eNGAGE: Resisting Shoulder surfing using Novel Gaze Gestures Authentication

Yasmeen Abdrabou
German University in Cairo
Bundeswehr University Munich
yasmeen.abdrabou@guc.edu.eg

Sherif Ismael
German University in Cairo
sherif.ismael@guc.edu.eg

Mohamed Khamis
University of Glasgow
Mohamed.Khamis@glasgow.ac.uk

Amr Elmougy
University of Canada in Egypt
amr.elmougy@uofcanada.edu.eg

Rana Mohamed Eisa
University of Canada in Egypt
rana.eisa@uofcanada.edu.eg

MUM '18,, November 25–28, 2018, Cairo, Egypt
ACM 978-1-4503-6594-9/18/11.
https://doi.org/10.1145/3282894.3289741

Abstract

Most of the already existing authentication schemes are subject to multiple types of side-channel attacks such as shoulder surfing, smudge attacks, and thermal attacks. Meanwhile, motion sensors and eye trackers are becoming more accurate. We propose a novel authentication technique that leverages a combination of mid-air gestures and gaze input for shoulder surfing resilient authentication. The aim is to complicate shoulder surfing attacks by dividing the attacker's attention onto 1) the user's eyes, 2) hand-gestures, and 3) the screen. We report on the concept and implementation of the approach using both random and fixed layouts.

CCS Concepts

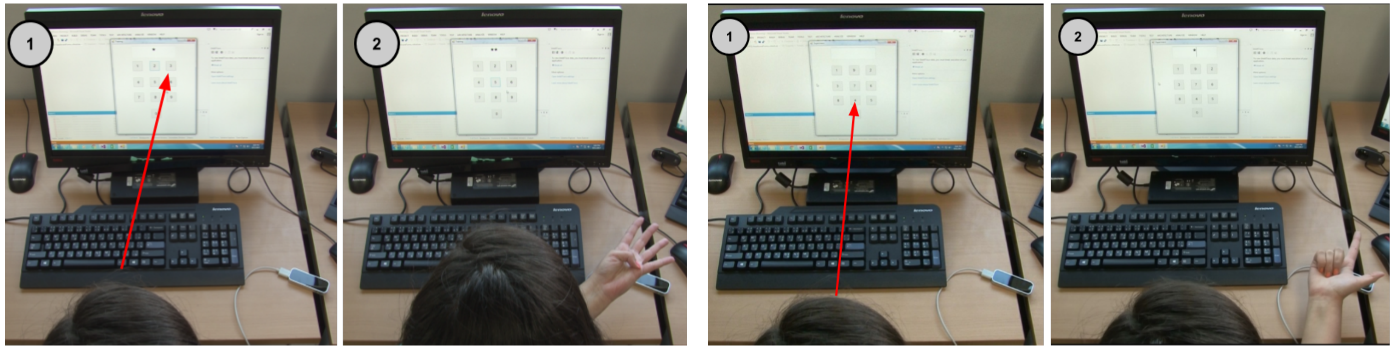
•Human-centered computing → Human computer interaction (HCI);

Author Keywords

Multimodal Authentication; Gaze; Gestures.

ACM Classification Keywords

H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous



(a) A user entering 2 by gazing at 6 and doing 4 by left-hand fingers, so the entered digit is 6 - 4 = 2

(b) A user entering 6 by gazing at the digit 4 and extended 2 right-hand fingers, hence the entered digits are 4 + 2 = 6

Figure 1: Gaze Gestures Authentication using fixed and random layouts

Introduction and Related work

Many authentication schemes are being introduced to solve the problems facing already existing systems. Many of the commonly used authentication systems are proven to be vulnerable to different types of side-channel attacks. For example, alphanumeric and graphical passwords are known to be vulnerable to shoulder surfing and video attacks [6, 11, 12]. Other forms of side-channel attacks include thermal and smudge attacks, which can reveal passwords entered on keyboards and touchscreens [1, 3, 10].

Previous work has shown that employing gaze [5, 9] and gestures [2, 7] can significantly improve authentication schemes in terms of observation resistance. Furthermore, the combination of multiple modalities can significantly complicate shoulder surfing attacks [4, 8]. An additional advantage of at-a-distance interaction modalities, such as gaze or gestures, is that they allow designing schemes that split the shoulder surfer‘s attention to (1) the user‘s input, and (2) the screen. For example, to shoulder surf a user‘s gaze input in response to on-screen cues, the attacker would have to observe the user‘s eye movements, in addition to the on-screen cues [9].

In this work, we propose a novel authentication mechanism that enhances gesture-based authentication by adding gaze to it. We introduce the concept, implementation of 2 authentication schemes:

1. **GazeGestures+Random:** Multimodal authentication using hand gestures and gaze with a randomized arrangement of on-screen digits.
2. **GazeGestures:** Multimodal authentication using hand gestures and gaze with a fixed arrangement of on-screen digits.

In our multimodal approaches, users authenticate by gazing at a digit on an on-screen number pad for 500 ms, then perform a hand-gesture "extend their fingers" to indicate an addition or subtraction operation to be applied on the gazed at digit. For example, to enter ‘5‘ the user could gaze at ‘2‘ and extend ‘3‘ right-hand fingers, or gaze at ‘6‘ and extend ‘1‘ left-hand finger.

Concept

The multimodal approach combines both, user‘s gaze and the performed gestures in one authentication method. This method was introduced as a way to make gestures authentication more secure. First, the user gazes at an on-screen digit and then performs a mid-air gesture by extending a number of fingers. Using right-hand fingers results in adding the gesture-based input to the gaze-based input, while the left-hand fingers result in a subtraction.

Figure 1b, shows an example where to enter 6, the user has to gaze at the digit 4 and extended 2 right-hand fingers, hence the entered digits are 4 + 2 = 6. On the other hand, Figure 1a, shows an example of a user gazing at 6 and doing 4 by left-hand fingers, so the entered digit is 6 - 4 = 2. This method is complicated as it needs basic math calculation in each digit entry, which will put an extra delay on the authentication time; however, it is expected to be secure. We refer to this system as GazeGestures. We implemented a version of GazeGestures with a randomized on-screen arrangement of digits and a version with a fixed one.

Implementation

The implementation is done using visual studio C# along with Leap Motion and Tobii‘s SDKs.

Screen layout

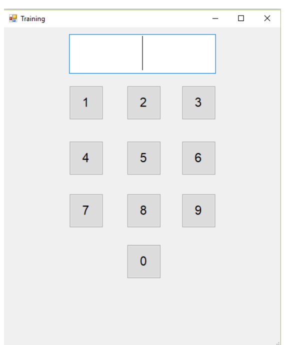
The screen layout looks like the default numbers keypad as seen in Figures 1b and 1a, with 10 digits from 0-9. A pilot study took place on 3 participants to check the layout (buttons size, distance..etc.) and the system usability. We received 2 comments. Accordingly, a button clicked sound is played after each digit entry. Also, the text area font has been enlarged and placed above the keypad. This way the user can sense the input without directly looking to the text area, accordingly reducing the gaze input error rate. The layouts can be seen in Figure 2.

Detecting Gaze

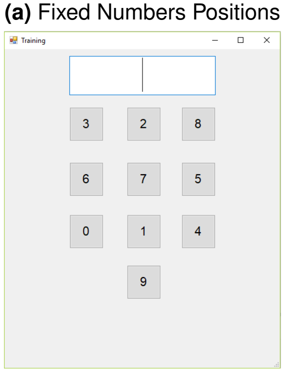
The gaze input is detected using Tobii 4C eye tracker with 90 frames per second. The digit is entered if the users fixed their eyes on the same digit for 500 ms (dwell time 500 ms). The dwell time was chosen according to a pilot study took place on 3 participants. The participants used our tool to authenticate by 3 different times (300, 500, 700) ms. The participants complained about the 300 ms as it‘s fast and 700 ms as it‘s slow. Thus the 500 ms was chosen. The user then can enter the next digit. If the user wants to enter a duplicate digit, then he has to move his eyes away from the digit and dwell on it again or to close his eyes and re-opens them.

Detecting Gestures

Gestures are tracked using a Leap Motion, it detects the hands and counts the fingers extended. The digit is entered if the user fixed their hand above the leap motion for 1 sec and none of their fingers orientation has changed. This condition was added to eliminate the unconscious finger movements entry and the faulty zero detected while changing from one digit to another. If the user wants to enter a duplicate digit, then the user has to remove their hands from the detecting area and enter it again or to close their palm and re-opens it. That movement was done to eliminate repeating the entered digit as long as the user is fixing their hand above the leap motion.



(a) Fixed Numbers Positions



(b) Random Numbers Positions

Figure 2: Approach‘s Layout

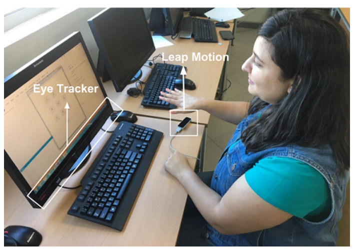


Figure 3: Proposed Usability study setup showing the leap motion, eye tracker positions and user to screen distance.

Multimodal Approach
For the multimodal digit entry, the user has to gaze on the digit first and then do the number gesture with his hand. The digit is not recognized and entered unless a valid number is entered by the gaze and the gestures. The Leap Motion is placed to the right of the keyboard in order to reduce the infrared interference of the eye tracker and the Leap Motion, also not to block the sight of the eye tracker path.

Proposed Study Design

The study design proposal suggests collecting a realistic set of login attempts to analyze usability, as well as video recordings to be used for evaluating the approach‘s security against shoulder surfing. The video recording should be captured from the back of the participant to show the screen layout and the participant‘s gestures. In addition, another video recording should be from the front to show the users‘s eye movement to simulate attacks. Also, in addition to the collected PINs, we will collect qualitative data from the participants through surveys. The proposed study setup can be seen in Figure 3.

Conclusion and Future work

In this paper, we introduced a novel authentication scheme for desktop settings as well as a proposed study design. We discussed the concept and implementation of the proposed approaches. For future work, we plan to investigate the proposed approach‘s usability and security against shoulder surfing attacks. In addition, we will study the effect of using fixed and random layouts on the success rate of the attacks.

REFERENCES

1. Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-based User Authentication. In *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems (CHI ’17)*. ACM, New York, NY, USA. DOI: http://dx.doi.org/10.1145/3025453.3025461
2. Ilhan Aslan, Andreas Uhl, Alexander Meschtscherjakov, and Manfred Tscheligi. 2016. Design and Exploration of Mid-Air Authentication Gestures. *ACM Trans. Interact. Intell. Syst.* 6, 3, Article 23 (Sept. 2016), 22 pages. DOI:http://dx.doi.org/10.1145/2832919
3. Adam J. Aviv, Katherine Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge Attacks on Smartphone Touch Screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies (WOOT’10)*. USENIX Association, Berkeley, CA, USA, 1–7. http://dl.acm.org/citation.cfm?id=1925004.1925009
4. Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2012. Counting Clicks and Beeps: Exploring Numerosity Based Haptic and Audio PIN Entry. *Interact. Comput.* 24, 5 (Sept. 2012), 409–422. DOI: http://dx.doi.org/10.1016/j.intcom.2012.06.005
5. Heiko Drewes, Alexander De Luca, and Albrecht Schmidt. 2007. Eye-gaze Interaction for Mobile Phones. In *Proceedings of the 4th International Conference on Mobile Technology, Applications, and Systems and the 1st International Symposium on Computer Human Interaction in Mobile Technology (Mobility ’07)*. ACM, New York, NY, USA, 364–371. DOI:http://dx.doi.org/10.1145/1378063.1378122

6. Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 11.

7. Ceenu Goerge, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Proceedings of the Network and Distributed System Security Symposium (USEC '17)*. NDSS. DOI: http://dx.doi.org/10.14722/usec.2017.23028

8. Mohamed Khamis, Regina Hasholzner, Andreas Bulling, and Florian Alt. 2017a. GTmoPass: Two-factor Authentication on Public Displays Using GazeTouch passwords and Personal Mobile Devices. In *Proceedings of the 6th International Symposium on Pervasive Displays (PerDis '17)*. ACM, New York, NY, USA, 9. DOI: http://dx.doi.org/10.1145/3078810.3078815

9. Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017b. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI 2017)*. ACM, New York, NY, USA, 446–450. DOI: http://dx.doi.org/10.1145/3136755.3136809

10. Keaton Mowery, Sarah Meiklejohn, and Stefan Savage. 2011. Heat of the Moment: Characterizing the Efficacy of Thermal Camera-based Attacks. In *Proceedings of the 5th USENIX Conference on Offensive Technologies (WOOT'11)*. USENIX Association, Berkeley, CA, USA, 6–6. http://dl.acm.org/citation.cfm?id=2028052.2028058

11. Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the Design Space of Graphical Passwords on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, Article 11, 14 pages. DOI: http://dx.doi.org/10.1145/2501604.2501615

12. Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A Comparison of Perceived and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, New York, NY, USA, 56–66. DOI: http://dx.doi.org/10.1145/1143120.1143128