Input Precision for Gaze-Based Graphical Passwords

Alain Forget
School of Computer Science
Carleton University
Ottawa, Canada
aforget@scs.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

CHI 2010, April 10–15, 2010. Atlanta, Georgia, USA
ACM 978-1-60558-930-5/10/04.

Abstract
Click-based graphical passwords have been proposed as alternatives to text-based passwords, despite being potentially vulnerable to shoulder-surfing, where an attacker can learn passwords by watching or recording users as they log in. Cued Gaze-Points (CGP) is a graphical password system which defends against such attacks by using eye-gaze password input, instead of mouse-clicks. A first user study revealed that CGP's unique use of eye tracking required special techniques to improve gaze precision. In this paper, we present two enhancements that we developed and tested: a nearest-neighbour gaze-point aggregation algorithm and a 1-point calibration before each password entry. We found that these enhancements made a substantial improvement to users' gaze accuracy and system usability.

Keywords
Eye tracking, graphical passwords, usable security

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces – Input devices and strategies
K.6.5 Computing Milieux: Security and Protection – Authentication

General Terms
Experimentation, Human Factors, Security

Introduction

Click-based graphical passwords [2] have recently been explored as a new method of user authentication. Despite having many usability and security advantages, click-based graphical passwords are potentially vulnerable to *shoulder-surfing*, whereby a user is observed logging in by an attacker who subsequently logs in with the observed credentials. *Cued Gaze-Points* (CGP) [9] addresses this vulnerability by using eye-gaze as input instead of the mouse. Since there is no cursor following users' gaze in CGP, it would be difficult for an observer to determine users' passwords. However, without the feedback of a cursor, increased eye-gaze accuracy is essential for CGP.

We initially hypothesised that CGP would be easy to use, but our first study's participants had difficulties entering gaze-based passwords. We found that unintentional eye and body movements led to erroneous gaze-points. In this paper, we present two new enhancements to increase gaze accuracy without compromising the system's usability or security. We implemented these software improvements in a second version of CGP. A second user study revealed that our enhancements effectively helped users more accurately enter gaze-based passwords. These enhancements were integrated into our main CGP system [9].

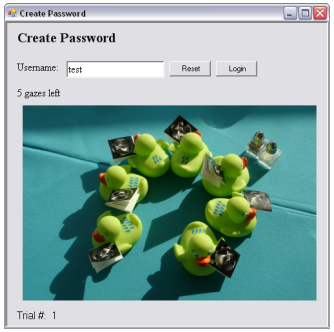

figure 1. Cued Gaze-Points password creation window.

Background

The advantage of graphical passwords over text passwords is the human ability to remember images more easily than text [13]. Biddle et al. [2] provide a recent survey of existing graphical password systems, including several other shoulder-surfing resistant graphical password schemes. These employ techniques such as image shuffling, mental computation, and revealing only a part of a shared secret. We focus on *cued-recall click-based graphical password* schemes where passwords consist of clicks on specific areas of one or more images. These systems offer quick login times and large theoretical password spaces (meaning potentially greater security). *Cued Click-Points* (CCP) [3] is a scheme where users sequentially choose one click-point on each of 5 different images. Each subsequent image is determined by the user's previous click-point location. If a user's login point is within a square *tolerance* region around the corresponding creation point, then the login point is considered correct.

Several recent graphical password proposals use eye-gaze input. Kumar et al. [11] first implemented a gaze-based authentication system, EyePassword, where users gaze at the letters of their password on an on-screen keyboard. De Luca et al. [6, 5] have proposed eye-gesture methods for shoulder-surfing resistant authentication. Dunphy et al. [8] tested gaze control with PassFaces, a recognition-based graphical password system. While these schemes show promise in terms of usability, CGP offers a large set of potential passwords and built-in cues to aid multiple password recall.

Gaze-point selection can use a *gaze-trigger* method, where users gaze at the desired location while pressing a button to explicitly indicate their gaze-point selection. Another method is *gaze-dwell*, where users' gaze dwelling on an object implies its selection. Kalman filters have been explored as a gaze-dwell method of continued-stream user input [12]. In our system, users' gaze must first be used to search for the correct location to enter the login point, which makes the more explicit gaze-trigger method preferable. Jacob and Karn [10] suggest that, in spite of many challenges in eye tracking technology (calibration, accuracy, etc.), eye trackers have provided many human-computer interaction insights. Vertegaal [14] found that eye tracking has properties relating to Fitt's Law, with some speed and accuracy advantages over mouse-based interaction.

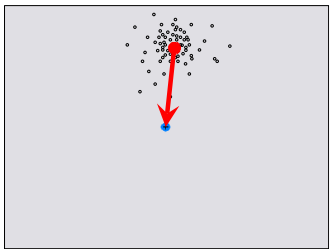

figure 2. Illustration of how 1-point calibration calculates the offset before password creation.

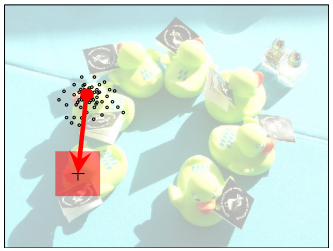

figure 3. Illustration of how 1-point calibration corrects drift during password creation.

Cued Gaze-Points Version 1 (CGP-1)

Cued Gaze-Points (figure 1) is an eye-gaze version of Cued Click-Points (CCP), where users select points on a sequence of images with their eye-gaze instead of the mouse cursor. As in CCP, CGP uses Centered Discretization [4] for gaze-point identification. In our studies, we used a 17" Tobii 1750 eye-tracker. Our first version of CGP (CGP-1) used the gaze-trigger method of gaze-point selection.

Methodology

To evaluate CGP-1's usability, we conducted a 16-participant user study following the published methodology for the CCP [3] study, including the same image set. Participants completed a 1-hour in-lab session of 6 trials, each including a new password creation, confirmation, and login.
Since eye-gaze is less precise than mice, we adjusted the system configuration. We used a 800×600 resolution, instead of CCP's 1024×768, to make the images in our study $\frac{1024}{800} = 1.28$ times larger linearly. People have full vision acuity within $\sim 1^\circ$ of their gaze's centre [7]. Thus, a 1° radial target on a 17" monitor with a 800×600 resolution that is $64\,cm (25"$ [1]) away from the user forms a circular target with a diameter of *51 pixels*. Kumar et al.'s [11] on-screen keys were a similar size. Although the area of full vision acuity forms a circular target on the screen, we used square tolerance regions because CGP needs a grid system to store passwords securely through discretisation [4].

CGP-1 Results

CGP-1's usability was much poorer than its click-based predecessor, CCP. CGP-1 participants had lower error-free confirm and login success rates (36% and 50% versus 83% and 96%), more mean confirm and login errors per trial (3.03 and 2.95 versus 0.39 and 0.05), and longer mean create and login times (42.23 and 38.87 versus 24.7 and 7.4 s) than CCP participants. We found two main problems when examining users' gaze patterns and behaviour.

First, users' gaze would sometimes jitter away from their desired target when pressing the button to record their gaze-point, causing the system to misinterpret the user's intended gaze-point. Second, throughout the study, users would naturally move their head and body. As the experiment session progressed, the system increasingly misinterpreted users' gazes and recorded all gaze-points as though they were offset from the users' intended target. This *drifting* meant that, although users were looking at the correct point, since their head or body position had changed, the eye tracker would misinterpret their gaze location.
This problem of calibration and drift are somewhat different in CGP than for other usages. Eye tracker use in CGP is brief and subsequent logins may be widely separated in time. Any calibration in CGP must be very quick, otherwise it takes longer than the password entry. Clearly, some sort of calibration is needed since users are unlikely to sit in the exact same position for each login and they need maximum precision to accurately select gaze-points. Furthermore, with greater precision, smaller tolerance squares can be used without compromising usability. This in turn makes for a larger number of possible distinct gaze locations on each image [4], which increases the theoretical password space and system security (against password guessing attacks).

Gaze Accuracy Enhancements

We developed the following two enhancements that we hoped would improve gaze accuracy.

Nearest-Neighbour Gaze Aggregation

Instead of recording users' current gaze-point when a button is pressed, the first enhancement has users record multiple gaze-points as they hold the space bar. When it is released, the system uses a nearest-neighbour algorithm to calculate the user's gaze-point for this image as the point with the most neighbours within tolerance. If there are several such

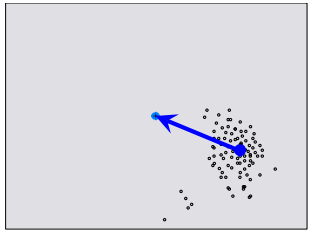

figure 4. Illustration of how 1-point calibration calculates the offset before login.

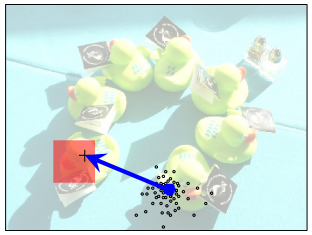

figure 5. Illustration of how 1-point calibration corrects drift during login.

points, their average is selected. We hoped that this method of gaze-point selection would more accurately reflect the user's intended gaze-point. However, we expected this might slow down gaze-point selection, since users hold down the space bar for a few seconds with each point.

1-Point Calibration

The second enhancement is a *1-point calibration* that users perform before they are about to enter a password (before creating, confirming, or logging in with their password). A blank image containing only a blue dot in the centre is displayed. Users stare at the dot and hold the space bar as though selecting a gaze-point. Upon releasing the space bar, the system calculates the offset distance between users' gaze-point (calculated using the nearest-neighbour gaze aggregation algorithm) and the actual location of the blue dot. This offset is then applied to all gaze-points recorded during that phase. We hoped that these quicker, more frequent calibrations would eliminate the drifting problem. The 1-point calibration is illustrated in figures 2 to 5. The blue circle in figures 2 and 4 denotes the centre of the calibration image. The red arrow in figure 2 and the blue arrow in figure 4 illustrate the offsets calculated during the corresponding create and login calibrations. Figures 3 and 5 show these offsets being respectively applied to a create and login gaze-point. The transparent red square represents the *tolerance region* around the password gaze-point. Without 1-point calibrations, this login would have failed, since the login point would have been outside the acceptable tolerance of the create point.

Users' foveal vision roughly covers a circular area when gazing straight at the screen. However, when gazing at the edges, the coverage is more elliptical. Eye trackers typically perform a 5-point calibration (centre and four corners) to ensure full-screen coverage. However, in CGP, users' gaze-points are only recorded within the displayed image, so a quicker calibration with only one point may provide sufficient coverage. In our setup (see CGP-1 section above), the image dimensions are $19 \times 15\,cm$, so distance between the image's centre and corner is $12.1\,cm$. This leads to an angle of $\sim 10.71^{\circ}$ between the centre of gaze from the image's centre to the image's corner. This projects an elliptical foveal area onto the monitor, centred at the corner of the image, with a major (longest) diameter of $\sim 2.31\,cm$. Comparatively, a circular foveal target at the centre of the image has a diameter of $\sim 2.23\,cm$, so there is at most a $\frac{2.31-2.23}{2} = 0.04\,cm < 1\,pixel$ radial margin of error when recording image gaze-points. Therefore, we believe that our 1-point calibration should not result in errors at the image edges, given the current system parameters (such as the position of the image, and size of the image and screen).

Cued Gaze-Points Version 2 (CGP-2)

We implemented these two enhancements in a second version of CGP (CGP-2). Following the same methodology as for CGP-1, we repeated the study to test CGP-2 with 25 new participants. We made the following hypotheses about CGP-2:

H1. CGP-2 will achieve higher success and lower error rates during password re-entry than CGP-1.

H2. CGP-2 will have longer login times than CGP-1.

H3. CGP-2's 1-point calibration will retain gaze accuracy at the edge of the images and not result in more errors at the edges of the images.

CGP-2 Results

Table 1 lists performance comparisons between CGP-1 and CGP-2 with significance test results. Table 1 shows that CGP-2 users successfully logged in more often and committed fewer mean login errors than CGP-1 users. The table also shows no significant differences in the time CGP-1

and CGP-2 users took to create or log in. These results support hypothesis H1, but H2 cannot be accepted. This means our enhancements resulted in higher success rates and fewer errors, without lengthening login times.

table 1. Performance comparisons between CGP-1 and CGP-2.

System	CGP-1	CGP-2	CGP-1 vs CGP-2 Sig. Tests
# of Participants	16	25	-
# of Trials	127	169	-
Successful Logins on 1st try	50%	73%	$\chi^2(1, 355) = 6.44, p < .05$
Successful Logins $\leq$ 3 tries	75%	93%	$\chi^2(1, 355) = 7.97, p < .01$
Mean Login Errors (per trial)	2.95	0.51	$t(355) = 4.27, p < .0001$
Mean (SD) Create Time (s)	42.2 (22.4)	44.2 (22.0)	not significant
Mean (SD) Login Time (s)	47.9 (64.2)	36.7 (35.9)	not significant

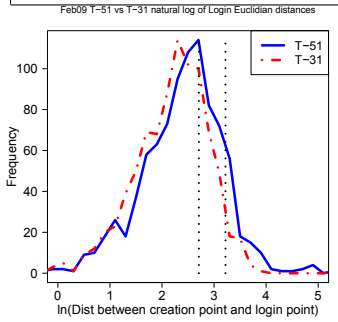

figure 6. Frequencies of the Euclidian distances between the creation and login points for passwords created, scaled by natural logarithm (ln). The vertical lines denote the boundary of each condition's tolerance square.

Figure 7 compares the x-coordinate of users' creation gaze-points to the horizontal distance (Delta X) between the respective creation and login points. Login points within tolerance are shown as blue circles, and those outside are red $\times$s. We see no more erroneous gaze-points at the figure's top and bottom than near the centre. The analogous y-coordinate graph is similar. This suggests our 1-point calibration did not introduce errors at the images' edges, which supports our earlier calculations and hypothesis H3. Apart from the 25 participants who tested CGP-2 with a tolerance square size of 51×51 (T-51), 20 additional participants tested CGP-2 with the same methodology and configuration, except for a smaller tolerance size of 31×31 (T-31) instead of 51×51. We found a noteworthy difference in gaze-point accuracy between these conditions. Figure 6 illustrates the frequencies of the Euclidian distances between the creation and login points for passwords created, scaled by natural logarithm. Values of 0 on the x-axis represent login points that were precisely on the creation point, and greater x-axis values represent login points that are increasingly further away from their corresponding creation points. Figure 6 shows that participants in the T-31 condition (a smaller tolerance square) gazed more closely to their initial creation gaze-point than T-51 users ($t(1756.60) = 5.65, p < .0001$). Note however that T-31 users succeeded to login on the first attempt significantly less often than T-51 users (54% vs 73%, $\chi^2(1, 254) = 10.46, p < .005$) [9]. This suggests that users can intentionally gaze more accurately when required. However, there is a physiological limit to how much more precisely users can gaze without further technological aid.

Conclusion

Graphical passwords offer a number of security and usability advantages over text passwords. Although click-based graphical passwords (such as Cued Click-Points) are potentially vulnerable to shoulder-surfing, Cued Gaze-Points offers a gaze-based alternative that is resistant to such attacks. An initial user study on CGP revealed that its unique use of eye tracking required special techniques to enhance users' gaze accuracy. We developed two novel gaze-accuracy enhancements: a quick 1-point calibration and a nearest-neighbour gaze-point aggregation algorithm. We implemented and user tested these enhancements in a second version of CGP. The two enhancements significantly improved users' gaze accuracy and the system's usability. Future work includes performing a long-term study of CGP to evaluate how usable the system is over time. Studies comparing the use of the one-point calibration and nearest-neighbour algorithms independently would improve our understanding of how either enhancement improves gaze accuracy. An extension of this would be to test either or both of these enhancements with other applications. A direct comparison of 1-point and multi-point calibrations or nearest-neighbour with other gaze-point aggregation techniques would also further research in this area.
Most monitors and laptops today have built-in cameras, and we expect eye tracking technology to become more

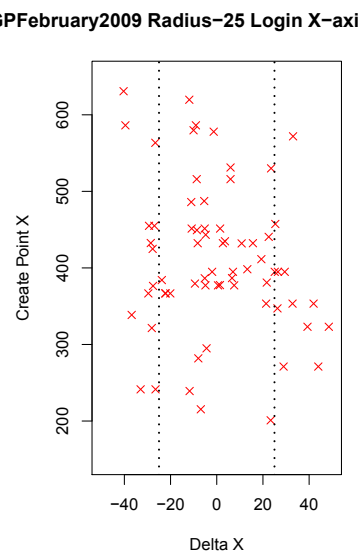

figure 7. Scatterplot of CGP-2 login gaze-points. The x-axis represents the horizontal distance between the creation point and the login point, and the y-axis represents the x-coordinate of the creation point. Blue circles are correct gaze-points and red Xs are incorrect. The dotted vertical lines show the tolerance region.

affordable in the near future, so it could have a place in everyday user interaction. Thus, eye tracking could be used by a variety of applications with properties similar to CGP: a very short time period of use with potentially long time periods between uses. We hope such applications would benefit from the two enhancements described in this paper.

Acknowledgements

We thank the referees whose comments improved this paper's clarity. This work was supported by the Natural Science and Engineering Research Council of Canada (NSERC). Partial funding from the NSERC Internetworked Systems Security Network (ISSNet) is also acknowledged.

References

[1] D. Ankrum. Viewing distance at computer workstations. *Workplace Ergonomics*, 2(5):10–12, September/October 1996.

[2] R. Biddle, S. Chiasson, and P.C. van Oorschot. Graphical passwords: Learning from the first generation. Technical Report TR-09-09, School of Computer Science, Carleton University, 2009.

[3] S. Chiasson, P.C. van Oorschot, and R. Biddle. Graphical password authentication using Cued Click Points. In *European Symposium On Research In Computer Security (ESORICS), LNCS 4734*, pages 359–374, 2007.

[4] S. Chiasson, J. Srinivasan, R. Biddle, and P.C. van Oorschot. Centered discretization with application to graphical passwords. In *Usability, Psychology, and Security (UPSEC)*. USENIX, 2008.

[5] A. De Luca, M. Denzel, and H. Hussmann. Look into my eyes! Can you guess my password? In *5th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2009.

[6] A. De Luca, R. Weiss, H. Hußmann, and X. An. EyePass - eye-stroke authentication for public terminals. In *SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 3003–3008. ACM, 2008.

[7] A. Duchowski. *Eye Tracking Methodology: Theory and Practice*. Springer, 2nd edition, 2007.

[8] P. Dunphy, A. Fitch, and P. Olivier. Gaze-contingent passwords at the ATM. In *4th Conference on Communication by Gaze Interaction (COGAIN)*, 2008.

[9] A. Forget, S. Chiasson, and R. Biddle. Shoulder-surfing resistance with eye-gaze entry in click-based graphical passwords. In *SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, 2010.

[10] R. Jacob and K. Karn. Eye tracking in human-computer interaction and usability research: Ready to deliver the promises. In J. Hyona, R. Radach, and H. Deubel, editors, *The Mind's Eye: Cognitive and Applied Aspects of Eye Movement Research*, chapter 4 commentary, pages 573–605. Elsevier Science, 2003.

[11] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *3rd Symposium on Usable Privacy and Security (SOUPS)*, pages 13–19. ACM, 2007.

[12] M. Kumar, J. Klingner, R. Puranik, T. Winograd, and A. Paepcke. Improving the accuracy of gaze input for interaction. In *Eye Tracking Research & Applications Symposium (ETRA)*, pages 65–68. ACM, 2008.

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

[14] R. Vertegaal. A Fitts' Law comparison of eye tracking and manual input in the selection of visual targets. In *10th International Conference on Multimodal Interfaces (ICMI)*, pages 241–248. ACM, 2008.