Using Gaze Based Passwords as an Authentication Mechanism for Password Input

David Rozado
ICT Centre - CSIRO

Traditional knowledge-based authentication techniques such as inputting a password with a keyboard are vulnerable to malicious observers using direct observation techniques (such as shoulder surfing) to grab user's authentication credentials. Videoculography gaze tracking can be used to input a password into a computer by gaze in a manner that is shoulder surfing resistant such as for instance by looking at a sequence of spatial positions in an image. I present here a user study comparing the speed and error rates of inputting a password using different gaze-based password methods as opposed to a traditional keyboard-based password. I also propose using the subject-specific gaze estimation parameters gathered during a calibration procedure for rendering impractical to another person to input a password by gaze even if the impostor knows the appropriate password. I show empirically how correct gaze-based passwords are not recognized by the system when using the gaze estimation parameters of a different user. The results of this work suggest the feasibility and advantages of using gaze-based methods for authentication purposes with a computer system.

Keywords: Eye Tracking, Gaze Tracking, password, security, authentication, identification, biometrics, eye tracking, gaze tracking, gaze gestures, HCI

Introduction

Traditional password authentication into a computer system with a keyboard is vulnerable to shoulder surfing attacks. Shoulder surfing refers to the usage of observation techniques, i.e. looking over someones shoulder, to obtain their password. Additionally, keyboard based password entry is inconvenient or unfeasible for handicapped computer users with limited or no mobility of their hands and for computer users interacting with a computer while their hands are engaged in other tasks, for instance during surgery. In this work, I propose and compare several mechanisms to input a password on a computer system by using gaze alone. The methods explored offer a shoulder-surfing resistant and hands-free mechanism for personal authentication. Furthermore, I also propose the usage of the user-specific parameters gathered during the gaze calibration procedure for gaze estimation to add and additional layer of security in the identification process with a computer system. Since gaze estimation algorithms are dependent on the features derived during the calibration procedure, and this features are user specific, an impostor trying to supplant a subject will most likely be unable to input a password correctly using gaze, even if the impostor knows the password of the user. This is due to the gaze estimation algorithms not producing accurate gaze estimations when using the gaze parameters derived from a calibration procedure carried out by a different user.

Personal identification refers to the mapping between a person and an identity. Identification can take place in the form of authentication where the individual authenticates a claimed identity or in the form of recognition where a person is matched to a database of person's biometric features known to the system. Biometric recognition strives to identify a user by using distinguishing physical or behavioral patterns that are matched against a database of previously established features. It is challenging however to find a biometric identification system that provides robust recognition for a variety of scenarios.

A person's gaze features and movement patterns can be considered a dynamic biometric signal that can be used for identification purposes and activity recognition (Bulling, Roggen, & Troster, 2011; De Luca, Weiss, & Drewes, 2007). Gaze dynamics based identification can be divided in task dependent and task independent identification. In task dependent identification, the user is forced to perform a task with his gaze. In task independent identification, a user can proceed with its usual gaze interaction with a computer while the system tries to identify the user and the background using his gaze dynamics.

In (Maltoni & Jain, 2004), the authors described

Corresponding author: david.rozado@csiro.au

a task dependent identification system, where subjects followed over several sessions a jumping stimulus point at 12 different positions. Features such as average velocity direction, distance to the stimulation, discrete Fourier transform an discrete wavelet transform were derived from the normalized signals. They reported an average recognition error of 8%. In the work from (Kinnunen, Sedlak, & Bednarik, 2010), authors showed the subjects to be identified a single stimulus consisting of a cross situated in the middle of the screen and displayed for one second. The eye features used were the pupil diameter and its time derivative, the gaze velocity, and the time varying distance between the eyes. Authors reported that the time derivative of the pupil size was the best dynamic feature which yielded just by itself identification rates up to 60%. In the same work, (Kinnunen et al., 2010) described also a task independent identification system based on eye movement dynamics. Their algorithm characterized gaze behavior as a histogram of all angles that the eye travels during a certain period. The accuracy of the system is better than chance, hence suggesting that there are individual information in eye movement dynamics which are specific for different persons and can be modeled.

Gaze has also been used in the realm of authentication based scenarios in which a user employs its gaze to convey a predefined pattern to a computer system. The first proposal in the literature for using gaze to input a password in a computer was made in (Kumar, Garfinkel, Boneh, & Winograd, 2007). That work described a system, named EyePassword, using an onscreen keyboard. In (De Luca, Weiss, & Drewes, 2007), authors evaluated three different eye gaze interaction methods for PIN-entry. Besides the classical eye input method, authors also proposed a new method of drawing numbers with gaze. Their evaluation concluded that the proposed approaches provided higher security against common attacks to steal authentication information compared to commonly used input methods. In (Pomarjanschi, Dorr, & Barth, 2012), authors investigated empirically the usability of gaze-contingent interaction as a solution to shoulder surfing in an ATM scenario using Passfaces graphical passwords. The authors noticed that the obstacles to commercial adoption aside from cost were the average time to login, 20 seconds, a significant deficit when compared to a typical PIN entry. Finally, the work from (Forget, Chiasson, & Biddle, 2010) uses image passwords using gaze to input a password on a computer system. The advantages of the system are the large password space, the shoulder-surfing resistance security and its cued-recall nature that helps users remember multiple distinct passwords.

Here, I compare the performance of several knowledge-based authentication systems using gaze to prevent the shoulder surfing problem. I use manual typing of text passwords with a keyboard as a baseline for comparison purposes. Specifically, I compare the following gaze based password input methods: gazing at a number pad on the screen to input a specific PIN, gazing at a sequence of predefined areas on an image, carrying out a gaze gesture and tracking a sequence of objects using smooth pursuit eye movements. I do this by carrying out a user study to find out the error rate of each password input mechanism analyzed as well as the time that each method takes, on average, to input a password. Additionally, I also propose and empirically verify that the security of gaze based authentication systems can be augmented by using a gaze calibration profile matched to each specific user authorized in the system. In such a system, a database associates the gaze profile derived from a gaze calibration session to a specific user identity. This security feature is based on the fact that gaze estimation algorithms need to determine a set of user specific parameters (radius of the corneal curvature, the distance between the center of the pupil and the center of the corneal curvature and the effective index of refraction of the cornea and the aqueous humor combined) during a calibration procedure in order to incorporate them in their gaze estimation model. When a specific user claims an identity, the system can retrieve the associated gaze calibration profile from the database and use those parameters to generate gaze estimations. Since the parameters required for accurate gaze estimation are user specific, an impostor with the knowledge of a gaze based password would not be able to convey the password correctly because the system would be estimating the wrong gaze coordinates during the password input period. This additional feature could augment the security of a gaze based and shoulder surfing resistant password input system.

Method

A user study (N=20) was carried out in order to test different gaze based password input methods for authentication purposes in terms of speed to completion and error rate. A traditional keyboard based password input method was used as a reference modality. We also tested the performance of inputting a password through gaze when using a gaze estimation algorithm tuned to the parameters of a different subject calibration. Prior to the experiment, participants were given a brief verbal introduction to each password input modality and some time to get acquainted with the system. Subjects underwent a 50 trial session in which they had to randomly perform each of the 5 types of password input methods 10 times.

Four different types of gaze based password input methods were analyzed in comparison to a traditional keyboard based password input method. Password lengths for each input method were selected so that the password space (total number of possible passwords) for each method used was within the same order of magnitude as the rest of the methods. The password space was in the order of 1.05 for all password input methods. The four password input methods are: **Tra-**

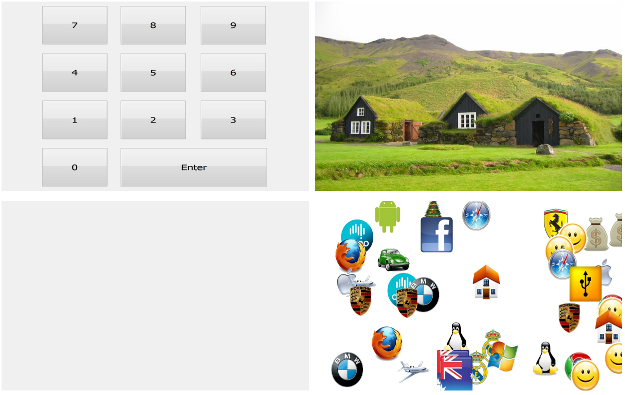

Figure 1. **Password Input Methods.** Subfigures *c*, *d*, *e* and *f* show screen captures of password input methods using gaze over a numberpad, a gaze based image password, a gaze gesture and a gaze based smooth pursuit of moving objects.

ditional keyboard: Usage of a traditional keyboard to manually input a password of length 4. **Gaze over numberpad password:** Usage of an on-screen number keypad to conveyed a number password by gazing at a pre-defined sequence of numbers of length 5. **Gaze image password:** Usage of an image on-screen to convey a password is conveyed by gazing at a sequence of 3 features in the image. **Gaze gesture password:** A password is conveyed by using a sequence of 6 gaze strokes over an empty background. **Object track password** A password is conveyed by using smooth pursuits gaze movements of a sequence of 4 objects moving on the screen.

The interested reader can visualize the manuscript's associated video[1] that provides a description of the different password input methods being compared in the user study. A screen capture of the different types of screen background for each type of password input method is shown in Figure 1.

The data collected was analyzed using paired t-tests and ANOVA (Analysis of Variance). The F-test statistic (F = variance between items / variance within items) is used for comparisons of the components of the total deviation. Differences between modality pairs were considered significant when the p-value fell below the 0.05 threshold.

Results

The average password entry times for the 5 password modalities under study can be visualized in Figure 2. An ANOVA analysis revealed statistically significant differences between groups, F(4,95)=115.38, p=1.38E-35. A Bonferroni-Holm posthoc test found significant individual pair differences between groups for all pairs except for the gaze image password and the gaze gesture password.

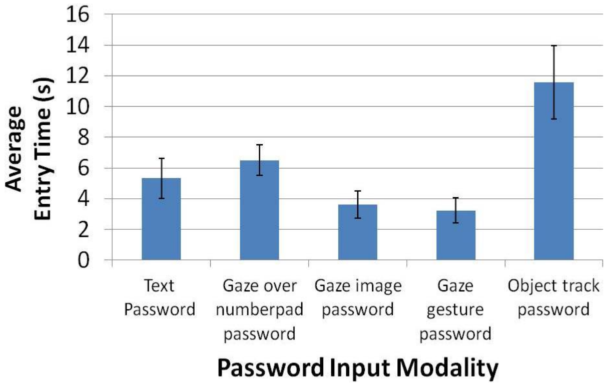

Figure 2. **Average Password Entry Time.** Average password entry time for the 5 password input modalities under study.

The average error rate for the 5 password entry modalities under study can be seen in Figure 3. Differences between groups were statistically significant with F(4,95)=17.06 and p=1.42E-10. A Bonferroni-Holm posthoc test found significant individual pair differences between the groups gaze over numberpad password and gaze image password, gaze over numberpad password and object track password, gaze over numberpad password and text password and gaze over numberpad password and gaze gesture password.

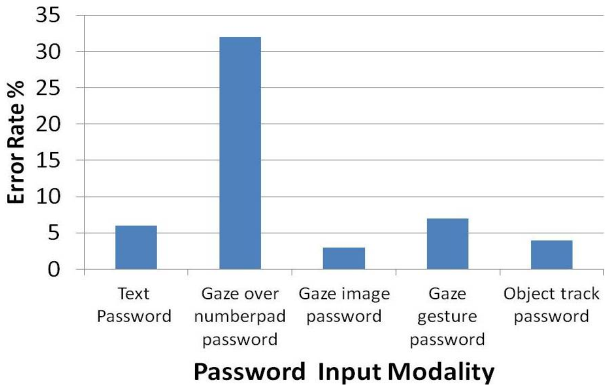

Figure 3. **Average Error Rate.** Displayed are the 5 password input modalities under study.

The password recognition rates when using another subject calibration on the gaze data of a given subject trying to perform a gaze-based password input method are shown in Figure 4. Differences in performance between gaze based password input methods failed to reach statistical significance.

Discussion

The results of this work show that gaze based identification systems can block the risks of shoulder surfing attacks during identification procedures by minimizing the information given away by the system to

[1] http://www.youtube.com/watch?v=Hui0s0YLnls

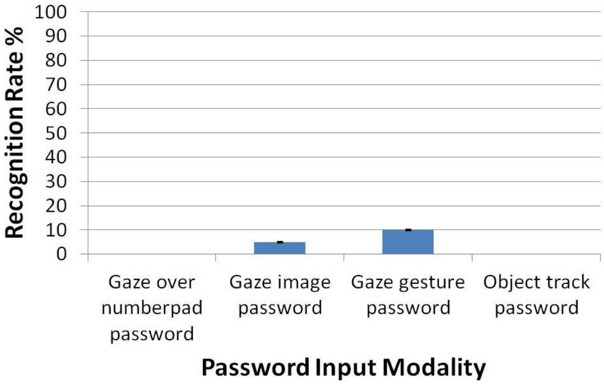

Figure 4. **Gaze Based Passwords When Using Wrong Gaze Calibration Parameters.** The Figure shows the inability to properly recognized a gaze based password when using the gaze calibration parameters of a different user.

potential bystanders. Three of the methods proposed, gaze image password, gaze gesture password and object track password generate error rates during the inputting stage as low as the traditional text based password input mechanism. Two of them, gaze image password and gaze gesture password are even faster to perform than inputting a password by means of a keyboard. Furthermore, this good results are achieved even though the subjects were trying out gaze based passwords for the very first time, pointing out at how intuitively this gaze based password methods are assimilated.

An additional feature of eye tracking systems that can aid in identification is the distinctive gaze estimation error signatures intrinsic for each user. This error signatures refer to the disparity between a subject actual gaze position and the gaze estimation coordinates inferred by the eye tracking software which is distinct for different users according to their ocular physiological differences. Our experimental results confirmed that using a gaze based password input mechanism with the right password sequence but the gaze estimation algorithm's parameters of another subject does not lead to correct password input. Hence, I propose here a system that keeps a database of gaze estimation models associated to each user (gathered through a calibration procedure). When a particular individual claims to represent a certain user, the system can load the corresponding gaze estimation model and prompt the user to input a gaze based password. Just knowing the correct password of a user with access would not allow an intruder to gain access to the system since a gaze estimation algorithm tuned to another person's calibration parameters would produce inaccurate gaze estimation and would not allow the impostor to input the proper password.

In summary, the combination of gaze based recognition and authentication can strengthen the security of identification and recognition of users in computer systems by making them more shoulder surfer resistant and more robust to impostors trying to supplant a user even when they have knowledge of their password.

References

Bulling, A., Roggen, D., & Troster, G. (2011, April). What's in the Eyes for Context-Awareness? *IEEE Pervasive Computing*, *10*(2), 48–57. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5467012 doi: 10.1109/MPRV.2010.49

De Luca, A., Weiss, R., & Drewes, H. (2007). Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In *Proceedings of the 19th australasian conference on computer-human interaction: Entertaining user interfaces* (pp. 199–202). New York, NY, USA: ACM. Retrieved from http://doi.acm.org/10.1145/1324892.1324932 doi: http://doi.acm.org/10.1145/1324892.1324932

De Luca, A., Weiss, R., & Drewes, H. (2007). Evaluation of eye-gaze interaction methods for security enhanced pin-entry. In *Proceedings of the 19th australasian conference on computer-human interaction: Entertaining user interfaces* (pp. 199–202).

Forget, A., Chiasson, S., & Biddle, R. (2010, April). Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the 28th international conference on human factors in computing systems - chi '10* (p. 1107). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?id=1753326.1753491 doi: 10.1145/1753326.1753491

Kinnunen, T., Sedlak, F., & Bednarik, R. (2010, March). Towards task-independent person authentication using eye movement signals. In *Proceedings of the 2010 symposium on eye-tracking research & applications - etra '10* (p. 187). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?id=1743666.1743712 doi: 10.1145/1743666.1743712

Kumar, M., Garfinkel, T., Boneh, D., & Winograd, T. (2007, July). Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on usable privacy and security - soups '07* (p. 13). New York, New York, USA: ACM Press. Retrieved from http://dl.acm.org/citation.cfm?id=1280680.1280683 doi: 10.1145/1280680.1280683

Maltoni, D., & Jain, A. K. (Eds.). (2004). *Biometric Authentication* (Vol. 3087). Berlin, Heidelberg: Springer Berlin Heidelberg. Retrieved from http://www.springerlink.com/content/jgfy7cmjcnrjd1np/ doi: 10.1007/b99174

Pomarjanschi, L., Dorr, M., & Barth, E. (2012, January). Gaze guidance reduces the number of collisions with pedestrians in a driving simulator. *ACM Transactions on Interactive Intelligent Systems*, *1*(2), 1–14. Retrieved from http://dl.acm.org/citation.cfm?id=2070719.2070721 doi: 10.1145/2070719.2070721