Introduction to Authentication using Behavioral Biometrics

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

Uwe Gruenefeld
University of Duisburg-Essen
Essen, Germany
uwe.gruenefeld@uni-due.de

Daniel Buschek
University of Bayreuth
Bayreuth, Germany
daniel.buschek@uni-bayreuth.de

Florian Alt
Bundeswehr University Munich
Munich, Germany
florian.alt@unibw.de

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

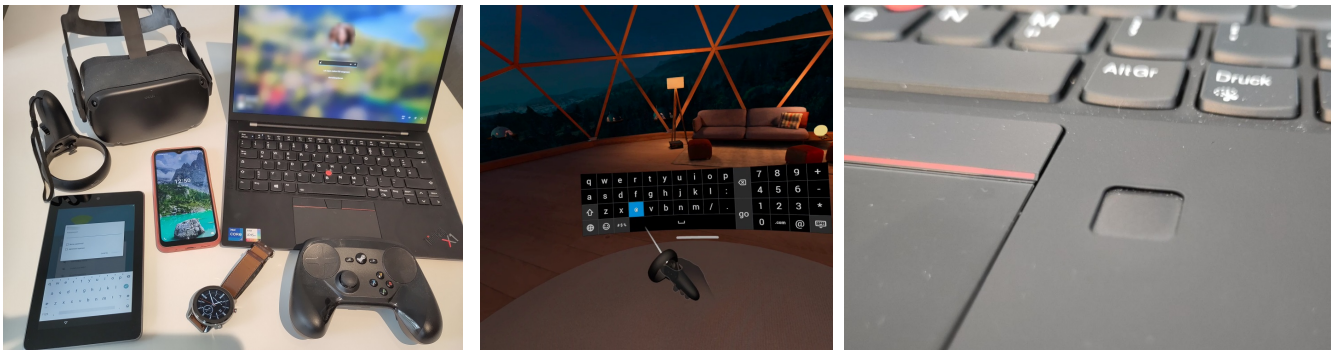

Figure 1: An increasing number of devices can benefit from knowing the user's identity to allow for adaptation and personalization (left). While passwords still dominate for over 60 years now, they fall short in terms of usability and user experience, as they increasingly overwhelm users mentally, and entering them on many devices is cumbersome, for example, in virtual reality (middle). Behavioral Biometrics is becoming a viable alternative to traditional authentication schemes and supersedes their counterparts (e.g., traditional biometrics such as fingerprint scanners (right)) in terms of user experience and usability as they often do not need explicit interactions but are implicit instead, allowing for continuous authentication.

ABSTRACT

The trend of ubiquitous computing goes in parallel with ubiquitous authentication, as users must confirm their identity several times a day on their devices. Passwords are increasingly superseded by biometrics for their inherent drawbacks, and Behavioral Biometrics are particularly promising for increased usability and user experience. This course provides participants with an introduction to the overall topic, covering all phases of creating novel authentication schemes. We introduce important aspects of evaluating Behavioral Biometrics and provide an overview of technical machine-learning techniques in a hands-on session, inviting practitioners and researchers to extend their knowledge of Behavioral Biometrics.

CHI EA '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9422-2/23/04.
https://doi.org/10.1145/3544549.3574190

CCS CONCEPTS

• **Human-centered computing** → *HCI design and evaluation methods*; • **Security and privacy** → *Usability in security and privacy.*

KEYWORDS

human-computer interaction, usable security, authentication, identification, machine learning

ACM Reference Format:
Jonathan Liebers, Uwe Gruenefeld, Daniel Buschek, Florian Alt, and Stefan Schneegass. 2023. Introduction to Authentication using Behavioral Biometrics. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3544549.3574190

1 INTRODUCTION

With today's computing devices' ubiquity and their overall increasing number, the number of times a person has to prove their identity per day to a computing system is also ever-increasing. Proving one's identity to a computing system (i.e., the process of *authentication*) is critical to ensure security and data privacy on the device. Additionally, knowing the user's identity also allows for personalization and adaptation of the device; hence this information is almost always required in any computing system used by humans. Consequently,

the trend of "ubiquitous computing" demands "ubiquitous authentication" in everyday life as well.

Users who interact with a computing device do so by usually following a primary task. However, the execution of the primary task is often interrupted by a required explicit interaction demanded by the device from the user. For example, the task of sending a message on a smartphone to another person is interrupted by the lock screen that demands the entry of a Personal Identification Number (PIN) from the user after the smartphone is activated and before the message can be sent. Nevertheless, with each device, the process of authentication is subject to the device's sensing capabilities, which vary widely; for example, proving one's identity to a website displayed on a notebook is widely different compared to authenticating on a smartwatch, which offers different input modalities. Traditional biometrics (e.g., fingerprints) are often similar to PINs or passwords in terms of demanding user's explicit interactions, such as having them move their finger explicitly to a fingerprint scanner (cf., Figure 1). Behavioral Biometrics in contrast promises to ease this process as they often can be elicited in an implicit way from the user without the user having to actively deal with the authentication system (e.g., user's typing behavior on smartphones [3, 4], their interactions in virtual reality [5, 7–10], or gaze behavior [6]).

For over sixty years, passwords have been the primary method used for authentication. Yet, there exists a wide consensus that passwords are insecure, and users are increasingly overwhelmed by them [2]. As a consequence, alternative methods for user authentication moved into the focus of research, where particularly Behavioral Biometrics has become a viable alternative, as they are very well suited for implicit and continuous authentication, which bear unique quality attributes and promise an enhanced user experience and usability [2].

1.1 Unique Benefits of Behavioral Biometrics

Utilizing Behavioral Biometrics is particularly beneficial for two reasons. First, they allow for *implicit authentication*, which means that they are particularly well suited to detect their user's identity without demanding explicit actions from the user [2]. Instead, implicit authentication methods use behavioral characteristics of the interaction that users perform with regard to their primary task for authentication [2]. Thereby, they can ideally authenticate users without interruption seamlessly in the background [2]. This is practical for usability, as users do not have to invest time in interacting with the authentication process. It also benefits their user experience, as their primary task is not interrupted.

Second, as the device can implicitly sample the user's behavior, the device can authenticate the user continuously [14]. *Continuous Authentication* (CA) stands in contrast to static authentication, which is currently most often performed [14]. In static authentication, the device checks the user's identity at the beginning of a session and unlocks itself [14]. However, if another person starts using the device, it will remain unlocked for that person. Continuous authentication changes this security issue, as a continuous authentication system frequently checks the current user's identity implicitly based on their behavior. Thereby, the device can lock itself by recognizing that another person uses it, effectively increasing security over what static authentication can offer.

1.2 Scope of Course

We first provide the theoretical foundations of authentication, connected aspects, and terms concerning their utilization in intelligent user interfaces. We do so by pointing out their strengths and weaknesses to aspects connected to Human-Computer Interaction (HCI), such as their implications for usability, user experience, and the system's security. We furthermore point out key aspects to consider when creating novel academic works within the domain, which we underline with key elements elicited from the scientific community and provide guidance around typical pitfalls. Finally, we complete the course with an introduction to machine learning approaches for Behavioral Biometrics, covering the steps of data analysis, visualization, preprocessing, models, and metrics.

2 TARGET AUDIENCE

This course addresses researchers and practitioners working in usable security at the crossroads of HCI and human-centered security, who work on creating novel mechanisms for user authentication. While the course primarily provides insights into the complete workflow of creating a novel academic contribution to the field, we also address participants with previous experience, as we provide insights from a survey on Behavioral Biometrics among the scientific community that explains what aspects are most often valued and criticized in novel works, thus should be considered.

3 PREREQUISITES

This is a stand-alone course that does not build on another course. The participants should prepare themselves for the course in an appropriate way that is communicated beforehand, while we try to keep any overhead of preparations low. Programming knowledge in Python is recommended to participate in the hands-on session.

4 COURSE OVERVIEW

The course is divided into two parts that build on each other and last 75 minutes each. The first part includes:

Introduction & Foundations. We introduce the overall topic of authentication, covering aspects of user recognition such as behavioral biometric modalities and the modes of verification and identification, which are used to secure information and enable which personalization of computing devices. Here, we establish a relationship with intelligent user interfaces. Additionally, quality dimensions such as implicitness and continuity and their relevance for usability and user experience are outlined and discussed.

Evaluation & Metrics. We present insights into how to evaluate a novel academic work and discuss the associated metrics (e.g., FAR, FRR, EER, F1-Score) among balanced and unbalanced datasets. We also discuss pitfalls to be aware of when designing a behavioral biometric authentication scheme. Additionally, the issues connected to open-set and closed-set identification are highlighted, and their implications on the employed machine learning models.

Academic perspective. We conclude the first part with insights from a survey conducted in 2022 among the scientific community on the key questions, what is most commonly valued and criticized in novel academic work. We also highlight indicators of rigor. Examples include study design and variables, the reported metrics, and an appropriate split of training, testing and validation data.

The second part of the course is the hands-on session. We provide an application that enables participants to capture behavioral biometric data on stand-alone virtual reality head-mounted displays [7, 8]. Participants' data is made available to participants in real time through a shared database. We will provide approximately 15 Meta Quest 2 devices with the application installed so that participants can elicit their own data that they will then explore and build an authentication system around, which is then evaluated.

Data elicitation. In the beginning, we will give participants the opportunity to capture their own behavioral biometric data on a virtual reality head-mounted display that we provide. Participation in this step is voluntary as we will additionally provide a backup dataset that is supported by a video of the elicitation.

Data Analytics & Visualization. Next, we provide Jupyter notebook templates in an easy-to-use environment (e.g., Google Colab or Jupyter) to participants that fetch data from the shared database. We introduce participants to common data exploration techniques, such as descriptive statistics on features and visualization techniques. Here, we use Python libraries such as pandas, matplotlib, and scikit-learn. We will focus on finding anomalies within the data that might result in side effects for evaluating a behavioral biometric system.

Machine Learning & Evaluation Metrics. Finally, we will guide participants in creating a machine-learning algorithm to enable the authentication process. We will focus on algorithms that are quick in execution (e.g., Random Forest) and are explainable to a certain degree. In the last step, we will show how to generate the standard metrics to be reported on in an academic publication, as well as any relevant previous preprocessing steps (e.g., trimming and normalization).

Course Format. The course is planned as an in-person event at CHI 2023, with a theoretical and practical part. Participants are encouraged to bring a notebook to participate in the practical parts and may have to install certain operating-system independent tools beforehand. Further information will be distributed in advance.

5 PRACTICAL WORK

In the practical hands-on session, we will enable participants to take part in the complete process of creating an authentication system using behavioral biometrics. The process requires three steps: i) data elicitation, ii) data exploration and visualization, and iii) the creation of an authentication system with the evaluation through key metrics.

For this purpose, we use head-mounted displays and a virtual reality application, which we provide and which makes the data recorded in the course accessible in real-time for all other participants. Providing the data is, of course, a voluntary action to participate in. The head-mounted displays will be shared in small groups of participants (approx. 3 ± 1 person). Additionally, we will provide a backup dataset.

The data collected in this way will be used in the next step by the participants to develop an authentication mechanism. In this process, Python will be used, including the common stack of scientific software libraries. We guide this process by supporting the participants and providing appropriate templates to embed their code.

6 RESOURCES

This course's informative course materials (slides, manuscripts, Jupyter notebooks, and the data) will be made available to participants electronically under a free license. Distributed source code used during the course will also be provided under the MIT License. For the practical work, this course requires a stable WiFi connection for the instructors and participants as well as a room with a free and even space of at minimum 3×3 meters. Participants ideally bring a notebook to participate in the hands-on session.

7 INSTRUCTORS

Jonathan Liebers obtained a bachelor's and master's degree in computer science at the University of Duisburg-Essen. He currently is a Ph.D. student at the Human-Computer Interaction Group, University of Duisburg-Essen and his research interest lies mainly within the field of usable security and implicit identification, particularly XR [7–9].

Uwe Gruenefeld is a postdoc researcher in human-computer interaction at the University of Duisburg-Essen, Germany. During his fellowship-funded Ph.D. at the University of Oldenburg, he focused on AR and VR technology. After his Ph.D., his research centered around cross-reality systems, usable security, and privacy. Uwe has been a tutorial and workshop chair for different conferences and organized various tutorials and workshops. He co-authored various publications within the field of usable security [1, 7–9, 11].

Daniel Buschek leads a research group at the University of Bayreuth, Germany. In his research, he combines HCI and AI to create user interfaces that enable people to use digital technology in more effective, efficient, expressive, explainable, and secure ways. His published research includes work on behavioral biometrics for mobile devices and VR. He has given a course on Intelligent User Interfaces at CHI'21 [13].

Florian Alt is a professor for Usable Security and Privacy at the Research Institute CODE (University of the Bundeswehr, Munich). Florian looks at the role of humans in security-critical systems, focusing on topics related to behavioral biometrics, physiological security, and usable security in novel application areas, such as smart homes and VR. Florian was a subcommittee chair for CHI'20 and CHI'21. He has previously run workshops and courses in CHI'21 [12].

Stefan Schneegass is an assistant professor of human-computer interaction at the University of Duisburg-Essen. His research interests include the crossroads of HCI and ubiquitous computing, particularly the development of implicit authentication mechanisms. Schneegass received a Ph.D. in computer science from the University of Stuttgart, Germany.

ACKNOWLEDGMENTS

This work was supported by the German Research Foundation (DFG) under Grant Nr. 426052422.

REFERENCES

[1] Yasmeen Abdrabou, Sheikh Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Makela, Stefan Schneegass, and Florian Alt. 2022. Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*, Paolo Bottoni and

Emanuele Panizzi (Eds.). ACM, New York, NY, USA, 1–9. https://doi.org/10.1145/3531073.3531106

[2] Florian Alt and Stefan Schneegass. 2022. Beyond Passwords—Challenges and Opportunities of Future Authentication. *IEEE Security & Privacy* 20, 1 (2022), 82–86. https://doi.org/10.1109/MSEC.2021.3127459

[3] Daniel Buschek, Benjamin Bisinger, and Florian Alt. 2018. ResearchIME: A Mobile Keyboard Application for Studying Free Typing Behaviour in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Regan Mandryk, Mark Hancock, Mark Perry, and Anna Cox (Eds.). ACM, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173829

[4] Daniel Buschek, Alexander de Luca, and Florian Alt. 2015. Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1393–1402. https://doi.org/10.1145/2702123.2702252

[5] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Henri Schmidt, Marinus Burger, Florian Alt, and Heinrich Hussmann. 2017. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Proceedings 2017 Workshop on Usable Security*. Internet Society, San Diego, CA, USA. https://doi.org/10.14722/usec.2017.23028

[6] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–21. https://doi.org/10.1145/3313831.3376840

[7] Jonathan Liebers, Mark Abdelaziz, Lukas Mecke, Alia Saad, Jonas Auda, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445528

[8] Jonathan Liebers, Sascha Brockel, Uwe Gruenefeld, and Stefan Schneegass. 2022. Identifying Users by Their Hand Tracking Data in Augmented and Virtual Reality. *International Journal of Human–Computer Interaction* 0, 0 (2022), 1–16. https://doi.org/10.1080/10447318.2022.2120845 arXiv:https://doi.org/10.1080/10447318.2022.2120845

[9] Jonathan Liebers, Patrick Horn, Christian Burschik, Uwe Gruenefeld, and Stefan Schneegass. 2021. Using Gaze Behavior and Head Orientation for Implicit Identification in Virtual Reality. In *Proceedings of the 27th ACM Symposium on Virtual Reality Software and Technology (VRST '21)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3489849.3489880

[10] 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 (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300340

[11] Alia Saad, Jonathan Liebers, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding Bystanders' Tendency to Shoulder Surf Smartphones Using 360-degree Videos in Virtual Reality. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*. ACM, New York, NY, USA, 1–8. https://doi.org/10.1145/3447526.3472058

[12] Albrecht Schmidt, Florian Alt, and Ville Mäkelä. 2021. Evaluation in Human-Computer Interaction – Beyond Lab Studies. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–4. https://doi.org/10.1145/3411763.3445022

[13] Albrecht Schmidt, Sven Mayer, and Daniel Buschek. 2021. Introduction to Intelligent User Interfaces. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 1–4. https://doi.org/10.1145/3411763.3445021

[14] Issa Traoré and Ahmed Awad E. Ahmed. 2012. Introduction to Continuous Authentication. In *Continuous Authentication Using Biometrics: Data, Models, and Metrics*, Issa Traore and Ahmed Awad E. Ahmed (Eds.). IGI Global, Hershey, PA, USA, 1–22. https://doi.org/10.4018/978-1-61350-129-0.ch001