study detailed in §3. The results of the user study (see §3) were examined and categorized for the following characteristics: global symmetry (reflective about vertical, horizontal, or diagonal axes, rotational, repetition, or none), number of strokes (1-3, 4-6, or > 6), centering within the grid (centered, approximately centered, or not centered), and for tendencies to try to use invalid DAS passwords (valid DAS password, follows grid lines, and/or crosses through cell corners). This section shows the results for each of these characteristics in tabular form, and discusses them below.

Vertical Reflective	Horizontal Reflective	Diagonal Reflective	Total Reflective	Rotational	Repetitive	Total Symmetric	Total Asymmetric
19%	8%	4%	31%	7%	7%	45%	55%

Table 1: Symmetry (global) for DAS passwords.

1-3 strokes	4-6 strokes	> 6 strokes
80%	10%	10%

Table 2: Number of composite strokes for DAS passwords. Note that when users did not follow the instructions to mark their start and end points, a judgement was made based on visual continuity of lines.

Centered	Approximately Centered	Not Centered
56%	30%	14%

Table 3: Centering of DAS passwords on the grid. If a password is "Approximately Centered", it is centered about a set of cells on either side of the center grid lines.

The results of this analysis support that the proposed class of memorable passwords (and related assumptions) [11] based on cognitive studies reflect a high percentage of user-chosen DAS passwords; approximately 45% of users chose symmetric passwords, $\frac{2}{3}$ of which are mirror symmetric (reflective). Additionally, in terms of the number of strokes chosen, approximately 80% of users chose passwords composed of 1-3 strokes, 10% chose passwords composed of 4-6 strokes, and 10% of users chose 6 or more strokes. Finally, in terms of the user centering the password about the grid, 56% of the passwords were centered, and an additional 30% more were approximately centered (meaning centered about a set of cells adjacent to the center grid lines).

Of particular interest are a few patterns observed outside of the selected categories: when users chose asymmetric passwords, they were most often composed of one or two strokes. Additionally, individual subjects that chose symmetric passwords chose symmetric passwords (of the same type e.g. reflective) for most of their passwords, and those who chose asymmetric passwords tended to choose mostly asymmetric passwords.

Valid	Crosses Grid Corners	Follows Grid Lines
71%	27%	12%

Table 4: Validity of DAS passwords. Note that a password that is invalid could both cross through cell corners and follow grid lines, explaining why the percentages do not add up to 100.

The last category, the validity of the DAS password, is to determine whether subjects would have a difficult time avoiding following the grid lines and crossing through cell corners in their password; this has a direct impact on the perceived usability of the DAS scheme since such passwords are disregarded at present (due to their difficulty to repeat exactly). This part of the analysis shows that 29% of passwords follow the grid lines or cross through a cell corner and would thus be invalid. The most common cause of invalid passwords is crossing through cell corners (27% of the passwords had this property). This result suggests that to enhance usability, future DAS implementations should eliminate such restrictions on user input.

5 Concluding Remarks and Future Work

The user study presented gives us some intuition of user graphical password choice. It supports that users choose graphical passwords with predictable characteristics (particularly those proposed as "memorable" [11]); if this study is indicative of the population, the probability in which some of these characteristics occur would reduce the entropy of the DAS password space. In the future, it would be interesting to perform user studies that test how well users recall their drawings, and how this affects the frequencies of the characteristics we have examined. Finally, this study highlights the need for DAS implementations to solve the problem of exact repeatability for passwords that make use of the grid lines, since almost $\frac{1}{3}$ of users used the grid cell corners and lines (presumably as points of reference). The problem of exact repeatability is addressed for another scheme discussed by Birget et al. [1], a potential solution worth exploring to enhance DAS's usability.

6 Acknowledgements

Both authors acknowledge Canada's National Sciences and Engineering Research Council (NSERC) for funding their Postgraduate Scholarships.

References

[1] J.-C. Birget, D. Hong, and N. Memon. Robust Discretization, With an Application to Graphical Passwords. Cryptology ePrint Archive, Report 2003/168, 2003. `http://eprint.iacr.org/`, site accessed Jan. 12, 2004.

[2] M.W. Calkins. Short Studies in Memory and Association from the Wellesley College Laboratory. *Psychological Review*, 5:451–462, 1898.

[3] D. Davis, F. Monrose, and M.K. Reiter. On User Choice in Graphical Password Schemes. In *13th USENIX Security Symposium (to appear)*, 2004.

[4] R. Dhamija and A. Perrig. Déjà Vu: A User Study Using Images for Authentication. In *9th USENIX Security Symposium*, 2000.

[5] J. Goldberg, J. Hagman, and V. Sazawal. Doodling Our Way to Better Authentication, 2002. CHI '02 extended abstracts on Human Factors in Computer Systems.

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

[7] E. A. Kirkpatrick. An Experimental Study of Memory. *Psychological Review*, 1:602–609, 1894.

[8] S. Madigan and V. Lawrence. Factors Affecting Item Recovery and Hypermnesia in Free Recall. *American Journal of Psychology*, 93:489–504, 1980.

[9] F. Monrose. *Towards Stronger User Authentication*. PhD thesis, NY University, 1999. `http://www.cs.nyu.edu/csweb/Research/Theses/monrose_fabian.pdf`, site accessed January 12, 2004.

[10] A. Perrig and D. Song. Hash Visualization: a New Technique to Improve Real-World Security. In *International Workshop on Cryptographic Techniques and E-Commerce*, pages 131–138, 1999.

[11] J. Thorpe and P.C. van Oorschot. Graphical Dictionaries and the Memorable Space of Graphical Passwords. In *13th USENIX Security Symposium (to appear)*, 2004. Available at: `http://www.scs.carleton.ca/~jthorpe`.