Graphical Passwords & Qualitative Spatial Relations

Di Lin
Computing Science
Newcastle University, UK
(+44) 191 246 4630
di.lin@ncl.ac.uk

Paul Dunphy
Computing Science
Newcastle University, UK
(+44) 191 246 4621
p.m.dunphy@ncl.ac.uk

Patrick Olivier
Computing Science
Newcastle University, UK
(+44) 191 246 4630
p.l.olivier@ncl.ac.uk

Jeff Yan
Computing Science
Newcastle University, UK
(+44) 191 2228010
jeff.yan@ncl.ac.uk

ABSTRACT

A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords. We present a variation of the Draw-a-Secret scheme originally proposed by Jermyn et al [1] that is more resistant to shoulder surfing through the use of a qualitative mapping between user strokes and the password, and the use of dynamic grids to both obfuscate attributes of the user secret and encourage them to use different surface realizations of the secret. The use of qualitative spatial relations relaxes the tight constraints on the reconstruction of a secret; allowing a range of deviations from the original. We describe QDAS (*Qualitative Draw-A-Secret*), an initial implementation of this graphical password scheme, and the results of an empirical study in which we examined the memorability of secrets, and their susceptibility to shoulder-surfing attacks, for both *Draw-A-Secret* and QDAS.

1. INTRODUCTION

The identification of users as the weakest link in security systems is particularly relevant in the context of the textual password scheme. The cognitive demands imposed by good password practices often give rise to users to setting weak passwords, e.g. dictionary words, or the names of family members, which are vulnerable to guessing. Passwords desirable from a security perspective have serious consequences for users who find them difficult to remember.

Graphical password schemes take advantage of the fact that our memory is significantly greater for images than for (syntactically or semantically meaningless) alphanumeric strings. If the components of a graphical scheme are significantly more memorable, it is hoped that more complex and stronger passwords should be more readily deployed by users.

We propose our extension of the *Draw-A-Secret* scheme: *Qualitative Draw-A-Secret (QDAS)* and evaluate an initial implementation with a user-study. Our study considers both memorability and susceptibility to shoulder surfing.

Symposium On Usable Privacy and Security (SOUPS) 2007, July 18-20, 2007, Pittsburgh, PA, USA.

2. QUALITATIVE DRAW-A-SECRET

QDAS extends the ideas pioneered within *Draw-a-Secret* (DAS). Both schemes are based on recall and require the user to create a free-form image on a drawing grid. The QDAS drawing-grid is initially similar to a typical DAS grid however each cell in QDAS is explicitly annotated using an integer index. As for DAS, QDAS assumes stylus-based input and the user must create a sequence of strokes that they feel they can remember. Also different techniques of drawing selection must be developed as the proportions of any meaningful drawing are removed by grid transformations.

The main aims of QDAS are to allow users to set strong secrets that do not impose load on long-term memory, and to be resistant to shoulder surfing. Similar to DAS, there is a one-to-many relationship between an encoding and the corresponding free-form images. QDAS introduces two components that distinguish it from its DAS counterpart: qualitative spatial [2] descriptions of strokes; and the use of dynamic grid transformations.

2.1 Qualitative Description of Strokes

QDAS employs a new way to encode each stroke. The raw encoding consists of its starting cell and the sequence of qualitative direction changes in the stroke relative to the grid. A *direction change* is considered to be when the pen crosses a cell boundary in a direction different to the direction that crossed in the previous cell boundary. For the stroke in figure 1, the encoding starts at 6, followed by “down”, “right”, and “up”. As can be seen, both long and short lines have identical encodings.

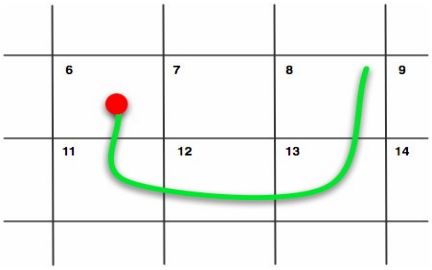


Figure 1. Stroke 6, “down”, “right”, and “up”

Every cell crossing the user makes in DAS is an important contribution to their secret. Authentication relies on the user recreating every cell-crossing in the correct order. QDAS differs as it enables users to deviate from the literal spatial definition of their secret.

2.2 Dynamic Grids

QDAS uses dynamic grid transformations to mask the on-going process of creating a secret, and provide a level of protection

against shoulder-surfing (figure 2). This shoulder-surfing resistance is brought about by the weakness of short-term memory and the hiding of the useful stroke information by the grid transformation. When creating a stroke, the important attributes are the reference number of the starting cell and the sequence of direction changes of the stroke. The longer this information is on-screen, the longer an attacker has to record it in memory.

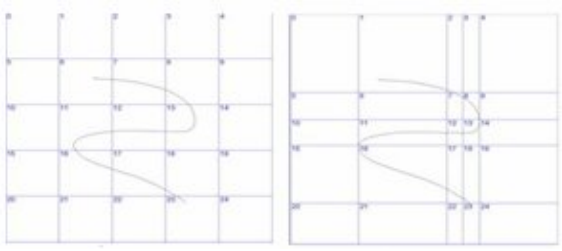
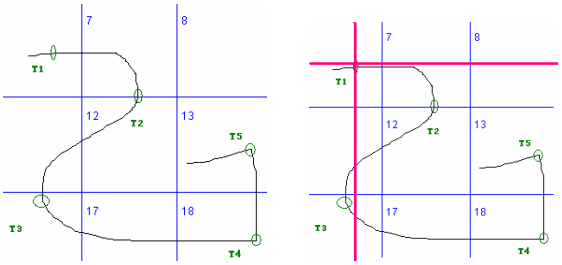


Figure 2: An example of the dynamic grids after a stroke

To transform the grids, first of all we begin by calculating the turning points in the stroke (figure 3a). For the first 4 of these turning points we draw a vertical line where x is equal to the x value of the turn, and draw a horizontal line where y is equal to the corresponding y value of the turning point. In the first instance the result is two perpendicular lines that intersect at the current turning point (figure 3b). For a 5x5 grid doing this with the next 3 points gives us a transformed grid.



a) **b)**

Figure 3: a) The turning points in an example stroke b) the first stage of grid transformation

There may be instances where the transformation process yields cells that would be very small and so make it difficult for users to draw through. To avert this, if a cell is deemed to be too small in height or width, we increase the size until it reaches a pre-defined minimum. Also when a stroke has no turning points, we pick 4 random points from the line, and apply the process from above where cells are too small.

2.3 Password Space

The password space for QDAS can be large. For example, we estimate that 2.8×10^{14} different passwords can be generated with 3 lines drawn on a 4×4 grid. The password space also significantly increases with the size of the grid and the number of strokes.

3. PRELIMINARY USER STUDY

A preliminary study was conducted using 20 computing science students. The experiment aimed to compare three aspects of the DAS and QDAS: usability, ease of shoulder surfing, and password memorability.

Subjects were given instructions and an information sheet describing the task and scheme to which they were assigned. After creating their secret and doing a short distracter task we asked subjects to repeat their password to 'login'. Subjects were allowed 3 attempts in total.

The second component of the study was a *shoulder-surfing* resistance test. For this, two example secrets were pre-designed. Video recordings of moderators drawing QDAS and DAS versions of the same secret were shown to the subjects who were advised that they should act as a shoulder surfer and try to capture enough information about the secret to actually re-create it themselves. Shoulder surfing is a spontaneous phenomenon and thus it is difficult to recreate appropriate conditions. Our limited goal was to provide the conditions in which we could test a subject's ability to remember somebody else's drawing

Finally *memorability* was tested by contacting subjects one week after the experiment. Subjects were asked to recreate their password in their assigned environment.

3.1 RESULTS

The usability element of the study simply examined if a subject was able to understand the scheme, after a few practice runs successfully set a password, and after a brief distraction repeat it. In the DAS condition, 9 subjects were able to do this successfully while one person failed. All QDAS participants were able to set a secret and repeat it successfully.

In the shoulder surfing study none of the participants in the QDAS condition managed to successfully recreate a *stolen* password. In the DAS condition seven of the ten subjects were able to successfully shoulder surf and recreate the password shown to them. Two of the three failures occurred for the random line drawing and the other for the house image.

The memorability test examined which of the subjects could remember their login after a period of one week. The results showed no significant differences between the two schemes however DAS performed marginally better. The DAS scheme yielded 6 correct and 4 incorrect responses, while QDAS yielded 5 correct and 4 incorrect responses (one participant withdrew from the experiment).

4. CONCLUSION & FUTURE WORK

QDAS is proposed as an improvement to the Draw-a-Secret scheme. QDAS uses qualitative spatial relations and dynamic grid transformations to improve potential problems aspects of usability and resistance to shoulder surfing encountered in DAS. In our preliminary empirical study QDAS proved to be more resistant to shoulder surfing than its DAS counterpart.

In future we plan to further analyze QDAS by running more studies, and in particular we hope to accurately simulate the context of shoulder-surfing scenario to improve the ecological validity of our findings.

REFERENCES

[1] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D., 1999. The design and analysis of graphical passwords. In: Proceedings of the Eighth USENIX Security Symposium, pp. 1–14.

[2] Freksa, C. Qualitative Spatial Reasoning. In: D. M. Mark and A.U. Frank (eds.), Cognitive and Linguistic Aspects of Geographic Space, 361-372. Kluwer Academic Publishers, Dordrecht, 19xx