Vision: Towards Fully Shoulder-Surfing Resistant and Usable Authentication for Virtual Reality

Tobias Länge*, Philipp Matheis*, Reyhan Düzgün†, Melanie Volkamer* and Peter Mayer*‡
*Karlsruhe Institute of Technology (KIT), Germany, {tobias.laenge, philipp.matheis, melanie.volkamer, peter.mayer}@kit.edu
†Ruhr University Bochum, Germany, reyhan.duezguen@ruhr-uni-bochum.de
‡University of Southern Denmark, Denmark, mayer@imada.sdu.dk

***Abstract*—Virtual reality (VR) is a growing technology with social, gaming and commercial applications. Due to the sensitive data involved, these systems require secure authentication. Shoulder-surfing, in particular, poses a significant threat as (1) interaction is mostly performed by means of visible gestures and (2) wearing the glasses prevents noticing bystanders. In this paper, we analyze research proposing shoulder-surfing resistant schemes for VR and present new shoulder-surfing resistant authentication schemes. Furthermore, we conducted a user study and found authenticating with our proposed schemes is efficient with times as low as 5.1 seconds. This is faster than previous shoulder-surfing resistant VR schemes, while offering similar user satisfaction.**

I. Introduction

Virtual reality (VR) has been introduced in a range of domains, from gaming and education to military [4], [1], [2]. Several of these applications access sensitive data and services. Authentication on today's VR head-mounted displays (HMDs) is different from authentication on other devices: First, when interacting with the device input is achieved using gestures and via a few buttons on a handheld controller, instead of touching a screen or using a keyboard. Second, only the user can see the content of the VR display[1]. Third, bystanders can easily observe the user's gestures because one cannot see their surroundings when wearing the VR HMD. Thus, shoulder surfing becomes a serious risk for knowledge-based authentication schemes.

Thus, one might consider alternatives to knowledge base authentication such as physiological biometric or the use of a second device (such as a smartphone). However these also have disadvantages: Biometrics have the problem that they can compromise privacy, expose the user to biometric attack vectors and cannot be changed once leaked. Furthermore, they are not always reliable enough and thus require knowledge-base authentication as fallback. Using a linked device would require the user to carry around a second device and take off the VR HMD for every authentication which is not very convenient. For behavioral biometrics, the increased threat of shoulder-surfing attacks still exists as the movements might be recorded. While continuous authentication could make recording more difficult, it is not a viable option for unlocking the device.

Therefore, we focus on knowledge-based authentication. To the best of our knowledge, no fully shoulder-surfing resistant scheme has been deployed in the real world, yet. Note, our definition of fully shoulder-surfing resistances takes the advancements in deep learning into account (e.g. Yang et al. [24], [25] demonstrated that the movements can be analyzed automatically in the future thus resistances against manual observations by persons is not enough): Fully shoulder-surfing resistances requires that a schemes does not allow any information about the secret to be obtained by any type of observation.

While past research has proposed shoulder-surfing resistant schemes, such as in [10], [19], [9], [8], [20], [26], we argue they are not fully shoulder-surfing resistant because they focused primarily on participants either directly observing the authentication process or watching a recording of the authentication. The goal of this paper is to: (1) analyze whether previously proposed authentication schemes for the VR context are fully shoulder-surfing resistant, (2) make own proposals - *Passimoji*, *C-Lock* and *Randomized PIN* - aiming to be fully shoulder surfing-resistant, and (3) explore the usability of these three schemes compared to previously proposed schemes and the classic PIN pad. Our preliminary user study suggests that our proposals provide faster authentication times while maintaining high user satisfaction. On the basis of user feedback from the study, we are planning a more in-depth investigation into these schemes and a more representative user study.

II. Related Work

In this section, we discuss the state of knowledge-based VR authentication in previous work as well as their approach towards shoulder-surfing resistance.

Existing VR authentication schemes. We consider those schemes identified in the literature review by Jones et al. [13] as well as one paper published afterwards: In 2017, George et al. [10] studied the suitability of classic PIN and pattern authentication schemes for VR. They tested various entry methods, including using a laser pointer, tapping with the controller and using a stylus, and found that using a pointer performed quite well. Besides PIN and pattern authentication [26], [20], researchers have also explored the use of the third dimension to enhance interaction and improve usability and security [9], [19], [8], [11], [17]. The majority of approaches

[1] During the authentication process, we expect any screen sharing functionality to be disabled (e.g., automatically by the operating system).

Symposium on Usable Security and Privacy (USEC) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-5-2
https://dx.doi.org/10.14722/usec.2024.23092
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

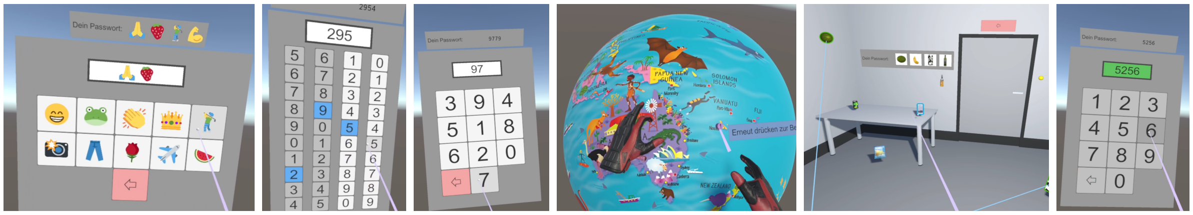

Fig. 1. The studied proposals are from left to right, the three new authentication schemes, *Passimoji*, *C-Lock* and *Randomized PIN*; two existing shoulder-surfing resistant schemes, *PassGlobe*[17] and *RoomLock*[9]; and *Classic PIN*, as baseline.

rely on pointer-based or tapping-based interaction, although some studies have investigated the use of head-tracking or eye-tracking [8], [19]. Another approach is challenge-response authentication [6], [22] that primarily focus on shoulder-surfing resistance but have not been assessed for their usability.

Analyzing Shoulder-Surfing Resistance. Several bespoke authentication methods have already been evaluated for their resistance to shoulder- surfing [10], [19], [9], [8], [20], [26]. Typically, this is done by having some participants or experts act as bystanders or by reviewing video recordings. These studies demonstrate that it is possible to observe and successfully guess a four-digit pin in 18% of cases after just three attempts [10]. Some methods have lower success rates because they make movements more difficult to observe, but they remain vulnerable [19]. Current research demonstrates additional ways to make shoulder-surfing easier by leveraging advances in computer vision and deep learning to infer keystrokes from camera recordings in both real-world scenarios [24] and virtual environments [25]. To address this increasing risk of shoulder-surfing, we aim for a stronger shoulder-surfing resistant requirement. As our understanding of fully shoulder-surfing resistant means being resistant against such attacks, there is no need to run experiments as described in the previous paragraph to measure the level of resistance.

III. Analysis of Existing Schemes.

We define authentication schemes to be **fully shoulder-surfing resistant** if no information[2] about the secret can be obtained by means of observation, even if repeated an arbitrary number of times. That is, an attacker cannot obtain information about the secret from (1) the movement of the hands, (2) the movements of the head, nor (3) the inputs on the controllers.

For the **analyses**, we considered all VR knowledge-based authentication schemes mentioned in the previous section. Most schemes are obviously not meeting the fully shoulder-surfing requirement [26], [11], [10], [20], [19], [9], [8]. For some of these schemes [10], [19], [9], [8], [20], [26], studies have already shown that even laypeople can observe the movements well and, for example, successfully guess a four-digit pin in 18 % [10] of cases after only 3 attempts. There are also schemes that have not been analyzed in this way but do not use randomization either, or parts are not random and the input is observable [11], [9].

For the remaining schemes, we identified three categories used to try to be shoulder-surfing resistant: (1) using eye-tracking for password entry, (2) implementing challenge-response procedures, and (3) randomizing screen elements. Eye tracking relies on the assumption that eye movements are not visible from the outside due to the VR HMD covering the eyes. However, this does not guarantee resistance against shoulder-surfing, as the user may still move their head instead of solely relying on their eyes, which can lead to successful attacks [8], [19]. Another drawback of eye tracking is that it requires additional hardware in the VR HMD. For these reasons, we did not investigate them further. The second method, challenge-response schemes [6], [22] are fully shoulder-surfing resistant, but can be expected to take a long time to authenticate. ZeTA [6], [12] requires the user to respond to at least 20 challenges to achieve the same guessing resilience as a 6-digit PIN. Moreover, each of these challenges requires the user to evaluate a logical condition, which is likely to require more cognitive effort than entering a password using traditional methods. The proposal by Wang et al. [22] requires fewer challenges by increasing the complexity and interaction time for each challenge. Due to these obvious usability issues, we decided not to investigate these schemes any further. The last method takes advantage of the private display feature so that observers cannot know which screen element has been selected. This is utilized by a few schemes [9], [17] which are discussed in the next paragraphs.

RoomLock. In the *RoomLock* authentication schemes by George et al. [9], the secret consists of a sequence of objects. During authentication, the user has to point at the matching objects in a virtual three dimensional room. Only one of their variants shuffles the objects before authentication starts. Due to the private display, it is impossible for an observer to know which objects have been selected. However, it can be observed if the same object appears more than once in the password. Thus, this proposal is only meeting the fully shoulder surfing resistance requirement if the secret cannot contain duplicates.

PassGlobe. In the *PassGlobe* authentication scheme by Länge et al. [17], the secret consists of a sequence of locations on a virtual 3D globe that can be rotated by the user. This scheme was also designed with shoulder-surfing resistance in mind, so that the globe is randomly rotated before each selection. However, the authors discuss the issue that users might align the globe along the equator before searching for their locations. This would allow an observer to gain knowledge of the approximate orientation, which leads to a reduction in password space. Thus, this proposal cannot be finally judged without having conducted a user study to see how users interact with it.

IV. Proposed Authentication Schemes

We propose three schemes for the third category in the previous sections: Our proposals randomize different types of screen elements in different ways. We briefly introduce all

[2] Not including the length of the secret, as this information might be obtained by other means and does not provide a significant advantage to an attacker

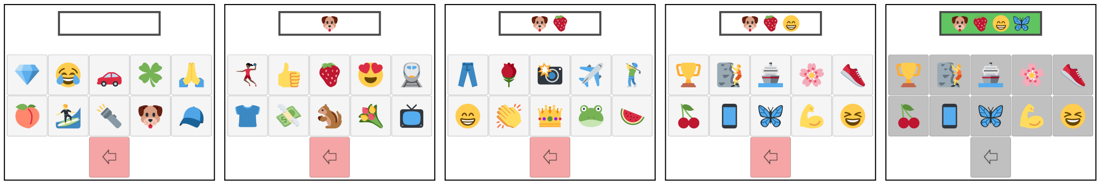

Fig. 2. Authentication process using *Passimoji*. Before entering each digit, the emojis of the corresponding set are randomly distributed. After entering a digit, it is displayed to the user. After the last digit is entered, the keys are locked and the password display turns green if authentication was successful. There is a unique set of emojis for each digit, containing emojis from different categories (e.g. animal, vehicle, etc.). Twitter emojis (Twemoji) are used, released under CC-BY 4.0 license.

three in this section while considering a password space of 10^4 for better comparability with other VR authentication studies. The functionality of the schemes is also demonstrated in a short video [16] about our study. Note, the last subsection describes the general user interaction for all three schemes.

A. Randomized PIN

In [10], the authors showed that established schemes, such as PIN, can achieve good usability in VR with input times of around 2.743 seconds. Furthermore, randomization seems to be the most promising approach to resist shoulder-surfing attacks. Thus, an intuitive idea is to combine these and use a randomized PIN pad with individual key randomization (IKR) as proposed by Maiti and Crager [18] for the mobile context. Thus, the first proposal is the *Randomized PIN* scheme. It works similarly to a classic PIN, except that the numbers on the pad are randomly shuffled before each number is entered. Note, this is no new concept (see [18], [23], [15]), but has not been studied in the VR context, yet.

B. Passimoji

The second proposal is taking advantage of the fact that images are known to be easier to remember [21]. Similar to VIP [5] and a scheme already proposed for the AR context [7], we aim to explore whether images provide an advantage over numbers in the VR context. Another advantage of images is that we are not limited to 10 different symbols, but can use different image sets for each digit of the secret. This way, users do not have to remember the correct order of the images in their secret, but only have to recognize the images that belong to their secret. This led us to the second proposal, *Passimoji*, an VR authentication scheme using emojis instead of numbers (see Fig. 2). As images we choose emojis since they are familiar to people and could offer comparable login times to PIN, as shown in the mobile context [14].

To evaluate *Passimoji* with a password space of 10^4, we choose 40 unique emojis, divided into 4 sets of ten. Since emojis can be well grouped into different categories, we decided to choose a unique emoji from each category for each digit of the secret. To make them easier recognizable, we choose emojis that differ in color and shape. Before each input, the emojis from the corresponding set are randomly distributed.

C. C-Lock

Our third approach adds some order to the random nature of the first proposal. Similar to a combination lock with a wheel for each digit, *C-Lock* keeps the numbers in order for each digit while changing the offset (see Fig. 1). All code wheels are shown simultaneously and the offsets are randomized only once at the beginning of the authentication process. Thus, users might notice the next digit in their peripheral field of view while searching for the current one. We anticipate faster input time with our method compared to Randomized PIN since numbers are not shuffled after each digit.

D. User Interaction of all Proposals

For all three schemes, the user interacts via a virtual pointer, as suggested by others [10]. A short tactile pulse on the controller indicates that they are pointing at a button. They can press the trigger button on the controller to select it. The previous entry can be undone with the delete button, except for the final digit, whose entry triggers the validation process. Unlike traditional PIN authentication on other devices, the entered digits are displayed above the input grid the entire time. This is possible due to the private display of VR devices and allows user to check that the entered secret is the one they wanted to enter.

V. User Study

A. Methodology

This study evaluates the usability (i.e., input time, success rate, and satisfaction) of the three schemes presented in the previous section with the most promising ones found in existing literature (see Section III) and a classic PIN as baseline. We used a within-subjects design with the following schemes: *Passimoji*, *C-Lock*, *Randomized PIN*, *Classic PIN*, *Room Lock*, and *PassGlobe* (see Fig. 1). We had four additional schemes as conditions in the study, bringing the total to 10. These schemes are intended as replacements for alphanumeric passwords and to provide resilience against offline attacks. Therefore, the evaluation results for these schemes are out of the scope of this paper and not reported in the following. Conditions were balanced using a balanced Latin square to mitigate order and carry-over effects.

Procedure. After being welcomed, participants were informed about the study, completed a consent form, and answered a demographic and VR experience questionnaire. Participants then put on the HMD and its functionality was explained. Playing fetch with a virtual robot dog in Valve's "The Lab" helped attendees become comfortable with VR. Next, the study application was launched. For each scheme, participants were first given an explanatory text about its functionality. After that, they performed two sets of authentication attempts: three training attempts, and five measurement attempts. During the training, participants had to repeat an attempt if they made a mistake to ensure they got familiar with the scheme before the measurement attempts started. For each authentication attempt, participants were first shown a randomly generated secret. They could then start the authentication anytime by pressing the start button. During authentication, the secret was permanently displayed above the input field, as comparing memorability was not in the scope of this study. An example of the process in study application is demonstrated in this video [16]. After completing the authentication attempts, the participants removed the VR HMD and answered a questionnaire about the scheme, including the System Usability Scale (SUS) [3] - a standardized questionnaire to measure the usability of a system - and qualitative feedback questions. Participants then repeated the same procedure for the next scheme. After completing the questionnaire for the final scheme, the study was complete and the participants received a compensation of 20€, as the study took about two hours.

Participant Sample. A total of 12 participants (3 female, 9 male), aged between 25 and 28, were recruited using convenience sampling, i.e., from the authors' families and friends. Four participants had never used a VR device, five had used one at least once, and three had used it more often. The study was conducted as a lab experiment using the Valve Index HMD with its controllers. Due to the COVID pandemic, local hygiene measures were followed.

Implementation and Adjustments. We implemented all schemes using the *Unity* game engine and the SteamVR plugin. Some additional parts of the study, such as the explanatory texts for each scheme, were implemented in the same application. We chose a password space of 10^4 to provide comparability with other VR authentication studies. Therefore, the PIN-based schemes, *Passimoji*, *C-Lock*, *Randomized PIN*, and *Classic PIN* were implemented using a 4-digit secret. The distance between the user and the input field was set to 1.5 m. The width of the input field (1.7 m) was chosen to occupy 60 degrees of the field of view, as done by George et al. [10]. This results in button sizes of 14 cm for *C-Lock* and 28 cm for the other schemes.

For *RoomLock*, we used the variant of *Room Lock* that randomizes objects and modified it to allow an object to appear only once in the secret (see Section III). To match the password space of 10^4 for a 4-digit secret, the number of objects was increased from 9 to 12. We used free assets from the Unity asset store to recreate the scheme as closely as possible to the authors' version [9].

For the *PassGlobe* scheme, we were able to use the original implementation by Länge et al. [17]. Here, the password space depends on the tolerance distance. If the distance between the target location and the user's input is within this tolerance, the input is considered correct. With their implementation, the distance is chosen so that it would be equivalent to dividing the globe into 350 areas of equal size. This results in a password space of about 10^5 for a 2-digit secret. We decided to keep it this way because it is questionable how well the usability would translate to different area sizes. In this way, this scheme has a slight disadvantage compared to the other schemes in our study. To display the secret in *PassGlobe* during enrollment, two markers are placed on the corresponding areas of the globe, like pins on a map, and users can rotate the globe to see and remember them. In addition, images of the areas are displayed above the globe.

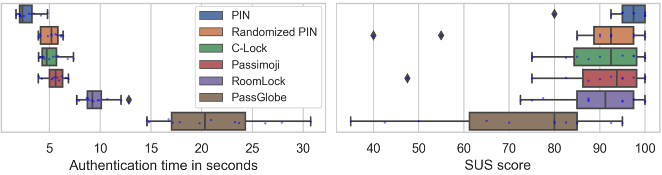

Fig. 3. Top: Mean authentication time in seconds. Bottom: Mean SUS score.

A delete button to undo the previous input was added to all schemes except *PassGlobe*. Here, the user can correct their inputs by moving the marker to another location before confirming the input (see video [16]). The delete button for *Passimoji* replaces the input field with the previous set of images in a random order again, while in the other schemes the state of the input field does not change and it just removes the last input.

Shoulder-Surfing Resistance. As discussed in sections II and III, our goal is to achieve fully shoulder-surfing resistant authentication. We chose not to perform a typical shoulder-surfing evaluation for this study because we can analyze potential threats in advance. There are three possible channels through which information about the secret can leak: (1) hand movement, (2) head movement, and (3) controller input. The schemes *Randomized PIN*, *Passimoji*, and the modified version of *Room Lock* are designed to prevent any information leakage to an attacker, even if they have access to all information about (1), (2), and (3) because they do not know the random order displayed on the HMD's screen. In addition, we cannot think of a way for the user to leak information about the order by their movements. However, *PassGlobe* and *C-Lock* have a natural order, which makes them vulnerable to information leakage by user's behavior. Länge et al. [17] previously noted that users of *PassGlobe* may orient the globe with the equator horizontal. Additionally, we see a small risk that users of *C-Lock* may always start their search at the zero button. We will monitor participants for these behaviors during the study.

B. Results

We collected 360 measurements during the study: 12 participants × 6 schemes × 5 attempts. For each scheme, we evaluated (1) the authentication time for each attempt, starting when the start button was pressed and ending when the last digit was entered, (2) the success rate, (3) the SUS score, and (4) feedback from the questionnaire. In the next sections we first report our results and then perform a Friedman test to analyse the data. For post-hoc pairwise comparison we use the Wilcoxon signed-rank test with the zero method by Pratt and Bonferroni-Holm correction.

Authentication Time. To calculate authentication times, we only included successful authentication attempts to avoid skewing the results due to speedy incorrect entries. *Classic PIN* (Mean M = 2.75, Median Med = 2.31, Standard Deviation SD = 0.97) without any protection against shoulder-surfing is the fastest. Followed by *Randomized PIN* (M = 5.09, Med = 5.18, SD = 0.91), *C-Lock* (M = 5.11, Med = 4.71, SD = 1.11), and *Passimoji* (M = 5.51, Med = 5.61, SD = 1.05). The slowest authentication schemes are *RoomLock* (M = 9.62, Med = 9.23, SD = 1.56) and *PassGlobe* (M = 21.14, Med = 20.34, SD = 5.28). The results are summarized in Fig. 3. Friedman's test shows a significant difference in authentication time ($\chi^2(5) = 53.286, p < .001$). Post-hoc pairwise comparison reveals significant differences between *Classic PIN* and all other schemes ($Z = -3.059, p = .033$). Additionally *Passimoji*, *C-Lock* and *Randomized PIN* each have a significantly lower authentication time than *RoomLock* and *Passglobe* ($Z = -3.059, p = .033$). All other pairwise comparisons show no significance ($p > .408$).

Success Rate. We consider an authentication attempt to be successful if the submitted secret matches the given secret. The success rate is calculated as the ratio of successful authentications to the total number of authentications. There are no differences in the success rates of *Classic PIN*, *Passimoji*, and *RoomLock*, as no secrets were entered incorrectly (M = 100.00, Med = 100.00, SD = 0.00). One error out of $12 \times 5 = 60$ attempts was made with *PassGlobe* and *C-Lock* (M = 98.33, Med = 100.00, SD = 5.77) and three with *Randomized PIN* (M = 95.00, Med = 100.00, SD = 9.05). Friedman's test shows no significant difference in success rate ($\chi^2(5) = 10.789, p = .056$).

Satisfaction (SUS). The SUS score is highest for the familiar *Classic PIN* (M = 96.04, Med = 97.50, SD = 5.69). *C-Lock* (M = 90.42, Med = 92.50, SD = 9.40), *RoomLock* (M = 89.38, Med = 91.25, SD = 9.84), *Passimoji* (M = 88.54, Med = 93. 75, SD = 15.02) and *Randomized PIN* (M = 86.04, Med = 92.50, SD = 18.81) are also rated above 85. *PassGlobe* has the lowest score (M = 71.88, Med = 80.00, SD = 19.78). Friedman's test shows a significant difference in the SUS score ($\chi^2(5) = 23.078, p < .001$). Pairwise comparison shows only a significant difference between *Classic PIN* and *PassGlobe* ($Z = -3.024, p = .037$). All other pairwise comparisons show no significance ($p > .242$).

Observations. During the study, we made a few notable observations: (1) Sometimes, people started authenticating without really looking at the secret because they realized they could see it all the time. (2) For *PassGlobe*, we observed all the problems the authors [17] speculated about regarding usability and security (see Section III). (3) Rotating the globe contributed most to the authentication time instead of the time needed to accurately select the target location. (4) The amount of head movement required to see all the objects in *RoomLock* was criticized by two people. (5) One person said that the categories in *Passimoji* confused them more than helped them. (6) We did not observe any participant starting their search at a specific number when using *C-Lock*. (7) Overall, participants corrected their input only a few times: Three times using *C-Lock* and *RoomLock*, and twice using *Randomized PIN*.

VI. Discussion and Limitations

In our study *Passimoji*, *C-Lock* and *Randomized PIN* all show promising results. With a mean authentication time of 5.1 - 5.5 seconds, they are on average only 2.3 - 2.7 seconds slower than *Classic PIN*, trading higher security for slightly lower usability. Furthermore, they outperform other shoulder-surfing resistant schemes with authentication times $\geq$ 9.6 seconds while maintaining similar performance in terms of success rate ($\geq$ 95 %) and user satisfaction (SUS $\geq$ 86). The fact that *Randomized PIN* has the fastest authentication time of all shoulder-surfing resistant schemes may be due to familiarity with PIN schemes. *Passimoji* may see faster times once users have memorized their emojis and can recognize them more quickly.As all schemes use a simple 2D interface for interaction, these schemes might also be suitable for the AR/MR context.

Compared to the results from the original paper for *RoomLock* (14.3 seconds [9]), authentication time in our study is lower (9.6 seconds), despite having more objects (12 vs. 9). It is possible that our implementation was significantly different or that our participants were able to complete the task at a faster rate. However, our average authentication time for *Classic PIN* (2.8 seconds) is higher than that measured by George et al. (2.38 seconds [10]). Therefore, no clear trend becomes apparent in comparison to prior work.

In our evaluation, the existing schemes *RoomLock* and *PassGlobe* demonstrated flaws. The main problem participants encountered when using *RoomLock* was that the password elements were further apart than in the other schemes. This could be alleviated by moving the objects closer in the user's field of view, which would make it very similar to *Passimoji* with 3D objects instead of 2D images. For the *PassGlobe* scheme, we found that it is not fully resistant to shoulder-surfing in the real world, and therefore is not suitable for shoulder-surfing resistant VR. Although this could be mitigated by using a larger password space, we don't see a way to significantly improve authentication time. Although participants in our study did not show any information-leaking behavior when using *C-Lock*, this is something that should be evaluated in a larger study before deciding to declare it fully shoulder-surfing resistant.

It is also important to keep in mind the limitations of increasing the password space. This would result in more columns for *C-Lock*, more objects for *RoomLock* and new unique sets of emojis for *Passimoji*. This could lead to a negative influence on usability, but might be mitigated with adjustments to the schemes. Some other limitations of our study to consider: small sample size using convenience sampling, narrow age range, long duration of the study, assigned password visible during authentication, and different password space for *PassGlobe*. These result in a study that is less representative of the overall population, but may still provide a good indication of potentially promising authentication schemes for VR that are resistant to shoulder-surfing and might be worthwhile to study with a larger sample and a study setting that results in a higher external validity of the results.

VII. Conclusion

In this paper, we presented three shoulder-surfing resistant authentication schemes for VR HMDs. All employ a virtual pointer to interact with the 3D space and randomization to completely withstand shoulder-surfing attacks. The concepts are PIN-based and build on previous work on authentication schemes. We conducted a user study comparing them to other VR authentication schemes. The study indicates that *Passimoji*, *C-Lock*, and *Randomized PIN* are promising authentication schemes as they deliver authentication times shorter than other shoulder-surfing resistant schemes and all have mean SUS scores of 86 or above. Thus, we plan to evaluate these schemes in a more extensive study with more participants.

Acknowledgment

This research was further supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

References

[1] K. Ahir, K. Govani, R. Gajera, and M. Shah, "Application on virtual reality for enhanced education learning, military training and sports," *Augmented Human Research*, vol. 5, pp. 1–9, 2020.

[2] L. P. Berg and J. M. Vance, "Industry use of virtual reality in product design and manufacturing: a survey," *Virtual reality*, vol. 21, pp. 1–17, 2017.

[3] J. Brooke, "Sus: A quick and dirty usability scale," *Usability Eval. Ind.*, vol. 189, 11 1995.

[4] D. W. Carruth, "Virtual reality for education and workforce training," in *2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. Piscataway, New Jersey: IEEE, 2017, pp. 1–6.

[5] A. De Angeli, M. Coutts, L. Coventry, G. I. Johnson, D. Cameron, and M. H. Fischer, "Vip: A visual approach to user authentication," in *Proceedings of the Working Conference on Advanced Visual Interfaces*, ser. AVI '02. New York, NY, USA: Association for Computing Machinery, 2002, p. 316–323. [Online]. Available: https://doi.org/10.1145/1556262.1556312

[6] R. Duezguen, P. Mayer, S. Das, and M. Volkamer, "Towards secure and usable authentication for augmented and virtual reality head-mounted displays," *CoRR*, vol. abs/2007.11663, 2020. [Online]. Available: https://doi.org/10.48550/arXiv.2007.11663

[7] R. Düzgün, P. Mayer, and M. Volkamer, "Shoulder-surfing resistant authentication for augmented reality," in *Nordic Human-Computer Interaction Conference*, ser. NordiCHI '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3546155.3546663

[8] C. George, D. Buschek, A. Ngao, and M. Khamis, "Gazeroomlock: Using gaze and head-pose to improve the usability and observation resistance of 3d passwords in virtual reality," in *Augmented Reality, Virtual Reality, and Computer Graphics*, L. T. De Paolis and P. Bourdot, Eds. Cham: Springer International Publishing, 2020, pp. 61–81.

[9] C. George, M. Khamis, D. Buschek, and H. Hussmann, "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)*. Piscataway, New Jersey: IEEE, 2019, pp. 277–285.

[10] C. George, M. Khamis, E. von Zezschwitz, M. Burger, H. Schmidt, F. Alt, and H. Hussmann, "Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality," in *In Proceedings of the Network and Distributed System Security Symposium (NDSS 2017)*, NDSS. San Diego, California, USA: NDSS, 02 2017.

[11] J. Gurary, Y. Zhu, and H. Fu, "Leveraging 3d benefits for authentication," *International Journal of Communications, Network and System Sciences*, vol. 10, no. 8, pp. 324–338, 2017.

[12] A. Gutmann, K. Renaud, J. Maguire, P. Mayer, M. Volkamer, K. Matsuura, and J. Müller-Quade, "Zeta-zero-trust authentication: Relying on innate human ability, not technology," in *2016 IEEE European Symposium on Security and Privacy (EuroS P)*. Piscataway, New Jersey: IEEE, 2016, pp. 357–371.

[13] J. M. Jones, R. Duezguen, P. Mayer, M. Volkamer, and S. Das, "A literature review on virtual reality authentication," in *Human Aspects of Information Security and Assurance*, S. Furnell and N. Clarke, Eds. Cham: Springer International Publishing, 2021, pp. 189–198.

[14] L. Kraus, R. Schmidt, M. Walch, F. Schaub, C. Krügelstein, and S. Möller, "Implications of the use of emojis in mobile authentication," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016. [Online]. Available: https://www.usenix.org/conference/soups2016/workshop-program/way2016/presentation/kraus

[15] Y. Li, Y. Cheng, Y. Li, and R. H. Deng, "What you see is not what you get: Leakage-resilient password entry schemes for smart glasses," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, ser. ASIA CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 327–333. [Online]. Available: https://doi.org/10.1145/3052973.3053042

[16] T. Länge and P. Matheis, "Vision: Towards fully shoulder-surfing resistant and usable authentication for virtual reality," Jan 2024. [Online]. Available: osf.io/3pjtw

[17] T. Länge, P. Matheis, R. Düzgün, P. Mayer, and M. Volkamer, "Passglobe: Ein shoulder-surfing resistentes authentifizierungsverfahren für virtual reality head-mounted displays," in *Mensch und Computer 2022 - Workshopband*, K. Marky, U. Grünefeld, and T. Kosch, Eds. Bonn: Gesellschaft für Informatik e.V., 2022.

[18] A. Maiti and K. Crager, "Randompad: Usability of randomized mobile keypads for defeating inference attacks," in *Proceedings of the IEEE Euro S&P Workshop on Innovations in Mobile Privacy & Security (IMPS)*. Piscataway, New Jersey: IEEE, 2017.

[19] F. Mathis, J. H. Williamson, K. Vaniea, and M. Khamis, "Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing," *ACM Trans. Comput.-Hum. Interact.*, vol. 28, no. 1, Jan. 2021. [Online]. Available: https://doi.org/10.1145/3428121

[20] I. Olade, H.-N. Liang, C. Fleming, and C. Champion, "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*, ser. ICVARS 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 45–52. [Online]. Available: https://doi.org/10.1145/3385378.3385385

[21] A. Paivio and K. Csapo, "Picture superiority in free recall: Imagery or dual coding?" *Cognitive psychology*, vol. 5, no. 2, pp. 176–206, 1973. [Online]. Available: https://doi.org/10.1016/0010-0285(73)90032-7

[22] J. Wang and B. Gao, *Analysis of Multi-attribute User Authentication to Against Man-in-the-Room Attack in Virtual Reality*. Cham, Switzerland: Springer International Publishing, 07 2021, pp. 455–461.

[23] D. K. Yadav, B. Ionascu, S. V. Krishna Ongole, A. Roy, and N. Memon, "Design and analysis of shoulder surfing resistant pin based authentication mechanisms on google glass," in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–297.

[24] Z. Yang, Y. Chen, Z. Sarwar, H. Schwartz, B. Y. Zhao, and H. Zheng, "Towards a general video-based keystroke inference attack," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 141–158. [Online]. Available: https://www.usenix.org/conference/usenixsecurity23/presentation/yang-zhuolin

[25] Z. Yang, Z. Sarwar, I. Hwang, R. Bhaskar, B. Y. Zhao, and H. Zheng, "Can virtual reality protect users from keystroke inference attacks?" *arXiv preprint arXiv:2310.16191*, 2023. [Online]. Available: https://doi.org/10.48550/arXiv.2310.16191

[26] Z. Yu, H.-N. Liang, C. Fleming, and K. L. Man, "An exploration of usable authentication mechanisms for virtual reality systems," in *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*. Piscataway, New Jersey: IEEE, 2016, pp. 458–460.