Security of Input for Authentication in Extended Reality Environments

Tiago Martins Andrade, Jonathan Francis Roscoe, and Max Smith-Creasey

BT Applied Research, Adastral Park, UK
jonathan.roscoe@bt.com

Abstract. In this concept paper, we evaluate the security impact of accelerometer data for authentication in extended reality (XR) environments. Currently, there is a lack of authentication mechanisms in VR/XR environments. Most authentication is carried out through PINs and passwords which detracts from the immersive experience and inconveniences the user. Motion-based gesture techniques have recently shown potential in authentication users in VR environments. However, the state-of-the-art works have not considered the issue of VR being a visible activity which would yield gestures used to authenticate vulnerable to mimicry. We demonstrate how subtle changes to a user interface (UI) can increase the complexity and cost of eavesdropping on users in VR environments, and propose directions for future research. We call on the industry to acknowledge and design around the unique security challenges of authentication in VR.

Keywords: Virtual reality, Authentication, Application security, Biometrics (access control), Keystroke dynamics, Computer security.

1 Introduction

Virtual reality (VR) and extended reality (XR) systems are very quickly becoming a mainstream and powerful technology, with the market expected to reach a total value of almost 300 billion US dollars in 2024 [1]. Whilst the use cases for VR/XR technologies thus far have largely been recreational there are developments in applications for VR headsets that require a level of security (such as virtual security operations centres (VSOCs) [5]). Such environments provide access to privileged information and therefore need a stringent level of authentication to keep non-authorised users out of the system. Insufficient authentication and authorisation mechanisms within a secure VR environment could have significant implications for operational security.

In order to protect against use from non-authorised users, many systems use authentication techniques such as passwords in which a user must use Bluetooth-connected controllers to input their password into a virtual keyboard or follow specific steps to unlock certain content. However, if the system has been compromised and the attacker is able to store all user movements, it's possible to trace all user steps one by one in a simulated environment within VR/XR. For example, if the user is writing down a password using a virtual keyboard, by mimicking all user movements and since the virtual keyboard is static, it's possible to extract the exact password and gain unauthorized access.

Users of XR are particularly vulnerable to eavesdropping on interactions due to their lack of awareness of their surroundings. There is a potential approach to attacks from visual observation as well as captured accelerometer data that could lead to password mimicry.

This concept paper proposes and conducts an investigation into the level of gesture robustness and the possibility of obfuscating that data from a mimicry attack with simple UI changes. We compare different approaches for the virtual keyboards (original layout, control layout, adjusted layout and randomised layout). We hypothesise that the randomisation of the entire keyboard layout will degrade the usefulness of the accelerometer data extracted from user movements.

1.1 Related Work

Most commonly, authentication is split into i) something the user *has*, ii) something the user *knows*, and iii) something the user *is*. The password remains the most common form of authentication today despite it often leaving users fighting against security for usability. Within the VR space, some authentication has used biometrics but the most prevalent form of authentication in VR systems today still only rely on the password [6]. However, some studies have found that the combination of knowledge *and* biometric information can yield better security [7]. The interaction with VR (such as the input of a password (or any text)) carries additional challenges because attackers that are able to collect the accelerometer data during input might be able to make inferences about the interaction [2].

Previous work has explored unconventional approaches to acquiring data such data surreptitiously, including human activity and video [8]. Consequently, collection of accelerometer data from a smartwatch or fitness wearable may be a viable attack mechanism for XR users[2]. Despite this research, there is a lack of investigation into the vulnerabilities such side-channels pose to user typing input (e.g.: a password) or possible solutions toward the mitigation of these side-channels.

2 Proposed Approach

2.1 General Idea

We can see from existing research that if a VR system or a wearable is accessed by an attacker that extracts the accelerometer data, that could allow the attacker to re-create activities [2]. Therefore, we hypothesize that slightly randomised changes (with differing levels of granularity) to the UI or 3D objects could be sufficient to obfuscate user actions on that data and at the same time not increase complexity or extra steps to the end user. Therefore, an experimental study to extract that information was conducted.

2.2 Implementation

To assess and collect user movements when interacting with a virtual keyboard, a VR application was created using Unreal Engine 4 [4]. The Head-Mounted Display (HMD) used in the experimental study was Oculus Quest connected to a computer by Oculus Link and the use of the Oculus Motion Controllers.

In the design process, to make Virtual Reality to be effective, it's important to fulfill the 3 illusions basic principles [9], to assure the user is immersed in the experience and all user perceptions match reality or at least the user expectations of an certain action/reaction. The 3 following illusions need to be in place are:

- **Place Illusion**: The feel of being in a virtual place, even though you know you are not there;
- **Plausibility Illusion**: Illusion of the perceived events to feel real for the user;
- **Body Ownership**: Your virtual body is connected to your body.

A simple virtual environment was created with a floor, a sky dome and default light/shadows. When the user starts the VR application, they are placed in the middle of that environment and presented 8 cubes with letters as shown in Figures 1, 2 and 3. This acts as a simplified keyboard where the user is tasked with writing a single word multiple times.

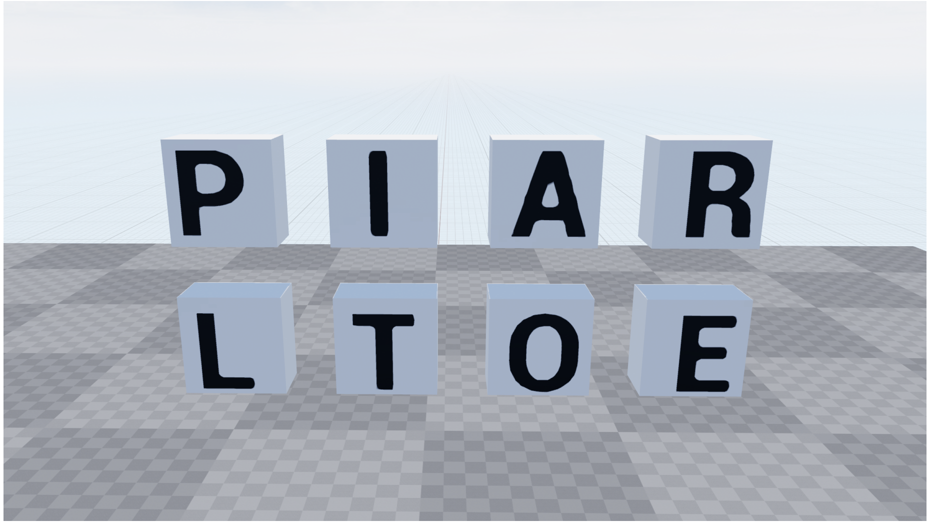

Fig. 1. Fixed key layout.

The keyboard keys can change shape, size and location during specific events to allow capture of the movements data to be analysed. There are 4 possible changes for the keyboard:

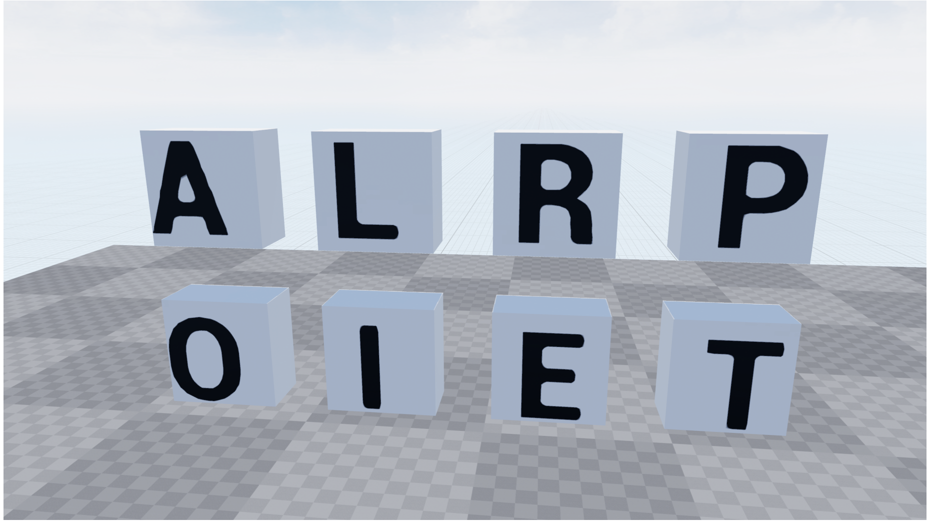

Fig. 2. Adjusted key layout.

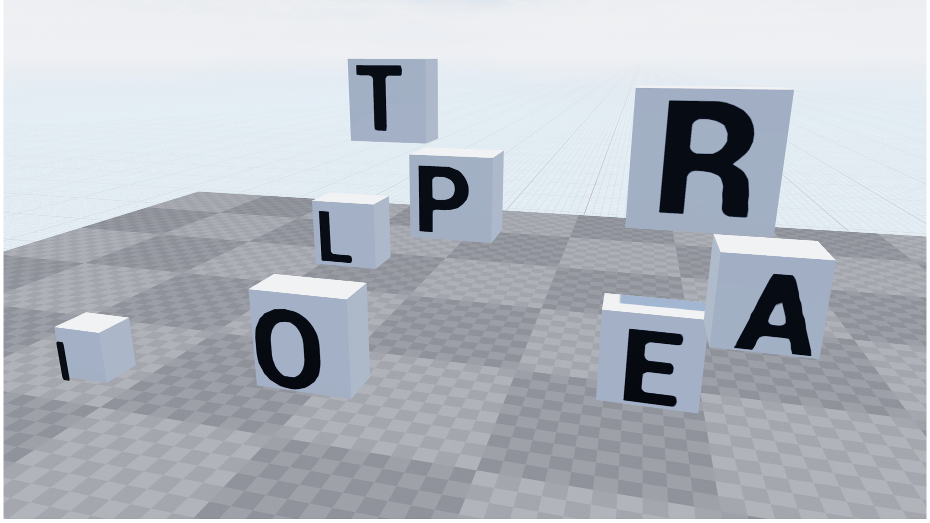

Fig. 3. Random key layout.

1. **Original layout**: This layout is static and predetermined by us (as shown in Fig. 1) and it will be always the same during sessions and for the entire experimental period.
2. **Control layout**: This layout is static and a full copy of the Original layout (as shown in Fig. 1). This will allow us to compare the same layout and verify if the movements will match (be the same) when using a static keyboard layout.
3. **Adjusted layout**: This layout is static but the keys will randomly change places at the beginning of the session for each user(as shown in Fig. 2).
4. **Randomised layout**: This layout is completely randomised. The key location, size and shape will randomly change at the beginning of each session and will be always different for each user (as shown in Fig. 3).

For each of these keyboard layouts, the user is tasked with entering the word 'PILOT' ten times. To do this, they point with their dominant hand at the appropriate cube and click the trigger button. Whilst the user is typing the word, the angular acceleration of the active controller is constantly logged.

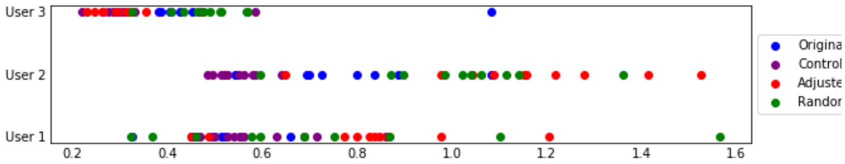

Fig. 4. Mean acceleration magnitude for different layouts, grouped by user.

3 Experimental Results & Discussion

To visualise result, we calculate the magnitude of angular acceleration measured during the authentication process. Angular acceleration is a three-dimensional vector of angular acceleration in rad/s2. We calculate magnitude (m) with:

$$m = \sqrt{x^2 + y^2 + z^2}. \tag{1}$$

Figure 4 visualises the magnitude of angular acceleration for all users, from which we can see the original and control layouts have significantly less total motion. In Figure 5 the mean magnitude for all samples is split by the input method and clearly shows the distribution is much greater for adjusted and randomised input methods.

It's notable that although there is a clear difference between the original and adjusted layouts, there is only a slight change in distribution for adjusted and randomised. This suggests that despite significant changes, the users are not making significant adjustments with their hand position, increasing the size of the field (i.e. utilising the 360° space, may enhance this).

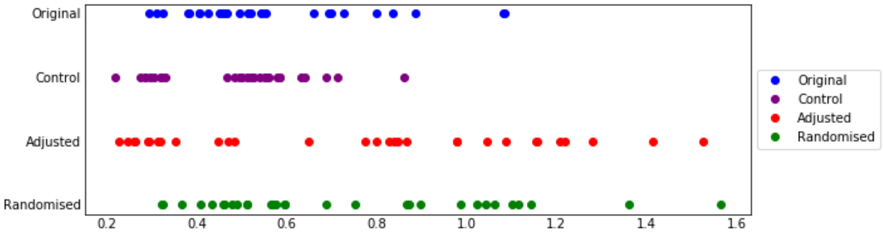

Fig. 5. Mean acceleration magnitude for all users, grouped by keyboard layout.

4 Conclusions & Future Work

Our initial results demonstrate that a UI with fixed layout results in a predictable range of motion, we posit that this indicates a potential for eavesdropping on an XR environment. We suggest that UI design should be carefully considered and may benefit from an element of randomness as standard practice.

The randomised layouts prevent a user from carrying out identical gestures and increasing the amount of motion when entering identical data, we propose a further range of adjustments to a virtual environment to introduce noise into eavesdropping attempts [3]. These can be tailored to have subtle impact on detectable user motion.

For the purposes of access, a further counter-measure could be the deployment of continuous authentication in XR environments that can constantly validate input from a user based on biometric characteristics. Another potential approach to mitigating some forms of eavesdropping is to increase user awareness of the external environment and potential malicious observers.

In future work, we wish to explore more fully the ability of a malicious observer to predict input with varying degrees of knowledge and conduct mimicry attacks, to understand the level of information extraction that may be achieved. With regards to the design of secure interfaces, we would like to experiment the spread of user input over a full 360° sphere.

References

1. Alsop, T.: Augmented reality (AR), virtual reality (VR), and mixed reality (MR) market size worldwide in 2021 and 2028 (Mar 2021), https://www.statista.com/statistics/591181/ global-augmented-virtual-reality-market-size/
2. Andrade, T.M., Smith-Creasey, M., Roscoe, J.F.: Discerning user activity in extended reality through side-channel accelerometer observations. In: 2020 IEEE International Conference on Intelligence and Security Informatics (ISI). pp. 1–3 (2020). https://doi.org/10.1109/ISI49825.2020.9280516
3. Andrade, T.M., Smith-Creasey, M., Roscoe, J.F.: Security method for extended reality applications (Patent GB22003313, January 2022)
4. Epic Games: Unreal engine (2019), https://www.unrealengine.com

5. Hercock, R.: Why AI is here to stay in cyber defence (Feb 2021), https://www.globalservices.bt.com/en/insights/blogs/why-ai-is-here-to-stay-in-cyber-defence
6. Jones, J.M., Duezguen, R., Mayer, P., Volkamer, M., Das, S.: A literature review on virtual reality authentication. In: International Symposium on Human Aspects of Information Security and Assurance. pp. 189–198. Springer (2021)
7. Mathis, F., Fawaz, H.I., Khamis, M.: Knowledge-driven biometric authentication in virtual reality. In: Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems. p. 1–10. CHI EA '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3334480.3382799, https://doi.org/10.1145/3334480.3382799
8. Roscoe, J.F., Smith-Creasey, M.: Unconventional mechanisms for biometric data acquisition via side-channels. In: 13th International Conference on Security of Information and Networks. pp. 1–4 (2020)
9. Slater, M.: Implicit Learning Through Embodiment in Immersive Virtual Reality, chap. 1, pp. 19–33. Springer Singapore, Singapore (2017). https://doi.org/10.1007/978-981-10-5490-7_2, https://doi.org/10.1007/978-981-10-5490-7$_2$