# Can eye gaze reveal graphical passwords?

Daniel LeBlanc[1] Sonia Chiasson[1,2] Alain Forget[1,2] Robert Biddle[1]
[1]Human-Oriented Technology Lab, [2]School of Computer Science
Carleton University, Ottawa, Canada
dblanc@connect.carleton.ca

## 1. INTRODUCTION

Graphical passwords have been proposed as an alternative to text passwords. These new authentication mediums are of much interest to researchers today due to their potential for usability and security. However, we must also consider new threats they may present. We are interested in the effects that visual attention and visual search have on the creation and maintenance of graphical passwords, and whether eye fixations can predict the location of these passwords. If eye fixations are good predictors, then the security of graphical passwords is considerably weakened.

Eye trackers, which detect eye movements on a screen, are becoming readily available. We hypothesize that gaze points gathered from any user could potentially be used to form an attack dictionary to guess other users' graphical passwords. This may be possible because people tend to look at visual scenes in similar patterns. We conducted a lab study examining eye gaze patterns as users selected graphical passwords and then used this gaze data to form an attack dictionary. Surprisingly, we found that eye gaze is not a good predictor of passwords.

## 2. PASSPOINTS

Wiedenbeck et al.'s [8] PassPoints graphical password scheme consists of users selecting 5 individual click-points on a pre-determined image; this set of 5 click-points comprises the password. It is important to note that the 5 click-points need to be remembered and entered in the order in which they were selected. Previous research shows that this type of password scheme is quite usable [1][8]. There are, however, security concerns in dealing with graphical passwords. Hotspots, the clustering of popular click-points across all users of a particular image, are of considerable concern since they may provide valuable information for attacking passwords. Security analysis [3][7] of PassPoints click-points has shown that it is possible to determine hotspots by gathering passwords from a small number of users or through image processing techniques. By using this small sample of click-points based on hotspots, it is then possible to create an attack dictionary used to guess users' passwords.

## 3. VISUAL ATTENTION AND SEARCH

When we look at any given image, we tend to look for things that are interesting to us, which are salient, and that are not too obstructed by distracters. The attentional spotlight and spatial cueing are largely responsible for how we divide our visual attention among a myriad of available stimuli in our immediate environment. We can think of the attentional spotlight as a directional beam of light that reveals, and is limited to, what is within its path [6]. As such, humans can shift their attention from one location to another, but cannot absorb all of the information from both locations at one time. Spatial cueing in the environment allows us to divert our attention from one thing to another by simply suggesting to our visual system where our focus should be. Each targeted visual stimulus is preceded by a visual cue. Examples of such visual cues are: brighter colors against a darker colored background, recognizable patterns and shapes, and spatial location motivating shapes such as arrows pointing to specific things within the visual environment [2].

Visual search is another important part of visual attention. Visual search makes it easier for us to locate things in visual space when we've become familiar with what we are looking at or searching for. Visual search can be characterized in two ways: bottom-up and top-down visual processing. In bottom-up visual processing, or endogenous attention, our attention is drawn by nearby salient objects, such as the flashing lights of an emergency vehicle, or the neon lights of a passing road sign; this process is done automatically and effortlessly. In top-down visual searches, or exogenous attention, our attention is under our control, in that we decide where we want to look, and what we want to look for. In other words, it is said to be goal-driven, where we guide our attention to locate a specific object within the environment. An example of top-down visual processing would be an attempt to locate a green object within a myriad of grey objects in a given visual field [2].

In visual search, quite often both bottom-up and top-down processing are used to some degree to allow for the best visual search possible. Visual processes relate to a particular task and, for example, reading and driving show similar processes across individuals [5]. We suggest that graphical passwords might also show similar patterns.

## 4. STUDY

As visual search and attention are important determinants of where people tend to look in visual scenery, we propose that gaze data may be a good predictor of graphical passwords. Such a correlation would be detrimental to the security of graphical passwords; if attackers are in fact able to predict passwords based solely on gaze data, this may affect the viability of this new password medium.

In our lab study, users created several graphical passwords while a Tobii 1750 eye tracker recorded where they were looking on the screen. Human vision typically involves a series of fixations where the eye rests on a particular target, separated by saccades when the eye moves. The apparatus gathered fixation data from each participant for each trial. In this current analysis, we focus on the fixation data during password creation due to our interest in the gaze patterns of users when they are searching for acceptable click-points for their graphical passwords.

We used identical methodology to previous graphical password studies [1]. We used 8 participants for this study. Each participant created graphical passwords on between 6 and 17 images, as time permitted. Each password comprised of five different points on a given image. Each trial consisted of three phases: creating a graphical password, confirming the same graphical password and,

finally, logging in. Participants were instructed to create graphical passwords that would be safe from anyone guessing their password.

## 5. RESULTS

Our initial analysis consisted of two dictionary attacks on a previously collected dataset from a large field study [1] which used two of the same images as this present study. We focus on one of these images for the current analysis. Figure 1 depicts the click-point hotspots from the earlier field study.

Our first attack dictionary was comprised of hotpots formed by the 40 click-points collected in this study. Our second dictionary included hotspots formed by the gaze fixation data collected from the eye tracker as participants created their passwords; areas where users collectively looked at the most were identified as gaze hotspots. To form the dictionaries, we grouped points by proximity, chose unique representatives from each group, and then sorted them by the size of each group. We used both these dictionaries to attack the 1035 click-points from the field study.

As shown in Figure 2, the click-points dictionary was effective in guessing field study click-points even with only a small sample of passwords (e.g. the top 15 hotspots guessed 26% of click-points). Conversely, the gaze hotspots were much less effective in predicting these same click-points even though there was a large sample of gaze fixations from which to form hotspots (e.g. the 15 most popular fixations guessed 8% of click-points).

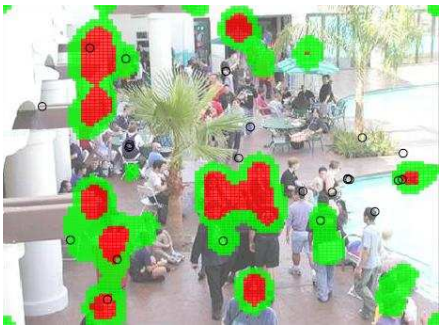

**Figure 1. *Pool* image click-points density map.**

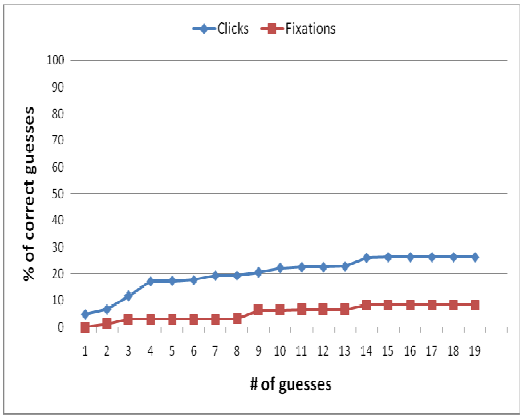


**Figure 2. Effect of dictionary attacks by click-points and by fixations.**

## 6. CONCLUSION

In this brief paper we have reported on a lab study assessing the relationship between click-points and gaze-points in click-based graphical passwords. Our lab study took already-existing data from a previous study and, by creating attack dictionaries in order to attempt to guess users' graphical passwords, we were able to determine that gaze data is not a good predictor of graphical passwords. This could be due to several factors. We believe the most significant factor is that when users search for possible locations on an image to select their click-points, they do not follow the established patterns of visual attention and visual search. This is surprising given that these patterns have an impact on many other search tasks, including driving, reading, and so forth. We plan to undertake further studies to determine the nature of visual patterns relating to graphical passwords.

## 7. REFERENCES


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

[2] Chun, M. M., & Wolfe, J. M. 2000. Visual Attention. Blackwell Handbook of Perception. E.B. Goldstein.

[3] Dirik, A. E., Memon, N., & Birget, J-C. 2007. Modeling user choice in the PassPoints graphical password scheme. ACM SOUPS.

[4] Koike, T. & Saiki, J. 2006. Stochastic saliency-based search model for search asymmetry with uncertain targets. Journal of Neurocomputing, 69, 2112-2126.

[5] Rayner, K. 1995. Eye movements and cognitive processes in reading, visual search, and scene perception. In Findlay, Walker, & Kentridge (eds), Eye Movements Research: Mechanisms, Processes, and Applications, 3-21. New York, Elsevier.

[6] Sperling, G. (1960). The information available in brief visual presentations. Psychological Monographs: General and Applied, 74, 1-29.

[7] Thorpe, J. & van Oorschot, P.C. 2007. Human-seeded attacks and exploiting hot-spots in graphical passwords. USENIX Security Symposium.

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