Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality

Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt
Florian Alt, Heinrich Hussmann
LMU Munich, Media Informatics Group, Germany
{ceenu.george, mohamed.khamis, emanuel.von.zezschwitz, florian.alt, heinrich hussmann}@ifi.lmu.de
{h.schmidt, marinus.burger}@campus.lmu.de

***Abstract*—**

Virtual reality (VR) headsets are enabling a wide range of new opportunities for the user. For example, in the near future users may be able to visit virtual shopping malls and virtually join international conferences. These and many other scenarios pose new questions with regards to privacy and security, in particular authentication of users within the virtual environment. As a first step towards seamless VR authentication, this paper investigates the direct transfer of well-established concepts (PIN, Android unlock patterns) into VR. In a pilot study ($N = 5$) and a lab study ($N = 25$), we adapted existing mechanisms and evaluated their usability and security for VR. The results indicate that both PINs and patterns are well suited for authentication in VR. We found that the usability of both methods matched the performance known from the physical world. In addition, the private visual channel makes authentication harder to observe, indicating that authentication in VR using traditional concepts already achieves a good balance in the trade-off between usability and security. The paper contributes to a better understanding of authentication within VR environments, by providing the first investigation of established authentication methods within VR, and presents the base layer for the design of future authentication schemes, which are used in VR environments only.

I. Introduction

Virtual Reality has recently become popular amongst consumers [27], [31] due to the technological advancements and the increased usability of the latest devices. The latter is influenced by two developments: Firstly, Head Mounted Displays (HMDs) such as the HTC Vive and the Daydream View [36], [37] are readily available for households. Secondly, these devices allow users to experience a virtual world at their leisure with a great level of immersiveness [23].

HMDs are ubiquitous devices and high-end models are striving towards being wireless [2]. Without the physical connection to the PC, the device becomes a self contained headset with no external [physical] display. It is no longer possible to login via keyboard and similarly not obvious who is logged in when mounting the headset. Furthermore, sharing them within a household or organization is a sought after context, thus evolving from a single-user interaction model to a multi-user one.

USEC '17, 26 February 2017, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2017.23028

Fig. 1: We investigate how to create seamless and secure authentication in VR. In particular, we compare different screen sizes, input modalities, and password types with regard to how secure they are against attackers in the real world. The left image shows a sample view of a [virtual] large display supporting lock pattern input in VR. The right image shows a user in the real world, authenticating in this environment whilst being observed by an attacker. The user is wearing a head mounted display (HMD) and holding one controller in each hand to enable interaction in VR.

Although early adopters of VR have mainly been game developers, some players in the e-commerce industry are entering the market [11]. In addition, previous research has highlighted the need for convenient authentication during payment [26]. We opted to focus on e-commerce, especially the authentication process, as the most relevant use case. However, there are numerous other scenarios where authentication would be needed, such as telepresence meetings or access to virtual resources owned by a company. Digital real-time handshakes may be done through authentication, for example at a virtual conference, where it will be crucial for the perception of security to confirm the identity with a known attribute between multiple subjects in VR. The above points combined with the fact that users long for a perception of security and trust during engagement in VR [35], motivate the need for authentication within the virtual world.

While authentication has been explored for multiple do-

mains [52], [57], to our knowledge, seamless authentication in VR, without taking the HMD off, has not been explored. We argue that it is not acceptable from a user experience viewpoint to require users to constantly take off the VR headset in order to provide credentials (e.g., credit card number) to perform an in-app purchase. A simple solution might be that users could provide their sensitive credentials only once on a desktop computer. Users could then access these credentials by seamlessly authenticating from within the VR environment without having to take off the headset. It is an interesting question whether existing concepts for authentication in the real world can be transferred to interaction within virtual worlds. Furthermore, we believe VR has the potential to act as a feasible research tool for usable security studies. We envision that authentication methods will be an essential part of VR in the near future and understanding their constraints allows the design of more adequate solutions. To close this gap, this paper evaluates whether currently established methods from other domains (e.g., [physical] public displays [34] and mobile phones) are feasible in a VR environment. Our choice to model virtual counterparts of [medium sized physical] public displays and [small sized physical] mobile phones into virtual reality is due to their difference in size and placement, allowing us to build on existing research to create a broad design space for virtual authentication surfaces in VR. We conducted a lab study which explored eight concepts (2 password types $\times$ 4 input modalities) to understand their usability, and applicability to VR. Furthermore, we explore the security of these schemes by evaluating their resistance to observation attacks. We observed that VR experiences differ from previous research on observation-resistant authentication because (1) the observer does not have any visual cues (such as a [physical] mobile display), (2) mid-air interactions (with [virtual] controllers) provide a new channel for observing password related information or hints about the observed password, and (3) users that are immersed in the VR experience do not notice that someone is observing them during authentication, leading to a decrease in awareness of their surroundings. Thus, we conducted a security study to measure the observability of the previously mentioned methods.

A. Contribution Statement

The contributions of this work are threefold: (1) We describe the concept development and implementation of multiple authentication methods for VR, which are based on previous work in the domains of [physical] public displays and [physical] mobile devices. (2) We report on our findings from a lab study ($n = 25$) where we investigated the usability and security of the proposed methods. (3) We discuss the usability and security implications of authentication in VR. Our findings are valuable to designers and practitioners working on authentication mechanisms in VR who need to get a better understanding of this problem and design space before creating novel ideas.

II. Related Work

Our work builds on two main strands of related work: (1) Interaction in virtual reality, and (2) established authentication concepts in other environments.

A. Interaction in VR

One challenge of interaction with objects in VR is the lack of tactile feedback. This issue is known to influence the usability of input systems in VR [15]. Over the years, haptic or force feedback has tried to fill this gap with promising results: One example is in VR training [49], where surgical procedure is practised in VR and interactions are aided by haptic feedback to mimic real world progress. According to Leung et al. [28], this form of feedback was also shown to reduce cognitive load on mobile devices when it replaces certain parts of the graphical interface. This finding is interesting for VR, as the 3D environment relies heavily on graphical interfaces and could hence benefit from reducing the visual cognition, which often leads to visual fatigue [48]. As a result of these findings, we implemented haptic feedback into our concepts.

Using pointers (i.e., virtual laser beam) was discouraged as an interaction method in VR, as (1) they are not a natural way of interacting in real life without additional hardware and (2) due to (previous technological) lack of precision [19]. However, the accuracy, that state-of-the-art HMD controllers provide, combined with the successful results of pointer interaction on [physical] public displays [46], [10], encourage revisiting the usability of this input method. Another way to interact in VR is by tapping, which was also shown to be promising for interactions in the real world [4]. Hence we decided to consider both, tapping and pointers in our concept development.

According to McGill et al. [32] "Immersiveness is quantified by presence" and presence is affected by the visual quality of the scene. Other factors that influence presence include the quality of the HMD's head tracking, and even how users interact with virtual objects [22]. All of the above mentioned points have increased in quality and usability over the last few years, which leads to fully immersed users in VR who are less aware of their surroundings [32]. With this lack of awareness, VR users become more susceptible to observers from the real world, who could eavesdrop users as they authenticate in VR.

B. Authentication concepts in other environments

Previous research on authentication in virtual environments on 2D devices has highlighted the value of 3D passwords as an alternative to common authentication mechanisms, with the assumption that they are highly secure whilst also being less prone to shoulder surfing attacks [3], [12], [29]. As 3D passwords are not yet widely accepted, we start with accepted methods, namely PINs and Patterns (Android Unlock Pattern). They (1) are the status-quo for time-efficient authentication [52] and (2) are well integrated in current infrastructures (e.g., database backends). Although PINs and Patterns are widely used on mobile devices, one of the main drawbacks of this authentication mechanism is that they are prone to observation attacks [24], [30], [50], [52], [58].

Biometric authentication is gaining in popularity on commercial devices [17]. However, unlike knowledge-based schemes, biometric passwords are hard to reissue. Furthermore, privacy aware users are hesitant towards sharing their biometric data with third-parties [38]. Although biometric authentication is an important ongoing research area for HMD interaction [40], [42], this paper only focuses on the still indispensable knowledge-based authentication mechanisms.

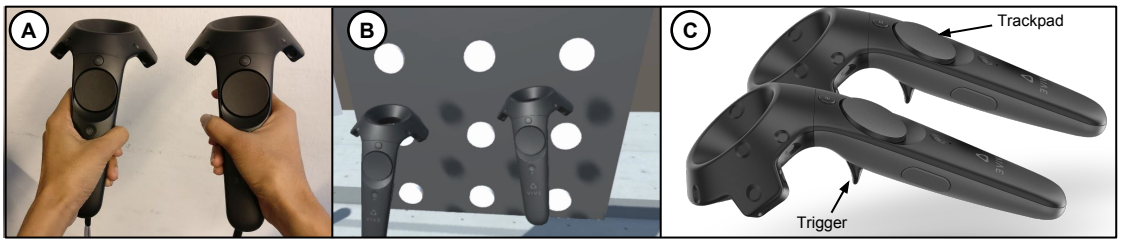

Fig. 2: HTC Vive controllers have the same look and feel in the virtual and real world. Figure (A) shows a view of the physical controllers in the real world during the study. Figure (B) shows how they are replicated in the virtual world. Figure (C) shows the buttons we utilized for the different input modalities: *Pointer* uses only the trigger whereas $Pointer_{onclick}$ uses a combination of the trigger and trackpad.

Mid-air authentication schemes have been evaluated in real world scenarios [7], [39], [56], [57], showing promising results from a usability and security perspective. Yadav et. al [57] explored PIN entry in augmented reality systems which were perceived to be usable but entry times were substantially higher than on mobile phones (Google Glass = $\sim$ 8s-14s, Mobile Phone = $\sim$1.96s [20]). However the combination of existent visual cues and mid-air interactions has not been explored in prior research to our knowledge.

Although observers do not perceive the visual cues (view of VR scene) that the users see, previous research has pointed out other sources that support guessing the password. For example, Sasamoto et. al [41] found that haptic feedback from the input system provides insight into the correct password. Previous work investigated risk of side channel attacks through oily residues [8], [43], [53] and heat traces [1], [33] of the users' fingers left on the hardware. Although these types of attacks may be applicable to the VR setting in the future, for example after development of biometric authentication, we do not believe that they are applicable at this point in the technological development of the HMD. In this paper we provide the first evaluation of the usability and security of different established authentication methods in VR based on PINs and patterns, to provide an understanding for authentication during commercial and collaborative scenarios in VR.

III. Threat Model

In our threat model, the victim is wearing an HMD and interacting with a virtual world (virtual or mixed reality). The victim is authenticating in that environment in the presence of others. In our scenario the setting is a personal living room, where friends and family are present [21]. Anyone surrounding the victim in the real world has perfect sight on the hand movements that are performed in order to interact with the authentication system, but cannot see what the user sees in the HMD. Unlike shoulder surfing in the real world [16], the attacker in our threat model has the advantage of not being seen by the user. The victim authenticates with PIN and pattern in order to complete an in-app purchase during game play and immediately after authenticating, she takes off the headset in order to step out for a break. The attacker picks up the headset, continues playing the game and when prompted authenticates for another in-app purchase with the victim's password.

IV. Pilot study and Concept Development

At the outset of our work we conducted a pilot study to identify important design factors and explore different modalities. In particular, we compared (1) different input modalities, (2) different sizes of the input screen, and (3) different password types. Results from the pilot study serve as the basis for an in-depth investigation of security in the subsequent main study.

A. Study Design

The study followed a repeated measure design, with size of input surface, password type, and input modality being the independent variables. Password types (PIN and pattern) and input modalities are based on existing research in the field of usable security as well as on properties of commercial VR controllers, such as the [phyisical] HTC Vive controllers that the user is always holding during the study (Fig.1). The size of input surfaces was chosen based on [virtual] interactive surfaces that we expect to be commonly available in VR environments.

The following sections describe the independent variables and their characteristics. With these variables, we are describing variations of the input modalities and input surfaces which are offered to the user in the virtual world. In adherence with established interaction practices for VR [6], [25], [47], we also displayed a virtual representation of the physical controller in virtual reality (Figure 2AB). There was a one-to-one mapping between the two, hence the location and the visual representation of the controllers were the same in the real and virtual world.

1) Input Modalities: We defined six different input modalities. They are motivated by the input capabilities of state-of-the-art VR controllers.

Firstly, we compare different [virtual] laser pointers that differ in how selections are made on the [physical] controller.

Pointer This [virtual] pointer is constantly visible during the authentication process, casting a [virtual] beam on the authentication interface. Selections are made by a button press (Figure 2C).

$Pointer_{onclick}$ In contrast to the first [virtual] pointer, a [virtual] beam is only cast upon a button press on the [physical] controller. To make a selection, a second [physical] button press is required (Figure 2C).

Furthermore, we included two versions of tapping by means of the [physical] VR controller.

Tap For this interaction modality, users authenticate by tapping the [virtual] authentication surface with the [virtual] VR controller. This is an adopted form of touching a screen,

Input Modalities	Size of input interface		
	$\text{Surface}_{\text{large}}$	$\text{Surface}_{\text{medium}}$	$\text{Surface}_{\text{small}}$
Pointer	Large/Pointer	Medium/Pointer	
$\text{Pointer}_{\text{onclick}}$	$\text{Large/Pointer}_{\text{onclick}}$	$\text{Medium/Pointer}_{\text{onclick}}$	
Tap		Medium/Tap	
$\text{Tap}_{\text{onclick}}$		$\text{Medium/Tap}_{\text{onclick}}$	
Stylus			Small/Stylus

TABLE I: Overview of conditions used in the pilot study. Highlighted concepts showed promising results in the pilot study, hence they were defined as conditions in the main study.

as we know it from [physical] public displays [5], using ones hand.

$\text{Tap}_{\text{onclick}}$ We included a modality, where users would press a [physical] controller button, subsequently hover over the [virtual] element to select, and finally release the [physical] button to make the selection. This mimics the behavior of pattern input on a [physicial] touch screen where only lifting the finger finalizes the input, instead of a dedicated confirm button [13].

Finally, we included a stylus type interaction modality.

Stylus Adapted from the interaction on [physical] mobile devices, a pen-like interaction modality, commonly known as stylus, was modelled into VR to allow for interaction with small [virtual] surfaces.

2) Size of Input Surface: We experimented with three sizes of the input surface in the pilot study. Due to their size and nature, each of them can only be navigated with a specific input modality.

$\text{Surface}_{\text{large}}$ Unlike in the real world, VR allows interactive surfaces to be easily integrated with arbitrary objects. Hence, authentication can be seamlessly integrated with the user's task. We found the idea to enable interaction on a large-sized [virtual] surface particularly compelling, since this could allow authentication from afar as well as while the user is moving.

$\text{Surface}_{\text{medium}}$ Motivated by work on [physical] public displays, we opted to investigate medium-size [virtual] surfaces where interaction is within arm's reach [9]. As input modalities we compare both [virtual] pointer and both [virtual] tap modalities.

$\text{Surface}_{\text{small}}$ Finally, we decided to include small surfaces as known from personal devices, such as smartphones. Here, the [virtual] authentication interfaces were projected onto the [virtual] controller held by the user's non-dominant hand (Fig.2B). As interaction modalities we used the [virtual] stylus.

In the pilot study the above mentioned *input surfaces* and *input modalities* were tested as combined concepts. All tested combinations are depicted in Table I.

3) Password Types: Our research focuses on the usability and observability of established *Password types*, namely PIN and Pattern. PIN describes a numerical authentication method and Pattern is based on the Android Lock Pattern. Our implementation of the authentication schemes was similar to the respective implementations on mobile devices. The interface of PINs (Figure 3A) consisted of 10 digits (0-9), a button to clear the last digit, and a submit button. While the interface of Patterns (Figure 3B) consisted of a 9-point grid.

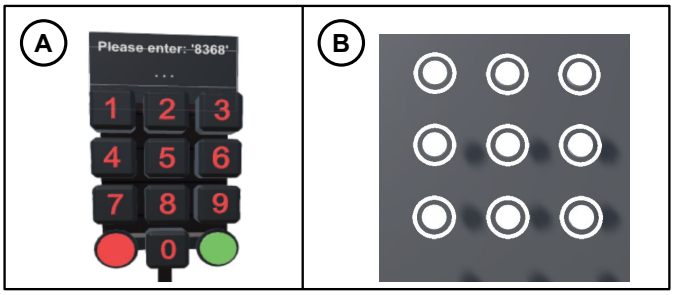

Fig. 3: Our [virtual] implementation of the PIN pad imitates the usage on mobile phones. The special characters (e.g., back button) are replaced by a red button for deleting the last digit and a green button for submitting the four digit PIN (A). The [virtual] interface of patterns consisted of a 9-point grid (B).

B. Apparatus

We used Unity 3D and an HTC Vive headset with controllers for our prototype implementation. For interfacing with the HTC Vive we relied on the SteamVR Plugin for Unity provided by Valve software, which handles camera and controller tracking while providing easy access to button states and haptic feedback. The latter was provided to the customer through the [physical] controller (Figure 3C), upon selection of a button for PIN and upon selection of a cell grid for pattern. All programming was done in C#.

We created a controller script which (1) would alternate the input methods presented to the participants according to a predefined latin square and (2) generate the visual of the correct password to be entered. This script would then also track successful and failed input attempts and automatically advance to the next step after the desired number of inputs.

C. Procedure

A total of 5 participants (mean age=24 SD=1.6, 2 females) took part in the pilot study. To start, we asked them to sign a consent form. Then they were taken through a training in virtual reality and introduced to the input surfaces and interaction modalities. Once they felt comfortable, they were asked to enter a pre-defined PIN and password for each condition.

D. Results and Implications

The concepts in Figure I showed promising results. As such they were chosen to be analyzed further as part of the main study. In the following we summarize the results that led to our concept choices and discuss in detail the implications for their designs. In the main study they are defined as conditions. The following naming convention is used: SurfaceSize/Modality.

1) Large Surfaces: When authenticating with a [virtual] pointer on the large [virtual] surface, we noticed that users performed noticeable head movements. We found this to clearly aid the observability of the entered password/PIN. To weaken the effect, we decided to adjust the size of the authentication surface (γ), considering the field of view in the HMD (FOV: 110°), the degree of perception for near-peripheral vision (α:

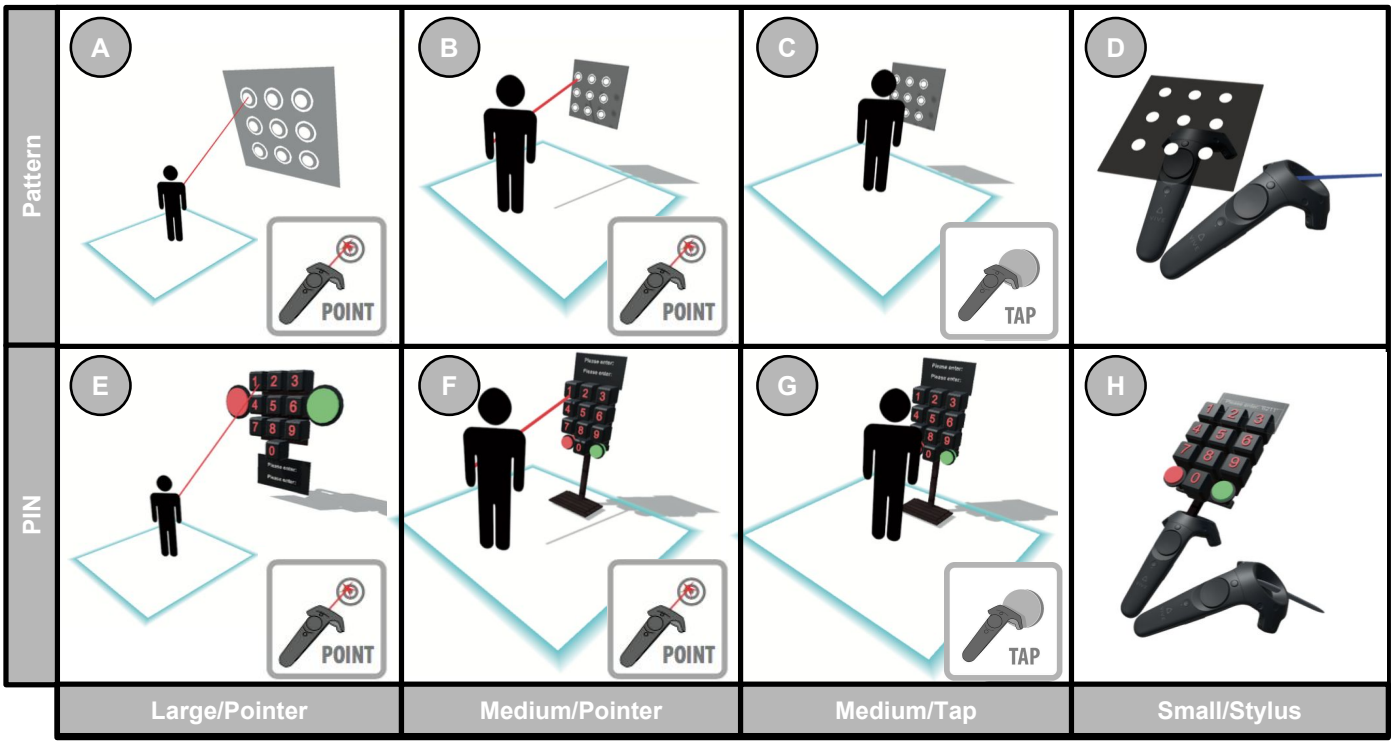

Fig. 4: The figure illustrates the different [virtual] *input surfaces* and [virtual] *input methods* that we experimented with for patterns (A, B, C and D) and PIN based interfaces (E, F, G, and H). We covered pointer-based input methods (A, B, E, F), where a [virtual] laser-like pointer is used to signal input, [virtual] tap-based methods (C, G), in which the user touches the UI elements with the [virtual] representation of the physical controller held by the user, and finally stylus-based methods (D, H), where the user had a [virtual] short-range pointer that allows interaction with small [virtual] close-by surfaces. The images show the [virtual] presentation of the input surfaces. The stylus-based methods (D, H) also show the [virtual] representation of the physical controller, in addition to a [virtual] input surface is mounted onto the [virtual] controller. The [virtual] avatar is a mock-up representation of the [physical] participant in each condition to illustrate the proportional distance to the [virtual] input surfaces.

60°), and the distance to input modality (β: 3.17m) using the following formula:

$$tan(\frac{1}{2} \times \alpha) \times 2 \times \beta = \gamma \quad (1)$$

Participants were able to perform accurate input with both [virtual] pointers on the large [virtual] surface. Yet, participants had a preference for the always visible [virtual] pointer. In addition they found it quite challenging to press two [physical] buttons concurrently while focusing on the authentication task. Hence, we decided to exclude the onclick [virtual] pointer from further investigations. For the main study we defined a condition: Large/Pointer (Figure 4A,E).

2) Medium Surfaces: Also for medium size [virtual] surfaces, participants performed well with both the regular [virtual] pointer and with the onclick [virtual] pointer. Yet, again, the onclick feature turned out to be distracting during the main task of authentication. As a result we decided to use only the regular [virtual] pointer for the main study. We made similar observations for [virtual] tap. While the regular [virtual] tapping could be easily performed, participants struggled to understand how the [physical] controller can be used in the onclick variant. Therefore, we chose to use Tap for interaction with medium size [virtual] surfaces.

Hence we added two more conditions to the main study: Medium/Pointer and Medium/Tap (Figure 4B,F).

3) Small Surfaces: Participants performed well with the [virtual] stylus, which is in line with prior research where text entry with short [virtual] laser pointers was found to be efficient [14]. However, we found that collisions between [physical] controllers frequently occurred as participants tried to make a selection with the [virtual] stylus controller in the dominant hand on the small [virtual] surface that was attached to the virtual representation of the controller held in the non-dominant hand. Hence, we display the [virtual] authentication interface at a small distance.

This resulted in adding another condition to the main study: Small/Stylus (Figure 4D,H).

E. Summary and Implications

Based on the results, we defined 8 input methods for the main study: 4 for PIN and 4 for patterns (see Figure 4).

Since password complexity can influence both usability (entry time, error rate) and security (observation resistance), we included passwords in the pilot study, that had a variety of characteristics. We chose characteristics that were shown to have an influence on the usability and security of passwords: Knight Moves, Intersections, and Overlaps. A knight move is a term used by von Zezschwitz et.al to describe the connection of two non-neighbouring cells on a pattern grid [51]. In addition

to characteristics defined in prior work, we added "Translations" which we define as PINs/patterns that can exist in multiple relative locations on the authentication grid (see example in Figure 5). We found that translatable PINs/patterns are more difficult to observe due to the absence of visual cues from the observer's perspective.

Similarly, we considered characteristics of PINs that could potentially influence the difficulty of entering and observing them, for example repetitive or neighbouring digits [57], and translations. For the main study we decided to focus on translations exclusively, since the effect is similar to neighbouring digits. Repetitions were excluded for that they decrease the password space.

V. Main Study

We conducted a lab study to (1) examine whether established usable security mechanisms can be adapted to virtual reality systems with HMDs and (2) explore the usability and security of the tested authentication methods in Virtual Reality.

There is no IRB for these kinds of studies at our institution, nonetheless we adhered to known standards (e.g., collected data anonymously) within the research area, made participants aware of the data sharing policy, and obtained their consent to publish the results.

A. Study Design

1) Independent Variables: The study followed a repeated measure design. Conditions were counterbalanced using a Latin square. We specified two independent variables, as described in the previous section:

1) Four combinations of [virtual] surface size and input modality: (a) Large/Pointer, (b) Medium/Pointer, (c) Medium/Tap, and (d) Small/Stylus (see Figure 4)
2) Password type: (a) PIN, and (b) Pattern.

PINs had a length of four digits, while patterns had a length between five and six cells. This was done to make sure that PINs and patterns covered a comparable theoretical password space and hence were comparable [53]. Both password types were randomly generated, whilst also ensuring that the properties mentioned in the pilot study were equally distributed across the password space. Each participant had a random set of passwords and none of them were the same.

2) Dependent Variables: The dependent variables of the usability study were (1) *entry time*, captured from the start of the engagement with the [virtual] interface until the password was entered through an "Enter" button (standard interaction for PIN) or the end of the drawing action (for Pattern); and (2) *error rate*, measured with a binary system, such that if all cells were correctly entered the system would provide a success message (visual and in form of text).

For the observability study, the *success rate* of attacking a password was measured in two ways: Firstly binary, by measuring how many passwords were attacked successfully (1=successful, 0=unsuccessful). Successful means that the observed password matched all cells of the attacked password. Secondly, we evaluated the degree of success by using an (adapted) evaluation tool based on the Damerau-Levenshtein distance algorithm. For patterns, the algorithm calculates how many lines (connected by two cells) would have to be adjusted in order to match the correct password. Although participants had three guesses, only the guess with the least distance was considered for further analysis; that is, the guess that was closest to the correct password.

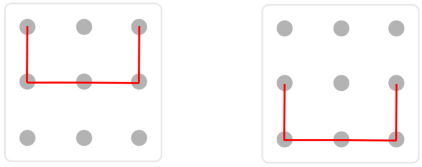

Fig. 5: Patterns that can exist at multiple locations on the grid. We refer to this move as a "Translattion"

B. Procedure

We used the same apparatus as in the pilot study. As participants arrived in the lab, participants did the usability study first. In the initial briefing they were given a printed paper with details on the procedure of the study. They were taken through the instructions and had the opportunity to ask questions. Then they were asked to complete a short questionnaire to capture demographic data and a likert scale questionnaire to obtain previous experience with virtual reality and password entry methods.

This was followed by an instruction on using the HTC Vive, the room setup and their play area (cf. Figure 1). Participants were also advised about possible risks when using an HMD and encouraged to stop at any point during the study if unwanted side effects occurred. Then, the HMD was mounted onto participants' heads and they were advised about the various forms of video recording. Whenever they felt ready in the virtual world, they were asked to verbally instruct to start the study. At the beginning of each study, participants were asked to complete a training session, which involved entering each password type three times successfully for each input method.

Upon completing the training session, participants proceeded with the actual study. Each password had to be successfully entered in each of three rounds to proceed to the next password. Participants were not limited in time and number of attempts within each round. However, after a possible second failed attempt, they were given additional verbal support by the instructor. After a successful attempt, the system would automatically move onto the next round. After all passwords were entered, the usability session was concluded by a questionnaire where participants provided subjective feedback about the input methods, and the perceived level of presence [44].

Subsequently, the security session was conducted (Figure 1, participant without an HMD is acting as the attacker) Participants were first explained the procedure: their task was to observe a user while authenticating in VR in real-time, and try to guess the entered password. Participants were given a pen and draft paper on which they could take notes while observing. We further provided participants with templates in which they could draw the observed patterns. The experimenter walked the

participants through the template and explained how to indicate the starting and ending node of each observed pattern. Each session consisted of 16 shoulder surfing attacks (2 attacks per condition). The passwords were entered by an expert VR user in order to reduce possible errors and to maintain a constant complexity level for all observations. The same expert VR user authenticated throughout the security session. Before each attack, the participant was told which password type and input method will be used, and was guided using the illustrations shown in Figure 4. Each of them had already taken part in the usability study with the same passwords, they were once again introduced to all the variants and educated to a point that they could be considered expert attackers. Participants were encouraged to move around freely within the physical space of the room to better observe the password in the real world. For each attack, participants could provide up to three guesses. They were then informed about the rewarding mechanism; in addition being offered a 10 EUR online shop voucher, all participants joined a raffle for an additional 20 EUR where each participant's chances of winning increased depending on how many passwords were successfully observed. This was done to encourage participants to put an effort in observing the passwords. We concluded with a semi-structured interview and a likert scale questionnaire to capture feedback on the tested input modalities.

C. Participants

Twenty-five participants were recruited from University mailing lists. A demographics questionnaire revealed that the average age was 23.28 (SD=2.5), and that 62% had no prior experience with VR but 80% used either PINs or Patterns before. There were 15 male and 10 female participants. All twenty-five participants took part in the usability and security study.

VI. Results

Our research did not aim at showing that one of the methods is superior to the other. Therefore we did not include hypotheses but rather followed a descriptive research approach to understand the performance of established methods.

The usability was measured with Likert scale questionnaires, by capturing entry times, error counts and by conducting semi-structured interviews. The shoulder-surfing vulnerability was measured in terms of performance and user opinion captured by a Likert scale questionnaire and a semi structured interview. We did not find any outstandingly performing participants in the usability and the security study.

A. Usability

1) Perceived Usability – After Usability Task: On a 5-point Likert scale (1=strongly disagree; 5=strongly agree), participants indicated preferences for ease of password entry and perception of security. Friedmans test showed that there was a statistically significant difference in perceived usability depending on which type of method was used for authentication, $\chi^2(7) = 23.99, p = 0.001$. Post hoc analysis with Wilcoxon signed-rank tests with Bonferroni correction elicited a statistically significant difference in usability perception between $\text{Medium}_{\text{pointer}}$ and $\text{Medium}_{\text{tap}}$ (Z = -2.64, p = 0.008). However, median usability rating was 4.0 for all conditions. There were no significant results found between the other methods (Figure 8). The Likert scale also showed that participants experienced a good presence (median=3).

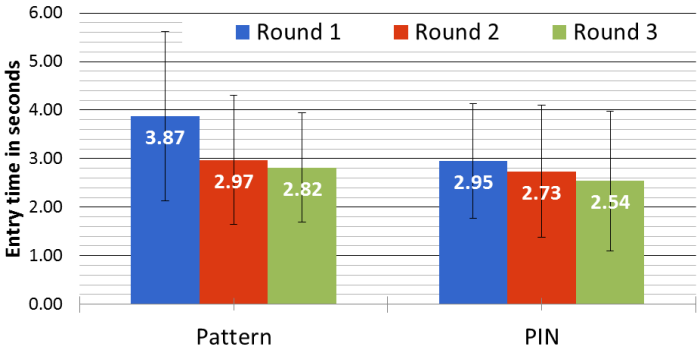

Fig. 6: Mean values and standard deviations for entry times across password type and round.

2) Entry Time: Visual inspection showed that our data was normally distributed and Mauchly's Test of Sphericity indicated that the assumption of sphericity had not been violated for the results described in this section.

A repeated measures ANOVA determined that password type had a significant effect on entry time ($F_{1,24} = 19.667$, $p < 0.001$). Post-hoc analysis showed a significant difference ($p < 0.001$) between pattern ($Mean = 3.22$, $SD = 0.118$) and PIN ($Mean = 2.743$, $SD = 0.126$).

Results showed that entry time differed statistically depending on configuration ($F_{3,72} = 16.877$, $p < 0.001$) across all passwords entered. $\text{Medium}_{\text{tap}}$($Mean = 3.6$, $SD = 0.18$) is significantly slower ($p < 0.001$) than all other methods for both PIN and Pattern entry time. The same phenomenon was also found to be true when comparing methods within each password type separately (Figure 7).

Figure 6 shows results that also indicated a positive learning curve for both password types ($F_{2,48} = 64.253$, $p < 0.001$). Pairwise comparisons confirmed ($p < 0.05$) that in round 3 ($Mean = 2.679$, $SD = 0.120$) participants completed the input 22% quicker than in round 1 ($Mean = 3.414$, $SD = 0.127$).

3) Error Rate: We also logged the number of errors performed by the users. The error rate was a binary value that is either true or false based on whether or not the user provided the entire PIN/Pattern successfully. Note, that in this study users were provided the passwords by experimenters.

From 81 wrong attempts (of a total of 1281 entries) across all rounds and passwords, 82% occurred during pattern entry and 18% during PIN entry. A possible explanation for this could be that pattern entry is a motor task. It has been shown that learning such tasks is in general slow and users get easily disrupted [45], which may have been the case in our VR setting.

B. Security

1) Perceived Security – Before Observation Task: We analyzed the perceived security after participants had entered passwords, but before they had started the observation task. Friedmans test showed that there was a statistically significant

difference in perceived security depending on which type of method was used for authentication, $\chi^2(7) = 35.40, p = 0.001$. Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significant difference in perception of security between $\text{Medium}_{\text{pointer}}$ and $\text{Medium}_{\text{tap}}$ (Z = -3.098, p = 0.002) for Patterns. This was also found to be true for the password type PIN (Z = -2.951, p = 0.003).

2) Success rate and Levenshtein distance: The majority of observation attacks was unsuccessful, as out of 400 entered passwords 18% were guessed correctly. This is significantly smaller compared to the attacker success rate for PIN and pattern on mobile phones [50], [51]. However, within the number of successfully observed passwords, we found significant results:

We ran an ANOVA test with the Damerau-Levenshtein distance between the guess and the most correct password of the three guess attempts as a DV. The data was normally distributed, sphericity was not violated (Mauchly's Test: X'(2)(5) = 3.081, p=0.688) and there were no significant outliers. Results showed that success rates for guessing PINs differed statistically significantly depending on *Input Method* ($F_{3,72} = 4.8$, $p < 0.01$). We found observations made from the $\text{Medium}_{\text{pointer}}$ ($Mean = 0.48$, $SD = 0.57$) to be significantly smaller in distance ($p < 0.01$) to the correct pattern than for $\text{Large}_{\text{pointer}}$ ($Mean = 0.7$, $SD = 0.45$) and $\text{Medium}_{\text{tap}}$ ($Mean = 0.66$, $SD = 0.49$), where 1 is a perfect match to the correct password and 0 is an unsuccessful attack. This means that guesses against $\text{Medium}_{\text{pointer}}$ are closer to the correct PIN compared to $\text{Large}_{\text{pointer}}$.

After evaluating Patterns with the same analysis, we found that success rates differed statistically significantly depending on *Input Method* ($F_{3,72} = 5.2$, $p < 0.01$). However, observations made from the $\text{Medium}_{\text{pointer}}$ (($Mean = 0.43$, $SD = 0.06$)) were found to be significantly larger in distance ($p < 0.05$) to the correct pattern than for $\text{Large}_{\text{pointer}}$ (mean=0.2, SD=0.04) and $\text{Medium}_{\text{tap}}$ (($Mean = 0.19$, $SD = 0.09$)), where 1 is a perfect match to the correct password and 0 is an unsuccessful attack.

3) Perceived Security - After Observation Task: Further data gathered after completion of the security study from the likert scale questionnaires showed that there was a statistically significant difference in perceived security depending on which type of method was used for authentication, $\chi^2(7) = 46.69, p = 0.001$. Post-hoc analysis with Wilcoxon signed-rank tests with a Bonferroni correction applied, elicited a statistically significant difference in experienced usability between $\text{Medium}_{\text{pointer}}$ and $\text{Medium}_{\text{tap}}$ (Z = -3.22, p = 0.001) for Patterns. This was also found to be true for the password type PIN (Z = -3.84, p = 0.001).

Qualitative feedback from the semi structured interviews also showed that multiple participants were looking for haptic cues from the [physical] HTC Vive controller in order to guess passwords, as investigated in previous research [41]. However, our quantitative data did not show that participants performed better who noticed these cues.

VII. Limitations

This paper provides first insights into authentication in virtual reality and as such we were only able to investigate 8 concepts (4 input modalities and 2 passwords). Our research focuses on importing well established methods from authentication on [medium sized physical] public displays and [small sized physical] mobile devices into virtual reality. However, we are aware that there are other feasible methods that have proven to show a good trade-off between security and usability, which are also applicable to a VR environment. We believe that this is a first step to establish authentication in VR, opening doors for further detailed comparisons of methods and interaction opportunities.

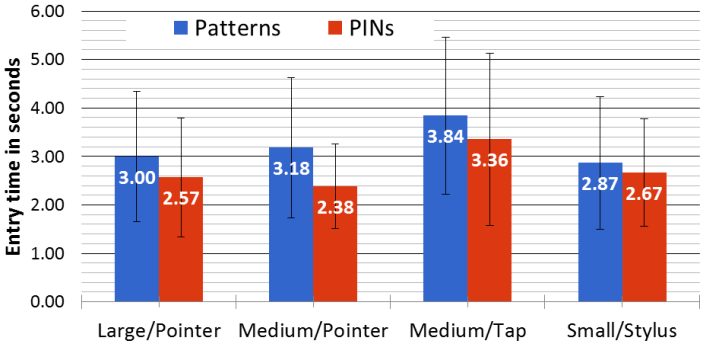

Fig. 7: Mean values and standard deviations for entry times across password type and input modality.

Due to the usage of university mailing lists for recruiting participants, our sample only reflects a certain demographic: We believe that they may be more technology aware, compared to the general population and that the majority were students. However, this is one of the main target groups for our concepts.

VIII. Discussion

We investigated the feasibility of established authentication methods in virtual environments. In addition to specific results according to usability and security, we gathered general insights into the characteristics of seamless authentication. This section points out the main findings and discusses their implications.

A. Established Concepts are Usable in Virtual Reality

The results indicate that currently established real-world authentication methods can be directly transferred into virtual reality. In fact, the measured performance matches the data collected in previous real-world experiments. Summarizing all tested conditions, PIN users required an overall average of 2.7 seconds to authenticate while pattern users needed 3.2 seconds. Comparing the performance of PINs and patterns on mobile devices in a controlled setting (PINs = 1.5 s, patterns = 3.14 s) [52] to their performance in VR suggests that established concepts are promising to be run and evaluated in VR. Although patterns were measurably more error-prone than PINs, both concepts were rated to be comparably easy to use by participants. Using established methods is relatively beneficial for both the user and remote services. While users face a lower barrier to entry for authentication in virtual environments when they are already familiar with the used systems, remote services are not required to modify their back-end. Thus they can serve real-world users and virtual reality users with the same infrastructures.

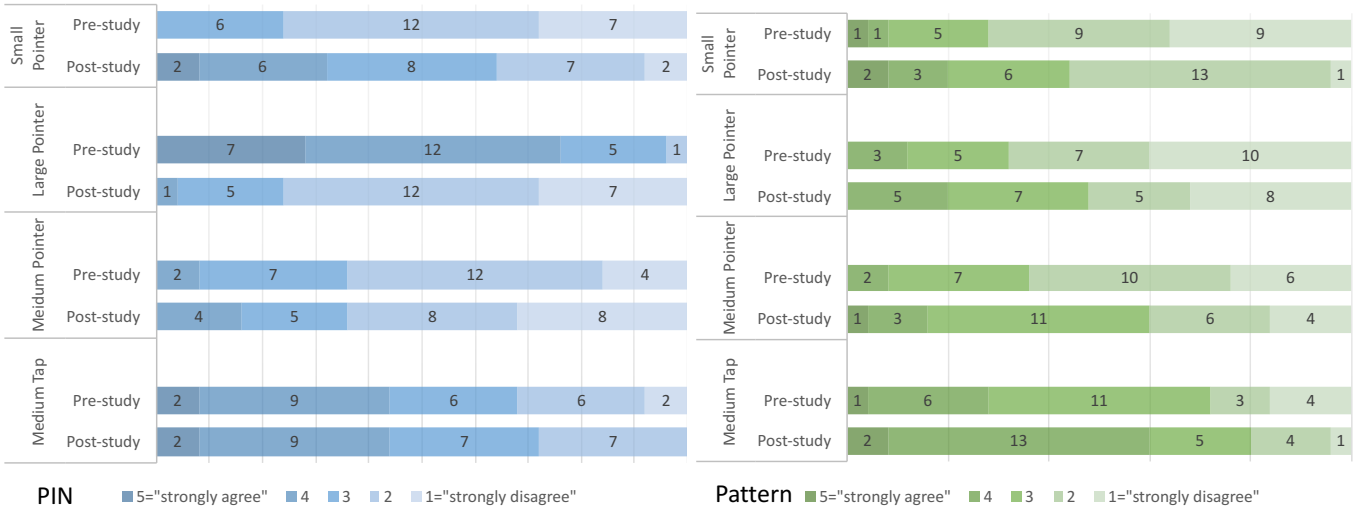

Fig. 8: Results of likert scale questionnaire "How much do you agree with the following statement: "It is difficult to guess a password that is entered with this input modality"? in median values.

However, even if our findings indicate that established authentication methods are usable in virtual environments, we do not claim that they represent the optimal solution for any use case. We assume that some scenarios may benefit from novel authentication concepts. We argue that there are practically no limits to support a user's mental model in the virtual world. For example, a novel concept could mimic a physical key chain which opens a visualized password safe to illustrate the functionality of such tools.

B. Seamless Authentication Improves Practical Security

In addition to the promising usability results, we found that seamless authentication made established methods like PIN and patterns more resistant to observation attacks. This indicates that seamless authentication in virtual environments can solve practical security problems without reducing usability. Related work revealed that both Android unlock patterns [51] and PINs [50] are prone to shoulder surfing attacks, when used in the physical world. That is, the user's credentials face practical risks when users have to interrupt their virtual experience to authenticate with a service in the physical world. In contrast, seamless authentication in the virtual world makes authentication more observation resistant and at the same time improves user experience.

We argue that authentication in virtual environments can improve practical security as the HMD serves as a secret channel between the user and the system. While established methods already perform well, we assume that the security could be further improved by switching to already published security-optimized concepts (e.g., [18], [54], [55]).

C. Interaction Style and Presentation Matter

While the results of both patterns and PINs were promising in terms of usability and security, we found that the characteristics of interaction and presentation have significant effects on authentication speed. Overall, we tested three different surface sizes and two different interaction methods and found that not every condition works equally well. Overall the pointer conditions performed better, especially tapping on medium surfaces performed significantly worse than pointing on medium surfaces. In other words, we found a tendency that mimicking [physical] mobile authentication (i.e., small surface) and horizon-based authentication (i.e., large surface) outperformed the simulation of authentication on [physical] public displays (i.e., medium surface).

On one hand, this finding generally implies that presentation and interaction style have significant impact on usability. On the other hand, this points out in detail that feasible solutions are not required to mimic scenarios of the physical world. Indeed, one of the conditions which worked better (i.e., horizon-based authentication with a laser pointer) has no physical counterpart.

The advantages of [physical] smartphone-like authentication [on small surfaces] over [physical] public display-like authentication [on medium sized surfaces] may be explained by the fact that users were more familiar with [physical] smartphones than with [physical] public displays. This would indicate that mimicking familiar authentication environments can be beneficial in terms of usability. Nevertheless, such effects need to be systematically evaluated to draw valid conclusions.

D. Virtual Reality as a Feasible Research Tool

The evaluation of established authentication mechanisms in virtual environments showed that virtual reality is a feasible test bed for usable security studies. If adequate precautions are taken (e.g., training tasks), virtual reality environments can be utilized to simulate the real world or to create scenarios which are not bound to the physical world. We argue that this makes virtual reality a useful and valid research tool for usable security studies.

On one hand, the virtual environment can be used as a cost-effective way to gather preliminary insights on environmental impact without the need to perform a real-world field study. For example, one could simulate authentication in crowded places or effects of different light conditions. On the other hand, the virtual world enables user studies which cannot be realized in the real world. One example would be to test the effects of

visual feedback for free-hand gestures by visualizing the path of the user's hands. However, even though our results indicate that the performance in virtual environments is comparable to the performance in the physical world, the relation of these two worlds needs to be further investigated in the future.

IX. Conclusion and Future Work

In this paper, we presented a systematic evaluation of established authentication mechanisms for virtual reality (VR) with head mounted displays. For this purpose, we designed eight authentication concepts using PIN and patterns. The [virtual] concepts were based on different interaction mechanisms and presentation styles. Our results indicate that well-established methods from previous research, gathered from real world scenarios on [small sized physical] mobile phones and [medium sized physical] public displays, can successfully be adopted into VR. It was found that [virtual] pointer interactions on small and large [virtual] surfaces worked best for authentication in VR. The tested concepts were comparably usable as in the real world but input was significantly harder to observe. We therefore conclude that seamless authentication in VR environments can solve practical security problems without reducing usability.

Since this work showed promising results for VR authentication, future work should focus on the methods that inclined to work better in VR, most importantly the ones that had no physical counterpart (i.e., large surface pointer interaction). We plan to analyse how the user's mental model can be supported better, when defining a password as well as during the real-time authentication process. Furthermore, we want to explore additional use cases for VR authentication, such as collaboration, where digital handshakes may be done through authentication. For example, visitors of a virtual conference could greet each other with a secure handshake by authenticating in real-time in VR, thus enabling seamless and secure collaborations. Finally, we argue that virtual reality could serve as a feasible test bed to simulate and evaluate complex authentication scenarios. Therefore, we strive at further understanding the comparability of the virtual and the physical world in the context of usable security.

References

[1] Y. Abdelrahman, M. Khamis, S. Schneegass, and F. Alt, "Stay cool! understanding thermal attacks on mobile-based user authentication," in *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017. [Online]. Available: http://dx.doi.org/10.1145/3025453.3025461

[2] M. Abrash, "The future of vr research," 10 2016, Michael Abrash's Oculus Connect 3 Keynote Speech in San Jose, CA.

[3] F. A. Alsulaiman and A. El Saddik, "A novel 3d graphical password schema," in *2006 IEEE Symposium on Virtual Environments, Human-Computer Interfaces and Measurement Systems*. IEEE, 2006, pp. 125–128.

[4] F. Alt, T. Kubitza, D. Bial, F. Zaidan, M. Ortel, B. Zurmaar, T. Lewen, A. S. Shirazi, and A. Schmidt, "Digifieds: Insights into deploying digital public notice areas in the wild," in *Proceedings of the 10th International Conference on Mobile and Ubiquitous Multimedia*, ser. MUM '11. New York, NY, USA: ACM, 2011, pp. 165–174. [Online]. Available: http://doi.acm.org/10.1145/2107596.2107618

[5] C. Ardito, P. Buono, M. F. Costabile, and G. Desolda, "Interaction with large displays: A survey," *ACM Comput. Surv.*, vol. 47, no. 3, pp. 46:1–46:38, Feb. 2015. [Online]. Available: http://doi.acm.org/10.1145/2682623

[6] F. Argelaguet, L. Hoyet, M. Trico, and A. Lécuyer, "The role of interaction in virtual embodiment: Effects of the virtual hand representation," in *Virtual Reality (VR), 2016 IEEE*. IEEE, 2016, pp. 3–10.

[7] I. Aslan, A. Uhl, A. Meschtscherjakov, and M. Tscheligi, "Mid-air authentication gestures: An exploration of authentication based on palm and finger motions," in *Proceedings of the 16th International Conference on Multimodal Interaction*, ser. ICMI '14. New York, NY, USA: ACM, 2014, pp. 311–318. [Online]. Available: http://doi.acm.org/10.1145/2663204.2663246

[8] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens." *WOOT Journal*, vol. 10, pp. 1–7, 2010.

[9] B. Badillo, D. A. Bowman, W. McConnel, T. Ni, and M. G. d. Silva, "Literature survey on interaction techniques for large displays," 2006.

[10] R. Ballagas, M. Rohs, and J. G. Sheridan, "Sweep and point and shoot: Phonecam-based interactions for large public displays," in *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '05. New York, NY, USA: ACM, 2005, pp. 1200–1203. [Online]. Available: http://doi.acm.org/10.1145/1056808.1056876

[11] A. Bogle, "ebay launches a world-first virtual reality department store," May 2016, Lastchecked: 2017-01-22, http://mashable.com/2016/05/18/ebay-virtual-reality-shopping/#MqZVNlqvUEqf.

[12] M. B. Borkar, M. S. Sheikh, and P. Kaware, "4d password mechanism," *Imperial Journal of Interdisciplinary Research*, vol. 2, no. 5, 2016.

[13] W. Buxton, "A three-state model of graphical input," in *Human-computer interaction-INTERACT*, vol. 90, 1990, pp. 449–456.

[14] A. Doronichev, "Daydream labs: exploring and sharing vr's possibilities," May 2016, Lastchecked: 2017-01-22, https://developers.googleblog.com/2016/05/daydream-labs-exploring-and-sharing-vrs.html.

[15] R. A. Earnshaw, *Virtual reality systems*. Academic press, 2014.

[16] M. Eiband, M. Khamis, E. von Zezschwitz, H. Hussmann, and F. Alt, "Understanding shoulder surfing in the wild: Stories from users and observers," in *Proceedings of the 35th Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '17. New York, NY, USA: ACM, 2017. [Online]. Available: http://dx.doi.org/10.1145/3025453.3025636

[17] A. Goode, "Bring your own finger–how mobile is bringing biometrics to consumers," *Biometric Technology Today*, vol. 2014, no. 5, pp. 5–9, 2014.

[18] J. Gugenheimer, A. De Luca, H. Hess, S. Karg, D. Wolf, and E. Rukzio, "Colorsnakes: Using colored decoys to secure authentication in sensitive contexts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '15. New York, NY, USA: ACM, 2015, pp. 274–283. [Online]. Available: http://doi.acm.org/10.1145/2785830.2785834

[19] K. S. Hale and K. M. Stanney, *Handbook of virtual environments: Design, implementation, and applications*. CRC Press, 2014.

[20] M. Harbach, A. De Luca, and S. Egelman, "The anatomy of smartphone unlocking: A field study of android lock screens," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: ACM, 2016, pp. 4806–4817. [Online]. Available: http://doi.acm.org/10.1145/2858036.2858267

[21] M. Harbach, E. von Zezschwitz, A. Fichtner, A. D. Luca, and M. Smith, "It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception," in *Symposium On Usable Privacy and Security (SOUPS 2014)*. Menlo Park, CA: USENIX Association, 2014, pp. 213–230. [Online]. Available: https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

[22] D. B. Kaber and T. Zhang, "Human factors in virtual reality system design for mobility and haptic task performance," vol. 7, no. 1, pp. 323–366, 2011.

[23] P. Kayatt and R. Nakamura, "Influence of a head-mounted display on user experience and performance in a virtual reality-based sports application," in *Proceedings of the Latin American Conference on Human Computer Interaction*, ser. CLIHC '15. New York, NY, USA: ACM, 2015, pp. 2:1–2:6. [Online]. Available: http://doi.acm.org/10.1145/2824893.2824895

[24] M. Khamis, F. Alt, M. Hassib, E. von Zezschwitz, R. Hasholzner, and A. Bulling, "Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices," in *Proceedings of the 2016 CHI Conference*

Extended Abstracts on Human Factors in Computing Systems, ser. CHI EA '16. New York, NY, USA: ACM, 2016, pp. 2156–2164. [Online]. Available: http://doi.acm.org/10.1145/2851581.2892314

[25] K. Kilteni, I. Bergstrom, and M. Slater, "Drumming in immersive virtual reality: the body shapes the way we play," *IEEE transactions on visualization and computer graphics*, vol. 19, no. 4, pp. 597–605, 2013.

[26] C. Kim, W. Tao, N. Shin, and K.-S. Kim, "An empirical study of customers' perceptions of security and trust in e-payment systems," *Electronic Commerce Research and Applications*, vol. 9, no. 1, pp. 84–95, 2010.

[27] P. Lee, D. Stewart, and C. Calugar-Pop, "Technology, media and telecommunications predictions 2016." [Online]. Available: http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-tmt-prediction-2016-full-report.pdf

[28] R. Leung, K. MacLean, M. B. Bertelsen, and M. Saubhasik, "Evaluation of haptically augmented touchscreen gui elements under cognitive load," in *Proceedings of the 9th International Conference on Multimodal Interfaces*, ser. ICMI '07. New York, NY, USA: ACM, 2007, pp. 374–381. [Online]. Available: http://doi.acm.org/10.1145/1322192.1322258

[29] D. Lu, T. Lee, S. Das, and J. Hong, "Examining visual-spatial paths for mobile authentication," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, 2016. [Online]. Available: https://www.usenix.org/conference/soups2016/workshop-program/way2016/presentation/lu

[30] J. Maguire and K. Renaud, "You only live twice or "the years we wasted caring about shoulder-surfing"," in *Proceedings of the 26th Annual BCS Interaction Specialist Group Conference on People and Computers*, ser. BCS-HCI '12. Swinton, UK, UK: British Computer Society, 2012, pp. 404–409. [Online]. Available: http://dl.acm.org/citation.cfm?id=2377916.2377975

[31] J. Maida, "Md sales to increase following the development of eye-tracking technology in hmds: Technavio," September 2016, http://www.businesswire.com/news/home/20160912005356/en/HMD-Sales-Increase-Development-Eye-tracking-Technology-HMDs.

[32] M. McGill, D. Boland, R. Murray-Smith, and S. Brewster, "A dose of reality: Overcoming usability challenges in vr head-mounted displays," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 2143–2152. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702382

[33] K. Mowery, S. Meiklejohn, and S. Savage, "Heat of the moment: Characterizing the efficacy of thermal camera-based attacks," in *Proceedings of the 5th USENIX Conference on Offensive Technologies*, ser. WOOT'11. Berkeley, CA, USA: USENIX Association, 2011, pp. 6–6. [Online]. Available: http://dl.acm.org/citation.cfm?id=2028052.2028058

[34] J. Müller, F. Alt, D. Michelis, and A. Schmidt, "Requirements and design space for interactive public displays," in *Proceedings of the 18th ACM International Conference on Multimedia*, ser. MM '10. New York, NY, USA: ACM, 2010, pp. 1285–1294. [Online]. Available: http://doi.acm.org/10.1145/1873951.1874203

[35] T. Partala, "Psychological needs and virtual worlds: Case second life," *International Journal of Human-Computer Studies*, vol. 69, no. 12, pp. 787–800, 2011.

[36] D. Phelan, "Google daydream vr review: Comfy, capable and affordable but not enough content yet," November 2016, Lastchecked: 2017-01-22, http://www.independent.co.uk/life-style/gadgets-and-tech/features/google-daydream-view-vr-review-virtual-reality-pixel-xl-headset-is-it-worth-it-a7444226.html.

[37] N. Pino, "Htc vive review," November 2016, Lastchecked: 2017-01-22, http://www.techradar.com/reviews/wearables/htc-vive-1286775/review.

[38] A. P. Pons and P. Polak, "Understanding user perspectives on biometric technology," *Commun. ACM*, vol. 51, no. 9, pp. 115–118, Sep. 2008. [Online]. Available: http://doi.acm.org/10.1145/1378727.1389971

[39] F. Roesner, T. Kohno, and D. Molnar, "Security and privacy for augmented reality systems," *Commun. ACM*, vol. 57, no. 4, pp. 88–96, Apr. 2014. [Online]. Available: http://doi.acm.org/10.1145/2580723.2580730

[40] C. E. Rogers, A. W. Witt, A. D. Solomon, and K. K. Venkatasubramanian, "An approach for user identification for head-mounted displays," in *Proceedings of the 2015 ACM International Symposium on Wearable Computers*, ser. ISWC '15. New York, NY, USA: ACM, 2015, pp. 143–146. [Online]. Available: http://doi.acm.org/10.1145/2802083.2808391

[41] H. Sasamoto, N. Christin, and E. Hayashi, "Undercover: authentication usable in front of prying eyes," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008, pp. 183–192.

[42] S. Schneegass, Y. Oualil, and A. Bulling, "Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: ACM, 2016, pp. 1379–1384. [Online]. Available: http://doi.acm.org/10.1145/2858036.2858152

[43] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, "Smudgesafe: Geometric image transformations for smudge-resistant user authentication," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, ser. UbiComp '14. New York, NY, USA: ACM, 2014, pp. 775–786. [Online]. Available: http://doi.acm.org/10.1145/2632048.2636090

[44] T. W. Schubert, "The sense of presence in virtual environments: A three-component scale measuring spatial presence, involvement, and realness." *Zeitschrift für Medienpsychologie*, vol. 15, no. 2, pp. 69–71, 2003, http://www.igroup.org/pq/ipq/index.php.

[45] R. Shadmehr and H. H. Holcomb, "Neural correlates of motor memory consolidation," *Science*, vol. 277, no. 5327, pp. 821–825, 1997.

[46] A. S. Shirazi, C. Winkler, and A. Schmidt, "Flashlight interaction: A study on mobile phone interaction techniques with large displays," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '09. New York, NY, USA: ACM, 2009, pp. 93:1–93:2. [Online]. Available: http://doi.acm.org/10.1145/1613858.1613965

[47] M. Slater and M. Usoh, "Body centred interaction in immersive virtual environments," *Artificial life and virtual reality*, vol. 1, pp. 125–148, 1994.

[48] K. Ukai and P. A. Howarth, "Visual fatigue caused by viewing stereoscopic motion images: Background, theories, and observations," *Displays*, vol. 29, no. 2, pp. 106 – 116, 2008, health and Safety Aspects of Visual Displays. [Online]. Available: //www.sciencedirect.com/science/article/pii/S0141938207001047

[49] O. A. J. van der Meijden and M. P. Schijven, "The value of haptic feedback in conventional and robot-assisted minimal invasive surgery and virtual reality training: a current review," *Surgical Endoscopy*, vol. 23, no. 6, pp. 1180–1190, 2009. [Online]. Available: http://dx.doi.org/10.1007/s00464-008-0298-x

[50] E. von Zezschwitz, A. De Luca, B. Brunkow, and H. Hussmann, "Swipin: Fast and secure pin-entry on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 1403–1406. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702212

[51] E. von Zezschwitz, A. De Luca, P. Janssen, and H. Hussmann, "Easy to draw, but hard to trace?: On the observability of grid-based (un)lock patterns," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 2339–2342. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702202

[52] E. von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices," in *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, ser. MobileHCI '13. New York, NY, USA: ACM, 2013, pp. 261–270. [Online]. Available: http://doi.acm.org/10.1145/2493190.2493231

[53] E. Von Zezschwitz, A. Koslow, A. De Luca, and H. Hussmann, "Making graphic-based authentication secure against smudge attacks," in *Proceedings of the 2013 international conference on Intelligent user interfaces*. ACM, 2013, pp. 277–286.

[54] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the Working Conference on Advanced Visual Interfaces*, ser. AVI '06. New York, NY, USA: ACM, 2006, pp. 177–184. [Online]. Available: http://doi.acm.org/10.1145/1133265.1133303

[55] C. Winkler, J. Gugenheimer, A. De Luca, G. Haas, P. Speidel, D. Dobbelstein, and E. Rukzio, "Glass unlock: Enhancing security

of smartphone unlocking through leveraging a private near-eye display," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 1407–1410. [Online]. Available: http://doi.acm.org/10.1145/2702123.2702316

[56] C. Xu, P. H. Pathak, and P. Mohapatra, "Finger-writing with smartwatch: A case for finger and hand gesture recognition using smartwatch," in *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*, ser. HotMobile '15. New York, NY, USA: ACM, 2015, pp. 9–14. [Online]. Available: http://doi.acm.org/10.1145/2699343.2699350

[57] 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*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–297. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-48051-9_21

[58] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, "Shoulder surfing defence for recall-based graphical passwords," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ser. SOUPS '11. New York, NY, USA: ACM, 2011, pp. 6:1–6:12. [Online]. Available: http://doi.acm.org/10.1145/2078827.2078835