Knowledge-driven Biometric Authentication in Virtual Reality

Florian Mathis
University of Glasgow
Glasgow, United Kingdom
florian.mathis@glasgow.ac.uk

Mohamed Khamis
University of Glasgow
Glasgow, United Kingdom
mohamed.khamis@glasgow.ac.uk

Hassan Ismail Fawaz
University of Haute-Alsace
Mulhouse, France
hassan.ismail-fawaz@uha.fr

Abstract

With the increasing adoption of virtual reality (VR) in public spaces, protecting users from observation attacks is becoming essential to prevent attackers from accessing context-sensitive data or performing malicious payment transactions in VR. In this work, we propose RubikBiom, a knowledge-driven behavioural biometric authentication scheme for authentication in VR. We show that hand movement patterns performed during interactions with a knowledge-based authentication scheme (e.g., when entering a PIN) can be leveraged to establish an additional security layer. Based on a dataset gathered in a lab study with 23 participants, we show that knowledge-driven behavioural biometric authentication increases security in an unobtrusive way. We achieve an accuracy of up to 98.91% by applying a Fully Convolutional Network (FCN) on 32 authentications per subject. Our results pave the way for further investigations towards knowledge-driven behavioural biometric authentication in VR.

Author Keywords
Authentication; Virtual Reality; Deep Learning

CCS Concepts
- Human-centered computing → Human computer interaction (HCI); - Security and privacy → Authentication;
Introduction
Virtual reality (VR) is becoming more and more popular due to its affordability and portability. Untethered head-mounted displays (HMDs) such as the Oculus Quest [32] contribute to an increasing interest in VR across a larger population. However, new interaction methods present opportunities for attackers as non-technology savvy users might be overwhelmed by such new technologies and underestimate possible threats.

This is crucial in situations where users have to authenticate to access confidential data or enter credentials such as PINs [20] to perform transactions. Users are often unaware of bystanders [10], especially whilst being immersed in VR [14, 27], who were shown to be able to infer the VR user’s input (e.g., PINs) [14, 16, 40]. As researchers and practitioners in VR are very keen in creating immersive and mature technologies to increase users’ experience and embed such novel technologies into our mundane life [18, 36], research to protect actual users against attacks (e.g., observation attacks, guessing attacks, or video attacks where attackers record and play back user’s authentication [8, 15]) is still limited. RubikBiom protects users from such attacks even if attackers have access to the correct secret as it provides users with an additional security layer.

To our knowledge, RubikBiom is the first exploration into the use of knowledge-driven behavioural biometric authentication in VR (Fig. 1) in combination with deep learning (DL). RubikBiom makes successful attacks less common as an attacker has to a) derive the secret a user entered and b) precisely replicate the user’s behaviour.

Our contribution is two-fold. First, we show that human behavioural biometrics collected during knowledge-driven natural asymmetrical bimanual cooperation [19] are promising for establishing an additional security layer in VR by applying state-of-the-art deep learning architectures for time series classification (TSC) [21]. Second, we propose knowledge-driven behavioural biometric authentication, a novel promising direction for authentication in VR.

Background and Related Work
Knowledge-based Authentication in VR
Existing approaches to improve authentication in VR rely on knowledge-based authentication such as entering a PIN or pattern [12, 15, 17, 40]. However, at the point where attackers derive entire secrets based on observations, they can access private data or make them publicly available. George et al. [17] investigated the direct transfer of well-established authentication schemes into VR. Their study showed that attackers could derive 18% of users' PINs and patterns through observations. Similarly, Yu et al. [40] highlighted that most people can guess the input from watching videos showing a user authenticating in VR.

Behavioural Biometric Authentication in VR
Recent research shows that it is possible to improve security of VR users by tracking users’ movements when performing natural goal-oriented tasks in VR environments. For instance, Kupin et al. [25] showed that it is possible to authenticate users solely on throwing a ball within the virtual environment. In their pilot study they achieved a matching accuracy of up to 92.86%. Similarly, Yi et al. [39] leveraged head movement patterns for authentication in VR and achieved an authentication accuracy of 92%. However, Mustafa et al. [28] recommend to use such functionality as an added layer of security in security-sensitive VR applications as pure behavioural biometrics might not be feasible in a large scale setting. This is inline with findings from Pfeuffer et al. [29] who highlight the logarithmic decrease of accuracy with increasing group size, thus, making behavioural biometrics on its own not feasible for authentication in VR.
Based on findings and lessons learnt from previous works [12, 15, 17, 25, 28, 29, 39, 40], we focus on the combination of a knowledge-based authentication scheme and corresponding human behavioural biometrics to increase security against observations. We apply DL on users’ movement patterns during their knowledge-based authentication to make authentications more resistant to attacks (e.g., observation attacks, guessing attacks) in an unobtrusive way.

**Concept**

To evaluate the suitability of human behavioural biometrics collected during knowledge-based authentication, we developed RubikBiom, a novel authentication scheme in VR (Fig. 2). RubikBiom is based on Guiard’s kinematic chain model [19] that incorporates human asymmetrical bimanual cooperation. This means that user’s non-dominant hand controls the pose of RubikBiom and user’s dominant hand performs the pointing and selection. The benefits of applying Guiard’s kinematic chain model are three-fold. It is a) a natural way of two-handed interaction [6, 22] and takes human skills into account that are already in place [22], b) adds complexity to observation attacks as attackers have to observe multiple interactions simultaneously [9], and c) allows leveraging human behavioural biometrics such as hand movements for authentication in VR. Users enter a 4-digit RubikBiom PIN by tapping on the corresponding digits and confirming the selection by pressing the HTC VIVE trigger button. Each PIN consists of 4 digit/surface combinations, e.g., 1 (green), 2 (white), 1 (red), 8 (white).

**User study**

The aim of this study is to investigate the feasibility of human behavioural biometrics (e.g., hand movements) for knowledge-driven authentication in VR and to collect these for the following evaluation.

**Demographics**

We collected hand movements from 23 participants (13 females, 10 males) aged between 18 and 54 years ($\mu=27.65$, $\sigma=8.26$) within a lab study. Participants were recruited via internal university mailing lists. Most of them were students or staff members with a technical background. Half of our participants (52%) used VR at least once.

**Data Collection**

During each authentication, we capture feature information regarding the Cartesian values ($x, y, z$) and Unity’s Quaternion (i.e., rotations in 3D space) [33] of users’ dominant (DH) and non-dominant hand (N-DH).

**Procedure**

We introduced participants to RubikBiom and ran training sessions before actually tracking their movements. Participants then entered 12 RubikBiom PINs. All participants entered the same set of RubikBiom PINs four times each (4 repetitions $\times$ 12 PINs = 48 authentications). We highlighted the PINs the participants have to enter directly on RubikBiom (Fig. 3). Participants were compensated by £8.

**Apparatus**

We used Unity C# for the implementation of RubikBiom and data collection. As head-mounted display, we used an HTC VIVE ($2160 \times 1200$ px) and SteamVR Plugin for controller communication. For applying the deep learning architecture, we built upon Ismail Fawaz et al.’s implementation [21] using Keras 2.2.4 [7] based on the TensorFlow backend.

**Data Processing**

In total, we collected human behavioural biometrics from 23 participants who performed 48 trials each, making it a total of 1104 authentications. We pre-processed our dataset and splitted it into a training (36 authentications, 75%) and a test dataset (12 authentications, 25%) for each user [24].
Table 1: We calculated the top-1 classification accuracies. A **Fully Convolutional Network (FCN)** and a **Residual Neural Network (ResNet)** achieved the highest accuracies with 98.91% and 98.55%, respectively. **Bold** and **italic** denote category 1st and 2nd best, respectively.

**Metrics**
Similar to previous work [29], we report top-1 classification accuracies (i.e., number of correct classifications divided by the total number). All our datasets are balanced as the number of authentications is the same for each class (user). An architecture that predicts the outcome solely based on random guesses would achieve an accuracy of 4.35% (1 out of 23 users).

**Results**
Table 1 shows the top-1 classification accuracies of the six deep learning architectures that we applied on our multivariate datasets. A **Fully Convolutional Network (FCN)** [35] achieved overall the best accuracy (98.91%) and achieved the highest accuracy when leveraging users’ dominant hand position + rotation together with users’ non-dominant hand position + rotation. Increasing the number of dimensions results in more accurate results, and thus, avoids false negatives. Note that false negatives can only happen in **RubikBiom** when a user entered the correct PIN in a step before.
The number of dimensions we use to train our models varies directly with the classification accuracy. This suggests that leveraging more dimensions results in higher classification accuracies. The graph depicts the direct variation across all DL architectures. All reported accuracies are mean values of clustered accuracies in Table 1.

When training a model on one feature (e.g., DH rotation) we achieved accuracies between 31.20% and 89.86% whereas two features (e.g, DH position and rotation) resulted in accuracies of 67.40% to 98.19%. Leveraging four features (e.g., DH + N-DH position and rotation) resulted in even higher accuracies of 88.41% to 98.91%. Figure 5 shows these increases of accuracies that follow a direct variation.

### Lessons Learnt and Discussion

Following a knowledge-driven behavioural biometric approach for user authentication in VR yielded promising results with classification accuracies up to 98.91% (N=23). This is noticeably higher than in previous works with a matching accuracy of 92.86% (N=14) [25] and 63.55% (N=22) [29]. This highlights the security benefits of applying DL on human behavioural biometrics collected during knowledge-driven authentication where a user enters their 4-digit PIN on RubikBiom (Figure 2). As shown in Table 1 and Fig. 5, multi-feature datasets (e.g., DH Position + Rotation) result in more accurate top-1 classification accuracies compared to single-feature datasets (e.g., DH position).

### The Future of Authentication in VR

Previous research transferred knowledge-based authentication schemes into VR [15, 16, 40] or leveraged head movements [2, 28], hand movements [2, 25, 29], or gait signatures [31] for authentication in VR. In the case of behavioural biometric authentication [2, 25, 28, 29, 31], the direction is quite clear as researchers try to eliminate explicit authentication. This is mainly attributed to the fact that authentication is a secondary task users have to go through (e.g., unlocking a device) before being able to perform a main task (e.g., interacting in VR) [30]. However, it has been argued that behaviour biometrics should be used to enhance knowledge-based schemes for VR rather than replace them [28, 29], especially because behaviour might not be unique for a large group size.

Although using fingerprints for authentication found its application (e.g., to unlock a smart phone), they remain a challenge as they cannot be changed and there are fears about how this data could be abused [13, 26]. Following a knowledge-driven behavioural biometric authentication approach as presented with RubikBiom protects users from...
Attackers in a seamless and unobtrusive way in different contexts. Note that fingerprints, facial recognition, or voice patterns might not work in situations where users are exposed to high humidity, different lighting conditions, or noisy environments [1, 4, 5]. For these reasons, it is important to investigate the potential of knowledge-driven behavioural biometric authentication. In particular, future authentication systems could leverage additional metrics (e.g., eye movements) to expand the input space for authentication in VR.

Adaptive Authentication
RubikBiom's aim is to make authentication more secure against attacks (e.g., observation attacks, guessing attacks, video attacks) by introducing an additional human behavioural security layer. However, protecting users with an additional security layer may affect usability. Previous research highlighted the importance of incorporating contextual factors such as different environments and/or human factors when designing and developing authentication schemes [23]. A knowledge-driven behavioural biometric authentication scheme such as RubikBiom can deactivate the additional behavioural biometric security layer easily in a context where observation attacks might not occur as frequent as in public spaces (e.g., at home). This raises further interesting questions, for instance: in which contexts do users prefer such an additional security layer?

In future work we plan to investigate long-term usage of knowledge-driven biometric authentication schemes to investigate users’ usage of such a system and investigate how a knowledge-driven biometric approach affects usability and security in a real-world use case with multiple authentications over time. We believe that knowledge-driven biometric authentication systems are promising for future adaptive authentication schemes that contribute to more secure systems without negatively affecting users’ experience.

Limitations
Our results are based on a user study that incorporates RubikBiom and requires two-hand interactions. Two-handed interaction might not be suitable for users with motor disabilities. To work towards hands-free interactions that are accessible for a larger population, alternative knowledge-driven biometric authentication schemes could train models based on eye or head movements.

Moreover, we experimented with a time series length of 13 time stamps $\times 50$ ms each time stamp $= 0.65$ s. Higher frequencies might affect architectures’ performance and result in even higher classification accuracies [38]. Yet, leveraging longer time series for user classification implies that we have to rely on longer authentication times. Authentication is perceived to be a secondary task and should therefore be fast and effortless [30]. Follow-up work could experiment with different time series lengths to study its effect on classification accuracy.

Conclusion
In this paper, we introduced RubikBiom, a knowledge-driven biometric authentication scheme for user authentication in VR. We collected human behavioural biometrics from 23 participants and applied current state-of-the-art deep learning architectures for time series classification. We trained 56 models on nine different features and six deep learning architectures. We found that a Fully Convolutional Network (FCN) is the most accurate architecture with a classification accuracy of up to 98.91%. Our results provide first insights into applying deep learning for time series classification within the context of authentication in VR. We conclude that the use of human behavioural biometrics greatly enhances the security in a seamless and unobtrusive way and introduces a new direction for future authentication schemes in VR.
REFERENCES


   https://www.oculus.com/quest/

   https://docs.unity3d.com/Manual/QuaternionAndEulerRotationsInUnity.html

Recognition Letters 119 (2019), 3 – 11. DOI:
http://dx.doi.org/https://doi.org/10.1016/j.patrec.2018.02.010 Deep
Learning for Pattern Recognition.

classification from scratch with deep neural networks:
A strong baseline. In 2017 International Joint
Conference on Neural Networks (IJCNN). 1578–1585. DOI:
http://dx.doi.org/10.1109/IJCNN.2017.7966039

PlaneVR: Social Acceptability of Virtual Reality
CHI Conference on Human Factors in Computing
Systems (CHI ’19). ACM, New York, NY, USA, Article
80, 14 pages. DOI:
http://dx.doi.org/10.1145/3290605.3300310

[37] QIANG YANG and XINDONG WU. 2006. 10
CHALLENGING PROBLEMS IN DATA MINING
RESEARCH. International Journal of Information
Technology & Decision Making 05, 04 (2006), 597–604. DOI:
http://dx.doi.org/10.1142/S0219622006002258

[38] Shuochao Yao, Shaohan Hu, Yiran Zhao, Aston
Zhang, and Tarek Abdelzaher. 2017. DeepSense: A
Unified Deep Learning Framework for Time-Series
Mobile Sensing Data Processing. In Proceedings of
the 26th International Conference on World Wide Web
(WWW ’17). International World Wide Web
Conferences Steering Committee, Republic and
Canton of Geneva, Switzerland, 351–360. DOI:
http://dx.doi.org/10.1145/3038912.3052577

GlassGesture: Exploring head gesture interface of
smart glasses. In IEEE INFOCOM 2016 - The 35th
Annual IEEE International Conference on Computer
Communications. 1–9. DOI:
http://dx.doi.org/10.1109/INFOCOM.2016.7524542

exploration of usable authentication mechanisms for
virtual reality systems. In 2016 IEEE Asia Pacific
Conference on Circuits and Systems (APCCAS).
458–460. DOI:
http://dx.doi.org/10.1109/APCCAS.2016.7804002