Gaze-based Authentication in Virtual Reality

Jonathan Liebers
jonathan.liebers@uni-due.de
University of Duisburg-Essen
Germany

Stefan Schneegass
stefan.schneegass@uni-due.de
University of Duisburg-Essen
Germany

ABSTRACT

Authentication in virtual reality (VR) is a challenging topic since the common input modalities in VR (e. g., hand-held controllers) are limited and easily observable from the perspective of a bystander. Yet, as applications in VR are increasingly allowing access to private information and commercial applications appear (e. g., virtual shopping, social media), the secure identification and verification of a person is a major concern. This challenge is aggravated, as the wearer of a head-mounted display (HMD) does not perceive the surrounding real environment through the HMD. As more and more HMDs are released to the market with built-in eye-tracking functionality, we seek to understand how we can seamlessly utilize gaze-based authentication and connected methods in VR applications.

CCS CONCEPTS

• **Security and privacy** → *Usability in security and privacy*; • **Human-centered computing** → *Human computer interaction (HCI)*.

KEYWORDS

gaze-based authentication, usable security, behavioral biometrics

ACM Reference Format:
Jonathan Liebers and Stefan Schneegass. 2020. Gaze-based Authentication in Virtual Reality. In *Symposium on Eye Tracking Research and Applications (ETRA '20 Adjunct), June 2–5, 2020, Stuttgart, Germany*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3379157.3391421

1 INTRODUCTION

Authentication continues to be an important research topic, as new technologies appear and enter the consumer market. One example are applications in virtual reality (VR) and the associated head-mounted-displays (HMD). Applications for VR often require knowledge about the identity of a person, as they can serve private information to the user (e. g., social media) or can be utilized commercially (e. g., in-app purchases, virtual shopping). We expect that with the growing VR market the need for secure and usable authentication methods will further expand in the future.

Research has shown that the common input modalities for HMDs are insecure for the purpose of authentication (e. g., entering a PIN or password throughout a controller) [George et al. 2017]. Not only is this interaction of entering the PIN or password easily observable by a third party, (i. e., a shoulder-surfing bystander), the person that wears the HMD is furthermore not able to perceive his or her environment, thus being easily exploitable [George et al. 2017].

We believe that eye-tracking and especially gaze-based authentication methods can solve this problem of authentication in VR to a great extent. Currently, more and more HMDs are released to the market that include a built-in eye-tracking-system (e. g., HTC Vive Pro Eye[1, 2] or Pico Neo 2 Eye[3]). Gaze-based authentication is also favorable from a security perspective, as the eyes of a user in VR are covered by the HMD and not visible from the outside, reducing the potential attack vector to a minimum (e. g., mimicry attacks) [Kumar et al. 2007].

Instead of employing the traditional, knowledge-based authentication methods in VR, we argue to focus on the utilization of gaze-based behavioral biometric authentication methods. The reason lies within the unique benefit of behavioral biometrics to allow implicit authentication. This type of authentication does not interrupt the interaction of a user with a VR system due to the need of performing an authentication, as it is performed throughout actions, the user "would carry out anyway" [Jakobsson et al. 2009]. Behavioral biometrics share this feature inherently with functional biometrics [Liebers and Schneegass 2020]. The required visual stimuli can ideally be seamlessly integrated into the virtual environment, making the gaze-based authentication unnoticeable and more secure than current approaches.

2 AUTHENTICATION IN VR

Traditional authentication methods such as PINs, passwords or pattern locks have been implemented for virtual reality applications [Yu et al. 2016]. Only a very few authentication methods were specifically designed for usage in VR and take advantage of the possibilities [John et al. 2018; Khamis et al. 2018; Lohr et al. 2018].

To fulfill the requirements for secure and usable authentication in VR, behavioral biometrics can be employed. Mustafa et al. have created a system that classifies motion sensor data from the HMD, reporting an equal error rate of 7% [Mustafa et al. 2018]. Similarly, Shen et al. implemented a gait recognition system based upon the HMD's sensors [Shen et al. 2018]. Pfeuffer et al. utilized body motion and body relations by letting the users of the HMD perform tasks such as as pointing, grabbing, walking, or typing [Pfeuffer et al. 2019]. Kupin et al. created a similar approach by imposing a task upon the user such as throwing a ball and comparing the trajectories of the pick-up, poising and throwing motion [Kupin et al. 2019].

ETRA '20 Adjunct, June 2–5, 2020, Stuttgart, Germany

ACM ISBN 978-1-4503-7135-3/20/06.
https://doi.org/10.1145/3379157.3391421

[1] https://www.vive.com/de/product/vive-pro-eye/
[2] https://pupil-labs.com/products/vr-ar/
[3] https://www.pico-interactive.com/us/neo2.html

In contrast to authentication methods that are especially suited for VR, authentication methods based on gaze characteristics are well established. The approaches range from the classification of saccades [Rigas et al. 2016] and smooth pursuit movements [Khamis et al. 2018] to the triggering of reflexive eye movements [Sluganovic et al. 2016] and pupil characteristics [Yano et al. 2013]. Traditional gaze-based password entry is also a possibility [Kumar et al. 2007].

3 CONCEPT

To leverage security in virtual reality applications, we argue for fully utilizing the benefits of behavioral gaze-based biometrics in virtual environments. We envision a continuous, implicit authentication system based upon the HMD with no external requirements. Several objects and elements within a virtual environment can be used as a stimulus to enable the authentication.

Dynamically moving elements. When an object in virtual reality is intended to catch the attention of a user, gaze guidance techniques are often employed to make the user focus on the targeted object [Grogorick et al. 2017]. Using a gaze guidance technique such as dynamic stimulus positioning, we can induce smooth pursuits and saccadic eye movements in a controlled manner that can be classified based upon user specific characteristics usable for authentication [Rigas et al. 2018].

Interaction. Similar to selecting an object with a mouse in a traditional computing environment, an interaction with a virtual object is preceded by a saccade and a fixation. This opens up the opportunity to analyze the gaze behavior of the saccade and fixation for user specific information, from which an assumption about the identity might be derived. Moreover, the interaction with elements and the environment is fully controllable in VR. When a user examines a virtual object in detail, vestibulo-ocular movements could be measured for specific characteristics. The abrupt presentation of new information in the field of view can trigger reflexive eye movements [Sluganovic et al. 2016]. Also, a variation of the brightness of the virtual environment can lead to a controlled change in pupil diameter [Yano et al. 2013]. Furthermore, we envision that some unique metrics can be gathered from the negative effects of the vergence accomodation conflict [Kramida 2015] especially in connection with the pupil diameter and the imposed fatigue.

4 CONCLUSION

As authentication in virtual reality (VR) is a difficult topic due to the limited input modalities that common hand-held controllers provide, we give an overview of usable elements in a virtual environment that can serve as a stimulus. Thereby we seek to incorporate well-understood gaze-based authentication methods in VR by utilizing those elements, enabling a secure and usable process of authentication, that ideally is implicit. Therefore we provide a research direction to leverage usable authentication methods.

ACKNOWLEDGMENTS

The presented work was funded by the German Research Foundation (DFG) under project no. 426052422.

REFERENCES

Ceenu George, 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. NDSS.

Steve Grogorick, Michael Stengel, Elmar Eisemann, and Marcus Magnor. 2017. Subtle Gaze Guidance for Immersive Environments. In *Proceedings of the ACM Symposium on Applied Perception* (Cottbus, Germany) *(SAP '17)*. Association for Computing Machinery, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/3119881.3119890

Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. 2009. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*. 9–9.

Brendan John, Pallavi Raiturkar, Arunava Banerjee, and Eakta Jain. 2018. An evaluation of pupillary light response models for 2D screens and VR HMDs. In *Proceedings of the 24th ACM Symposium on Virtual Reality Software and Technology*. 1–11.

Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. 2018. VRpursuits: interaction in virtual reality using smooth pursuit eye movements. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces*. 1–8.

Gregory Kramida. 2015. Resolving the vergence-accommodation conflict in head-mounted displays. *IEEE transactions on visualization and computer graphics* 22, 7 (2015), 1912–1931.

Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-Surfing by Using Gaze-Based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. ACM, New York, NY, USA, 13–19. https://doi.org/10.1145/1280680.1280683

Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. Task-driven biometric authentication of users in virtual reality (VR) environments. In *International Conference on Multimedia Modeling*. Springer, 55–67.

Jonathan Liebers and Stefan Schneegass. 2020. Introducing Functional Biometrics: Using Body-Reflections as a Novel Class of Biometric Authentication Systems. In *CHI '20 Extended Abstracts on Human Factors in Computing Systems* (Honolulu, HI, USA). ACM, New York, NY, USA. https://doi.org/10.1145/3334480.3383059

Dillon Lohr, Samuel-Hunter Berndt, and Oleg Komogortsev. 2018. An Implementation of Eye Movement-Driven Biometrics in Virtual Reality. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research and Applications* (Warsaw, Poland) *(ETRA '18)*. Association for Computing Machinery, New York, NY, USA, Article 98, 3 pages. https://doi.org/10.1145/3204493.3208333

Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. 2018. Unsure How to Authenticate on Your VR Headset? Come on, Use Your Head!. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics*. 23–30.

Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. ACM, New York, NY, USA. https://doi.org/10.1145/3290605.3300340

Ioannis Rigas, Lee Friedman, and Oleg Komogortsev. 2018. Study of an extensive set of eye movement features: Extraction methods and statistical analysis. *Journal of Eye Movement Research* 11, 1 (2018), 3.

Ioannis Rigas, Oleg Komogortsev, and Reza Shadmehr. 2016. Biometric recognition via eye movements: Saccadic vigor and acceleration cues. *ACM Transactions on Applied Perception (TAP)* 13, 2 (2016), 1–21.

Yiran Shen, Hongkai Wen, Chengwen Luo, Weitao Xu, Tao Zhang, Wen Hu, and Daniela Rus. 2018. GaitLock: Protect virtual and augmented reality headsets using gait. *IEEE Transactions on Dependable and Secure Computing* 16, 3 (2018), 484–497.

Ivo Sluganovic, Marc Roeschlin, Kasper B Rasmussen, and Ivan Martinovic. 2016. Using reflexive eye movements for fast challenge-response authentication. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 1056–1067.

Vitor Yano, Lee Luan Ling, and Alessandro Zimmer. 2013. Biometric Authentication Based on Pupillary Light Reflex Using Neural Networks. In *International Conference Image Analysis and Recognition*. Springer, 89–96.

Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. 2016. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*. IEEE, 458–460.