CueVR: Studying the Usability of Cue-based Authentication for Virtual Reality

Yomna Abdelrahman
yomna.abdelrahman@unibw.de
University of the Bundeswehr Munich
Munich, Germany

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

Pascal Knierim
pascal.knierim@unibw.de
University of the Bundeswehr Munich
Munich, Germany

Axel Kettler
A.Kettler@campus.lmu.de
University of the Bundeswehr Munich
Munich, Germany

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

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

ABSTRACT

Existing virtual reality (VR) authentication schemes are either slow or prone to observation attacks. We propose CueVR, a cue-based authentication scheme that is resilient against observation attacks by design since vital cues are randomly generated and only visible to the user experiencing the VR environment. We investigate three different input modalities through an in-depth usability study (N=20) and show that while authentication using CueVR is slower than the less secure baseline, it is faster than existing observation resilient cue-based schemes and VR schemes (4.151 s – 7.025 s to enter a 4-digit PIN). Our results also indicate that using the controllers' trackpad significantly outperforms input using mid-air gestures. We conclude by discussing how visual cues can enhance the security of VR authentication while maintaining high usability. Furthermore, we show how existing real-world authentication schemes combined with VR's unique characteristics can advance future VR authentication procedures.

CCS CONCEPTS

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

KEYWORDS

Authentication, Virtual Reality, Usable Security

ACM Reference Format:
Yomna Abdelrahman, Florian Mathis, Pascal Knierim, Axel Kettler, Florian Alt, and Mohamed Khamis. 2022. CueVR: Studying the Usability of Cue-based Authentication for Virtual Reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces (AVI 2022), June 6–10, 2022, Frascati, Rome, Italy*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3531073.3531092

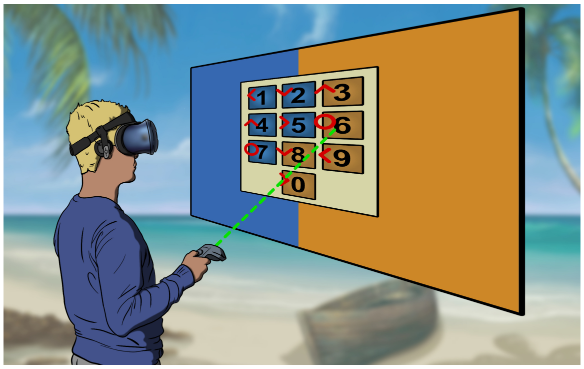


Figure 1: We report on CueVR, a cue-based VR authentication system. We investigated the performance when using two different input methods (i.e., Trackpad (B) and Motion Controller (C)) and used PIN entry (Laserpointer (A)) as our baseline. To enter "2" using the Trackpad, the user points towards the blue side (digits 1, 2, 4, 5, 7) and presses "down" on the Trackpad because the cue on "2" points downwards. For Motion Controller (C), "2" is entered by moving the controller downwards while pointing at the blue side.

1 INTRODUCTION

The growing number of immersive virtual reality (VR) applications in which users' identity needs to be verified underline the need for usable and secure authentication in VR. Although plethora of user-centered authentication schemes exist for desktop computers (e.g., [4, 5, 9, 34]) and smartphones (e.g., [2, 6, 15, 16, 28, 38]), only recently the community began studying usable and secure authentication schemes leveraging the interaction affordances possible in VR [11, 13, 14, 21, 23]. On the downside, current VR authentication methods, such as PIN entry on a virtual display, are prone to observation attacks by bystanders [14]. While researchers proposed several new schemes to mitigate this, many suffer from slow entry times or high error rates resulting in low usability.

We present the implementation and usability evaluation of CueVR, an authentication scheme for VR that is highly secure against observation attacks by design and achieves reasonable usability with authentication times between 4.151 s – 7.025 s, depending on the input method. In CueVR, users authenticate by responding to visual cues displayed on a 10-digit keypad, using either one or two handheld controllers. Cues are randomly assigned at every input, meaning that observers would not know which cues the user is responding to. This concept is often referred to as cue-based authentication in the literature [17, 22, 23, 38]. Our work is the first

AVI 2022, June 6–10, 2022, Frascati, Rome, Italy

to employ and evaluate the usability of system-generated cues for authentication in VR. We evaluate the usability of CueVR in a within-subject user study in which 20 participants authenticated using a traditional PIN pad (baseline) and two variants of CueVR: one requiring using the controller's trackpad to indicate input, while the other requires moving the controller along its axis. Besides, we compared one-handed and two-handed input. The results indicate that authentication time using CueVR is in line with that of previous VR authentication schemes, while being resistant to observations by design. Authentications using the trackpad resulted in much lower physical demand compared to controller movement while mental demand, temporal demand, performance, effort, and frustration were largely similar for both.

Requiring input depending on the visual cues displayed through a head mounted display (HMD) means that observers will not know which cues the user is responding to, making observation attacks infeasible. For this reason, we focus on evaluating CueVR's usability in our user study and discuss potential attack vectors and how CueVR performs against them. We also discuss how cue-based authentication can be used in VR, which situations CueVR is ideal for, and which situations we do not recommend CueVR for.

Contribution Statement. The contribution of our work is threefold: (1) We introduce the concept of cue-based authentication for VR (CueVR). (2) We present an in-depth usability study in which we evaluate CueVR, using two different input methods (Trackpad and Motion Controller) and compare its usability against Laserpointer input (a traditional 10-digit PIN pad baseline). (3) We discuss CueVR in the light of previous real-world authentication schemes that rely on cues for user authentication and conclude with a discussion about CueVR 's security and how such a cue-based authentication scheme can be transferred to other mixed reality (MR) systems.

2 RELATED WORK

We review previous works in 1) the authentication research domain, with a particular focus on cue-based authentication, and 2) works that proposed novel knowledge-based MR authentication schemes.

2.1 Cue-based Authentication

There is a large body of authentication research that looked particularly into a user's responses to cues, so-called cue-based authentication [17]. Roth et al. [32] relied on user responses to black and white-colored cues. This resulted in an additional effort compared to regular PIN entry, but both perceived and objective security were higher [32]. In SwiPIN [38], users authenticated by responding to cues in the form of arrows displayed on the digits of a PIN pad. SwiPIN was developed for mobile devices. CueAuth [17] transferred the SwiPIN concept to situated displays and experimented with responding to cues using touch, mid-air, and gaze input. Another cue-based authentication scheme for mobile devices is GazeTouchPIN [16], where users gaze left or right to confirm the PIN digit selection based on a layout that is randomly selected. While the aforementioned systems rely on visual cues, Bianchi et al. [3] introduced a unimodal non-visual input technique for PIN entry that is based on the human ability to accurately and rapidly count the number of sequential cues. De Luca et al. [8] made use of tactile cues to add an overhead of "lies" to users' input and increase the resistance against observations while maintaining high usability.

In summary, previous work showed that cue-based systems are promising for user authentication and such systems may be useful in many application areas (e.g., ATMs or ticket vending machines). Researchers already looked into adapting and evaluating established knowledge-based authentication systems for VR [14]. However, despite the promising cue-based authentication research leveraging cues for MR, such schemes have not received much attention so far and little is known about how well they perform in VR.

2.2 Authentication in Mixed Reality

The different forms of Virtual and Augmented reality [31] create an increasing need for authentication [1]. As a result, usable security researchers spent significant effort in designing, developing, and evaluating novel schemes. There are two dominant streams of research to authenticate users in MR: knowledge-based (e.g., [11, 13, 14, 23, 29]) and using (behavioral) biometrics (e.g., [18, 19, 21, 24, 25, 35]). Behavioral biometric authentication systems achieved promising results, but their accuracy drops significantly when evaluated across different systems [25]. It has been argued that biometrics should only be applied to enhance knowledge-based authentication schemes rather than replace them [21, 27]. Pure biometric authentication systems often require special hardware (e.g., bone conduction technology), and it is particularly challenging to change such biometric passwords (e.g., when they are stolen [37]). It is also worth mentioning that not all users are willing to share biometrics [30] and that the security of biometric systems can often be bypassed using a knowledge-based authentication approach. For example, mobile device authentication systems (e.g., Face ID or Touch ID) provide fallback options for when biometrics are not available and argue that developers should not rely on biometric authentication only. As such, we aim to improve knowledge-based authentication for MR devices as there will (at least for the foreseeable future) always be a need for those, and it has also been argued that there is a need for security mechanisms that can easily be integrated into existing and upcoming MR systems [7].

One of the earliest MR authentication schemes was by Yu et al. [40]. The MR schemes resulted in relatively long authentication times of ≈ 10.5 s for pattern lock and PIN, and ≈ 19 s for 3D passwords. While the authors did not conduct a formal security analysis, they argued that most people can observe pattern lock and PIN authentication, whereas observing 3D passwords is more resistant against observations [40]. Follow-up work by George et al. [14] confirmed that existing authentication methods such as PIN or pattern are observable by bystanders (18% of input was observed successfully). Depending on the input method and virtual interface size (e.g., pointing at a large screen is easier to observe than on a medium-sized screen), authentication using traditional PINs and lock patterns took between 2.57 s and 3.84 s. In a similar work by Olade et al. [29], authentications using lock patterns resulted in entry times of ≈ 1 s to ≈ 1.8 s, depending on the input method, and 20% – 40% of observations were successful when having access to video recordings. As a result, researchers investigated how VR's unique characteristics can contribute to more usable and secure MR authentications. George et al. [13] investigated the third dimension for MR authentication and found that authentications using their system takes at least 8.58 s, with in-situ observation attacks being successful 12.5% of the time and post-hoc attacks being not successful at all. Funk et al. [11] showed how passwords composed of spatial and virtual targets can improve user authentications' in MR environments with virtual passwords being fully resistant against observations. Mathis et al. [23] showed how the use of coordinated 3D manipulation and pointing can lead to fast and highly secure authentications, with 1.69 s – 4.92 s authentication times and shoulder surfing resistance between 96% and 99.55%, depending on the input method (i.e., controller tapping, head pose, eye gaze).

In summary, previous systems had promising authentication times and high usability, but were not fully resilient to shoulder surfing (e.g., [14, 23]). It has also been shown that different input methods (e.g., touch, eye gaze) can significantly impact the usability and security of MR authentication schemes [23, 29]. While George et al. [14] provided some first evidence of the transferability of well-established authentication systems for VR, their investigation did not involve cue-based authentication schemes which can, as evidenced by previous authentication research in the real world (e.g., [8, 17]), contribute to more usable and secure user authentication. Through our work, we fill this gap and investigate how cue-based authentication performs in MR, and if different input methods impact such a cue-based authentication system when used in MR.

3 CUEVR– CONCEPT & IMPLEMENTATION

We extend the concept of cue-based authentication [17, 22, 38] for VR environments (see Figure 1). We chose this concept because it uses PINs which are considered to be one of the most widely used authentication schemes. Users are familiar with PIN-based authentication, and our scheme can be easily integrated or replace existing solutions. Moreover, our concept relies on visual cues displayed on the virtual PIN-Pad, which make it resilient to observations. CueVR addresses a threat model in which the attacker is observing the user's input. An attacker can easily approach the immersed VR user since their visual and auditory perception is usually overlaid with virtual content. Thus, an attacker can closely observe how the user interacts and moves the controller but cannot access to the randomly generated vital cues required for successful PIN entry. Current VR systems ensure that the virtual environment can not be screen cast during user authentication. This threat model has been used a lot in previous work on VR authentication [11–14, 20, 21, 23].

In addition to adapting cue-based authentication for VR, we implement different input methods: Laserpointer, Trackpad and Motion Controller. Each can be used with one or two hands. Unlike other approaches relying on additional hardware, e.g., eye trackers [17, 22], CueVR does not require additional hardware apart from what is provided with most VR headsets: one (or two) controllers.

In CueVR, users enter 4-digit PIN codes on a PIN pad (consisting of the digits 0-9), split into *Blue* (digits 1, 2, 4, 5, 7) and *Orange* (digits 3, 6 , 8 , 9, 0), as shown in Figure 2. These color assignments always remain the same. Each digit has one of five cues randomly assigned to it. The cues consist of *Up, Down, Center (annotated with a circle), Left, and Right.* The five cues are randomly assigned to digits of each color in a way that ensures every color-cue combination being unique. We use 4-digit PINs in our evaluation to ensure comparability with prior work [13, 14, 21, 23, 38]. However, CueVR can support any PIN length. Entering each digit is divided into three steps: (1) Choosing the side/color of the digit; (2) recognizing the cue assigned to the digit; and (3) providing input based on the cue. After entering a digit, all cues get randomly reassigned. Step (2) is the same for all inputs, but the execution of steps (1) and (3) varies depending on the input method and whether it is one or two-handed input, which we explain in more detail below. For adversaries to guess the correct PIN, they would have to observe (1) the cues in VR which are not visible to anyone except the headset user, and (2) the user's input in response to the cue.

3.1 Laserpointer (baseline)

We treat Laserpointer as the baseline in our study because it resembles traditional PIN pads and PIN entry [14]. Laserpointer is one of the most widely used input techniques in VR [14] and in today's Oculus Quest. Since Laserpointer forms our baseline, there are no cues used and the user only selects the digits to enter the PIN.

One-Handed Laserpointer. The Laserpointer includes a virtual pointer that is always visible to the user during authentication. The user casts the virtual beam on the PIN pad and selects the PIN by pressing the trigger button (Figure 1A) using only one controller.

Two-Handed Laserpointer. Here, users utilize both controllers to enter the PIN. Similar to one-handed input, the virtual beam is used for pointing and trigger button is pressed for selection.

3.2 Trackpad

The second input variant of CueVR requires using the controller's trackpad to indicate input. As shown in Figure 2, the trackpad is divided into five areas corresponding to the five cues. Trackpads (or joysticks) are a common input method in many consumer VR headsets, such as HTC Vive, Vive Index, and Oculus Quest 2, and have already been leveraged for reorientation in virtual environments [39] and for different types of VR input [33, 36].

One-Handed Trackpad. The virtual beam of one controller is first used to point at one of the sides to choose the color of the desired digit. Then, the user presses one of the five areas on the trackpad to indicate their response to the cue (see Figure 1B).

Two-Handed Trackpad. Unlike the one-handed Trackpad, the two-handed Trackpad supports entry using both controllers. Each controller has a colored beam associated with one of the two sides (right controller: orange, left controller: blue). The user then presses one of the five areas on the trackpad of the controller that corresponds to the color of the digit they want to select.

3.3 Motion Controller

The third input variant of CueVR requires using the controller's motion to indicate input. As shown in Figure 2, five motions are implemented to correspond to the five cues. Motions are performed in three steps: (a) Pressing the Trigger button to indicate the start of input; (b) moving the controller in a straight line either up, down, left, right or forward to indicate input in response to the cue displayed on the desired digit (see Figure 2); (c) releasing the trigger button to end the motion and input the digit. Pressing and holding the trigger during input is done to avoid unintended input.

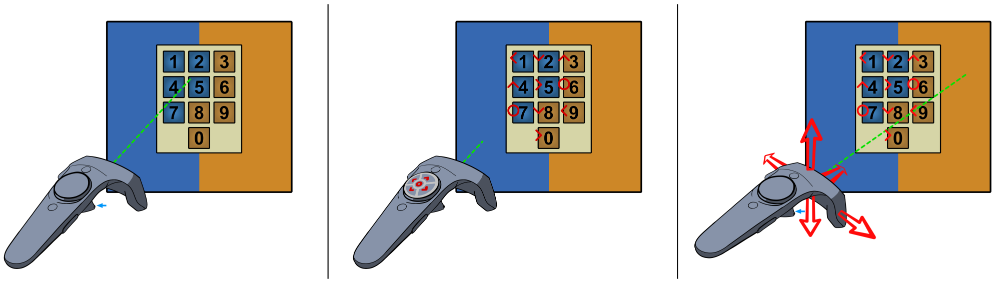


Figure 2: The three different input methods for CueVR. Laserpointer (left): PIN input is carried out by pointing and clicking each digit. Trackpad (center): PIN input is carried out by selecting a color via pointing, and then responding to the cue displayed on the desired digit by pressing one of the trackpad's five buttons. Motion Controller (right): PIN input is carried out by selecting a color via pointing, and then translating the controller according to cue displayed on the desired digit. Because all above examples involve one-handed input, the user needs to point at one of the two colored areas. In two-handed input, however, the user does not need to point using their controller; instead, they use the right controller for selecting orange digits, and the left one to select blue digits.

One-Handed Motion Controller. The user utilizes only one controller and moves it to indicate their input. Similar to one-handed Trackpad, a virtual beam is used to point at one of the sides to choose the color. After that, the controller is moved to provide input.

Two-Handed Motion Controller. Like two-handed Trackpad, each controller has a colored virtual beam matching the color of one of the two sides. To provide input, the user translates the controller with the matching color in response to the cues on the desired digit.

3.4 Limitations

We study the impact of both single-handed and two-handed input on cue-based VR authentication. While two-handed input can make such systems inaccessible to users with certain types of disabilities, CueVR still performs well when input is provided using one hand only. We encourage future research to contribute to even more accessible systems and find ways to further improve them. Furthermore, we study only one cue-based authentication scheme, but the literature has proposed several others (e.g., [10]).

In this work, we focus on a visual cue-based authentication scheme that leverages VR's unique characteristics (i.e., the private visual channel). Future work could look into ways to further improve the usability of cue-based VR systems through the help of, for example, haptic cues. However, it is important to keep in mind that introducing any type of feedback could also support attackers. Therefore, haptic cues could lead to less secure systems without necessarily improving the user's authentication experience.

4 EVALUATION

This study evaluates the effects of the authentication scheme and input method on users' authentication performance, specifically input time, success rate, and perceived workload. We used a repeated-measure within-subjects study design with the independent variable INPUT and HANDS. There were three levels for INPUT: Laserpointer, Trackpad, and Motion Controller. HANDS had two levels: one-handed and two-handed. The order of conditions was counterbalanced using a Latin square.

4.1 Participants

We invited 22 participants (7 female, 15 male) through social media and mailing lists. Participants were aged from 20 to 57 ($M = 24.5, SD = 7.8$) and had normal or corrected-to-normal vision. Twelve participants had previous experience with VR. Eighteen participants were right-handed.
Due to COVID restrictions, we initially planned the study to be entirely remotely with participants that already own an HTC Vive. Restrictions were eased after the first two participants, so we switched to an in-person lab study with the remaining 20 participants. Unfortunately, we had to exclude the data of two participants for technical issues with the controller touchpad. This left us with 20 participants: 18 in-person and two remote. All participants were compensated by a 10 € voucher.

4.2 Apparatus and Implementation

We built CueVR using Unity3D C# and made it accessible to participants via an HTC VIVE Pro headset (2880 × 1600 pixels combined, 90 Hz, 110° fov), using the SteamVR plugin[1]. The application was running on a stationary HP VR backpack computer with Windows 10. Participants were asked to stand at a marked spot to view the PIN pad within the 4 m × 4 m tracking space, covered by two VIVE base stations (Gen 2.0). Participants' view could be monitored from the Unity ingame view. This was done for observing the participants during the study. However, deployments of CueVR are assumed to block screencasting and other users in the virtual environment from seeing the user's PIN pad and input during authentication. This is a reasonable assumption and is in fact the case in today's Oculus and HTC VIVE systems. This means that only the bystander in the real world can observe the user's input in response to the cues, but they cannot observe the cues.

[1] https://assetstore.unity.com/packages/tools/integration/steamvr-plugin-32647 last accessed April 27, 2022

4.3 Procedure

After welcoming participants[2], we asked them to sign the consent form and fill out the demographics questionnaire. Subsequently, we explained the course of the study, including all relevant interaction concepts and VR control mechanisms.
In the last preparation step, we adjusted the HMD to the participant's head before starting with the authentication task.

The participant's task was to enter a four-digit PIN in VR using our scheme. For each condition, participants performed two sets (training/evaluation) of four authentication trials. For each trial, a new randomized PIN was displayed on top of the floating PIN pad. PINs had different complexity by changing the number of required transitions from one colored-side to another. The complexity of PIN was counterbalanced. After participants memorized the PIN, they were asked to press the menu button to start the PIN entry process. During the training phase, the PIN was presented again on failure, and we provided assistance on request. Subsequent to four successful PIN entries, the evaluation phase started, in which participants were requested to authenticate four times as fast and as accurately as possible. In case of input error, we gathered additional information on the type of failure, e.g., failure to recall PIN, failure to input PIN, or others. After successfully completing the task, participants exited the VR and filled out the NASA-TLX questionnaire alongside Likert-scale questions targeting perceived speed and ease of use. Subsequently, they repeated the procedure using the next condition. We presented all conditions in a counterbalanced order, using Latin square to prevent sequence effects. In the final step, we asked participants to rank all presented authentication schemes.

We ensured the procedure is the same for the remote and in the lab study. The program with instructions was sent along with the consent form to the participant prior to the study. The participant had to be in a call via Discord[3] with the experimenter and had to share their HMD screen. The questionnaires were sent to the participant in digital form during the study.

5 RESULTS

Overall we collected and analyzed 480 entries: 20 participants × three INPUT methods × two HANDS (one-handed and two-handed) × four authentication trials. We measured 1) the authentication time (AuthTime) – the time needed to enter the 4-digits PIN, 2) the preparation+authentication time (PAuthTime), including the time starting from showing the PIN pad, 3) the error rate, 4) the perceived workload using the NASA TLX, 5) and feedback through responses to the Likert-scale questions.

5.1 Authentication Time

Authentication time (AuthTime) was measured from the moment the first of four digits was entered until the last one was entered. To avoid biases due to errors, we only considered correct PIN entries when measuring AuthTime.

Descriptive analysis shows that mean AuthTime using two-handed Laserpointer is fastest (Mean = 1783 ms, SD = 2463 ms), followed by one-handed Laserpointer (Mean = 1944 ms, SD = 677 ms). Other mean AuthTime were: Mean = 4422 ms, SD = 2463 ms for one-handed Trackpad, Mean = 4151 ms, SD = 1946 ms for two-handed Trackpad, Mean = 4977 ms, SD = 1989 ms for one-handed Motion Controller, and Mean = 4151 ms, SD = 1946 ms for two-handed Motion Controller.

The results are summarized in Figure 3. We ran a two-way repeated measures ANOVA to analyze the impact of INPUT and HANDS on AuthTime with Greenhouse-Geisser correction, due to the violation of the assumption of sphericity according to Mauchly's test. We found a significant effect of INPUT ($F_{1,67.79} = 166.68$, $p < 0.001$) and HANDS on AuthTime ($F_{1,79} = 12.9$, $p < 0.001$). No interaction effects between INPUT and HANDS were found (p > 0.05). Post-hoc analysis with Bonferroni corrected p-values revealed that two-handed input is significantly faster than one-handed input -322 ms (95% CI, 137 ms to 506 ms), p < 0.001. It also showed that Laserpointer is significantly faster than both Trackpad -2423 ms (95% CI, -2919 ms to -1926 ms), p < 0.001, and Motion Controller -2865 ms (95% CI, -3225 ms to -2505 ms), p < 0.001, and that Trackpad is significantly faster than Motion Controller -442 ms (95% CI, -811 ms to -73 ms), p < 0.013.

5.2 Preparation+Authentication Time

Preparation+Authentication time (PAuthTime) was measured from the moment the participant was shown the PIN pad until the moment the last of the four digits was entered. Similarly, we also considered correct PIN entries only when measuring PAuthTime.

Descriptive analysis shows that PAuthTime is fastest in case of two-handed Laserpointer (Mean = 2920 ms, SD = 1001 ms), followed by one-handed Laserpointer (Mean = 3033 ms, SD = 901 ms). Next comes the two-handed variants of Trackpad (Mean = 6039 ms, SD = 2557 ms), and Motion Controller (Mean = 6294 ms, SD = 2180 ms). Finally, the slowest are the one-handed variants of Trackpad (Mean = 6394 ms, SD = 3382 ms) and Motion Controller (Mean = 7024 ms, SD = 2565 ms).

The results are summarized in Figure 3. A two-way repeated measures ANOVA showed a significant interaction effect between INPUT and HANDS when they impact PAuthTime ($F_{2,158} = 3.29$, $p < 0.04$). This led us to run follow-up one-way ANOVA tests to study the impact of INPUT in each of two-handed and one-handed input. Post-hoc analysis with Bonferroni-adjusted p-values showed that in case of one-handed input, Laserpointer is significantly faster than both Trackpad -3360 ms (95% CI, -4217 ms to -2503 ms), p < 0.001 and Motion Controller -3991 ms (95% CI, -4588 ms to -3393 ms), p < 0.001, and Trackpad is significantly faster than Motion Controller -630 ms (95% CI, -1217 ms to -43 ms), p < 0.035. In case of two-handed input, Laserpointer is also significantly faster than Trackpad -3068 ms (95% CI, -3625 ms to -2512 ms), p < 0.001, and Motion Controller 3323 ms (95% CI, -2795 ms to -2851 ms), p < 0.001. We did not find significant differences between the last pair (Trackpad vs Motion Controller) when using two hands (p > 0.05).

5.3 Error Rate

A PIN entry was considered incorrect if at least one digit was incorrect. Whenever a participant's entered PIN contained any errors, participants had to reenter the PIN. Before that, they were prompted to indicate whether the error was because 1) they *forgot*

[2] All local health and hygiene regulations to prevent the spread of COVID-19 and create a safe study environment were implemented.

[3] https://discord.com/, last accessed April 27, 2022

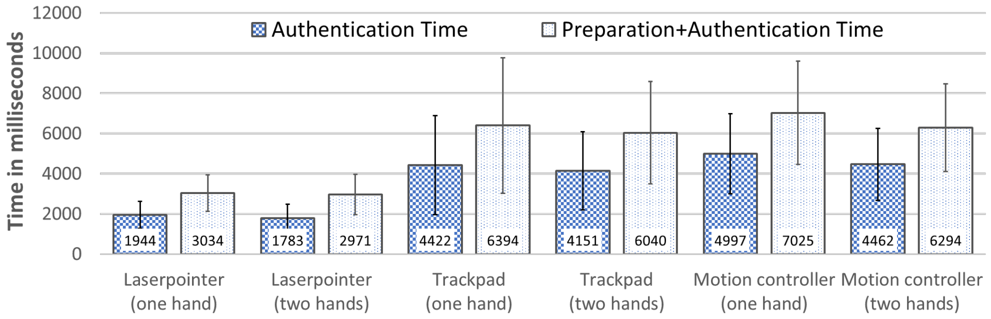


Figure 3: Authentication time (AuthTime) is the time from the first entry until the last entry of a 4-digit PIN, Preparation+Authentication Time (PAuthTime) is the time from the moment the PIN pad is shown to the user. Using two hands for entry is faster using all INPUT. Laserpointer is the fastest, followed by Trackpad and Motion Controller. These differences are all statistically significant, except for the PAuthTime when using two-hands in Trackpad vs Motion Controller.

the PIN they had to enter, 2) they remembered the PIN but made an *input error* nevertheless, or 3) due to something else. None of our study participants selected (1) or (3).

Overall, there were 86 *input errors*: 5 in one-handed Laserpointer, 2 in two-handed Laserpointer, 14 in one-handed Trackpad, 28 in two-handed Trackpad, 21 in one-handed Motion Controller and 16 in two-handed Motion Controller. A repeated-measures ANOVA revealed an interaction effect between HANDS and INPUT ($F_{2,38}$ = 4, $p < 0.027$) in error rate. This means that the impact of HANDS on error rate depends on which INPUT is in question. This led us to run follow-up one-way ANOVA tests to study the impact of INPUT in each of two-handed and one-handed input. In case of two-handed input, Bonferroni-adjusted comparisons indicated that Laserpointer was significantly less error-prone than Trackpad -1.3 (95% CI, -2.2 to -0.41), p < 0.004, and Motion Controller -0.7 (95% CI, -1.13 to 0.27), p < 0.001. We found no significant differences between two-handed Trackpad and Motion Controller (p > 0.05). We also found no significant differences between all pairs in case of one-handed input.

5.4 Perceived Workload

The perceived workload was measured for each of the 6 conditions (3 INPUT x 2 HANDS) using a NASA TLX questionnaire. The results are illustrated in Figure 4. Overall, perceived workload is least when using Laserpointer. Mean scores for mental demand, temporal demand, performance, effort and frustration are largely similar for Trackpad and Motion Controller. Physical demand for Trackpad is much lower than that for Motion Controller.

5.5 Perceptions towards CueVR

We collected feedback through 5-point Likert scale questions. Participants reported Laserpointer (one- and two-handed) to be easiest, fastest, most intuitive, most likely to be often used, and most suitable for public use (see Figure 5). However, it was also perceived to be less secure and that it does not make good use of VR. Trackpad (one- and two-handed) are rated as the most secure. Motion Controller (one- and two-handed) are the techniques that utilize VR the most, yet might require more training to perform better.

Table 1: Weighted ranks for Laserpointer (LP), Trackpad (TP), and Motion Controller (MC). Weighted ranks were calculated by multiplying each instance in which a participant ranked a method as first by 6, second by 5 and so on. Thus the maximum score a method can get is 120 (20 participants × 6).

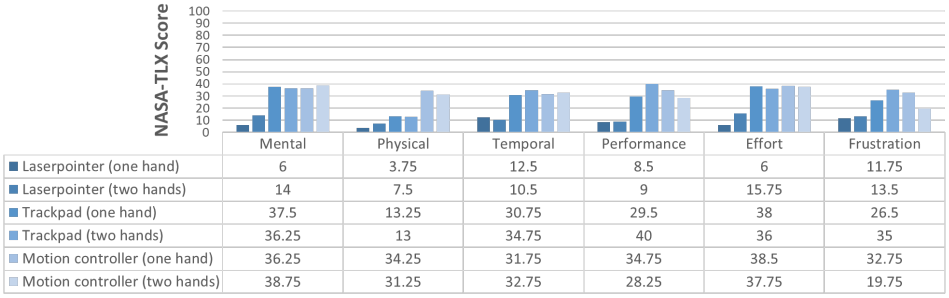
INPUT	LP		TP		MC	
HANDS	1	2	1	2	1	2
Most liked	**91**	85	62	52	62	68
Most Secure	42	55	70	**89**	76	**88**
Easiest	**114**	95	67	47	49	48

5.6 Ranking of Input Methods

At the end of the study, participants were asked to rank each INPUT method in terms of how much they 1) like them, 2) perceive them to be secure, and 3) find them easy to use. Table 1 shows the weighted scores. Participants liked one-handed Laserpointer the most (weighted score = 91). They perceived two-handed Trackpad and two-handed Motion Controller to be the most secure (weighted scores 89 and 88 respectively). In terms of easiness, one-handed Laserpointer received the highest weighted score (114), followed by two-handed Laserpointer (95) and then one-handed Trackpad (67).

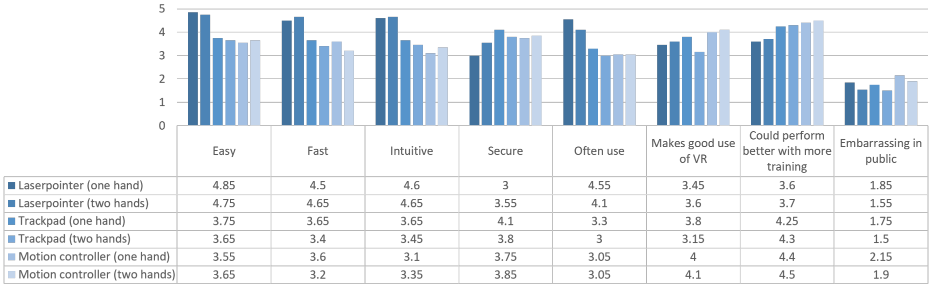
6 DISCUSSION

Our study showed that cue-based VR authentication takes 4.151 s – 7.0125 s, with Trackpad, significantly outperforming Motion Controller. Thus, our recommendation is to use Trackpad rather than Motion Controller for input in CueVR. However, both Trackpad and Motion Controller are significantly slower than the traditional PIN-pad using a Laserpointer (our baseline). This means that CueVR improves security at the expense of slightly lower usability. While not ideal, CueVR still advances state of the art cue-based authentication which is usually significantly slower as it requires the user to not only input a password/PIN, but also observe the cues and respond to them. The fact that authentication using CueVR cannot be observed by bystanders and keeps authentication times low (e.g., 4.15 seconds using two-handed Trackpad) means that it achieves a good balance between usability and security. Other cue-based systems from recent and prior work require 12–30 seconds



	Mental	Physical	Temporal	Performance	Effort	Frustration
■ Laserpointer (one hand)	6	3.75	12.5	8.5	6	11.75
■ Laserpointer (two hands)	14	7.5	10.5	9	15.75	13.5
■ Trackpad (one hand)	37.5	13.25	30.75	29.5	38	26.5
■ Trackpad (two hands)	36.25	13	34.75	40	36	35
■ Motion controller (one hand)	36.25	34.25	31.75	34.75	38.5	32.75
■ Motion controller (two hands)	38.75	31.25	32.75	28.25	37.75	19.75

Figure 4: Mean scores for mental demand, temporal demand, performance, effort and frustration are largely similar for Trackpad and Motion Controller. Trackpad's physical demand is much lower than Motion Controller's. Laserpointer is less demanding than the more secure Trackpad and Motion Controller.



	Easy	Fast	Intuitive	Secure	Often use	Makes good use of VR	Could perform better with more training	Embarrassing in public
■ Laserpointer (one hand)	4.85	4.5	4.6	3	4.55	3.45	3.6	1.85
■ Laserpointer (two hands)	4.75	4.65	4.65	3.55	4.1	3.6	3.7	1.55
■ Trackpad (one hand)	3.75	3.65	3.65	4.1	3.3	3.8	4.25	1.75
■ Trackpad (two hands)	3.65	3.4	3.45	3.8	3	3.15	4.3	1.5
■ Motion controller (one hand)	3.55	3.6	3.1	3.75	3.05	4	4.4	2.15
■ Motion controller (two hands)	3.65	3.2	3.35	3.85	3.05	4.1	4.5	1.9

Figure 5: Means of the rated aspects of the INPUT methods on 5-point Likert Scales (1=Strongly Disagree; 5=Strongly Agree).

to authenticate while not entirely eliminating observation attacks [10, 17]. For example, CueAuth [17], which is a recent cue-based authentication scheme, is resistant to observation attacks only when using eye gaze, which requires 30+ seconds to enter a 4-digit PIN. At the same time, the faster variants of CueAuth require 3.7 to 5.1 seconds to authenticate but are vulnerable to observation attacks: 64% – 74% of input was successfully observed [17].

CueVR also fares very well in *comparison to recent XR authentication schemes*, where schemes are either highly secure against observations or slow. RoomLock [13], for example, achieved high shoulder surfing resistance (87.5% - 100%), but it took participants 8.58 s – 14.33 s to authenticate. Other systems are notably fast but prone to observations. One of the fastest VR authentication systems is the work by Olade et al. [29]. Their work resulted in authentications between 1.0 s - 1.8 s but at the same time input was successfully observed by bystanders by up to 60%. This makes their system very suitable for day-to-day unlocks but not for protecting access to sensitive data/actions. A recent authentication system, RubikAuth [23], achieved both fast (1.69 s – 4.92 s) and secure authentications (resistant against 96% – 99.55% of the observations). However, unlike our CueVR, RubikAuth is still not bulletproof against observations, and it has also been argued that threat models beyond classical one-time observations can break its resistance to observations [23]. While an attacker who familiarized themselves with systems like RubikAuth [23] or RoomLock [13] over a long period of time and analyzed a user's input in depth may find the user's input, the attacker would still not be able to increase their chance of guessing the correct CueVR PIN due to the lack of knowledge of the cues.

There is often a trade off between usability and security, and improving the security of authentication often results in lower usability. This is not to undermine the importance of usability. Improving security at the expense of usability means that users may be less likely to use the more secure methods, which ultimately results in less security. However, there are situations where users may benefit from authenticating using a method that is resilient to observations as we discuss further in section 6.2.

6.1 Security of CueVR

CueVR uses the same theoretical password space as traditional 4-digit PINs. Our implementation of Laserpointer (baseline) matches today's implementation of PIN entry on Oculus. This approach was shown to be vulnerable to shoulder surfing [14] because bystanders are able to guess the user's input by observing how they move their hands. At the same time, approaches that rely on visual cues delivered through the user's headset, as done in CueVR, are resistant to observation attacks by design because attackers will not know which of the randomized cues the user is responding to. This means that if an attacker observes the user's responses to cues, and then puts on the user's headset to attempt to repeat them, there would only be a $\frac{1}{10^n}$ chance that the attacker will be successful, where n is the length of the PIN. If the attacker further observes which side the input is in all four entries by, for example, observing which of the two hands provided input or observing in which direction the one-handed input was provided. Then this increases the chance of successful attacks to $\frac{1}{5^n}$, where n is the length of the PIN. Guessing and observation attacks are not the only possible attack vectors. In the following, we discuss further types of attacks and discuss how they can be used against CueVR.

6.1.1 Intersection Attacks. Wiese and Roth showed that by using intersection attacks, cue-based schemes such as SwiPIN [38] can be broken in less than 11 observations. Intersection attacks in this scenario would be done as follows: the attacker would observe parts of the user's input and parts of the cues in multiple occasions, where each attack builds on knowledge gathered from the previous attack. Again, these attacks would not succeed against CueVR because attackers do not know what cue the user is responding to.

6.1.2 In-VR Observation Attacks. In this work, we assume that bystanders, in VR cannot see the user's movements and/or cues. This is a reasonable assumption as systems can detect that the user is performing a sensitive action and obscure them or freeze them in the view of their peers in VR. In fact, Oculus and HTC Vive systems do not allow screen casting the VR user's view during authentication. We recommend reinforcing this in a similar way for any VR authentication scheme.

6.1.3 Password Space. While CueVR supports any PIN length, we chose to conduct the usability study with a 4-digit PIN to ensure comparability to prior work. Thus, the theoretical password space matches that of traditional PINs of an equal length. The practical password space may not necessarily be the same as for a traditional PIN pad where input is provided the same way every time. For example, the positions of the digits relative to each other, and the user's mental model of the layout and the way input is provided is not changed at every input when using a traditional PIN pad as opposed to CueVR. This makes investigating the practical password of CueVR in a longitudinal field study an interesting direction for future work. This could also help understand how likely guessing attacks are to succeed against CueVR.

6.2 When to use CueVR

CueVR has obvious security benefits but suffers from lower usability compared to the Laserpointer. Lower usability can result in lower security when users do not choose to use the secure method because of its low usability. Thus, choosing strategically when to employ CueVR is important. We do not recommend using CueVR for frequently occurring actions (e.g., to unlock the headset), but rather in less frequent situations and in situations in which the user is at higher risk. This includes, for example, confirming a purchase, or entering a PIN when a bystander is around. The latter can be achieved by using the headset's depth sensing. If the headset detects that there are bystanders and, thus, the user is at risk of being shoulder surfed during authentication, then it would require the use of CueVR instead of, for example, Laserpointer. This can go further to identifying whether the bystanders are "trusted" by the user (e.g., through block/allow lists) to determine whether the user is at risk. However, note that this may have privacy implications on bystanders. For example, if identifying the bystander requires facial recognition, then the bystander's consent should be obtained before collecting and processing photos of their face. Any recognition of bystanders needs to be done locally on the headset before discarding the data.

6.3 Transferability to Other Systems

We studied CueVR using an HTC Vive but its concept, authenticating based on cues and gestures, is transferable to various mixed reality systems. The Oculus Quest 2, for example, comes with a joystick capable of left, right, up, and down input gestures. CueVR can also be used on the Valve Index. The track button can be used as a trackpad or as a binary button with haptics. We expect that the relative differences between CueVR and its different input methods (Trackpad, Motion Controller) remain the same across different MR devices. CueVR could also find adoption on controller-free MR systems. Both Trackpad and Motion Controller could be implemented using hand tracking where the hand acts as the starting point of gestures. As such, CueVR is designed as an authentication system that can be easily integrated into existing MR systems and does not require any additional sensors or devices. Authentication research, especially in the context of mixed reality systems, is a fast growing research field that has received a lot of attention in the last few years. Despite the academics' interest in novel XR authentication systems (e.g., [11, 13, 21, 23, 25, 26, 29, 40], XR companies are less likely to integrate new features/hardware into headsets only to improve the usability and security of authentication. As a result, novel authentication schemes that do not require additional hardware and are easy to integrate into existing XR systems, such as CueVR, are needed to further contribute to usable and secure cross-device authentication systems in the long run [7].

7 CONCLUSION

In this work, we studied the usability of cue-based authentication for VR. We explored the impact of two input methods (Trackpad and Motion Controller) and one-handed/two-handed input on CueVR 's usability. Our usability study showed that authentications on CueVR are comparable fast as existing VR authentication schemes (authentications up to 4.151 s) and, at the same time, fully resilient against observations by design. We concluded with a discussion on CueVR 's security and the need for usable and secure VR authentication systems that are transferable to different mixed reality devices. Our work highlights the potential of cue-based authentication for VR and shows how existing real-world authentication schemes can be transformed to virtual reality and how this, in return, makes them resilient against observation attacks.

ACKNOWLEDGMENTS

This work has been funded, in part, by an EPSRC New Investigator Award (EP/V008870/1), by PETRAS National Centre of Excellence for IoT Systems Cybersecurity EPSRC (EP/S035362/1), by the University of Edinburgh and the University of Glasgow jointly funded PhD studentships, by the German Research Foundation (DFG) project no. 425869382, and by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr [Voice of Wisdom].

REFERENCES

[1] Florian Alt and Emanuel von Zezschwitz. 2019. Emerging Trends in Usable Security and Privacy. *i-com* (2019). https://doi.org/10.1515/icom-2019-0019

[2] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2011. Spinlock: A single-cue haptic and audio PIN input technique for authentication. In *International Workshop on Haptic and Audio Interaction Design*. Springer, 81–90.

[3] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2012. Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry. *Interacting with computers* 24, 5 (2012), 409–422.

[4] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C Van Oorschot. 2011. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing* 9, 2 (2011), 222–235.

[5] Sonia Chiasson, Paul C Van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*. Springer, 359–374.

[6] Sauvik Das, David Lu, Taehoon Lee, Joanne Lo, and Jason I Hong. 2019. The memory palace: Exploring visual-spatial paths for strong, memorable, infrequent authentication. In *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology*. 1109–1121.

[7] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. 2019. Security and Privacy Approaches in Mixed Reality: A Literature Survey. 52, 6, Article 110 (Oct. 2019), 37 pages. https://doi.org/10.1145/3359626

[8] Alexander De Luca, Emanuel von Zezschwitz, and Heinrich Hußmann. 2009. *Vibrapass: Secure Authentication Based on Shared Lies*. ACM, New York, NY, USA, 913–916. https://doi.org/10.1145/1518701.1518840

[9] Alexander De Luca, Emanuel von Zezschwitz, Laurent Pichler, and Heinrich Hussmann. 2013. *Using Fake Cursors to Secure On-Screen Password Entry*. ACM, New York, NY, USA, 2399–2402. https://doi.org/10.1145/2470654.2481331

[10] Gloria Dhandapani, Jamie Ferguson, and Euan Freeman. 2021. HapticLock: Eyes-Free Authentication for Mobile Devices. In *Proceedings of 23rd ACM International Conference on Multimodal Interaction - ICMI '21*. ACM, accepted to appear. https://doi.org/10.1145/3462244.3481001

[11] 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)*. ACM, 1–6. https://doi.org/10.1145/3290607.3312959

[12] Ceenu George, Daniel Buschek, Andrea Ngao, and Mohamed Khamis. 2020. GazeRoomLock: Using Gaze and Head-pose to Improve the Usability and ObservationResistance of 3D Passwords in Virtual Reality. In *Augmented Reality, Virtual Reality, and Computer Graphics*. Springer International Publishing. https://doi.org/10.1007/978-3-030-58465-8_5

[13] Ceenu George, Mohamed Khamis, Daniel Buschek, and Heinrich Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 277–285. https://doi.org/10.1109/VR.2019.8797862

[14] 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. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2017) (USEC '17)*. NDSS. https://doi.org/10.14722/usec.2017.23028

[15] 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 34th Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, 6 pages. https://doi.org/10.1145/2851581.2892314

[16] 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)*. ACM, 446–450. https://doi.org/10.1145/3136755.3136809

[17] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-Based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 22 pages. https://doi.org/10.1145/3287052

[18] Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. [n.d.]. Task-driven biometric authentication of users in virtual reality (VR) environments. In *International conference on multimedia modeling*.

[19] 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*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445528

[20] John M Jones, Reyhan Duezguen, Peter Mayer, Melanie Volkamer, and Sanchari Das. 2021. A Literature Review on Virtual Reality Authentication. In *Proceedings of the Fifteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2021)-Virtual Conference*.

[21] Florian Mathis, Hassan Ismail Fawaz, and Mohamed Khamis. 2020. Knowledge-Driven Biometric Authentication in Virtual Reality. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3334480.3382799

[22] Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2021. *RepliCueAuth: Validating the Use of a Lab-Based Virtual Reality Setup for Evaluating Authentication Systems*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3411764.3445478

[23] Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. 2021. Fast and Secure Authentication in Virtual Reality Using Coordinated 3D Manipulation and Pointing. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 6 (Jan. 2021), 44 pages. https://doi.org/10.1145/3428121

[24] Robert Miller, Ashwin Ajit, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. Realtime Behavior-Based Continual Authentication of Users in Virtual Reality Environments. In *2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. 253–2531. https://doi.org/10.1109/AIVR46125.2019.00058

[25] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2020. Within-System and Cross-System Behavior-Based Biometric Authentication in Virtual Reality. In *2020 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. 311–316. https://doi.org/10.1109/VRW50115.2020.00070

[26] Robert Miller, Natasha Kholgade Banerjee, and Sean Banerjee. 2021. Using Siamese Neural Networks to Perform Cross-System Behavioral Authentication in Virtual Reality. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*. 140–149. https://doi.org/10.1109/VR50410.2021.00035

[27] 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* (Tempe, AZ, USA) *(IWSPA '18)*. Association for Computing Machinery, New York, NY, USA, 23–30. https://doi.org/10.1145/3180445.3180450

[28] Ian Oakley and Andrea Bianchi. 2012. Multi-Touch Passwords for Mobile Device Access. , 2 pages. https://doi.org/10.1145/2370216.2370329

[29] Ilesanmi Olade, Hai-Ning Liang, Charles Fleming, and Christopher Champion. 2020. Exploring the Vulnerabilities and Advantages of SWIPE or Pattern Authentication in Virtual Reality (VR). In *Proceedings of the 2020 4th International Conference on Virtual and Augmented Reality Simulations* (Sydney, NSW, Australia) *(ICVARS 2020)*. Association for Computing Machinery, New York, NY, USA, 45–52. https://doi.org/10.1145/3385378.3385385

[30] Alexander P Pons and Peter Polak. 2008. Understanding user perspectives on biometric technology. *Commun. ACM* 51, 9 (2008), 115–118.

[31] Philipp A. Rauschnabel, Reto Felix, Chris Hinsch, Hamza Shahab, and Florian Alt. 2022. What is XR? Towards a Framework for Augmented and Virtual Reality. *Computers in Human Behavior* 133 (2022), 107289. https://doi.org/10.1016/j.chb.2022.107289

[32] Volker Roth, Kai Richter, and Rene Freidinger. 2004. A PIN-Entry Method Resilient against Shoulder Surfing. In *Proceedings of the 11th ACM Conference on Computer and Communications Security* (Washington DC, USA) *(CCS '04)*. Association for Computing Machinery, New York, NY, USA, 236–245. https://doi.org/10.1145/1030083.1030116

[33] Rufat Rzayev, Polina Ugnivenko, Sarah Graf, Valentin Schwind, and Niels Henze. 2021. Reading in VR: The Effect of Text Presentation Type and Location. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*.

[34] Tobias Seitz, Florian Mathis, and Heinrich Hussmann. 2017. The Bird is the Word: A Usability Evaluation of Emojis inside Text Passwords. In *Proceedings of the 29th Australian Conference on Computer-Human Interaction* (Brisbane, Queensland, Australia) *(OZCHI '17)*. ACM, 10–20. https://doi.org/10.1145/3152771.3152773

[35] Manimaran Sivasamy, VN Sastry, and NP Gopalan. 2020. VRCAuth: Continuous Authentication of Users in Virtual Reality Environment Using Head-Movement. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 518–523.

[36] Misha Sra, Xuhai Xu, and Pattie Maes. 2018. Breathvr: Leveraging breathing as a directly controlled interface for virtual reality games. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[37] Martin Stokkenes, Raghavendra Ramachandra, and Christoph Busch. 2016. Biometric Authentication Protocols on Smartphones: An Overview. In *Proceedings of the 9th International Conference on Security of Information and Networks* (Newark, NJ, USA) *(SIN '16)*. ACM, 136–140. https://doi.org/10.1145/2947626.2951962

[38] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. *SwiPIN: Fast and Secure PIN-Entry on Smartphones*. ACM, New York, NY, USA, 1403–1406. https://doi.org/10.1145/2702123.2702212

[39] Mengxin Xu, María Murcia-López, and Anthony Steed. 2017. Object location memory error in virtual and real environments. In *2017 IEEE Virtual Reality (VR)*. IEEE, 315–316.

[40] 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.