RubikAuth: Fast and Secure Authentication in Virtual Reality

RubikAuth: Fast and Secure Authentication in Virtual Reality

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

Kami Vaniea
University of Edinburgh
Edinburgh, United Kingdom
kvaniea@inf.ed.ac.uk

John Williamson
University of Glasgow
Glasgow, United Kingdom
johnh.williamson@glasgow.ac.uk

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

CHI '20 Extended Abstracts, April 25–30, 2020, Honolulu, HI, USA
ACM 978-1-4503-6819-3/20/04.
https://dx.doi.org/10.1145/3334480.3382827

Abstract

There is a growing need for usable and secure authentication in virtual reality (VR). Established concepts (e.g., 2D graphical PINs) are vulnerable to observation attacks, and proposed alternatives are relatively slow. We present RubikAuth, a novel authentication scheme for VR where users authenticate quickly by selecting digits from a virtual 3D cube that is manipulated with a handheld controller. We report two studies comparing how pointing using gaze, head pose, and controller tapping impacts RubikAuth's usability and observation resistance under three realistic threat models. Entering a four-symbol RubikAuth password is fast: 1.69 s to 3.5 s using controller tapping, 2.35 s to 4.68 s using head pose, and 2.39 s to 4.92 s using gaze and highly resilient to observations; 97.78% to 100% of observation attacks were unsuccessful. Our results suggest that providing attackers with support material contributes to more realistic security evaluations.

Author Keywords

Usable Security; Authentication; Virtual Reality

CCS Concepts

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

System	Authentication Time
RubikAuth	
eye gaze	2.39 s-4.92 s
head pose	2.35 s-4.68 s
tapping	1.69 s-3.5 s
RoomLock [10]	8.58 s-14.33 s
HoloPass [14]	16.69 s
LookUnlock [8]	≈6 s*
2D PINs [11]	2.38 s-3.84 s
2D/3D PINs [30]	≈10.5 s-19 s
VRPursuits [21]	21.40 s

System	Observation Resistance
RubikAuth	
eye gaze	100%
head pose	97.78%
tapping	97.78%
RoomLock [10]	87.5%-100%
HoloPass [14]	not reported
LookUnlock [8]	94.1%-100%
2D PINs [11]	not reported
2D/3D PINs [30]	not reported
VRPursuits [21]	not reported

Table 1: RubikAuth improves entry times and observation resistance over many existing schemes for VR and AR. All systems above use four-symbol PINs. (*) Based on the implementation of LookUnlock [8], we estimate that entering a four-symbol PIN takes at least 6 s (4×1.5 s).

Introduction and Related Work

The surge of new immersive virtual reality applications [2, 7, 23], and the availability of high-end untethered head-mounted displays (HMDs) [6, 27], has made VR ubiquitous. However, the ability to experience VR almost anywhere comes with security implications. Users are often required to authenticate in VR to, for example, make in-app purchases [17] or to verify their identity [16]. Recent research indicates established authentication methods such as PINs or 2D graphical PINs [11, 30] are prone to observation attacks when used in VR. The problem is exacerbated by the fact VR users are often unaware of bystanders [9, 24].

We present RubikAuth, a highly usable and secure 3D authentication scheme for VR. Through two user studies, we present an in-depth evaluation of the first concept and implementation of authentication in VR using a 3D manipulable object and the impact of three techniques for pointing at target digits during authentication on the usability (N=23) and observation resistance (N=15).

RubikAuth's novelty lies in its use of an easily manipulable environment-independent 3D object for authentication. We show that such an object makes authentications **a)** fast: users authenticate in 1.69 s to 4.92 s depending on the pointing method and complexity of the PIN, which is faster than previous work [8, 10, 14, 21, 30] and **b)** more secure against observations by trained attackers: 532 out of 540 (98.52%) attacks failed despite optimal conditions, and using gaze input creates even higher observation resistance (100%). Table 1 outlines the comparison to prior works.

RubikAuth: Concept and Implementation

RubikAuth is a knowledge-based authentication scheme, where users verify their identity by inputting digits on a virtual 3×3×3 cube (Fig. 1). The digits 1-9 are displayed on five of its six uniquely-coloured surfaces; we omitted the rear face as it is not easily reachable. The cube pose is directly linked to the sensed pose of an HTC VIVE controller held in the non-dominant hand. RubikAuth's efficiency derives from the use of Guiard's kinematic chain model for human asymmetrical bimanual cooperation [12, 13], its resistance to observation by splitting input on multiple coordinated input modalities [4, 29], and it is faster to select symbols from polygon 3D shapes than from 2D grids [18].

The advantage of using a manipulable 3D object for authentication in VR is threefold: **1)** it gives quick access to many targets in high speed using minimal wrist movements, **2)** it complicates attacks by requiring attackers need to observe both the cube manipulations, and the positions of the selected targets, and **3)** the intuitiveness of cube manipulations makes it easier for users to anticipate actions that improve observation resistance.

To authenticate, the user points at the target digit on the desired surface (Fig. 2), and then presses the trigger button on the dominant-hand HTC VIVE controller. All RubikAuth pointing methods use explicit selection by pressing the trigger button. Compared to dwell time, the use of a separate trigger has several advantages: a) it gives users more control [15], b) adds an additional channel that attackers must observe [19, 20], and c) significantly decreases best-case authentication time; reliable dwell selection requires at least 350 ms per selection [26, 28], implying a minimum of 1.4 seconds to enter a four-symbol PIN.

Threat Models

RubikAuth addresses three realistic threat models that ensure optimal conditions for the attacker (Fig. 3). These depict the scenarios where users are in a public space and are not aware of potential attackers. In all threat models,

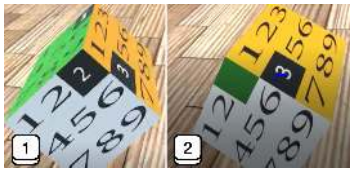

Figure 1: Users are in full control of RubikAuth as the cube pose is linked to their non-dominant hand. The digits and their order were visualised using white digits on a black background.

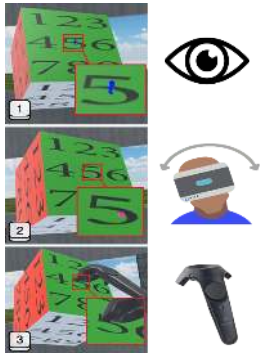

Figure 2: We experimented with **eye gaze**: looking at the target, depicted with a blue gaze trail; **head pose**: moving the target to the centre of the field of view, depicted with a pink dot; and **controller tapping**: moving the rendered right hand controller so that its tip intersects the target. We did not randomise digit order as randomising authentication interface elements reduces usability significantly [1, 3].

the attacker: a) has an optimal view of the user's interactions, b) can move freely, c) knows the beginning and the end of the authentication process, d) knows which pointing method will be used, and e) knows that the user will enter a four-symbol PIN. The attacker's knowledge of this information is realistic as previous work showed that bystanders are able to identify the user's task in VR [9].

Threat Model 1: Pen and Paper
The attacker observes the user during authentication. They note down observations on a paper on which an abstract 2D form of RubikAuth is drawn with labels showing the surface colours (Fig. 3-1).

Threat Model 2: 3D Replica
In recent work, attackers came up with ways to help them note down observations (e.g., folding paper to form a 3D version of a virtual environment [10]). Motivated by these strategies, in addition to the material used in threat model 1, the attacker uses a real-world replica of the 3D cube: a Rubik's cube with overlaid digits (Fig. 3-2).

Threat Model 3: Video Recordings
Motivated by the ubiquity of smartphones, here the attacker uses a smartphone (S7 EDGE, 12 MP Camera) to record and freely play back authentications, in addition to all material used in threat models 1 and 2 (Fig. 3-3). The attacker has the advantage of choosing the recording angle as the user is not aware of their presence due to the HMD [9, 24].

User Studies

We conducted two user studies (2$\times$1h) to study RubikAuth's usability and observation resistance. Both studies were designed as repeated measures lab experiments. Conditions were counter balanced using a Latin Square. All participants were compensated with an $\pounds$8 online shop voucher. Both studies complied with university's ethics procedure.

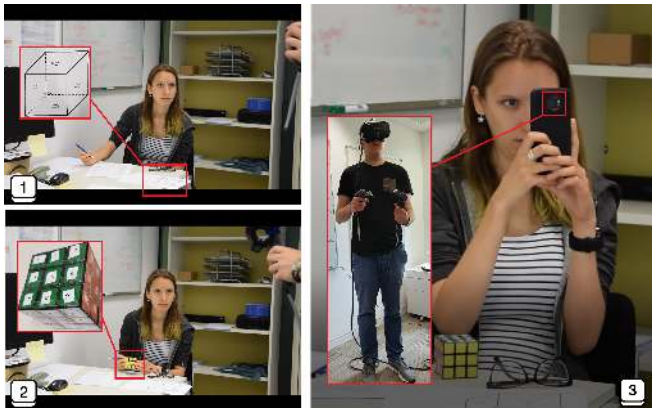

Figure 3: In the first threat model **(1)**, attackers observe the experimenter during authentication and use a pen and paper to note down observations. In the second threat model **(2)**, the attacker has a real-world 3D replica of RubikAuth to assist in visualising the user's input. In the third threat model **(3)**, attackers use a smartphone to record the experimenter during authentication and can freely play back the recordings.

Study 1: Usability Evaluation
We recruited 23 participants (13 females, 10 males) aged between 18 and 54 years (M=27.65, SD=8.26). 11 (47.83%) had never used VR before. There were two independent variables: **IV1) Pointing Method**: we compared pointing via gaze, head pose and controller tapping (three conditions, Fig. 2), and **IV2) Required Switches**: we studied the impact of the number of times the user switches from one surface to another while authenticating.

A four-symbol PIN in RubikAuth has either 0-switches, 1-switch, 2-switches, or 3-switches (four conditions). Entering a 0-switches PIN is equivalent to a classical PIN-pad, so we treat 0-switches as a baseline.

	Eye Gaze				
Switches	0	1	2	3	$\sum$
Threat 1	0	0	0	0	0
Threat 2	0	0	0	0	0
Threat 3	0	0	0	0	0
$\sum$	0	0	0	0	0
	Head pose				
Switches	0	1	2	3	$\sum$
Threat 1	**1**	0	0	0	**1**
Threat 2	**1**	0	0	0	**1**
Threat 3	**1**	0	**1**	0	**2**
$\sum$	**3**	0	**1**	0	**4**
	Tapping				
Switches	0	1	2	3	$\sum$
Threat 1	**2**	0	0	0	**2**
Threat 2	**1**	0	0	0	**1**
Threat 3	**1**	0	0	0	**1**
$\sum$	**4**	0	0	0	4

Table 2: Attacks against RubikAuth are rarely successful. Attacks were only successful against head pose and controller tapping.

Procedure

After filling a consent form and a demographics questionnaire, participants were introduced to VR and RubikAuth. They went through a training session by entering 3 PINs each with **eye gaze**, **head pose** and **controller tapping**. We excluded training runs from analysis. Participants then went through one block per pointing method, entering predefined PINs. In each block, participants entered 2 PINs$\times$4 switches$\times$4 repetitions = 32 PINs/block. Before each PIN entry, we showed participants which targets they should select directly on the cube. The order of the digits was highlighted with white numbers on a black background (Fig. 1).

Usability Evaluation Results

We logged 8 PINs $\times$ 3 pointing methods $\times$ 4 repetitions $\times$ 23 participants = 2208 authentications. We excluded 87 outliers due to tracking issues, such as moving out of the tracking range, or accidentally pressing the menu button on the HTC VIVE controller.

VR savvy vs. non-VR savvy participants

We compared the performance of participants who used VR before with those who did not. VR savvy users authenticated in $(M$=$3.27\,s, SD$=$0.623\,s)$ and made 9.56% errors. For non-VR savvy participants, the values were $(M$=$3.15\,s, SD$=$0.567\,s)$ and 10.25% respectively. None of the differences were significant ($p > .05$). This highlights the naturalness of interacting with RubikAuth gained from the use of Guiard's kinematic chain model [12, 13].

Authentication Time

We measured authentication time from the moment the first entry is made until the fourth symbol is selected. When analysing input time of these successful authentications, a two-way repeated measures ANOVA with Greenhouse-Geisser correction (due to violation of the sphericity assumption) revealed a statistically significant main effect

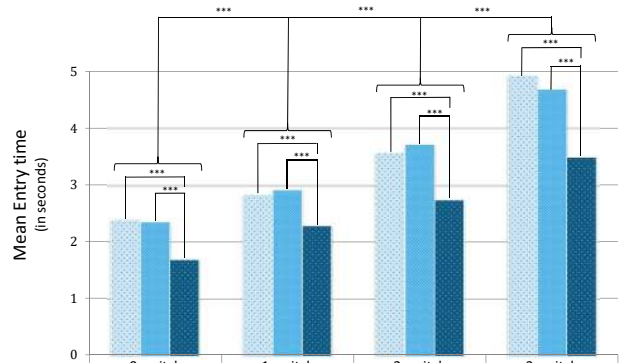

Figure 4: Controller tapping results in significantly faster authentications compared to gaze and head pose. Surface switches increase authentication time significantly. Significance of $p < .001$ is denoted by ***.

of pointing method ($F_{1.619,35.617} = 38.894$, $p < .05$) and number of switches on authentication time ($F_{2.477,54.497} = 309.887$, $p < .05$). It also showed a significant two-way interaction between pointing method and number of switches on authentication time ($F_{3.619,79.621} = 5.096$, $p < .05$).

Further analysis was conducted to distinguish the impact of each independent variable. Individual ANOVAs for each switches condition and post hoc t-tests with Bonferroni correction showed that across all switches, authentication time using controller tapping $(M$=$2.60\,s, SD$=$0.90\,s)$ is significantly faster ($p < .05$) than when using eye gaze $(M$=$3.60\,s, SD$=$1.35\,s)$ or head pose $(M$=$3.44\,s, SD$=$1.07\,s)$. We found no significant differences between gaze and head pose ($p > .05$). Results are summarised in Figure 4. We also found that authentication time is significantly different across switches ($p < .05$, Figure 4).

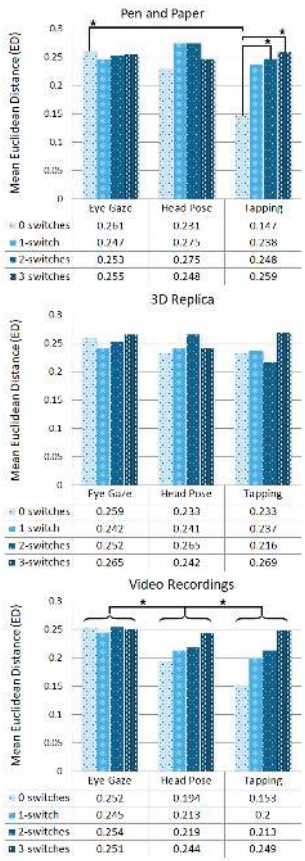

Figure 5: The mean Euclidean distances between attackers' guesses and actual PINs show that a) increasing switches improves security, and b) eye gaze is more secure compared to head pose and controller tapping, even in advanced threat models. Significance of p $<$ .05 is denoted by *.

Entry Accuracy

Entry accuracy is the number of correct entries during authentication. The average successful accuracy was 90.80% across all conditions with 88.2% $(SD$=$32.2\%)$ for eye gaze, 92.3% $(SD$=$26.8\%)$ for head pose, and 91.9% $(SD$=$27.3\%)$ for controller tapping. This is inline with prior work on authentication in VR with 82% [21] and 93% [11].

Study 2: Security Evaluation

We invited 15 participants (5 females, 10 males) aged between 17 and 44 years (M = 26.6, SD = 6.79) with the objective of role play bystanding attackers and observe the experimenter during authentications. To motivate participants to perform well, they took part in a lottery for an additional $\pounds 8$ voucher where the chance of winning increases as they correctly guess more PINs.

Design and Procedure

We added **IV3) Threat Model** with three conditions: Pen and Paper, 3D Replica, and Video Recordings as additional independent variable. We trained the participants by: a) introducing them to the arrangement of the digits and surface colours of RubikAuth, b) allowing them to enter multiple PINs using all pointing methods, and c) running training attacks on all pointing methods. PINs were entered by the experimenter, while we simulated the three threat models with the participant as the attacker. Each participant performed 36 attacks against: 1 PIN$\times$4 switches$\times$3 pointing methods$\times$3 threat models. This results in overall 540 observation attacks. Attacks were performed on 36 predefined unique PINs to ensure fairness of comparisons. Participants were told which pointing method will be used and the beginning and end of the authentication process.

Successful Attack Rate

We measured the successful attack rate, i.e., the percentage of times the correct PIN was guessed. Attacks were successful 8 out of 540 times (1.48%): 0 against eye gaze (0%), 4 against head pose (2.22%), and 4 against controller tapping (2.22%). 7 out of 8 (87.5%) successful attacks were on 0-switch PINs. Results are summarised in Table 2.

Attack Accuracy

To gain better insights on how close the guesses are to the entered PINs, we calculated the Euclidean distance between the centre of the entered PIN symbol (users' inputs) and the centre of each guessed PIN symbol (attackers' guesses). While previous work used Levenshtein distance to measure similarity of guesses [5, 11, 22], we opted for **Euclidean distance (ED)** because it better reflects spatial distances between targets on different surfaces. An attack is considered more successful if the resulting ED between the guess and the actual PIN is shorter.

To study the effect of the independent variables on similarity of their guesses to the correct PINs, we ran a three-way repeated measures ANOVA. No significant three-way interaction was found (p $>$ .05). We ran subsequent two-way ANOVA tests where two-way interaction effects were found, and followed those by pair-wise comparisons using t-tests. We used Bonferroni for controlling familywise errors.

In case of threat model 1, where attackers used pen and paper to note their observations, attacks against controller tapping are significantly (p $<$ .05) more successful when PINs contain 0-switches $(M$=$0.147, SD$=$0.102)$, compared to 2-switches $(M$=$0.248, SD$=$0.070)$ and 3-switches $(M$=$0.259, SD$=$0.056)$, where 0 is a perfect match to the correct PIN and 0.37 is an unsuccessful attack. We also found that RubikAuth PINs that contain 0-switches are significantly more secure when entered using eye gaze $(M$=$0.261, SD$=$0.075)$ compared to controller tapping $(M$=$0.147, SD$=$0.102)$ (Fig. 5). When attackers use a smart phone to record and play back the authentications

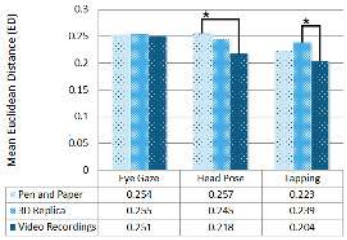

Figure 6: More advanced threat models resulted in significant more accurate successful attacks when input provided with head pose and controller tapping. Significance of p $<$ .05 is denoted by *.

Acknowledgements
We thank all participants for taking part in the study.

This publication was supported by the University of Edinburgh and the University of Glasgow jointly funded PhD studentships, and by the Royal Society of Edinburgh (award number 65040).

(threat model 3), entering PINs using gaze (M=0.251, SD=0.057) is significantly more secure (p $<$ .05) than head pose (M=0.218, SD=0.079) and tapping (M=0.204, SD=0.046) (Fig. 5).

To understand if the advanced threat models resulted in more successful attacks, we compared the accuracy of guesses by running multiple ANOVAs. We found a significant main effect of threat model on ED when using head pose ($F_{2,28}$ = 4.317, p $<$ .05) and tapping ($F_{2,28}$ = 5.576, p $<$ .05). Post hoc analysis using t-tests with Bonferroni correction confirmed the significant differences between threat model 3 (M=0.218, SD=0.079) and threat model 1 (M=0.257, SD=0.044) when using head pose, and between threat model 3 (M=0.204, SD=0.045) and threat model 2 (M=0.239, SD=0.059) when using tapping (Fig. 6).

Discussion and Future Work

Using Manipulable 3D Objects for Authentication
Our two user studies highlight the benefits of leveraging natural two-handed interaction for authentication in VR. Authentications with RubikAuth are fast and highly resilient to observation attacks, even in advanced threat models (100% for gaze-based interaction). This is also attributed to the high cognitive effort required to observe the manipulations and multiple visual channels, such as hand movements, at the same time [4, 19, 22, 29]. In a future work, we plan to conduct an in-depth analysis of users' and attackers' cognitive effort and plan to incorporate additional aspects of the human body such as foot-tapping for selection in RubikAuth as this could overwhelm attackers even more [25].

For high observation resistance when using controller tapping, we recommend to include at least one switch in RubikAuth PINs. Gaze performs well against all studied threat models even without switches but at the expense of longer authentication time. Qualitative feedback from the security study revealed that some poses allow selection from multiple surfaces without explicitly rotating the cube. This can be particularly effective against observations when combined with gaze pointing, and could potentially counteract the increased authentication time caused by rotating the cube. We recommend to leverage manipulable 3D objects for frequent authentications in VR as authentications are fast (1.69 s to 4.92 s) and highly secure (97.78% - 100%).

Employing Suitable Threat Models
Existing work focused mostly on one-time shoulder surfing attacks, and video attacks recorded using a stationary camera [8, 10, 11]. We employed three threat models that simulate a best case scenario for attackers. While successful attack rates did not differ significantly across the threat models, the accuracy of guesses increased significantly. This allowed us to gain a better understanding of the impact of switches and pointing methods on observation attacks. We argue that future evaluations of authentication schemes should employ advanced threat models like the ones considered in this paper to ensure realistic results.

Conclusion

We investigated authentication in VR using a manipulable 3D cube. We compared pointing using eye gaze, head pose, and controller tapping. We conducted two within-subjects experiments, a usability study (N=23) and a security study (N=15). We found that entering a four-symbol PIN using controller tapping is significantly faster (2.60 s) than head pose (3.44 s) and eye gaze (3.60 s). In terms of observation resistance, eye gaze outperformed head pose and controller tapping with a observation resistance of 100%, 97.78%, and 97.78% respectively. Our results suggest that providing attackers with support material contributes to more critical security evaluations.

REFERENCES

[1] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amrl Elmougy. 2019. Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-surfing Resilient Authentication. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications (ETRA '19)*. ACM, New York, NY, USA, Article 29, 10 pages. DOI: http://dx.doi.org/10.1145/3314111.3319837

[2] Andrew Graham Davies, Nick J Crohn, and Laura Anne Treadgold. 2018. Can virtual reality really be used within the lecture theatre? *BMJ Simulation and Technology Enhanced Learning* (2018). DOI: http://dx.doi.org/10.1136/bmjstel-2017-000295

[3] Antonella De Angeli, Mike Coutts, Lynne Coventry, Graham I. Johnson, David Cameron, and Martin H. Fischer. 2002. VIP: A Visual Approach to User Authentication. In *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI '02)*. ACM, New York, NY, USA, 316–323. DOI: http://dx.doi.org/10.1145/1556262.1556312

[4] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now You See Me, Now You Don'T: Protecting Smartphone Authentication from Shoulder Surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2937–2946. DOI: http://dx.doi.org/10.1145/2556288.2557097

[5] Alexander De Luca, Emanuel von Zezschwitz, Laurent Pichler, and Heinrich Hussmann. 2013. Using Fake Cursors to Secure On-screen Password Entry. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 2399–2402. DOI: http://dx.doi.org/10.1145/2470654.2481331

[6] DVPR. 2016. DPVR M2 PRO - A standalone virtual reality headset. (2016). http://dpvr.net/m2pro.html accessed 29 August 2019.

[7] Caroline Fertleman, Phoebe Aubugeau-Williams, Carmel Sher, Ai-Nee Lim, Sophie Lumley, Sylvie Delacroix, and Xueni Pan. 2018. A discussion of virtual reality as a new tool for training healthcare professionals. *Frontiers in public health* 6 (2018), 44. DOI:http://dx.doi.org/10.3389/fpubh.2018.00044

[8] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. 2019. LookUnlock: Using Spatial-Targets for User-Authentication on HMDs. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. ACM, New York, NY, USA, Article LBW0114, 6 pages. DOI: http://dx.doi.org/10.1145/3290607.3312959

[9] Ceenu George, Philipp Janssen, David Heuss, and Florian Alt. 2019. Should I Interrupt or Not?: Understanding Interruptions in Head-Mounted Display Settings. In *Proceedings of the 2019 on Designing Interactive Systems Conference*. ACM, 497–510. DOI: http://dx.doi.org/10.1145/3322276.3322363

[10] C. George, M. Khamis, D. Buschek, and H. Hussmann. 2019. Investigating the Third Dimension for Authentication in Immersive Virtual Reality and in the Real World. In *2019 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*. 277–285. DOI: http://dx.doi.org/10.1109/VR.2019.8797862

[11] Ceenu George, Mohamed Khamis, Emanuel von Zezschwitz, Marinus Burger, Henri Schmidt, Florian Alt, and Heinrich Hussmann. 2017. Seamless and Secure VR: Adapting and Evaluating Established Authentication Systems for Virtual Reality. In *Network and Distributed System Security Symposium (NDSS 2017) (USEC '17)*. NDSS. DOI: http://dx.doi.org/10.14722/usec.2017.23028

[12] Yves Guiard. 1987. Asymmetric Division of Labor in Human Skilled Bimanual Action. *Journal of Motor Behavior* 19, 4 (1987), 486–517. DOI:http://dx.doi.org/10.1080/00222895.1987.10735426 PMID: 15136274.

[13] Yves Guiard. 1988. The Kinematic Chain as a Model for Human Asymmetrical Bimanual Cooperation. In *Cognition and Action in Skilled Behaviour*, Ann M. Colley and John R. Beech (Eds.). Advances in Psychology, Vol. 55. North-Holland, 205 – 228. DOI: http://dx.doi.org/10.1016/S0166-4115(08)60623-8

[14] George Hadjidemetriou, Marios Belk, Christos Fidas, and Andreas Pitsillides. 2019. Picture Passwords in Mixed Reality: Implementation and Evaluation. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems (CHI EA '19)*. ACM, New York, NY, USA, Article LBW0263, 6 pages. DOI:http://dx.doi.org/10.1145/3290607.3313076

[15] Anke Huckauf and Mario H. Urbina. 2008. On object selection in gaze controlled environments. *Journal of Eye Movement Research* 2, 4 (Nov. 2008). DOI: http://dx.doi.org/10.16910/jemr.2.4.4

[16] Lucky VR Inc. 2019. PokerStars VR. (2019). https://store.steampowered.com/app/886250/PokerStars_VR/ accessed 29 August 2019.

[17] INQUIRER.net. 2016. Alibaba launches full VR shopping experience with Buy+. (2016). https://technology.inquirer.net/56131/alibaba-launches-full-vr-shopping-experience-buy accessed 29 August 2019.

[18] Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Does Image Grid Visualization Affect Password Strength and Creation Time in Graphical Authentication?. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces (AVI '18)*. Association for Computing Machinery, New York, NY, USA, Article Article 33, 5 pages. DOI: http://dx.doi.org/10.1145/3206505.3206546

[19] Mohamed Khamis, Florian Alt, Mariam Hassib, Emanuel von Zezschwitz, Regina Hasholzner, and Andreas Bulling. 2016. GazeTouchPass: Multimodal Authentication Using Gaze and Touch on Mobile Devices. In *Proceedings of the 34th Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)*. ACM, New York, NY, USA, 6. DOI: http://dx.doi.org/10.1145/2851581.2892314

[20] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction (ICMI 2017)*. ACM, New York, NY, USA, 5. DOI: http://dx.doi.org/10.1145/3136755.3136809

[21] Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. 2018a. VRpursuits: Interaction in Virtual Reality Using Smooth Pursuit Eye Movements. In *Proceedings of the 2018 International Conference on Advanced Visual Interfaces (AVI '18)*. ACM, New York, NY, USA, Article 18, 8 pages. DOI: http://dx.doi.org/10.1145/3206505.3206522

[22] Mohamed Khamis, Ludwig Trotter, Ville Mäkelä, Emanuel von Zezschwitz, Jens Le, Andreas Bulling, and Florian Alt. 2018b. CueAuth: Comparing Touch, Mid-Air Gestures, and Gaze for Cue-based Authentication on Situated Displays. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 174 (Dec. 2018), 21 pages. DOI: http://dx.doi.org/10.1145/3287052

[23] Denyse King, Stephen Tee, Liz Falconer, Catherine Angell, Debbie Holley, and Anne Mills. 2018. Virtual health education: Scaling practice to transform student learning: Using virtual reality learning environments in healthcare education to bridge the theory/practice gap and improve patient safety. (2018). DOI: http://dx.doi.org/10.1016/j.nedt.2018.08.002

[24] Mark McGill, Daniel Boland, Roderick Murray-Smith, and Stephen Brewster. 2015. 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 (CHI '15)*. ACM, New York, NY, USA, 2143–2152. DOI: http://dx.doi.org/10.1145/2702123.2702382

[25] Florian Müller, Joshua McManus, Sebastian Günther, Martin Schmitz, Max Mühlhäuser, and Markus Funk. 2019. Mind the Tap: Assessing Foot-Taps for Interacting with Head-Mounted Displays. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 477, 13 pages. DOI: http://dx.doi.org/10.1145/3290605.3300707

[26] Christian Müller-Tomfelde. 2007. Dwell-based pointing in applications of human computer interaction. In *IFIP Conference on Human-Computer Interaction*. Springer, 560–573. DOI: http://dx.doi.org/10.1007/978-3-540-74796-3_56

[27] Peter Rubin. 2019. REVIEW: OCULUS QUEST - The new stand-alone virtual-reality headset lets you roam without wires. This is the VR you've been waiting for. (2019). https://www.wired.com/review/oculus-quest

[28] Sophie Stellmach and Raimund Dachselt. 2013. Still Looking: Investigating Seamless Gaze-supported Selection, Positioning, and Manipulation of Distant Targets. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 285–294. DOI: http://dx.doi.org/10.1145/2470654.2470695

[29] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1403–1406. DOI: http://dx.doi.org/10.1145/2702123.2702212

[30] Zhen Yu, Hai-Ning Liang, Charles Fleming, and Ka Lok Man. 2016. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*. 458–460. DOI: http://dx.doi.org/10.1109/APCCAS.2016.7804002