EyeMove - Towards Mobile Authentication using EOG Glasses

Kirill Ragozin
Keio University
Japan
kirill@kmd.keio.ac.jp

Karola Marky
University of Glasgow
United Kingdom
karola.marky@glasgow.ac.uk

Jie Lu
Keio University
Japan
jie.lu@kmd.keio.ac.jp

Kai Kunze
Keio University
Japan
kai@kmd.keio.ac.jp

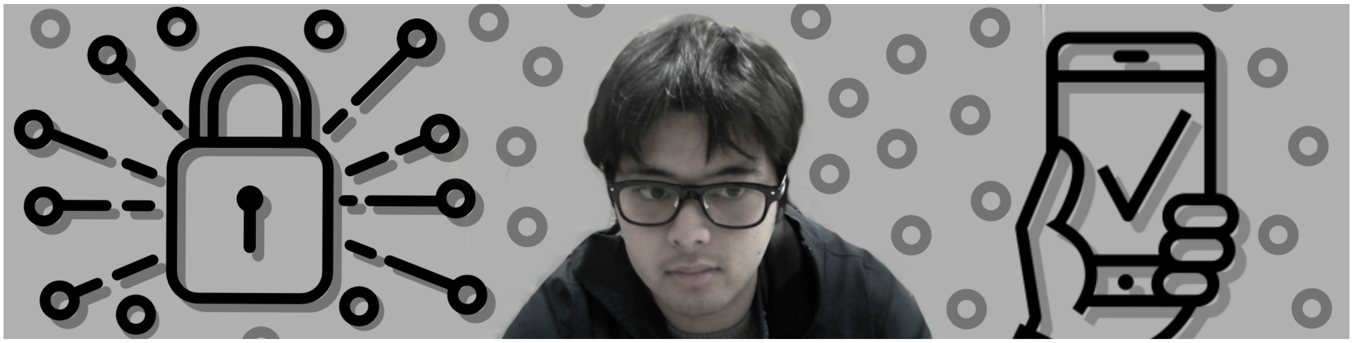

Figure 1: EyeMove Concept: Authenticate yourself using eye movements detected over EOG smart glasses.

ABSTRACT

Existing approaches for mobile authentication are prone to shoulder-surfing and side-channel attacks. Using gazes for authentication has been demonstrated to be more resistant to these attacks. Yet, existing solutions rely on eye-tracking by the device's front camera that is not always reliable. In this paper, we present an approach for EOG-based authentication by determining the gaze-based on the electronic potential of the eyes. Our approach runs on commercially available smart glasses and there is no need for the user to look at the device. Through a user study with 15 participants, we demonstrate the feasibility of the approach, its usability, and its adoption by mobile device users. Even users without regular glasses would adopt EOG-based authentication.

CCS CONCEPTS

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → *Interaction techniques.*

KEYWORDS

Multimodal Authentication, Gaze-Based Authentication, Mobile Authentication

ACM Reference Format:

Kirill Ragozin, Karola Marky, Jie Lu, and Kai Kunze. 2022. EyeMove - Towards Mobile Authentication using EOG Glasses. In *Augmented Humans 2022 (AHs 2022), March 13–15, 2022, Kashiwa, Chiba, Japan.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3519391.3519411

1 INTRODUCTION

Authentication mechanisms for (web) services and devices are a part of everyday life and users interact with them multiple times a day. To defend devices against an adversary different authentication mechanisms have been proposed and put into practice. Each of them belongs to one or to a combination of the following categories: 1) *something you know* (e.g., a password), 2) *something you have* (e.g., a token), and 3) *something you are* (e.g., a fingerprint) [8].

Mobile users unlock their devices several times a day. PINs, which are knowledge-based, are used predominantly on mobile devices. However, PINs could be observed by an adversary that is present in the user's vicinity, or obtained through a range of side-channel attacks, like thermal [1] or smudge attacks [3]. PINs also are the alternative or fall-back authentication of probabilistic schemes, such as FaceID or fingerprints. Gaze-based authentication has been demonstrated to be harder to observe [2, 11]. It has furthermore been shown that levering gazes as multimodal authentication factor is more secure compared to single-factor authentication [9, 10].

So far, the device's front camera has been used to enable this type of authentication [16]. Using the front camera is dependent on

AHs 2022, March 13–15, 2022, Kashiwa, Chiba, Japan

ACM ISBN 978-1-4503-9632-5/22/03…$15.00
https://doi.org/10.1145/3519391.3519411

the user's environment, light conditions, reflections of eyeglasses, or even make-up [12]. Electrooculography (EOG) is an alternative to track eye movements based on the electric potential [5]. It is more robust against environmental influences, does not require calibration, and the sensors can be easily integrated into glasses or nose clips.

In this paper, we present *EyeMove*, an approach for mobile authentication based on eye movements using commercially available smart glasses. We implemented an EOG-based unlock mechanism for mobile phones that can be either used as a standalone authentication mechanism or as a part of multimodal authentication to strengthen security. Through a user study with 15 participants, we investigated our proposed setup and live prototype. Our study demonstrates the feasibility and usability of our approach without the need to rely on the front camera or a complicated eye-tracking setup. Even if our setup is in a prototype state about half of the participants would like to use eye movements on a daily basis. Among those are participants that do not wear regular glasses and would wear smart glasses to interact with the mobile device. We see *EyeMove* as a first step towards using eye movements as a mobile authentication mechanism

2 BACKGROUND AND RELATED WORK

In this section, we present related work in the scope of (multimodal) gaze-based authentication and two-factor authentication.

To secure mobile devices from unwanted access, the devices employ unlock mechanisms. Initially, devices were unlocked either by entering a PIN or patterns. PINs and authentication patterns can be obtained by an adversary by several methods. Attackers might observe the user entering it (shoulder-surfing attack [15]), they could check smudges on the devices screen (smudge attack [3]), or observe traces of heat on the device's screen (thermal attack [1]). These attacks substantially weaken the security of PINs and authentication patterns. More recently, biometrical factors, such as the fingerprint or a faceID have become available. Those are probabilistic schemes and that use PINs as fallback alternative. Thus, they posses the same weaknesses as PINs. Since fingerprint sensors only use partials of the fingerprint, the authentication mechanism can be circumvent by the generation of partial fingerprints that impersonate a large number of users [13].

Gazed-based authentication based on the device's front-camera has been proposed in the literature as a usable alternative [11, 14, 16]. It, furthermore, has been investigated in other domains, such as AR or VR [7]. Studies of multimodal authentication that combines video-based eye tracking and touch input reveal that multimodal authentication offers an enhanced security while not putting too much burden on the user [9, 10].

Electrooculography (EOG) is another possibility to track eye movements [5]. It is based on the fact that our eyes are dipoles with a constant electrical potential. The cornea acts as the positive and the retina acts as the negative pole. The magnitude of this corneoretinal potential (CRP) is in the range of $0.4mV$ to $1.0mV$. If we move our eyes the dipole and the electrical potential move as well. This movement can be captured by using electrodes which are taped around the eye (usually measuring the potential change left/right for horizontal and up/down for vertical movement). This procedure is called Electrooculogram. EOG does not require calibration. It is robust against changes in the user's environment. Thus, it even works in the dark, or if the user's eyes are closed. EOG sensors can be easily integrated into regular glasses or small nose clips.

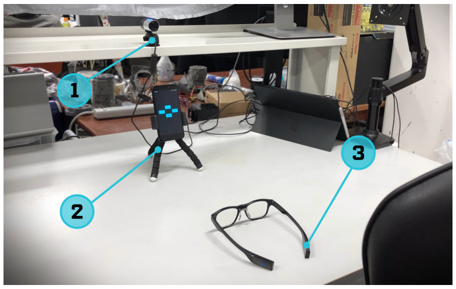

Figure 2: Experimental setup featuring a camera for facial recording (1), smartphone with the experiment application (2) and a pair of JINS MEME smart glasses (3).

Findling *et al.* evaluated passwords based on gazes and gestures using EOG [6]. Hereby, they focused on the security and possible password space of EOG-sensed gazes with opened and closed eyes. For their evaluation, they collected two data sets and analyzed the EOG data offline. Building upon this work, we provide the first prototype implementation standalone on a smartphone which can recognize the authentication gazes in real time. We also compare our system to PIN entry as baseline and evaluate EOG as a part of multimodal authentication.

3 EXPERIMENTAL SETUP

In order to conduct a user study, we developed a mobile application that allowed users to try three different authentication methods. The experimental setup (see Figure 2) consisted of a smartphone that ran the application and was mounted on a tripod in front of a user. A camera capturing the persons' face was placed behind the smartphone. The camera was not part of the authentication setup, we used it for capturing metrics of our experiment detailed below. In addition to that, the users were given a pair of EOG smart glasses that allowed detecting their eye movements. In particular, the eye movements were recognized by using a live peak detection algorithm applied to the vertical and horizontal EOG signal streams.

Within the study, we investigated the following three conditions: 1) PIN-based authentication (baseline), 2) EOG-based authentication, and 3) combination of EOG and PIN (PIN-EOG).

For the PIN scenario, the participants had to type a four-digit code (Figure 3-1). After that, they were redirected to an unlocked home screen. In the EOG scenario, the participants commenced by pressing a "start" button. Then, they were asked to wait until the end of a countdown that was shown in the middle of the screen on top of a small white circle (Figure 3-2). At the end of the countdown, the circle turned green and signaled "Look", indicating that the user should perform the interaction which consisted of one of the four basic eye movements: left, right, up, or down. Successful eye movements unlocked the smartphone, while unsuccessful ones indicated an error by briefly turning the circle red and restarted the countdown with a slightly reduced delay. There were two reasons

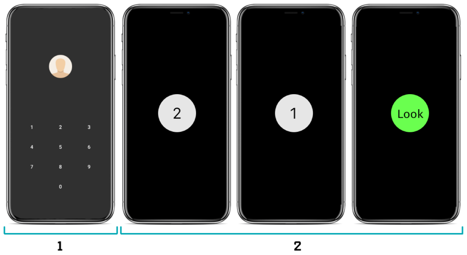

Figure 3: User interfaces of the experiment application. (1) shows the a PIN input, and (2) shows the gaze input with a countdown.

for introducing the delay. First, it allowed us to indicate the exact moment at which an eye movement would be expected by the system. Second, showing users a simple object to rest their eyes on before performing the gaze allowed us to get a clean EOG signal eliminating false-positive and false-negative attempts.

In a real-world scenario, such delays could be shortened significantly or removed completely. The PIN-EOG mechanic is the combination of the other two. It featured a PIN input screen followed by an EOG input screen with the countdown detailed above.

4 METHODOLOGY

To evaluate our concept with end-users, we conducted a user study with fifteen participants. To be able to control for environmental influences and to provide the participants with an eye tracker, we opted for a lab study. The experimental setup was set as explained above. Within our study, we investigated the three conditions PIN (baseline), EOG, and PIN-EOG as detailed above. Each participant interacted with all three conditions in a counter-balanced order based given by a Latin Square.

We used the camera behind the smartphone to review the interaction after the study. Figure 2 depicts the experimental setup. We assessed the subjective usability of each condition by the System Usability Scale [4] and gathered qualitative data via a questionnaire.

4.1 Study Procedure

The procedure of our study was as follows:

4.1.1 Informed Consent and Setup. We commenced by explaining the consent form and the data protection policy of the study. The participants were asked to read and sign both. We proceeded by explaining the scenario which is the unlocking of a mobile device, and the setup to the participant. Then, we provided them with smart glasses and a smartphone. To ensure that each participant received identical information, we provided them with information cards about each authentication mechanism.

4.1.2 Interaction and Questionnaires. Each participant interacted with all three conditions. Each condition had an individual information card with a description of the authentication mechanism and the tasks that the participants should fulfill with them. The card either contained a set of eye movement directions or the PIN that the participant was supposed to enter. Once, a participant reported completion they were given a questionnaire with four questions about the mechanism that they just used and the System Usability Scale questionnaire [4]. This procedure was repeated until the participant had interacted with all conditions.

4.1.3 Final Questionnaire. After interacting with all conditions, the participants received a final questionnaire which also included demographics. In this questionnaire, we asked the participants questions that compare the different mechanisms. Finally, the participants could ask questions about the study.

4.2 Participants and Recruitment

We recruited 15 participants at our institution by word-of-mouth, snowball sampling, and forums. We did not compensate the participants for participating in our study. Seven of them identified as female and eight as male. They were on average 27.5 years old ($SD = 3.7$, $Min = 24$, $Max = 36$) and all of them reported daily usage of mobile devices. Nine of them reported wearing regular glasses and five of them reported having experience with using smart glasses. Two thirds of the participants stated to use their fingerprint as primary authentication mechanism, three used FaceID, and two used PINs. One study session was on average 16.25 minutes long ($Min = 9.6$, $Max = 22.3$).

5 RESULTS

In this section, we present the results of our experiment.

5.1 Effectiveness

Considering effectiveness, all participants could perform all of the presented unlock procedures. For one participant, up and down movements could not be recognized by our system. They reported having had an eye surgery in which something got implanted in their eye. Thus, we concluded that this might have been the reason that this participant's up and down movements could not be recognized. There were on average two failed attempts over all participants. We observed these in the first condition.

5.2 Subjective Usability

Considering subjective usability, PIN-EOG received an average SUS score of 61 ($SD = 18.8$, $Min = 22.5$, $Max = 92.5$), EOG received on average 70 points ($SD = 13.6$, $Min = 45$, $Max = 90$), and PINs received 82 ($SD = 13.1$, $Min = 65$, $Max = 100$). The SUS scores are depicted by Figure 4A. We analyzed these ratings with a non-parametric Friedman test and found significant differences ($\chi^2 = 9.59$, $p = .008$). Then, we calculated pairwise comparisons which were Bonferoni-corrected. They reveal significant differences between PIN and PIN-EOG ($p < .001$).

5.3 Questionnaires

Within our experiment, we also gathered further feedback via questionnaires. Hereby, we aimed to gain insights on understandability, the participants' favorite schemes, their adoption of the presented setup, and usage contexts.

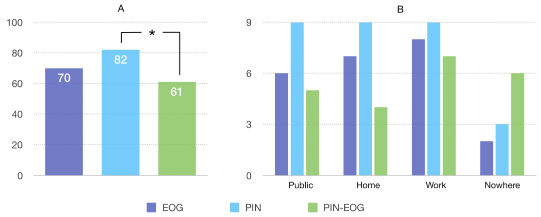

Figure 4: SUS scores (A) and answer distributions regarding the usage contexts (B). The asterisk (*) indicates a statistically significant difference.

To capture understandability, we asked the participants whether they consider the unlock mechanism as easy-to-understand. Answers could be given on a 5-point Likert scale. PINs were perceived as easiest to understand and received a mean value of 4.8. EOG was rated with 4.5, and PIN-EOG was rated 3.8. We analyzed these ratings with a non-parametric Friedman test and found significant differences ($\chi^2 = 12.4$, $p = .002$). Pairwise comparisons with Bonferroni correction reveal significant differences between PIN and gaze ($p = .008$), as well as between PIN and PIN-EOG ($p < .001$).

In the final questionnaire, we asked the participants which of the presented schemes they liked most. Two third of the participants favoured EOG. When asked to explain their answer, the participants named ease of use and the duration of the unlocking as main reasons for favoring gaze. Half of those ($N = 5$) would use EOG even if they do not wear regular glasses. Three participants (20%) favored the PIN based on being familiar with it and the concern that gazes might fail. Finally, two participants favored PIN-EOG.

We furthermore asked the participants if they would use one of the present mechanisms in real life. half of the participants stated that they would like to use EOG or PIN-EOG within the current setup. Three participants (20%) stated that they do not wish to use any of the presented unlock mechanisms because they like the unlock mechanisms that they currently use, such as fingerprints. Five participants (33%) would stick to using PINs. Four participants (26%) stated that they would like to use EOG again based on ease of use. Three participants (20%) would like to use PIN-EOG based on ease of use and security.

In the questionnaire between the conditions, we asked the participants about usage contexts of the presented unlock mechanisms. In particular, we asked where the participants would like to use the presented unlock mechanisms. This was a multiple choice answer with "in public", "at home", "at work", and "nowhere" as possible answers. The distribution of answers is given by Figure 4B.

The main reason for using PIN-EOG in public was the perception of additional security. Reasons for not using EOG outside of the home were a perceived discomfort since bystanders might misinterpret the gazes. Participants also considered the extra effort that is introduced by using PIN-EOG.

6 DISCUSSION AND LIMITATIONS

In this paper, we demonstrate the feasibility of EOG-based authentication on mobile devices using commercial smart glasses. We also conducted a first user study which supports the usability of EOG-based authentication.

All participants could perform the gazed-based unlock procedures. This shows that the unlock mechanisms based on that do not suffer from effectiveness issues. In our study, we could not find significant differences in terms of subjective usability and understandability between PIN and EOG. This indicates that using EOG on smart glasses can be a viable alternative to PINs. Furthermore, participants are not required to look at the device's screen for performing the unlock procedure and the gazes could be recognized with closed eyes which enhances shoulder-surfing resistance [6]. EOG-based authentication at its current state requires smart glasses or a nose clip. Even if this extra hardware is required participants in our user study that do not wear regular glasses would like to use the prototype. Since EOG sensors are becoming smaller they could be integrated into glasses or head-mounted displays for virtual or augmented reality to enable EOG-based authentication.

When comparing the combination of PIN and PIN-EOG, we found significant differences in terms of subjective usability and understandability. This could be explained by the extension of the PIN mechanism which results in a more effortful setup. On the other hand, from a security perspective, PIN-EOG is the most secure from the three investigated conditions [9]. Within the scope of authentication, there frequently is a trade-off between security and usability. While we investigated mobile authentication as a scenario, there might be other scenarios in which users are willing to spend the extra effort for the sake of security.

For the sake of our experiment, we needed to introduce a delay of four seconds in the gaze recognition. Therefore, we deliberately did not assess the execution time of the conditions. Performing one unlock with EOG took on average 10 seconds. This includes the delay of 4 seconds that is triggered by pressing the start button and the delay following the failed authentication attempts. Failed authentication attempts, however, decrease over time [9, 10] and we also observed this in our study. Assuming more complex gestures, a realistic unlock time of an improved prototype is likely to be around 3-4 seconds. Still, this has to be confirmed by future investigations. The authentication process was triggered by a button. However, using smart glasses enables authentication procedures without looking at the device's screen. Therefore, designing and evaluating different methods for triggering the authentication procedure form an important task for future work. These tasks could be pressing the power button, or lifting the device.

7 CONCLUSION

Common approaches for mobile authentication are either prone to different observation attacks or can be circumvented by exploiting fall-back mechanisms. Adding eye movements as a second factor has been demonstrated to be more robust against such attacks. In this paper, we presented an approach and functional prototype that enables EOG authentication in real time on commercially available smart glasses. All of the fifteen participants in our user study could successfully perform EOG-based authentication and half of them would even like to use our setup even if it is in a prototype state. This include participants that do not wear regular glasses.

8 ACKNOWLEDGEMENTS

This work is partly supported by the JST Presto Project Grant Number JPMJPR2132.

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 2017 CHI Conference on Human Factors in Computing Systems*. ., ., 3751–3763.

[2] Hassoumi Almoctar, Pourang Irani, Vsevolod Peysakhovich, and Christophe Hurter. 2018. Path Word: A Multimodal Password Entry Method for Ad-Hoc Authentication Based on Digits' Shape and Smooth Pursuit Eye Movements. In *Proceedings of the 20th ACM International Conference on Multimodal Interaction* (Boulder, CO, USA) *(ICMI '18)*. Association for Computing Machinery, New York, NY, USA, 268–277. https://doi.org/10.1145/3242969.3243008

[3] Adam J. Aviv, Katherine L. Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. *Proceedings of the USENIX Workshop on Offensive Technologies* 10 (2010), 1–7.

[4] John Brooke. 1996. SUS - A Quick and Dirty Usability Scale. *Usability Evaluation in Industry* 189, 194 (1996), 4–7.

[5] Andreas Bulling, Jamie A Ward, Hans Gellersen, and Gerhard Troster. 2010. Eye movement analysis for activity recognition using electrooculography. *IEEE transactions on pattern analysis and machine intelligence* 33, 4 (2010), 741–753.

[6] Rainhard Dieter Findling, Tahmid Quddus, and Stephan Sigg. 2019. Hide my Gaze with EOG! Towards Closed-Eye Gaze Gesture Passwords that Resist Observation-Attacks with Electrooculography in Smart Glasses. In *17th International Conference on Advances in Mobile Computing and Multimedia*. ., ., .

[7] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. 2019. LookUnlock: Using Spatial-Targets for User-Authentication on HMDs. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI EA '19)*. Association for Computing Machinery, New York, NY, USA, Article LBW0114, 6 pages. https://doi.org/10.1145/3290607.3312959

[8] Paul A. Grassi, James L. Fenton, and Michael E. Garcia. 2017. *Digital Identity Guidelines [Including Updates as of 12-01-2017]*. Technical Report. NIST Special Publication 800-63-3.

[9] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 2156–2164. https://doi.org/10.1145/2851581.2892314

[10] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction* (Glasgow, UK) *(ICMI '17)*. Association for Computing Machinery, New York, NY, USA, 446–450. https://doi.org/10.1145/3136755.3136809

[11] Dachuan Liu, Bo Dong, Xing Gao, and Haining Wang. 2015. Exploiting eye tracking for smartphone authentication. In *Proceedings of the International Conference on Applied Cryptography and Network Security*. Springer, ., 457–477.

[12] Päivi Majaranta and Andreas Bulling. 2014. Eye tracking and Eye-Based Human–Computer Interaction. In *Advances in Physiological Computing*. Springer, ., 39–65.

[13] Aditi Roy, Nasir Memon, and Arun Ross. 2017. MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems. *IEEE Transactions on Information Forensics and Security* 12, 9 (2017), 2013–2025. https://doi.org/10.1109/TIFS.2017.2691658

[14] C. Song, A. Wang, K. Ren, and W. Xu. 2016. EyeVeri: A Secure and Usable Approach for Smartphone User Authentication. In *Proceedings of the 35th Annual IEEE International Conference on Computer Communications (INFOCOM 2016)*. ., ., 1–9. https://doi.org/10.1109/INFOCOM.2016.7524367

[15] 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)*. ., „ 56–66.

[16] Xiaoyi Zhang, Harish Kulkarni, and Meredith Ringel Morris. 2017. Smartphone-Based Gaze Gesture Communication for People with Motor Disabilities. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2878–2889. https://doi.org/10.1145/3025453.3025790