Fast and Secure Authentication in Virtual Reality using Coordinated 3D Manipulation and Pointing

In ACM Transactions on Computer-Human Interaction (TOCHI)

Florian Mathis, University of Glasgow, United Kingdom
florian.mathis@glasgow.ac.uk
John H. Williamson, University of Glasgow, United Kingdom
JohnH.Williamson@glasgow.ac.uk
Kami Vaniea, University of Edinburgh, United Kingdom
kvaniea@inf.ed.ac.uk
Mohamed Khamis, University of Glasgow, United Kingdom
mohamed.khamis@glasgow.ac.uk

This is the author's final accepted version. There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

The published article wil be available in the ACM Digital Library. The DOI will be added to this cover page as soon as possible.

Fast and Secure Authentication in Virtual Reality using Coordinated 3D Manipulation and Pointing

FLORIAN MATHIS, School of Computing Science, University of Glasgow, Scotland, UK
JOHN H. WILLIAMSON, School of Computing Science, University of Glasgow, Scotland, UK
KAMI VANIEA, School of Informatics, University of Edinburgh, Scotland, UK
MOHAMED KHAMIS, School of Computing Science, University of Glasgow, Scotland, UK

Fig. 1. We propose RubikAuth, a novel authentication scheme for immersive virtual reality. Users wearing a head-mounted display and holding a controller in each hand are presented with a 3D cube that they can manipulate (i.e., rotate) to authenticate in VR. The figure shows how controller's pose affects the cube. To authenticate, users point at each desired digit and surface using either a) eye gaze, b) head pose, or c) tapping with the right-hand controller, and confirm using the left controller's trigger button. Through three user studies, we assess RubikAuth's usability, memorability, and observation resistance under three realistic threat models. Findings of our usability study reveal the advantages of coordinated 3D manipulation and pointing on a manipulable 3D object in VR. Our in-depth security study emphasises the importance of considering advanced threat models to accurately assess a system's security.

There is a growing need for usable and secure authentication in immersive virtual reality (VR). Established concepts (e.g., 2D authentication schemes) are vulnerable to observation attacks, and most alternatives are relatively slow. We present RubikAuth, an authentication scheme for VR where users authenticate quickly and secure by selecting digits from a virtual 3D cube that leverages coordinated 3D manipulation and pointing. We report on results from three studies comparing how pointing using eye gaze, head pose, and controller tapping impact RubikAuth's usability, memorability, and observation resistance under three realistic threat models. We found that 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 eye gaze and highly resilient to observations: 96% to 99.55% of observation attacks were unsuccessful. RubikAuth also has a large theoretical password space:

Authors' addresses: Florian Mathis, florian.mathis@glasgow.ac.uk, School of Computing Science, University of Glasgow, Scotland, UK, 18 Lilybank Gardens, Glasgow, Scotland, G12 8RZ; John H. Williamson, johnh.williamson@glasgow.ac.uk, School of Computing Science, University of Glasgow, Scotland, UK, 18 Lilybank Gardens, Glasgow, Scotland, G12 8RZ; Kami Vaniea, kvaniea@inf.ed.ac.uk, School of Informatics, University of Edinburgh, Scotland, UK, 10 Crichton Street, Edinburgh, Scotland, EH8 9AB; Mohamed Khamis, mohamed.khamis@glasgow.ac.uk, School of Computing Science, University of Glasgow, Scotland, UK, 18 Lilybank Gardens, Glasgow, Scotland, G12 8RZ.

© 2020 Association for Computing Machinery.
This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *ACM Transactions on Computer-Human Interaction*, https://doi.org/0000001.0000001.

45^n for an n-symbols password. Our work underlines the importance of considering novel but realistic threat models beyond standard one-time attacks to fully assess the observation-resistance of authentication schemes. We conclude with an in-depth discussion of authentication systems for virtual reality and outline five learned lessons for designing and evaluating authentication schemes.

CCS Concepts: • **Human-centered computing** → **Human computer interaction (HCI)**; **Virtual reality**; • **Security and privacy** → **Usability in security and privacy**.

Additional Key Words and Phrases: Authentication, Usable Security, Virtual Reality, Threat Modeling, Observation, Head-mounted displays

ACM Reference Format:
Florian Mathis, John H. Williamson, Kami Vaniea, and Mohamed Khamis. 2020. Fast and Secure Authentication in Virtual Reality using Coordinated 3D Manipulation and Pointing. *ACM Trans. Comput.-Hum. Interact.* 0, 0, Article 0 (October 2020), 44 pages. https://doi.org/0000001.0000001

1 INTRODUCTION

The surge of immersive virtual reality applications [24, 37, 77] and the availability of high-end untethered head-mounted displays (HMDs) [33, 111] are gradually making VR more 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 [62] or verify their identity [61]. Recent research indicates that established authentication methods such as PINs or 2D graphical passwords [42, 136] are prone to observation attacks when used in VR. The problem is exacerbated by the fact that VR users are often unaware of bystanders [34], especially whilst wearing an HMD [40, 88]. On the other hand, requiring users to take their HMD off to authenticate negatively impacts usability and immersion [55].

We present RubikAuth, a novel 3D authentication scheme for VR that is fast and resilient to observation attacks, even against advanced threat models. RubikAuth's users authenticate by selecting colour-digit combinations from a 3D cube (Figure 1). The orientation of the cube is linked to the user's left handheld controller, allowing quick and covert manipulation of the cube. This allows selecting digits from five of its six surfaces with high speed, accuracy, and ease. Each of the five surfaces has nine selectable digits, which translate to 45^n possible passwords of length n and is higher than the majority of proposed authentication schemes for VR [41, 42, 74, 100, 136]. For comparison, the password space of a four-symbol RubikAuth password is larger than four times that of a six-digit numerical PIN. Observation attacks require simultaneous recovery of both the cube's pose and the user's. Through three user studies and three advanced but realistic threat models, we present an in-depth evaluation of RubikAuth and the impact of three methods for pointing at target digits during authentication on the usability (N=23), memorability (N=21), and observation resistance (N=15) of RubikAuth. The pointing methods are a) eye gaze, b) head pose, and c) controller tapping. RubikAuth's novelty lies in its reliance on an easily manipulable 3D object that is environment-independent and manipulated through bimanual asymmetric interaction.

Through the studies, we show that RubikAuth makes authentication in VR **a)** fast: RubikAuth users authenticate in 1.69 s to 4.92 s depending on the pointing method and complexity of the password, which is faster compared to many previous authentication methods for VR [5, 41, 42, 49], **b)** secure against observations by trained and expert attackers: 657 out of 672 (97.8%) attacks failed despite optimal conditions, and even higher observation resistance (99.55%) when using gaze input and **c)** easy to integrate into existing VR applications as it does not depend on the environment. RubikAuth is also as accurate and its passwords are as memorable as previous work [41, 74]. Our memorability study indicated a successful recall rate of 42.86% to 95.24% depending on the password strength

(compared to 80.77% in [41]). Users authenticating on RubikAuth achieved entry accuracies between 85.80% and 97.83% (compared to 82% in [74]).

While we presented the concept and initial results in a CHI Late Breaking Work [85], this paper extends the published work by an in-depth analysis of results from our usability study (Study 1: Usability Evaluation), presenting results from an additional user study (Study 2: Memorability Evaluation), and an in-depth analysis of RubikAuth's observation resistance by introducing and evaluating expert observation attacks that were part of the security study (Study 3: Security Evaluation). Additionally, we contribute with an in-depth discussion of RubikAuth in the light of prior work on authentication in VR, provide insights into the current trends of authentication for VR, and present five lessons learned when designing and evaluating novel authentication schemes for VR. The contributions of this work are fourfold and situated within authentication for virtual reality and threat modeling, which is a key element when assessing a system's security [89, 112, 116]:

a) **Authentication for VR**

(1) We present the first concept and implementation of authentication in VR using an environment-independent manipulable 3D object and coordinated 3D manipulation and pointing derived from bimanual asymmetric interaction.
(2) We provide an in-depth evaluation of the impact of pointing using eye gaze, head pose, and controller tapping using a manipulable 3D object (RubikAuth) for authentication on usability, memorability, and resistance to observations.

b) **Realistic Threat Models and their Impact on Authentications**

(3) We introduce three realistic threat models and two different types of attackers (i.e., trained participants and an expert attacker) and study their impact on authentications on RubikAuth when providing input with the different pointing methods presented in this work.

c) **Lessons Learned: Design and Evaluation of Authentication Schemes for VR**

(4) Finally, we perform an in-depth discussion of RubikAuth in the light of prior work and derive a set of lessons learned to guide researchers and practitioners in the design and evaluation of knowledge-based authentication schemes for VR.

2 RELATED WORK

In this work, we propose and evaluate a novel 3D authentication scheme for virtual reality. To contextualise our work, we review authentication in mixed reality, that is, in virtual and augmented reality. We categorise prior work into authentication schemes that rely on knowing a secret (i.e., knowledge-based authentication) and those that rely on biometrics.

2.1 Knowledge-based Authentication in VR/AR/MR

Knowledge-based authentication refers to authenticating using "something the user knows". A number of knowledge-based schemes were proposed. For example, Hadjidemetriou et al. [50] proposed gesture-based authentication for mixed reality applications. They did not report entry time, but password creation time was 16.69 s. In Khamis et al.'s work [74], authentication in VR using smooth pursuit eye movements required 21.4 s for entering a 4-digit PIN using ten circulating 3D cubes. Both works above focused on evaluating usability rather than security and/or observation resistance.

Yu et al. [136] compared 3D patterns, 2D sliding patterns, and a 2D numeric keyboard for authentication in VR. They reported that 3D passwords were the most secure against observations,

and required 19 s to enter. Work that explored the "swipe" mobile device authentication system in VR [100] achieved promising results in terms of usability, with fast authentications up to ≈1.0 s-1.8 s. However, when attackers performed attacks on authentications with the help of video recordings, "swipe" authentications manifest a high guessability success rate of ≈20% - 40%, depending on the pattern. Similarly, George et al. [42] investigated how input techniques and interface sizes impact authentication in VR using established authentication methods, such as PINs and 2D patterns. They found that while authentication times can be as fast as 2.38 s, bystanders can observe up to 18% of passwords. They concluded that there is a need for VR authentication schemes that utilise the 3D environment and resist observation attacks.

A second category of work explored authentication by selecting 3D objects scattered in a virtual room [39, 41] and a real room (mixed reality) [39]. This approach resulted in a notable improvement in observation resistance. In George et al.'s RoomLock [41], real time observations were successful 12.5% of the time, but entry time was 8.58 s – 14.33 s. In LookUnlock [39], Funk et al. reported that observations were successful 0% to 5.9% of the time. Their participants needed 1.5 s to select each target, so we estimate entering a four-symbol password required ≈ 6 s. While these systems improved security, their usability was not on par with their less secure counterparts (e.g., [42, 100]).

In comparison, our analysis shows users authenticate using RubikAuth in 1.69 s – 4.92 s depending on the password strength and authentications are highly secure against observations: 96% to 99.55% resistance. While room-based VR schemes such as RoomLock [41] and LookUnlock [39] require loading an exclusive VR scene for authentication, RubikAuth is environment independent, and can be easily integrated into any VR scene. We discuss RubikAuth's usability and security along prior work on knowledge-based authentication for VR further in Section 6 and Table 4.

2.2 Biometric Authentication in VR/AR/MR

In contrast to the aforementioned schemes, biometric authentication relies on the inherence factor, i.e., something the user is. Li et al. [81] classified head movement-patterns to verify the identity of wearable device users (e.g., HMD users). They achieved a mean true acceptance rate of 95.57% and a mean false acceptance rate of 4.43%. More recently, Pfeuffer et al. [103] studied how different body motions can be used for behavioural biometrics in VR. They found that hand movements and small wrist rotations provide strong features to distinguish between multiple identities up to 63% accuracy. This is inline with findings from Mathis et al. [86] that show that hand movement patterns during knowledge-based authentication are promising for establishing an additional biometric security layer. In their study they achieved an accuracy of up to 98.91% when leveraging hand movements and rotations to identify users [86]. Work on seamless continuous biometric authentication by Ajit et al. [3] and Miller et al. [90] achieved a maximum accuracy of 93.03% when using the orientation of users' right handheld controller and HMD headset.

Researchers also leveraged other aspects of human behaviour for authentication in mixed reality applications. For example, Shen et al. [115] used gait recognition to authenticate users in virtual and augmented reality applications. Having users perform five steps achieved a recognition accuracy of up to 98%. Similarly, Mustafa et al. [95] leveraged head, hand, and body movements and Olade et al. [99] employed kinesiological patterns for biometric authentication in VR. Both works showed that human movement patterns are promising for user identification. Mustafa et al. [95] argued that human behavioural biometrics are promising for an additional security layer to decrease the number of successful observation attacks (equal error rate (EER) = 0.07) while Olade et al. [99] achieved an average identification confidence value of 0.98. Work by Luo et al. achieved an even lower equal error rate (3.55% and 4.97%) [83]. In their work they explore the entire human visual system (e.g., eyelid, extraocular muscles) for biometric authentication in VR. Another behavioural biometric scheme for

VR by Kupin et al. [78] matched the 3D trajectories of users as they perform a goal-oriented task, achieving an accuracy of 92.86%.

Although the above-mentioned works achieved promising identification accuracies, work by Miller et al. [91] showed that there is a noticeable drop in the accuracy when considering cross-system behaviour-based biometric authentication. Their analysis across multiple VR systems (i.e., Oculus Quest, HTC Vive, and HTC Vive Cosmos) achieved authentication accuracies between 58% and 85% [91]. It has also been argued that biometrics should only be used to enhance knowledge-based schemes for VR rather than replace them [86, 95, 103], especially because behaviour might not be unique for a large group size. For example, Sugrim et al. [124] showed that the accuracy of biometric classifiers can drop over 35% when participants count increases from 20 to 250 and Olade et al. [99] emphasised that physically similar attackers achieved higher confidence values when classifying them in their study. This was already found when conducting a whitebox penetration test with a sample size of 12 attackers [99].

2.2.1 Challenges of Biometric Authentication. While biometric authentication can be fast and implicit, it often requires sharing personal data with third parties, which can be (and have been [123]) remotely stolen. It is challenging to change biometric passwords, and users can be forced into using their physiological biometrics without consent (e.g., forcing a user's finger against a sensor). As a result, not all users are willing to use biometric authentication [105]. Moreover, VR applications would require long-term or permanent (in the case of continuous authentication) access to sensor data at a huge scale [110]. At the same time, biometric authentication raises ethical questions because collecting and storing such sensitive data could potentially leak private information [2, 22, 110, 134]. The plethora of different VR devices that come with different user tracking techniques (e.g., inside-out [111] vs. outside-in [104]) introduce further obstacles and challenge the generalisability and widespread adoption of behavioural biometrics for authentication in VR even more [91]. Furthermore, it is challenging to establish a minimally privacy-invasive behavioural biometric solution that protects users to the same extent as knowledge-based authentication. As Herley and van Oorshot [56] put it:

> *"Repeated and sustained effort has failed to uncover a silver-bullet replacement for passwords. It's time to admit that this is unlikely to change. No single alternative technology is likely to possess the combination of security, usability, and economic features that meet all goals in all situations"* [56].

This is not to say that biometric authentication is not promising. We note, however, that there are many challenges that need to be addressed before it can deliver reliable and secure authentication. In practice, most biometric schemes require a non-biometric fallback method; this is another avenue where RubikAuth can support biometric authentication as we discuss in Section 6.5.2.

2.3 Contribution over Prior Work

From prior work on knowledge-based authentication we learn that transferring 2D authentication schemes from the real world to VR often results in low observation resistance [42, 100, 136]. Research shows that leveraging the 3D element of virtual reality for authentication can improve security [39, 41, 42]. However, we also learn that room-scale authentication is relatively slow [39, 41], likely due to the need to search for items in virtual rooms. Prior work on biometric authentication revealed several challenges such as the non-uniqueness of human behaviour biometrics for large group sizes [99, 103, 124], data protection challenges and ethical issues [4, 110, 134], generalisability challenges [91], and that not all users are willing to use biometric authentication [105].

The above-mentioned points motivated us to explore a novel knowledge-based authentication scheme for VR: a manipulable 3D object that is independent of the environment. Allowing users to

manipulate a 3D object using simple wrist movements makes selections faster and harder to observe by bystanders. Another distinction of our work is that we compare three methods for pointing in this context that are promising for VR/AR/MR applications [39, 79, 117, 118]: *eye gaze*, *head pose*, and *controller tapping*. A further contribution of this work is that we consider three threat models that are realistic and effective in the context of VR. Namely, we assess observation resistance when attackers use: *Pen and Paper* to note down their observations, a *3D Replica* of the manipulable object, and *Video Recordings* of the user as they authenticate.

3 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. 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. To authenticate using RubikAuth, the user has to first 1) **manipulate** the object using wrist movements until they find an orientation from which the target is reachable, then 2) **point** at the target digit on the target surface, and finally 3) **select** the target by pressing the trigger button on the right-hand controller.

3.1 RubikAuth's Visual Design

RubikAuth's visual design is inspired by Rubik's Cube[a], a popular 3D combination puzzle. To determine the size of the RubikAuth cube in VR, we ran pilot tests with four participants where we experimented with different RubikAuth sizes keeping in mind that the radius of the HTC Vive controller's tip is ≈5cm. Based on the pilot tests, we decided to conduct all three user studies with a cube that is ≈ 4×larger than the original *Rubik's Cube*; our final implementation of RubikAuth has a size *"s"* of *25cm* × *25cm*. This translates to a visual angle ($\alpha = 2 \times \arctan(s/(2\times d))$ between ≈18° when users' non-dominant arm is fully stretched (d= 78.42cm [23]), and ≈60° when users hold the HTC VIVE controller (with a length of d≈22cm[b]) directly at their body. As previously mentioned, experimenting with a larger cube compared to the original *Rubik's cube* was necessary to enable us exploring the impact of controller tapping on usability and security as the HTC VIVE controller comes with a radius of its tip of ≈5cm.

We adopted the colour scheme from the original Rubik's Cube: white, red, blue, yellow, green, and orange (see Figure 1). However, RubikAuth supports different colours (including colour-blind safe) and different cube sizes. We aligned all individual surfaces identically to 2D PIN-pads: starting with the "1" at the top left side and the "9" at the bottom right side (see Figure 1).

We chose not to randomise the digit order and chose to fix the initial orientation, order of digits, and order of colours because prior work on authentication showed that randomising authentication interface elements reduces usability significantly [1, 25]. Furthermore, we wanted to test the limits of RubikAuth assuming a best case scenario for the attacker; if RubikAuth's security is already high without randomisation (as we indeed show in Section 4.5.4), then any security improvement due to randomisation will likely be relatively minor and out-weighted by the reduction in usability.

We discuss the benefits of a personalised RubikAuth orientation along with a personalised RubikAuth size further in Section 6.4.5.

3.2 Manipulating RubikAuth

The cube pose is directly linked to the sensed pose of an HTC VIVE controller held in the non-dominant hand (we refer to this as the "left" hand throughout, but the mapping can be flipped).

[a]Note that the Rubik's Cube reached its height of mainstream popularity in the 1980s, but it is still widely known and used (https://en.wikipedia.org/wiki/Rubik%27s_Cube, last accessed 17/07/2020).

[b]The length of an HTC VIVE controller (see https://www.vive.com/de/accessory/controller/, last accessed 17/07/2020) is ≈22cm.

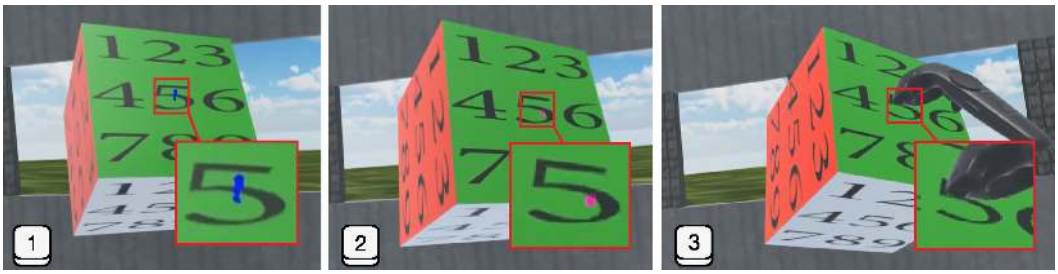


Fig. 2. We experimented with **(1) eye gaze**: looking at the target, depicted with a blue gaze trail; **(2) head pose**: moving the target to the centre of the field of view, depicted with a pink dot; and **(3) controller tapping**: moving the rendered right hand controller so that its tip intersects the target.

RubikAuth's efficiency derives from the use of Guiard's kinematic chain model for human asymmetrical bimanual cooperation [47, 48] and its resistance to observation by splitting input on multiple modalities. Asymmetrical bimanual cooperation allows RubikAuth users to set the frame of reference for the following interaction. This means that each hand in RubikAuth performs a different but connected subtask: left hand pose to manipulate RubikAuth's pose, an independent pointing control, and right hand trigger press for target selection. Buxton et al. [14] and Kabbash et al. [63] highlighted the naturalness and benefits of two-handed interaction: two-handed techniques can be designed such that they take skills that are already in place into account [63]. In case of RubikAuth, splitting the user's input also splits the attacker's attention, and thus complicates observation attacks [26, 131].

3.3 Pointing at Targets in RubikAuth

We implemented three pointing methods: 1) eye gaze: looking at the target; 2) head pose: moving the target to the centre of the field of view; and 3) controller tapping: moving the rendered right hand controller so that its tip intersects the target. The methods are illustrated in Figure 2. We explain the three methods and the rationale behind choosing them below.

3.3.1 Eye Gaze. Gaze is a very promising modality for authentication in general (see [65] for a review), and for authentication in VR in particular; immersive VR applications require wearing an HMD which hides the user's eye movements from bystanders and thereby concealing them from bystanders. Eye trackers are integrated in many HMDs today, including the FOVE 0 [38] and the HTC VIVE Pro Eye [59]. The plethora of applications of eye tracking in VR, such as foveated rendering [102] and gaze-based input [74], together with the potential of 3D gaze on HMDs for interaction design [58], suggest that eye trackers are becoming an integral part of HMDs. Thus, we assume that HMD users will have already configured and calibrated the eye tracker by the time they are attempting to authenticate. RubikAuth's **eye gaze** mode uses gaze pointing, while selection is done by pressing the trigger button of the right hand controller. The gaze point is visualised to the user using a blue trail (Figure 2-1).

3.3.2 Head Pose. Before eye tracking became widely-available, head tracking was used for hands-free pointing in VR, for example in Microsoft HoloLens [87], Oculus Rift [98], and Google Cardboard [46]. There are on-going debates as to whether head pose is a sufficient proxy for eye gaze in VR [6, 79]. Other works showed that head pose can outperform gaze in terms of error rate and selection times [107, 135]. Head pose has been successfully used for VR authentication [39], but head movements are more visible to bystanders than eye gaze. This motivated us to study how using head pose in RubikAuth impacts the usability-security trade-off. In RubikAuth's **head pose** mode,

users select targets by bringing them to the centre of view (visualised by a pink dot, Figure 2-2) and pressing the trigger button of the right hand controller.

3.3.3 Controller Tapping. Handheld controllers provide a natural way to interact with objects in VR. This is the dominant selection technique in commercial VR systems [92, 98, 104, 111]. Previous work on authentication in VR used handheld controllers [41, 42]. It was found that "tapping" close targets is faster than pointing at distant targets [42]. We therefore elected to use tapping instead of pointing using the controller in RubikAuth. In RubikAuth's **controller tapping** mode, users tap the target using the right-hand controller, and press the trigger button on the same controller. The right-hand controller is rendered in real time to reflect its pose and position (Figure 2-3).

3.4 Selecting Targets in RubikAuth

All RubikAuth pointing methods use *explicit selection* by pressing the trigger button. Compared to implicit selection methods like dwell time, the use of a trigger has several advantages: a) it gives users more control [60], b) adds an additional channel that attackers must observe [71, 73], and c) significantly decreases best-case authentication time; for example, reliable dwell selection requires at least 350 ms per selection [94, 119], implying at least 1.4 seconds to enter a four-symbol password.

3.5 Password Space and Password Length in RubikAuth

RubikAuth passwords depend on both the digit and the chosen surface. For example, a RubikAuth password could be: 5 (green), 3 (white), 4 (orange), 4 (blue). This means that there are (9 digits $\times$ 5 surfaces)^4 = 4,100,625 theoretical possible passwords that consist of four symbols. For comparison, there are 1,000,000 digit-only PINs of length *six*. We discuss the practical password space later in the paper based on results of the usability and memorability studies (Study 1: Usability Evaluation and Study 2: Memorability Evaluation). RubikAuth supports passwords of any length n. In our evaluations we chose n = 4 for comparability to prior work [39, 41, 42, 136].

3.6 Switches

RubikAuth allows users to enter digits on five of its six surfaces. A surface *switch* occurs when the user provides an entry on a surface that is different from the surface on which the previous entry resided. Switches have an important role in authentication as they require the attacker to keep track of the user's manipulations, but might also increase entry time or decrease entry accuracy.

The idea of switching between input surfaces or input modalities was shown to improve observation resistance [26, 71].

3.7 Implementation

RubikAuth was implemented in Unity, using C# as programming language. We used an HTC VIVE HMD (2160 px$\times$1200 px) with an integrated Tobii eye tracker (120 Hz update rate) [128] and the SteamVR Plugin for Unity 3D [21] for the HTC VIVE controller communication. We used the Tobii Pro VR SDK [128] for the eye gaze estimation and connected the HTC VIVE to a VR-ready laptop (Razer Blade 15, NVIDIA GeForce RTX 2080, Intel Core I7, 16GB RAM).

To facilitate comparisons of future work with ours, the source code is publicly available as recommended by [125] and can be downloaded from *https://github.com/FlorianMathis/RubikAuthSubmission*.

3.7.1 Pointing Methods. For **eye gaze**, we visualised user's gaze point using a blue trail (see Figure 2-1). We used a prefab called *[VRGazeTrail]* provided by the Tobii Pro VR SDK [128] which shows the position of the user's gaze. Each particle of the gaze trail has a size of *0.5 cm* and we used a particle count of 45. We did not modify any other variables of the prefab provided by the Tobii Pro VR SDK.

For the **head pose** pointing technique, we used a 1:1 mapping of the user's head position that was directly linked to the HTC VIVE HMD that we tracked through the HTC VIVE Lighthouse tracking system. We rendered a pink dot with a radius of *0.5 cm* (see Figure 2-2) in the middle of users' field of view (FOV). To consider the interpupillary distance (IPD) and the corresponding two lenses of the HTC VIVE, we rendered the dot at a distance (=depth in the virtual environment) of 35 cm (determined through pilot tests) of the user's actual head. This enabled users to clearly point at specific password elements of RubikAuth while rendering the dot as unobtrusive as possible to avoid putting it in a dominant position in their FOV.

For **controller tapping**, we used the SteamVR Plugin [21] to represent the right hand-held controller in VR (see Figure 2-3). Since it is possible that the HTC VIVE controller (virtually) collides with multiple RubikAuth password elements at the same time, we calculate the distances between the HTC VIVE controller and all collided elements to process user's input after pressing the trigger button. We then select the password element (e.g., "1" on RubikAuth's green surface) that is the *nearest* to controller's tip. We used *Vector3.sqrMagnitude* from Unity where *current* holds all password elements that collided with the HTC VIVE controller and *transform.position* represents the position of the HTC VIVE controller in the virtual environment. See Listing 1 that we attached to the *GameObject* (base class in Unity) of the HTC VIVE controller in users' dominant hand:

Listing 1. C# example code that shows the implementation of the controller tapping pointing method.

```
1  private List<GameObject> current = new List<GameObject>();
2  float previousDistance = float.MaxValue;
3  float distance = 0.0f;
4  GameObject nearest = null;
5  foreach (GameObject gameobject in current)
6      {
7      distance = (other.position - transform.position).sqrMagnitude;
8      if (distance < previousDistance)
9              {
10             previousDistance = distance;
11             nearest = gameobject;
12             }
13     }
```

Note that the tracking accuracy of the HTC VIVE controller for the controller tapping condition and the HTC VIVE headset for the head pose condition depends on the HTC VIVE Lighthouse tracking system. The accuracy of the eye gaze point depends on the integrated Tobii eye tracker and its corresponding 5-point HMD-based calibration that we used for all our studies[c]. The Tobii eye tracker used in our study has an estimated accuracy of 0.5°and a gaze data output frequency (binocular) of 120 Hz according to the manufacturer [106]. The Lighthouse tracking of the HTC VIVE HMD comes with a high precision of corresponding tracking measurements (tracker jitter (RMS) < 0.02 cm and 0.02°) and a low system latency (22ms) [12, 97].

4 USER STUDIES

4.1 Evaluation Overview

We conducted three user studies to study RubikAuth's a) usability, b) memorability, and c) observation resistance under three realistic threat models that we explain below. We designed our memorability

[c]We used in our usability and memorability study Tobii's HMD based calibration that is based on a typical calibration pattern for 5 points (see http://developer.tobiipro.com/commonconcepts/calibration.html, last accessed 17/07/2020)

study as a follow-up study of the usability study with the same set of participants. For the security study, we made an additional independent call for participants. All three studies were designed as repeated measures experiments. Conditions were counter balanced using a Latin Square. All experiments were approved by the relevant ethics board and written informed consent was obtained from all subjects. All participants were compensated with an £8 online shop voucher.

In this work, we were particularly interested in following three research questions:

- $\mathbf{R_{Q1}}$: How do eye gaze, head pose, and controller tapping impact authentication in VR using coordinated 3D manipulation and pointing?
- $\mathbf{R_{Q2}}$: How does the number of object manipulations (i.e., switches) influence authentications in terms of usability and security?
- $\mathbf{R_{Q3}}$: How do human-centred threat models beyond classical one-time observations impact the security evaluation of an authentication system as presented with RubikAuth?

With **RQ1** we consider the impact of input method (i.e., eye gaze, head pose, and controller tapping) on usability and security when authenticating. Gaze-based interaction should allow users to perform more secure authentications as eye movements are less obtrusive compared to head and hand movements, but may come at the cost of longer authentications. To this end, we measured input performance (i.e., authentication time, entry accuracy) together with the resistance to observation attacks when entering different passwords on RubikAuth.

$\mathbf{R_{Q2}}$ considers the impact of different RubikAuth password types on usability, memorability, and security. In particular, we investigate the effect of object manipulations (e.g., no rotations (0-switch password, baseline) vs. three rotations (3-switch password)) on usability and observation resistance.

With our third research question, $\mathbf{R_{Q3}}$, we explore the impact of three realistic threat models on RubikAuth's resistance to observations. Specifically, we conduct an in-depth evaluation of how supporting attackers with equipment vs attackers with no equipment affects RubikAuth's resistance to observation attacks.

4.2 Statistical Analyses

In all our statistical analyses, we examined our data on normality prior to applying any statistical tests. ANOVAs are considered to be fairly robust to deviations from normality and simulation studies, using a variety of non-normal distributions, have shown that the false positive rate is not affected very much by this violation of the assumption [45, 53, 82]. In cases where our data was not normally distributed (e.g., slightly skewed to the right) but distributions were fairly similar skewed (see Figure 4) we carried on with two-way repeated measures ANOVA.

For post hoc t-tests we applied Bonferroni corrections. Along our two-way repeated measures ANOVA we report η_p^2 (*partial eta square*), which is a standardised measure of effect size and the most commonly reported estimated effect size for ANOVAs (0.01 = small, 0.06 = medium, 0.14 = large, [19]) [64, 80, 109]. In the case of non-parametric data (e.g., 5-point Likert scales), we used Friedman tests with Wilcoxon signed-rank pairwise tests with Bonferroni correction. For our qualitative data, we conducted open coding guided by the grounded theory [17, 44].

4.3 Study 1: Usability Evaluation

4.3.1 Independent Variables. Given the research questions, we experimented with two independent variables. There were three levels for the *Pointing Method* and four levels for the *Number of Switches:*

Fig. 3. In the usability study, participants were asked to enter predefined passwords. The digits and their order were visualised using white digits on a black background (i.e., 1, 2, 3 and 4) as shown in (1) and (2). Upon selection of four digits, the entire cube turned green if the authentication was successful as shown in (3), or red if the input was incorrect.

- **IV1) Pointing Method:** We compared pointing in RubikAuth via eye gaze, head pose, and controller tapping. We were particularly interested in the impact of each pointing method on authentication time, entry accuracy, user preference, and observation resistance.
- **IV2) Number of Switches:** We studied the impact of the number of times the user switches from one surface to another while authenticating. A four-symbol password in RubikAuth has either 0-switches, 1-switch, 2-switches, or 3-switches (four conditions). Entering a 0-switches password is equivalent to a classical 2D PIN-pad [42], so we treat 0-switches as our baseline in this work. We discuss our choice of using RubikAuth's 0-switch condition as baseline further in Section 6.3.

4.3.2 Procedure. Participants were invited to our lab where the study was explained. After filling a consent form and a demographics questionnaire, participants were introduced to the virtual environment, and how to use the HTC VIVE controllers. They went through a training session where they tried RubikAuth and entered 3 passwords each with eye gaze, head pose and controller tapping. We excluded all training runs from the analysis. Participants then went through one block per pointing method, entering predefined passwords. In each block, participants entered 2 passwords$\times$4 switches$\times$4 repetitions = 32 passwords/block. Following each block, participants filled the NASA-TLX [52] and a customised questionnaire with 5-point Likert scale questions. Before each password 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 (Figure 3). After completing the three blocks, we conducted a semi-structured interview and asked participants to rank the pointing methods based on their preference and perceived security. In preparation for the memorability study, we concluded the usability study by asking the participants to use their most preferred pointing method to define three passwords: a weak, a medium-strong, and a strong password. Participants were asked to memorise these passwords for Study 2 and they then entered each of self-defined passwords three times. Our usability study lasted for about 1 hour for each participant.

4.3.3 Dependent Variables. We evaluated the usability of RubikAuth using both quantitative and qualitative measures. For the quantitative measures, we measured **authentication time**: the time from the first input until the last input, **entry accuracy**: the number of correct entries, and the **number of digit errors**. These measures were used to assess usability of authentication systems in previous work (e.g., [26, 27, 41, 42]). For the qualitative measures, the emphasis was on **understanding**

users' experience and **preferences** when interacting with RubikAuth, and their **perception of its security** against observation attacks. The following was collected for each pointing method:

- **Perceived Mental Workload (NASA-TLX):** We measured users' workload, recording mental, physical, and temporal demand, and effort, performance, and frustration. Participants self-reported their perceived workload by filling in the NASA-TLX questionnaire [52].
- **Perceived Usability** (similar to [42]), intended to measure the perceived ease, rapidity, and error proneness when entering RubikAuth passwords with different pointing methods.
  - **Ease of entering a PIN on RubikAuth:** *"It was easy to enter the PIN with the [method] pointing method."*, 5-point Likert scale from Strongly Disagree to Strongly Agree.
  - **Rapidity of entering a PIN** on RubikAuth: *"It was fast to enter the PIN with the [method] pointing method.", 5-point Likert scale from Strongly Disagree to Strongly Agree.*
  - **Error Proneness** when entering a PIN on RubikAuth: *"Entering the PIN with the [method] pointing method was very error prone in my case."*, 5-point Likert scale from Strongly Disagree to Strongly Agree.
- **Perceived Observation Resistance:** *"It is difficult to guess a PIN that was entered with [method] as input modality."*, 5-point Likert scale from Strongly Disagree to Strongly Agree.
- **User rankings** (1 = best; 3 = worst, based on the rank sum weight calculation [120]); intended to elicit user preferences of the pointing methods regarding usability and security.
  - **Usability:** *"Please rank the input techniques based on your perception of usability."*.
  - **Security:** *"Please rank the input techniques based on your perception of security (i.e., when someone observes you from the real world during authentication)."*.
- **User Preference:** *"Consider the situation where you can use one of the previously experienced pointing methods for authentication on RubikAuth in VR in the future. In terms of both, usability and security, which pointing method would you prefer to use?"*; intended to elicit their preference in a daily use without focusing on security or usability separately.

At completion of the study, semi-structured interviews were conducted to collect qualitative feedback.

4.3.4 Usability Evaluation Results. We recruited 23 participants (13 females, 10 males) aged between 18 and 54 years (M=27.65, SD=8.26). Out of 23 participants, 11 (47.83%) self-reported that they had never used VR before. We logged 8 passwords × 3 pointing methods × 4 repetitions × 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. We measured a) authentication and preparation time, b) entry accuracy and error rate, c) perceived workload, and d) perceived usability and security.

Authentication Time. We measured authentication time from the moment the first entry is made until the fourth symbol is selected. This allows us to compare authentication times with previous authentication schemes in VR (e.g., [39, 41, 42, 50, 74, 136]).

We verified our interpretation of the histograms in Figure 4 by running a Shapiro-Wilk's test of normality. Authentication times were not normally distributed. However, ANOVAs are considered to be fairly *robust* to deviations from normality [45, 53, 82], especially in the case of a marginal skewness; therefore we continued with our analysis. 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 of pointing method ($F_{1.619,35.617} = 38.894$, $p < .05$, $\eta_p^2 = 0.639$) and number of switches on authentication time ($F_{2.477,54.497} = 309.887$, $p < .05$, $\eta_p^2 = 0.934$). It also showed a significant two-way interaction

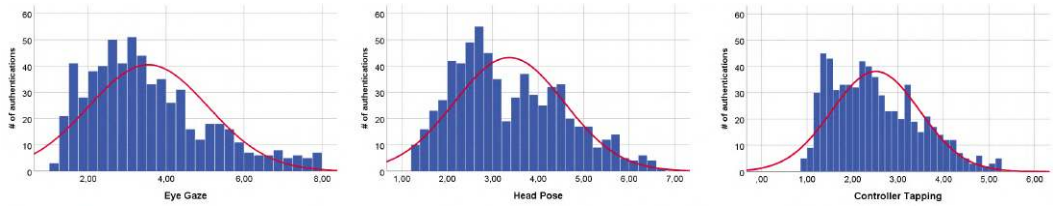
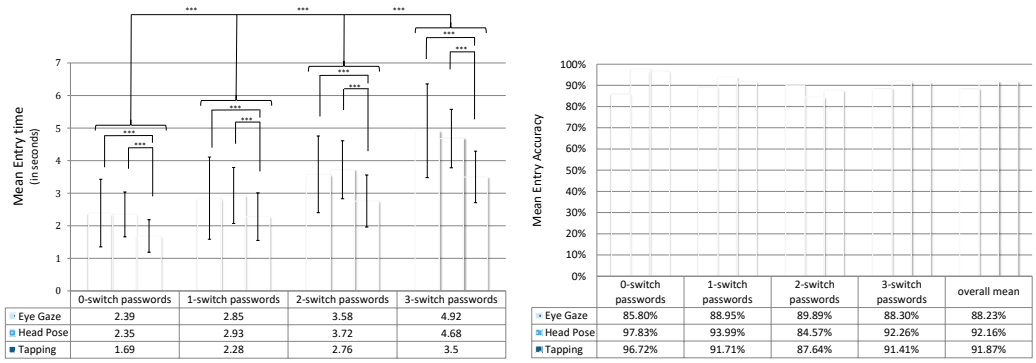


Fig. 4. Shapiro-Wilk's test of normality ($p < 0.05$) and the histogram of the authentication times revealed that authentication times were not normally distributed and manifest a positive skewness (slightly skewed to the right). **Left,** the authentication times for eye gaze, in the **middle** for head pose, and on the **right** for controller tapping.



	0-switch passwords	1-switch passwords	2-switch passwords	3-switch passwords
Eye Gaze	2.39	2.85	3.58	4.92
Head Pose	2.35	2.93	3.72	4.68
Tapping	1.69	2.28	2.76	3.5

	0-switch passwords	1-switch passwords	2-switch passwords	3-switch passwords	overall mean
Eye Gaze	85.80%	88.95%	89.89%	88.30%	88.23%
Head Pose	97.83%	93.99%	84.57%	92.26%	92.16%
Tapping	96.72%	91.71%	87.64%	91.41%	91.87%

Fig. 5. Controller tapping results in significantly faster authentications compared to gaze and head pose. Surface switches increases authentication time significantly. $p < .001$ denoted by ***. Mean entry accuracy when using head pose (92.16%) is slightly higher compared to controller tapping (91.87%) and eye gaze (88.23%). No significant differences were found ($p > .05$). Error bars show the standard deviation.

between pointing method and number of switches on authentication time ($F_{3.619,79.621} = 5.096$, $p < .05$, $\eta_p^2 = 0.188$).

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 eye gaze and head pose ($p > .05$). Results are summarised in Figure 5.

Finding 1: Users authenticate using a four-symbol password on RubikAuth in 1.69 s to 4.92 s. Controller tapping is the fastest pointing method for RubikAuth, but there is no evidence that eye gaze or head pose result in significantly different input times.

Authentications on RubikAuth are faster than most values reported for existing VR authentication schemes [41, 42, 50, 74, 136]. We also found that authentication time is significantly different across switches ($p < .05$, Figure 5).

	0 digit errors	1 digit error	2 digit errors	3 digit errors	4 digit errors
Eye gaze	623 (88.2%)	23 (3.26%)	34 (4.82%)	14 (1.98%)	12 (1.7%)
Head pose	655 (92.3%)	21 (3%)	18 (2.5%)	9 (1.3%)	7 (1%)
Controller Tapping	648 (91.9%)	25 (3.5%)	17 (2.4%)	9 (1.3%)	6 (0.9%)

Table 1. When providing input on RubikAuth with eye gaze, participants made more entry errors compared to head pose (+4.1%) and controller tapping (+3.7%).

Finding 2: Input times are significantly faster when users switch cube faces less frequently.

We also measured the preparation time, which is the time it takes a user to make the first entry on RubikAuth. We measured preparation time as done by von Zezschwitz et al. [131], which is on average 1.33 s (SD=*0.62 s*): 1.40s *(SD=0.58s)* for eye gaze, 1.30 s *(SD=0.56 s)* for head pose, and 1.29 s *(SD=0.71 s)* for controller tapping. As a result, RubikAuth's preparation time is in line with [131] (1.2 s to 1.3 s). In the work by Olade et al. [100] the preparation time was reported as "pre-login delay time" with ≈ 350 ms to 820 ms (according to Figure 5 in [100]), depending on the input modality. No other comparisons to authentication schemes in VR can be made as these values were not reported in previous work – we summarise all publicly available values for comparison in Table 4 as part of our discussion.

Entry Accuracy. The average successful entry rate, the percentage of correct entries during authentication, is 90.80% across all conditions. This is in line with prior work on authentication in VR [42, 74] and also reinforces our decision to experiment with a *25cm×25cm* cube. The work by Olade et al. [100] only reports that they noticed *"very high"* error rates. The rates for RubikAuth are 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. Figure 5 shows the entry accuracy for all conditions. We did not find statistically significant differences in accuracy between the pointing methods ($p > .05$).

Finding 3: Entry accuracy when using RubikAuth is 90.80% on average. There is no evidence that pointing methods, or number of switches impact accuracy.

Entry Errors. Entry errors is the number of digit errors made during authentication when providing input with one of the pointing methods. A Friedman test was run to determine if there were differences in the number of errors between the input modalities. Post hoc pairwise comparisons were performed using Wilcoxon signed-rank tests. The number of errors was statistically significantly different depending on the input modality, $\chi^2 = 7.432$, $p = .024$. Post hoc analysis revealed statistical significant differences in the number of errors between eye gaze and controller tapping ($Z = -2.245$, $p < .05$), between eye gaze and head pose ($Z = -2.148$, $p < .05$), but not between head pose and controller tapping ($Z = -0.637$, $p = 0.524$).

Qualitative feedback from our participants revealed that their pointing task when using eye gaze was often one step ahead of the selection task (i.e., pressing the trigger button to confirm the selection).

Thus, by selecting four digits which are in close proximity, e.g., when selecting $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$ on the same surface, participants had already moved their gaze to the following digit, e.g., confirmed the selection of digit 2 instead of digit 1. This resulted in more PIN entry errors in eye gaze compared to controller tapping and head pose. Table 1 shows the number of entry errors for each pointing method.

Perceived Workload. The perceived workload was measured using NASA-TLX [52] out of 100. No evidence for significant effects of pointing methods on perceived workload was found. Perceived workload of using controller tapping (M=31.85, SD=4.94) is slightly lower than that for eye gaze (M=36.45, SD=4.61) and head pose (M=36.41, SD=5.26). Comparisons of perceived workload when using RubikAuth to previous authentication schemes for VR is unfortunately not possible as we could not find any reported values. The only exception is the work by George et al. [41] that assessed perceived workload when authenticating in VR, but did not report the values.

Finding 4: There is no evidence that one pointing method is more demanding than the others.

Single dimensions of the perceived mental workload by using NASA-TLX [52] are depicted in Figure 10 together with attackers' perceived workload that we measured in the security study. We report on both as this allows us to assess the perceived workload when using RubikAuth in relation to observing authentications on RubikAuth.

Impact of Prior Experience in VR. We also compared the performance of participants who used VR before with those who did not. VR experienced users authenticated in (M=3.27 s, SD=0.623 s), made 9.56% errors, and had a perceived workload score of 34.17. For non-VR experienced participants, the values were (M=3.15 s, SD=0.567 s), 10.25%, and 36.41. 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 [47, 48].

Finding 5: There is no evidence that prior experience with VR has an impact on authentications in RubikAuth. We found no significant differences between non-VR and VR experienced users in terms of authentication time, error rate, and perceived workload.

As previously mentioned, ≈52% of our participants used VR at least once, which is comparable to prior work where 48% [42], 60% [100], and 67% [41] of participants had experience using VR. In contrast, Hadjidemetriou et al. [50] stated their participants had no or limited experience with VR.

Perceived Usability and Security. Participants reported whether they perceived the pointing methods to be easy, error-prone, and fast on 5-point Likert scales (1=strongly disagree;5=strongly agree). No significant effects of pointing method were found on the ease of use and error-proneness ($p > .05$); on average, participants found all pointing methods easy (Med=4). Standard deviations are 1.03, 0.98 and 0.56 for gaze, head pose, and tapping respectively. Gaze is perceived more error-prone (Med=3, SD=0.95) than head pose (Med=2, SD=1.03) and controller tapping (Med=2, SD=0.90). Participants perceived controller tapping to be significantly faster (Z = -2.424, $p < .05$) than head pose, as confirmed by a Friedman test ($\chi^2(2) = 6.778$, $p < .05$) and Wilcoxon signed-rank pairwise tests with Bonferroni correction. The other pairs were not significantly different ($p > .05$).

The median speed rating is 4.0 for all methods, while standard deviations are 0.99, 1.08 and 0.63 for gaze, head pose, and tapping respectively.

User Rankings. We asked participants to rank the methods based on their usability and security (1=best;3=worst). Raw scores were multiplied by their weight factor: $\times 3$ for rank 1, $\times 2$ for rank 2, and $\times 1$ for rank 3, and then summed up to compute weighted scores (based on [120]). The weighted scores of eye gaze, head pose and controller tapping are 44, 39, and 55 respectively for usability, and 67, 46, 25 for security. This means gaze is perceived the most secure, and tapping the most usable.

User Preference. We asked our participants which pointing method they prefer in terms of both usability and security when authenticating using RubikAuth. 14 (60.87%) participants voiced that they prefer to enter their passwords using eye gaze, 5 (21.74%) using head pose, and 4 (17.39%) using controller tapping. Additionally, we asked them to define three different passwords using the preferred modality mentioned before: a weak, medium-strong, and strong password. This was done in preparation for the memorability study where they had to recall their self-defined passwords.

Finding 6: Users prefer gaze in terms of security, and controller tapping in terms of usability. In terms of both usability and security, most participants prefer gaze.

General Qualitative Feedback. Participants enjoyed using RubikAuth (Figure 6). P15 remarked "*I like the idea immensely. I think it could be a really secure [and] fun method to enter a password.*". Participants also saw the benefits RubikAuth offers. For example, they appreciated the improved password space and highlighted the added security by making "*more options available to set passwords*" P13 and "*[offering] a bigger set of possible characters*" P9. Participants also indicated that they found the system usable.

Fig. 6. Two participants in the usability study interacting with RubikAuth. We received positive feedback from our participants in terms of usability and user experience when interacting with RubikAuth.

P9, for example, highlighted that learning effects will result in faster authentications: "*[cube rotation and digit selection] is a skill that can be improved over time*". P3, who also participated in the following memorability study, added that it is "*easy to remember movements*". P23 even suggested that it would be promising to use RubikAuth at a real automated teller machine (ATM).

4.4 Study 2: Memorability Evaluation

We re-invited participants to a memorability study exactly a week later; 21 of the 23 participants in our usability study attended. We asked them to re-enter the three passwords they had set and were asked to remember (Section 4.3.2), using the same pointing method they used when setting the password in the usability study. This was followed by a semi-structured interview to get further information about users' perception and memorising approaches of passwords with different strengths. The memorability study lasted for about 20 minutes for each participant.

4.4.1 Memorability Evaluation Results. We collected 3 passwords $\times$ 23 participants = 69 passwords from the usability study participants, and invited them to this follow-up study to assess memorability. The following recall success rates are based on 21 participants. Two did not return for the memorability study (drop-out rate 8.7%). 20 participants (95.24%) recalled their weak, 13

Password Strength	Switches 0	1	2	3
weak	**22** (95.65%)	0	0	1 (4.35%)
medium-strong	**12** (52.17%)	6 (26.09%)	2 (8.70%)	3 (13.04%)
strong	4 (17.40%)	2 (8.70%)	7 (30.43%)	**10** (43.48%)

Table 2. When asked to choose weak, medium-strong and strong passwords, users chose digits from several surfaces, especially for strong passwords. This suggests the practical password space utilises the majority of the theoretical space.

(61.90%) their medium-strong, and 9 (42.86%) their strong password. This is despite two participants saying they did not realise they had to memorise their passwords despite being asked to.

Finding 7: Users recall RubikAuth passwords, but with lower accuracy when there are many switches involved in the authentication process.

When asking participants about the reasons for not being able to recall their medium-strong and strong PINs, they outlined that it was challenging for them to recall the correct colours due to the fact that the format of the PIN (i.e., combination of digit and surface) was new to them. P4 explicitly mentioned that they experienced VR the very first time and that the authentication scheme was novel to them and that the combination of both might have affected their recall performance. Interestingly, another participant, P8, mentioned that they did not use the PIN within the last week; thus they could not establish some kind of muscle memory. They also mentioned that more repetitions and an increased usage within the last week would consolidate the specific motor task to rotate the cube into their memory through repetition.

Analysis of Users' Chosen Passwords. 22 of the 23 weak passwords had 0-switches, i.e., included one surface only (Med=1, SD=0.63). For medium-strong passwords, 11 participants used 1-, 2-, or 3-switch passwords, while 12 used 0-switch passwords (Med=1, SD=1.07). For strong passwords, 17 participants used 2- or 3-switches (Med=3, SD=1.13). Users' chosen password characteristics are summarised in Table 2. From participants' feedback and our own observations, participants perceived two main factors contributing to strong passwords: **a) More variation in the selected password:** the defined strong passwords involved non-adjacent targets that also span over multiple surfaces, and **b) Inconspicuous password entry:** some participants held the cube in an orientation that allows selecting from multiple surfaces, especially when providing input with eye gaze. Some even suggested faking cube rotations to trick attackers.

Finding 8: Users perceive passwords with more switches to be more secure against observations.

Users' Approach to Memorise RubikAuth passwords. To understand users' approach when trying to memorise passwords generated on RubikAuth, we asked our participants to tell us their memorability approaches. The majority of our participants (N=22) considered only one surface for their weak RubikAuth password. They mentioned things like *"it is weak, no specific measures were taken"* **(P5)**, *"put all on one face in a line"* **(P8)**, *"a simple sequence"* **(P18)**, *"even numbers"* **(P16)**, and *"consecutive numbers"* **(P12)**. While two participants (P15, P21) mentioned that their RubikAuth

password was related to personal details (e.g., birth date), two other participants (P1, P23) outlined that they tried to memorise it by re-visualising the cube's rotations in their head multiple times.

Regarding the semi-strong password, P9, P10, and P18 mentioned that they used numbers which were familiar to them or sequential. P8 voiced that their approach to memorise the strong RubikAuth password was focusing on the manipulations. They explicitly mentioned that they tried to memorise the cube rotations.

Surprisingly. 13 participants (56.5%) transferred the weakest 4-digit PIN (*"1234"*, [7]) without any modifications (i.e., all four digits on the same surface) to RubikAuth. Feedback from participants revealed that they treated the cube as an ordinary numeric keyboard during the creation process of the weak RubikAuth password. This reinforces our decision to treat 0-switches as a baseline for its similarity to traditional 2D PIN pads. On the other hand, when defining a stronger PIN, participants leveraged RubikAuth's characteristics and rotations to define stronger passwords and memorise them.

To get further insights into participants' memorability of different PIN strengths, we conducted an open-coding guided by the grounded theory [17, 44] on participants' responses when asking them about their approach to memorise their different RubikAuth passwords. The lead author performed an initial open coding. After the open coding, we had nine codes for the memorability of weak passwords, and six codes regarding medium-strong and strong RubikAuth passwords. We then conducted an affinity diagram [70] of the open codes and organised the codes into groups. We outline the most frequent voiced strategies below, together with the number of times the comment was made:

- **Memorability: Weak RubikAuth Password**
  - **Spatial Proximity (N=9):** Participants selected their password based on the spatial proximity (i.e., digits on the same surface and next to each other, in a line on one single surface).
  - **Effortless Memorability (N=9):** Participants voiced that they memorised their weak password with minimal effort and that they did not have to take specific measures (i.e., it was easy to remember "1234" on the same surface without rotating the cube). A weak password is considered to be easy to guess and also easy to memorise.
  - **The Attacker's Perspective (N=4):** Participants selected their weak password knowing that weak passwords are those that are easy to guess (e.g., "1234") by attackers.

- **Memorability: Medium-Strong RubikAuth Password**
  - **Password Cues (N=9):** Participants transferred their existing PINs to RubikAuth. They also used cube rotations/surface colours as password cue and tried to create a story with the help of the rotations and surface colours; for example, a participant entered their partner's year of birth on the red surface as they associate the colour with their relationship.
  - **Visual Patterns (N=5):** Participants selected passwords in a sequence that resembles a pattern (e.g., a cross).

- **Memorability: Strong RubikAuth Password**
  - **Mental Visualisation (N=9):** The password was memorised by mentally visualising the password (i.e., sequence of the digits, spatial positioning of the digits) multiple times or by recalling the movements and rotations of the cube.
  - **Physical Movement and Rotation (N=4):** Participants held the cube in a specific pose and used specific rotations (e.g., the sequence of rotations) as a cue for memorising the password.

The overall storyline of the qualitative description of strategies to memorise passwords can be read as a way to improve the memorability of the selected passwords. In particular, participants memorability approaches indicate that they tried to leverage the third dimension in VR to improve memorability of

their passwords, i.e., spatial proximity of digits on different surfaces, and used physical movements, i.e., cube rotations, to make their passwords more memorable.

4.5 Study 3: Security Evaluation

4.5.1 Independent Variables. We studied the impact of the same variables that we used in the usability study on security: **IV1) Pointing Method** and **IV2) Number of Switches**. We added **IV3) Threat Model** and studied the impact of different realistic threat models on the observation resistance of RubikAuth. Our threat models are described below in detail.

Threat Models. To understand RubikAuth's observation resistance in worst case scenarios, we evaluated the resistance to observations under three threat models that ensure optimal yet realistic conditions for the attacker. In all threat models, 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 password. 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 [40]. Similar to untethered HMD systems [38, 111], we assume that the user's view is not cast on any nearby display.

- **Threat Model 1: Pen and Paper** The attacker observes the user during authentication. They note down observations on a pen and paper on which an abstract 2D form of RubikAuth is drawn with labels showing the surface colours (Figure 7-1).

- **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 [41]). 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 (Figure 7-2).

- **Threat Model 3: Video Recordings** Motivated by the ubiquity of smartphones, here the attacker uses a smartphone (Samsung Galaxy S7 EDGE, Dual Pixel Camera 12MP) to record and freely playback authentications, in addition to all material used in threat model 1 and 2 (Figure 7-3). The attacker has the advantage of choosing the recording angle as the user is not aware of their presence due to the HMD obscuring their view [40, 88].

4.5.2 Procedures. Similar to the procedure in the usability study, participants were invited to our lab where we studied the observation resistance of RubikAuth. After filling a consent form and a demographics questionnaire, participants were introduced to the virtual environment, and how to run observation attacks. In a training session, we a) introduced them to the arrangement of the digits and surface colours of RubikAuth, b) allowed them to enter multiple passwords using all pointing methods, and c) allowed them to run training attacks on all pointing methods. The study was split into two stages. In stage 1, the participant took the role of the attacker and observed the experimenter. In stage 2, they switched roles: the experimenter was the attacker and observed the participant.

In stage 1, passwords 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 password$\times$4 switches$\times$3 pointing methods$\times$3 threat models. Attacks were performed on 36 predefined unique passwords to ensure fairness of comparisons. Participants were told which pointing method will be used and the beginning and end of the authentication process.

In stage 2, the participant and the experimenter switched roles. Studying the attacking performance of the experimenter against the participants' has several advantages. The experimenter implemented RubikAuth; his expertise resulting from implementing the system, using it for several months,

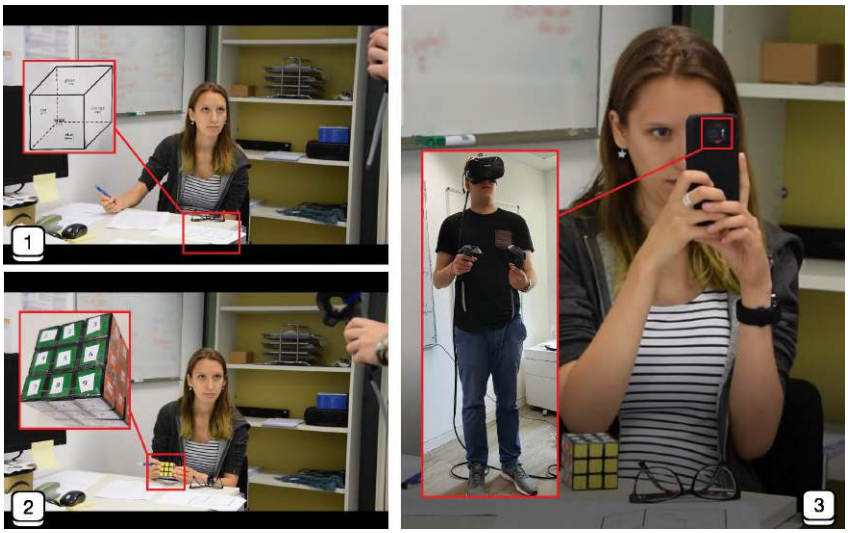


Fig. 7. In the first threat model **(1)**, attackers observe the experimenter during authentication and use a pen and paper to note down observations. **(2)** In the second threat model, the attacker has a real-world 3D replica of RubikAuth to assist in visualising the user's input. **(3)** In threat model 3, attackers use a smartphone to record the experimenter during authentication and can freely playback the recordings.

overseeing the security study and training other participants gives him an advantage as an attacker. The participant self-defined and entered three passwords of different strengths: weak, medium-strong and strong using each pointing method. The experimenter was not aware of the passwords beforehand. He performed: 3 password strengths$\times$3 pointing methods$\times$15 participants = 135 attacks. We could not perform three attacks on one participant when using eye gaze due to inaccurate eye tracking when wearing glasses.

The security study concluded with a semi-structured interview and lasted for about 1 hour for each participant. To motivate participants to perform well, they took part in a lottery for an additional £8 online shop voucher where the chance of winning increases as they correctly guess more passwords.

4.5.3 Dependent Variables. We evaluated the observation resistance of RubikAuth using both quantitative and qualitative measures. For the quantitative measures, we examined the **successful attack rate**: the number of successful attacks, and the **attack accuracy**: the distance between the guess of the attacker and the correct PIN. These values were measured for each attack. As for the qualitative measures, we aimed to understand how participants perform their attacks. To this end, we analysed their attack behaviour by re-watching their observation attacks that we recorded, conducted semi-structured interviews, and collected further data through questionnaires:

- **Perceived Observation Resistance:** *"It is difficult to guess a password that is entered with the [method] pointing method."*, 5-point Likert scale from Strongly Disagree to Strongly Agree. Participants answered this question before and after performing the attacks (similar to [42]). We were interested if there is a change in participants' perceived observation resistance of the pointing methods.

- **Perceived Mental Workload (NASA-TLX)**: We measured attackers' workload using the NASA-TLX questionnaire [52] after switching from attacks on one pointing method to the next. This allowed us to assess the mental workload associated with attacking passwords entered using eye gaze, head pose, and controller tapping.

- **Confidence during Observation Attacks:** *"I am confident that I observed the PIN correctly."*, 5-point Likert scale from Strongly Disagree to Strongly Agree. This data was collected after each observation attack to measure their confidence in their observation.

- **Perceived Observation Ease:** *"It was easy to observe PINs when they were entered with [method] as pointing method."*, 5-point Likert scale from Strongly Disagree to Strongly Agree. This data was collected after running all observation attacks.

At completion of the security study, we asked participants to let us know about their observation approach when running the attacks on eye gaze, head pose, and controller tapping: *"Please briefly describe how you tried to observe the PIN entries when a) eye gaze was used to enter the PIN, b) when head-pose was used to enter the PIN, and c) when tapping was used to enter the PIN."*.

4.5.4 Security Evaluation Results. We invited 15 participants (5 females, 10 males) aged between 17 and 44 years (M = 26.6, SD = 6.79) to the security study. The call for participants was independent of the usability and memorability study. We analysed 672 observation attacks: 540 by trained participants, and 132 by the expert experimenter. We measured a) perceived observation resistance b) successful attack rate, c) attack accuracy, d) perceived attacker confidence, e) perceived workload of attackers, and f) perceived observation ease.

Perceived Observation Resistance. Friedman tests were run to determine whether or not there are differences in the perceived observation resistance of the pointing methods.

- **Before Observation Attacks** Perceived security was statistically significantly different between the pointing methods, $\chi^2(2) = 9.692$, $p < .05$. Post hoc analysis with Wilcoxon signed-rank tests revealed a significant difference in the perception of the security between eye gaze and controller tapping (Z = -2.632, $p < .05$) and head pose and controller tapping (Z = -2.495, $p < .05$), but not between eye gaze and head pose ($p > .05$). The median for controller tapping was 3, and 4 for eye gaze and head pose on a 5-point Likert scale where 5 means highly secure and 1 highly insecure.

- **After Observation Attacks** Perceived security was statistically significantly different between the pointing methods, $\chi^2(2) = 18.053$, $p < 0.01$. Post hoc analysis with Wilcoxon signed-rank tests revealed a significant difference in the perception of the security between eye gaze and controller tapping (Z = -3.025, $p < .05$), and head pose and eye gaze (Z = -2.495, $p < .05$), but not between controller tapping and head pose ($p > .05$). (Z = -1.342, p = .180). The median for eye gaze changed from 4 to 5 and for controller tapping from 3 to 4. There was no change in the median of head pose (Md = 4).

The increase in perceived observation resistance of eye gaze (4 to 5) and controller tapping (3 to 4) indicates that participants underestimated the observation resistance of the two methods.

Finding 9: Participants perceive eye gaze as the most secure pointing method, followed by head pose. After performing observation attacks on their own, participants perceived eye gaze and controller tapping as more secure than previously.

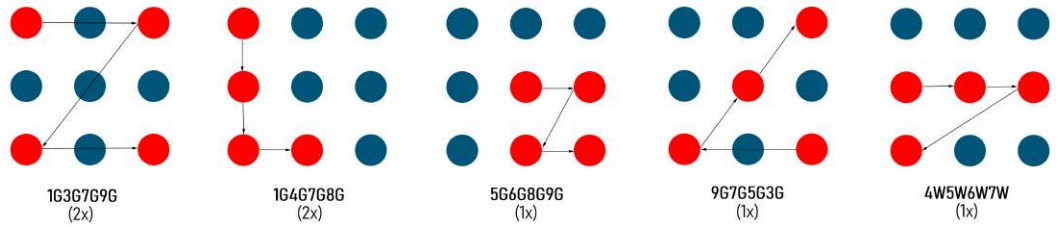


Fig. 8. The patterns depict the successfully attacked 0-switch RubikAuth passwords. The figure shows that attackers were more successful when passwords were entered on single surfaces and followed specific patterns. For example, the most left pattern shows the selected RubikAuth password *"1G3G7G9G"* where the numbers (*1,3,7,9*) were selected on the green surface (*G*) and depict a *"Z"*. This password was successfully guessed two times *(2x)*. All successfully attacked passwords were entered with head pose or controller tapping.

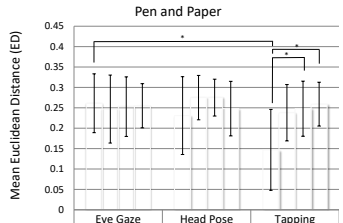
	Eye Gaze				Head pose				Tapping				
Switches	0	1	2	3	0	1	2	3	0	1	2	3	Total
Threat 1	0	0	0	0	**1**	0	0	0	**2**	0	0	0	**3**
Threat 2	0	0	0	0	**1**	0	0	0	**1**	0	0	0	**2**
Threat 3	0	0	0	0	**1**	0	**1**	0	**1**	0	0	0	**3**
All Threats	0	0	0	0	**3**	0	**1**	0	**4**	0	0	0	
Total		**0**				**4**				**4**			**8**

Table 3. Attacks against RubikAuth are rarely successful. Attacks were only successful against head pose and controller tapping. Not a single attack on eye gaze was successful.

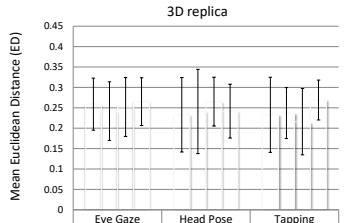
Successful Attack Rate. We measured the successful attack rate, i.e., the percentage of times the correct password was guessed. Participant attacks were successful 8 out of 540 times: 0 successes against eye gaze, 4 against head pose, and 4 against controller tapping. All successful attacks were either against 0-switch (7) or 2-switch passwords (1). Interestingly, the majority of the successfully attacked passwords were entered on a single surface and followed relatively simple patterns, see Figure 8. The overall results are summarised in Table 3. In the experimenter's attacks, 7 out of 132 were successful: 1 in eye gaze and head pose, and 5 in controller tapping.

Finding 10: RubikAuth resists 98.52% of observations by trained participants, and 94.7% of those by an expert attacker. No attacks on 3-switch passwords were successful.

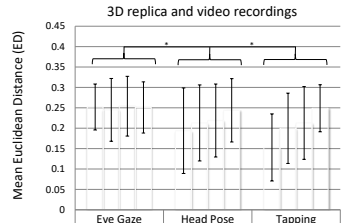
Attack Accuracy. To gain better insights on how close the guesses are to the entered passwords, we calculated the Euclidean distance between the centre of each of the four entered password symbols, and the centre of the corresponding symbols of the password guessed by the attacker. While previous work used Levenshtein distance to measure similarity of guesses [28, 42, 76], we opted for Euclidean distance because it better reflects spatial distances between targets on different surfaces of the 3x3x3 cube. An attack is considered more successful if the Euclidean distance is shorter. To study the effect of the independent variables on the Euclidean distance between the input and the attack, we ran a three-way repeated measures ANOVA. No significant three-way interaction was found ($p > .05$). We



	Eye Gaze	Head Pose	Tapping
0-switches	0.261	0.231	0.147
1-switch	0.247	0.275	0.238
2-switches	0.253	0.275	0.248
3-switches	0.255	0.248	0.259



	Eye Gaze	Head Pose	Tapping
0-switches	0.259	0.233	0.233
1-switch	0.242	0.241	0.237
2-switches	0.252	0.265	0.216
3-switches	0.265	0.242	0.269



	Eye Gaze	Head Pose	Tapping
0-switches	0.252	0.194	0.153
1-switch	0.245	0.213	0.2
2-switches	0.254	0.219	0.213
3-switches	0.251	0.244	0.249

Fig. 9. The mean Euclidean distances between the attackers' guesses and the actual passwords show that a) increasing switches significantly improves security, and b) eye gaze is significantly more secure compared to head pose and controller tapping even against advanced threat models. Significance of $p < .05$ is denoted by *. Error bars show the standard deviation.

ran subsequent two-way ANOVA tests where two-way interaction effects were found, and followed those by pair-wise comparisons using t-tests with Bonferroni corrected p-values.

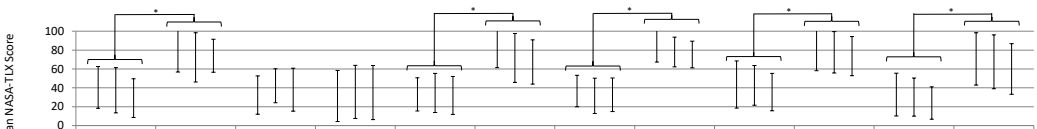
In case of threat model 1, where attackers used pen and paper to note their observations, attacks against controller tapping are significantly ($p < .05$) more successful when passwords contain 0-switches (M=0.147, SD=0.102), compared to 2-switches (M=0.248, SD=0.070) and 3-switches (M=0.259, SD=0.056), where 0 is a perfect match to the correct password and 0.37 is an unsuccessful attack. We also found that RubikAuth passwords that contain 0-switches are significantly more secure ($p < .05$) when entered using eye gaze (M=0.261, SD=0.075) compared to controller tapping (M=0.147, SD=0.102). Results are summarised in Figure 9.

Finding 11: Increasing surface switches when authenticating using RubikAuth significantly improves observation resistance when using controller tapping. Using gaze pointing while entering 0-switch passwords is still highly secure, but relatively error-prone (Figure 5).

In threat model 3, where attackers use video recordings, entering passwords using eye gaze (M=0.251, SD=0.057) is significantly more secure ($p < .05$) than head pose (M=0.218, SD=0.079) and controller tapping (M=0.204, SD=0.046).

Finding 12: Using gaze for pointing in RubikAuth makes passwords more secure against basic and advanced observation attacks that utilise real-world 3D replicas and video recordings.

To understand if certain threat models result in more successful attacks, we compared the accuracy of guesses by running multiple ANOVAs. We found a significant main effect of threat model on Euclidean distance when using head pose ($F_{2,28} = 4.349$, $p < .05$, $\eta_p^2 = 0.237$) and controller tapping ($F_{2,28} = 5.426$, $p < .05$, $\eta_p^2 = 0.279$). 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 controller tapping.



	Mental (User)	Mental (Attacker)	Physical (User)	Physical (Attacker)	Temporal (User)	Temporal (Attacker)	Performance (User)	Performance (Attacker)	Effort (User)	Effort (Attacker)	Frustration (User)	Frustration (Attacker)
Eye gaze	40.43	80.33	32.39	31.33	33.04	81.33	36.52	86.67	43.48	80.67	32.83	70.67
Head pose	37.39	72.33	42.17	35.67	34.57	71.67	31.52	78.00	42.61	77.67	30.22	67.67
Tapping	29.13	74.00	38.04	35.00	31.96	67.33	32.61	75.33	35.43	73.67	23.91	60.00

Fig. 10. Perceived workload of RubikAuth users is significantly lower than the perceived workload of attackers. The high NASA-TLX scores in the security study indicate that observation attacks on RubikAuth are demanding. Significance of $p < .05$ is denoted by *. Error bars show the standard deviation.

Finding 13: Video recordings and real-world replicas of RubikAuth significantly improve attack accuracy, although not enough to significantly increase the number of successful attacks.

As for the experimenter's attacks, a two-way repeated measures ANOVA showed a significant effect of password strength on attack accuracy ($F_{2,\,24} = 12.562$, $p < .05$, $\eta_p^2 = 0.511$). We neither found a significant effect of pointing method nor an interaction effect ($p > .05$).

Post hoc analysis using t-tests with Bonferroni correction revealed significant differences ($p < .05$) between all pairs: weak RubikAuth passwords (M=0.130, SD=0.095) are more vulnerable to observation attacks than medium-strong passwords (M=0.169, SD=0.089). Both are more vulnerable than strong passwords (M=0.255, SD=0.095).

Finding 14: Users' perceptions of what makes RubikAuth passwords secure matches reality.

Confidence during Observation Attacks. Participants reported on their subjective confidence of conducting successful observation attacks on a 5-point Likert scale. Participants' confidence was lowest in threat model 2 when using the 3D replica (*M=2.05,Med=2,SD=1.1*). It was slightly higher in threat model 1 when using pen and paper (*M=2.10,Med=2,SD=1.04*), and was at its highest in threat model 3 when using video recordings (*M=2.24,Med=2,SD=1.03*). This shows a tendency that participants were more confident in threat model 3. However their confidence (Md = 2) was still relatively low.

Similar to participants' observation attacks, we measured the perceived confidence of the **expert's observation attacks**. The subjective confidence of successful observation attacks was in general low. The expert rated the statement "I am confident that my observation attack was successful." with an average of 2.33 (SD = 1.27, Md = 2).

Finding 15: Both the trained participants and the expert attacker were not confident about their guesses during observation attacks.

Perceived Workload of Observations. The perceived workload of attacks was measured using NASA-TLX [52] out of 100. Overall score for eye gaze is higher (M=71.83, SD=20.50) than for head pose (M=67.17, SD=15.92) and controller tapping (M=64.22, SD=15.42). But we found no significant differences ($p > .05$). All NASA-TLX raw scores are significantly higher for attackers

compared to RubikAuth users, as confirmed by multiple independent t-tests ($p < .05$), except for the raw scores of physical demand. This indicates that observation attacks on RubikAuth are significantly more demanding than using RubikAuth (Finding 4 and Figure 10).

Finding 16: Attacks on RubikAuth are demanding. There is no evidence that attacks on one pointing method are more demanding than the others.

Perceived Observation Ease. When asking participants at the end of the study how easy it was for them to run successful observation attacks on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree), all participants perceived gaze to be the most difficult to attack (Med=1, SD=0). Head pose (Med=2, SD=0.65) (Z = -3.217, $p < .05$) and controller tapping (Med=2, SD=0.88) (Z = -3.126, $p < .05$) are perceived easier to attack, as confirmed by a Friedman test ($\chi^2(2) = 22.400$, $p < .05$) and Wilcoxon signed-rank tests with Bonferroni correction. There is no difference of perceived observation ease of pointing method between head pose and controller tapping ($p > .05$). This is in line with our findings when asking our participants before and after the observation attacks about the perceived observation resistance of each pointing method.

Finding 17: Gaze is perceived to be the most difficult to attack. There is no evidence that the perceived difficulty is significantly different for head pose and controller tapping.

Attackers' Strategies. We analysed participants' attack behaviour by reviewing video recordings of the study sessions.

- In **threat model 1** where participants used only a pen and a paper, participants focused mostly on guessing surfaces instead of digits as the latter was perceived as too challenging. Participants tried to visualise the cube rotations to repeat the gestures themselves (Figure 11-1).
- In **threat model 2** participants tapped on the physical 3D replica of the cube to simulate the authentication and gazed at the cube to visualise the authentication. Interestingly, one participant did not interact with the 3D replica. We assume that they did not see an advantage of explicit interactions with the replica. To summarise, when using the real-world replica of the 3D cube most participants tried to replicate the rotations performed by the user during their authentication (Figure 11-2).
- In **threat model 3** where attackers had access to the 3D replica and to the recorded authentications on the smartphone, they repeated the entire physical movements during their attack and tapped on the 3D cube in parallel to watching the video recordings multiple times (Figure 11-3).

Independent of the threat model, during attacks on eye gaze attackers focused primarily on the rotation of the non-dominant hand and tried to spot slight head movements. The one successful observation attack by the experimenter on eye gaze relied on slight head movements. More attention is paid to head movements when passwords are entered with head pose, and to dominant hand movements when passwords are entered with controller tapping to derive the spatial relation of RubikAuth's password elements.

5 GENERALISABILITY, VALIDITY AND LIMITATIONS

Like many empirical studies, it is important to note that the below-mentioned technological and experimental design limitations should be considered when interpreting our findings.

Fig. 11. In threat model 1, participants imitated cube rotations and pointing actions (1). In threat models 2 and 3, participants made use of the 3D replica (2) and video recordings (3).

5.1 Experimental Design Limitations

As opposed to real authentications where a user authenticates less frequently than in our usability study, excessive gaze-based inputs could have resulted in longer entry times due to eye fatigue [75], or faster entry times due to learning effects. Moreover, multiple consecutive authentications likely have an influence on the reported feedback and perceived workload for all three pointing methods. Since participants provided input an equal number of times using each pointing method, we expect that relative results across the conditions will remain the same. Providing users with unfamiliar PINs could also have had an effect on some of our measures (e.g., authentication time). Similar to prior work (e.g., [41, 42]), we had a training phase where users entered predefined passwords on RubikAuth. Further, we used relatively short passwords (i.e., 4-digit PINs). Prior work found that short passwords do not appear to follow a significant habituation trend [126].

A limitation in our memorability study is the lack of rewards for correctly recalling the password, and that participants did not use the created password for a week before the memorability study. In real scenarios, the user is incentivised to remember their passwords to, for example, maintain access to data or be able to perform purchases, and will likely use their password frequently after setting it [54, 84, 122]. This suggests our memorability results might be on the lower edge of performance in the real world which is likely to be better.

Regarding the security study, our participants put in a lot of effort in terms of time and attention, as they performed overall 36 observation attacks. The entire security study lasted one hour per participant. Arguably, the number of observation attacks performed by an attacker varies in a real-world setting and conducting multiple observation attacks within a short time period as in our security study may lead to fatigue. To prevent significant fatigue, we had several short breaks between each observation attack, and longer breaks before switching to a different threat model. Another limitation worth to mention is that the attackers were aware of a) the length of the password, and b) the start and end of the authentication. In the real world, users may create longer RubikAuth passwords and attackers will not be aware of that.

5.2 Generalisability of RubikAuth's Concept

Although we studied only one manipulable 3D object in VR (in our case RubikAuth, a 3D cube), we showed through three user studies that leveraging the concept of coordinated 3D manipulation and pointing through bimanual asymmetric interaction [14, 63] results in fast and highly secure authentications. We note that using shapes that are easily understandable (e.g., a 3D cube) has a

positive impact on security. Users are generally familiar with the 3D cube structure from their real world experiences, which in turn contributes to their awareness of what makes passwords strong as presented in our work (see Section 6.4.3). For example, our results suggest that in the case of 0-switch passwords *(defined as weak passwords by our participants*, see Table 2) users transferred more or less well-known weak passwords from existing authentication schemes to RubikAuth. In the case of strong passwords *(mostly 2-switch and 3-switch passwords*, see also Table 2), the defined passwords by our participants manifested indeed a higher resistance to observations.

It should also be noted that the benefits of asymmetrical bimanual cooperation combined with a manipulable 3D object as presented with RubikAuth for authentication in VR may not be fully transferable to all types of 3D objects (e.g., more complex 3D objects).

5.3 Threats to Validity

While our study designs and evaluation approaches are common in research on HCI, Usable Security and Privacy, and VR, some of our specific decisions have limitations to keep in mind.

5.3.1 Internal and External Validity. We contributed with several factors to avoid confounding variables and ensure high internal validity. Our usability and memorability studies were conducted in the same highly controlled lab setting for all study sessions. The security study was conducted in a different room, but with all sessions in the same room. For all studies, we counter-balanced all conditions and participants were not aware of the RubikAuth password categories (e.g., 2-switch) they have to input in the usability study or guess in the security study. We also used a study protocol in all three studies. This minimised the potential of introducing additional variables in some sessions but not in others. All these factors contributed to high internal validity.

Although our evaluation of RubikAuth is based on three user studies: a usability ($\approx$ 23 hours), memorability ($\approx$ 4 hours 20 minutes), and security study ($\approx$ 15 hours), all evaluations of RubikAuth were in the lab. Conducting the security evaluation in a controlled setting as done in our work depicts a best-case-scenario for attackers and highlights RubikAuth's resistance to observation attacks. Therefore, attackers in a real-world setting would yield similar attack rates or perform even worse due to additional noise such as bystanders who may cover parts of a victims interaction when authenticating, or their lack of awareness of the length of the password. In terms of our lab-based usability and memorability study, participants were standing still and did not move during the authentication task. VR users are generally fully immersed and unaware of physical surroundings [40, 88]; thus, it is rather unlikely that there are significant movements (e.g., walking) during authentication in VR, especially when considering the safety of the user (and their bystanders).

When talking about the ecological validity, it is likely that users' provided passwords in the memorability study do not match their real-world passwords. This is mainly because of the lower ecological validity of password studies [35] and due to the fact that existing authentication systems in the real world do not provide users with multiple surfaces to select their password from (e.g., an ATM represents only a 2D PIN-pad).

Furthermore, given the resources available, we had sample sizes of N=23, N=21, and N=15 for our three studies. Although these sample sizes are common in HCI research [15], statistical tests indicating significant differences do so only for our sample and may not have a significant high external validity regarding the generalisability to the wider population that manifests varying demographics such as age, gender, cultural background, VR experience. However, our early comparison between VR-experienced and non VR-experienced users in Section 4.3.4 suggests that there is no significant difference between those two groups when interacting with RubikAuth.

5.3.2 Conclusion Validity. Regarding conclusion validity *(also known as statistical validity)*, we performed our analyses with statistical tests that are well-recognised, commonly used in HCI research,

and also used by prior work on authentication in VR (e.g., [39, 41, 42, 100]). Our sample sizes (N=23, N=21, N=15) are in line with prior works that studied authentication in VR (e.g., [41, 42, 100] and noticeably larger than user studies within the HCI community as pointed out by [15]. Furthermore, our analysis was performed on overall 2208 authentications in the usability study and 672 attacks in the security study. We reported the partial eta squared values (η_p^2) as a measure for the estimated effect size [64, 80, 109]. According to [19] our analyses manifest large effect sizes (all $>$0.14).

Although our sample sizes are typical in HCI research and in line with previous work, it is important to keep the sample size discussion in Section 5.3.1 in mind.

Additionally to presenting a novel authentication scheme for VR and introducing three realistic threat models for assessing the system's resistance to observations, our work also outlines learned lessons for designing and evaluating novel authentication schemes as presented with RubikAuth, to guide further research when studying authentication in VR and human-centred threat models.

6 DISCUSSION AND FUTURE WORK

First, when comparing RubikAuth's entry time and observation resistance to prior work, we achieved fast entry times (Finding 1) and high observation resistance (Finding 10) for authentication in VR. RubikAuth's recall and input accuracy are high (Findings 3 and 7) and consistent with previous work [42, 74]. A comparison of RubikAuth's memorability is limited as we only found one prior work on authentication in VR ([42]) that reports on memorability evaluation results. Although the work by Olade et al. [100] reports memorability in terms of pre-login delay time [121], we cannot compare it to our work due to the use of different metrics. Table 4 outlines all comparisons to prior work on knowledge-based authentication in VR.

6.1 Implications for Research Questions

In the following we discuss our research questions in the light of our findings from our usability, memorability, and security user studies.

6.1.1 Usability, Memorability and Security of RubikAuth.

> **R_{Q1}**: *How do eye gaze, head pose, and controller tapping impact authentication in VR using coordinated 3D manipulation and pointing?*

The quantitative results of the usability study show that using controller tapping in RubikAuth results in the fastest authentications and high entry accuracy. This is confirmed by participants' perception; they perceived controller tapping to be significantly faster than eye gaze and head pose. The perceived ease of providing input with eye gaze, head pose, and controller tapping in RubikAuth suggests that participants found all pointing methods easy to use.

In contrast, while gaze-based input resulted in significantly longer authentications and more entry errors, our security analysis under three realistic threat models suggested that eye gaze is significantly more secure than controller tapping and head pose. This is in line with the qualitative feedback. The subjective user ranking together with the analysis of the perceived security clearly indicate that gaze-based pointing in combination with coordinated 3D manipulation is perceived as most secure.

To conclude, **eye gaze** manifests the highest observation resistance when using coordinated 3D manipulation and pointing for authentication in VR, but at the expense of longer authentication times. **Controller tapping** leads to significantly faster authentications than eye gaze and head pose, and is still highly secure against observation attacks, but not as secure as eye gaze. Both the quantitative and qualitative analyses suggest that head pose is a valid alternative to gaze-based interaction in RubikAuth that achieves fast authentications, but at the expense of lower observation resistance. **Head**

Authentication System	Entry time	Observation Resistance	Memorability
RubikAuth			strong password: 42.86% medium-strong password: 61.90% weak password: 95.24%
eye gaze	2.39 s - 4.92 s	99.55%	-
head pose	2.35 s - 4.68 s	97.78%	-
controller tapping	1.69 s - 3.5 s	96%	-
VRPursuits [74]	21.40 s	Not reported	Not reported
RoomLock [41]	8.58 s - 14.33 s	87.5% - 100%	80.77%
HoloPass [50]	16.69s	Not reported	Not reported
LookUnlock [39]	≈6 s̃	94.1% - 100%	Not reported
2D PINs & 2D Patterns [42]	2.38 s - 3.84 s	82%	Not reported
VR Swipe [100]	≈1.0 s - 1.8 s*	≈60% - 80%*	Not reported
2D sliding patterns [136]	≈10.5 s	Not reported	Not reported
2D numeric keyboard [136]	≈10.5 s	Not reported	Not reported
3D patterns [136]	19 s	Not reported	Not reported

Table 4. RubikAuth improves entry time and observation resistance over many existing schemes for VR/AR systems. All systems above use four-symbol passwords, expect [100] who used *6 SWIPE Passwords*. We did not report perceived mental workload of the prior works as none of them reported these values. There is one work [41] that assessed users' perceived workload, but they did not report the values. (̃) The implementation of LookUnlock [39] indicates that entering a four-symbol password takes at least 6 s (4×1.5 s). (*) We report the average authentication times according to [100, Fig. 4] and the observation resistance under "attacker scenario B" since this is the most comparable scenario to our security analysis.

pose does not stand out in any evaluations; however, we see head pose as a promising alternative to eye gaze, but with the downside of lower observation resistance.

> **R$_{Q2}$**: *How does the number of object manipulations influence authentication in terms of usability and security?*

To reflect on **R$_{Q2}$**, we want to distinguish between three factors that are noticeably affected by the number of object manipulations during authentication. These factors are **authentication time**, **memorability**, and **observation resistance**.

Our usability study shows that the number of object manipulations increases authentication time. This is not surprising as more object manipulations include more physical movements (i.e., hand rotations). However, our qualitative findings also suggest that additional object manipulations are promising for tricking bystanders that are observing the authentication. For example, one could rotate the cube multiple times back and forth while selecting all password elements from the same surface.

Related to this, qualitative feedback during the memorability study suggests that these object manipulations could support users' recall process. In particular, participants mentioned that the cube pose and corresponding arm rotations acted as cues for memorising their RubikAuth password. However, to the contrary, our quantitative analysis also indicates that passwords that manifest more object manipulations are harder to memorise. Nevertheless, we believe that our recall success rates are the result of a lab study where participants used an authentication scheme like RubikAuth for their first time and did not use RubikAuth passwords within the week before the memorability study.

Regarding observation resistance, our quantitative analysis of the security study revealed that object manipulations result in more secure authentication, independent of the pointing method. Along

this, our participants manifest a basic understanding of what makes a password secure when using RubikAuth– more RubikAuth rotations are not only perceived as more secure, they are objectively more secure as indicated by the security study.

6.1.2 The Impact of Advanced Threat Models on Security Evaluations.

> **R_{Q3}**: *How do human-centred threat models beyond classical one-time observations impact the security evaluation of an authentication system as presented with RubikAuth?*

Our quantitative results from our security study suggest that supporting attackers with additional equipment supports their attacks. Although the rate of successful attacks still remained low due to RubikAuth's high resistance to observation attacks, our in-depth analysis of the attack accuracy revealed that there are indeed significant differences between our studied threat models. For example, we found significant differences of the attack accuracy between threat model 3 (video recordings) and threat model 1 (pen and paper) when using head pose, and threat model 3 (video recordings) and threat model 2 (3D replica) when using controller tapping. This suggests that human-centred threat models beyond classical one-time observations impact a system's security evaluation.

Moreover, attackers were more confident when they had access to physical props (e.g., 3D replica of RubikAuth and smartphone) during their observation attacks. Qualitative feedback and our video recordings of attackers' observation strategy also revealed that our participants made use of the additional physical props (threat model 2 and 3) that we provided.

To conclude, **human-centred threat models beyond classical one-time observations** as simulated with our three threat models **improve attacks** and **result in advanced security evaluations**. Such advanced threat models as presented in our work together with threat models that involve multiple attackers at the same time as presented in [72] are vital to evaluate a system's security.

In light of RubikAuth's security results and our lessons learned through the security study we highly encourage researchers and practitioners conducting research on authentication to consider advanced threat models as presented in this work to increase the validity of security evaluations and consider contexts where attackers may have access to additional support material.

6.2 Using Manipulable 3D Objects for Authentication

While previous work used 3D objects in the environment [39, 41] and static 2D and 3D selectable targets for authentication in AR and VR [42, 74, 136], in this work we use a 3D cube that is independent from the environment, is directly linked to controller motion, and has nine targets on five of its six sides. The advantage of this design is manifold: **1)** it gives quick access to many targets in high speed using minimal wrist movements and low workload, **2)** the coordinated 3D manipulation and pointing likely taps into muscle memory particularly when using controller tapping, **3)** it complicates attacks by requiring attackers need to observe both the cube manipulations and the positions of the selected targets, **4)** it significantly increases the theoretical password space, and **5)** the intuitiveness of cube manipulations makes it easier for users to anticipate actions that improve observation resistance.

Our quantitative analysis indicates that authentications in VR on RubikAuth are not affected by users' prior experience with VR (Finding 5).

The usability study shows that RubikAuth is fast. It is also as fast or faster than many observation resilient authentication schemes for mobile devices and public displays, RubikAuth is faster than schemes like SwiPIN (3.7 s) [131] and CueAuth (3.73 s-26.35 s) [76], and faster than gaze-based PIN entry on computer screens (5.3 s-6.28 s, [1]; 8.14 s-12.68 s, [36]). Note that similar to RubikAuth, the entry times above were reported for four-symbol passwords. RubikAuth's fast authentications also confirm Katsini et al.'s [68] findings when evaluating a three-dimensional graphical authentication

scheme on a desktop computer. Their results show that users who used the three-dimensional graphical authentication scheme created their passwords in less time compared to those who used the two-dimensional one.

Continued use of RubikAuth is likely to result in faster authentications due to learning effects; muscle memory [114] might aid participants in recalling and performing manipulations. The high authentication speed can also be attributed to the fact that muscle memory [114] aids users in entering RubikAuth passwords faster. It is also likely that muscle memory helps improve the memorability of the passwords over time. This is not the case when using controller tapping only, as rotating the cube is possible even when using head pose or eye gaze for pointing in RubikAuth. Some of our participants mentioned during the memorability study that they tried to establish some kind of muscle memory based on the cube rotations in their non-dominant hand despite the fact that they only entered their RubikAuth passwords three times to memorise them. One participant voiced that they did not have *"enough time [to establish] muscle memory."* **(P8)**. Additional entries over a long time would allow them to support their recall process at a later time by consolidating the specific motor task, which is necessary to interact with different surfaces, into their memory.

The security study showed that RubikAuth is resilient to observations by expert and trained attackers (Finding 10), even in advanced threat models (Finding 13). This is attributed to the high cognitive effort required to observe the manipulations and multiple visual channels, such as head movements and hand movements, at the same time (Finding 16 and Figure 10). This is in line with prior work [26, 71, 76, 131] that overwhelm the attacker by requiring them to keep track of a lot of information. Additional aspects of the human body such as foot-tapping for selection in RubikAuth could overwhelm attackers even more in the future [93]. Increasing the number of surface switches improves security significantly (Finding 11).

For high observation resistance when using controller tapping, we recommend to include at least one switch in RubikAuth passwords. Gaze performs well against all studied threat models even without switches (Findings 11 and 12), but at the expense of longer authentication time, and relatively lower accuracy in case of 0-switches. A longitudinal study of fast gaze-based input showed that input time decreases after several hours of training [129]. Due to the fact that our participants provided gaze-based input on RubikAuth only for a few minutes during the usability study, we assume that long-term gaze-based interaction on RubikAuth would depict a similar decrease in authentication time. Similarly to gaze-based interaction, increasing the number of switches increases authentication time (Finding 2). In total, authentications on RubikAuth are fast (1.69 s to 4.92 s) and highly secure (97.78% - 100%); therefore we recommend to leverage similar manipulable 3D objects for frequent authentications in VR.

6.3 RubikAuth's baseline: the 0-switch condition

Additionally to the discussion of RubikAuth's usability and security in Section 6.1.1, here, we compare RubikAuth to previous works on authentication for VR/AR (see Table 4) and discuss RubikAuth's performance with respect to the baseline condition (0-switch RubikAuth passwords).

Treating the 0-switch condition as our baseline was motivated by the fact that there are no cube rotations required when using 0-switch passwords for authentication, and that the surface facing the user resembles a traditional PIN-pad as already explored by, for example, George et al. [42] and Olade et al. [100]. In fact, our 0-switch condition is functionally equivalent to a 2D PIN/Pattern-pad that is positionally tracked. Our findings from three user studies show that introducing 3D manipulations (e.g., physical cube rotations to enter 3-switch PINs) enhance user authentications in many ways (see Section 4.3.4, 4.4.1, and 4.5.4). Moreover, previous work highlighted overwhelming attackers leads to more secure systems [26, 71, 76, 131]. We hypothesised that 1-switch, 2-switch, and 3-switch passwords lead to more secure authentications, similarly to the work by Khamis et al. [71, 73].

Note that while in the work by Khamis et al. [71, 73] a switch is defined as a change in the used input modality during authentication, in RubikAuth we refer to surface switches as described in Section 3.6, similarly to the work by De Luca et al. [26].

In the following we discuss RubikAuth's usability and security along the 0-switch condition.

6.3.1 Usability. Our usability study revealed that 0-switch authentications are significantly faster than 1-switch, 2-switch, or 3-switch RubikAuth authentications. We also learned that cube rotations do not necessarily reduce the entry accuracy and can be used to trick attackers, even when inputting a 0-switch RubikAuth password through "fake rotations".

Furthermore, our memorability study revealed that more than half of our participants transferred the password *"1234"* to RubikAuth, which is considered to be the weakest PIN on a 2D PIN-pad [7]. We also learned from qualitative feedback that participants treated the cube as a 2D PIN-pad in the case of a 0-switch password. Interesting is users' perception of "weak RubikAuth passwords". As highlighted in Table 2, 22 participants (95.65%) defined a 0-switch password as a weak password. This is interesting since most authentication schemes (e.g., [42, 100, 136]) rely on 2D PIN-pads and are similar to RubikAuth and a 0-switch password. Regarding memorability, our qualitative feedback revealed that weak passwords (defined as 0-switch RubikAuth passwords by our participants) were more memorable. Mainly because participants could transfer their existing mental model of passwords from other authentication schemes (e.g., ATMs, 2D PIN-pads) to RubikAuth.

While the same does not hold true for 1-switch, 2-switch, and 3-switch passwords, RubikAuth's characteristics (e.g., cube rotations) could augment users' mental model in the long run through, for example, establishing muscle memory.

6.3.2 Security. RubikAuth comes with a larger theoretical password space compared to previous authentication schemes for VR and AR [39, 41, 74], especially compared to 2D-PIN pads [42, 100, 136]. When considering 0-switch passwords only, RubikAuth comes with a theoretical password space that is equal to authentication schemes studied in prior works (e.g., [41, 100, 136].

In light of RubikAuth's other conditions (e.g., 3-switch passwords), the theoretical password space is much larger. Still, there is no additional value in a large theoretical password space if users only rely on a small subset of the theoretically possible password space (practical password space [113]). The practical password space is often much smaller because of the scheme-dependent predictability of user choices [11].

We indeed showed in our work that providing users with a fully manipulable 3D object as done with RubikAuth nudges users to create more diverse passwords. For example, when asking users to create a strong RubikAuth password, they utilised the majority of the theoretical password space, rather than just considering one surface of RubikAuth (see Table 2). While this shows that the additional password space of RubikAuth is used by users, it is not clear at this stage if authentications that take use of the larger theoretical password space are more secure against attacks. Yet, our security study revealed that increasing the number of switches significantly improves security (see Figure 9). Furthermore, as for the experimenter's attacks, strong passwords (3-switch passwords) were significantly more secure than weak passwords (0-switch passwords, baseline).

To conclude, we explicitly neglected to use a simple 2D surface with digits as our baseline because entering a 0-switch PIN on RubikAuth does not involve any cube rotations, and thus it is similar to entering a PIN on a 2D surface, and because there is already work that conducted in-depth studies on 2D authentication schemes for VR [42, 100] that we used for comparison in Table 4. Further, our three user studies, particularly also qualitative feedback from our participants during the usability and memorability study (see Section 4.3.4 and 4.4.1), and our human-centred approach to generate different password strengths on RubikAuth, show that our baseline, RubikAuth's 0-switch condition, was indeed treated similar to a 2D PIN/pattern-pad.

6.4 Gaze-based Authentication, Threat Modeling, and RubikAuth's Characteristics

We further discuss gaze-based authentication on RubikAuth, the significance of advanced, yet realistic, threat models when assessing a system's resistance to observations, and RubikAuth's characteristics along promising future work directions.

6.4.1 A Closer Look on Gaze-based Interaction on RubikAuth. Although gaze is the most preferred pointing method and highest ranked in the security ranking by participants, authentications are slower and slightly more error-prone. Participants explained that the relatively lower input accuracy of gaze and 0-switch passwords is due to the high speed of gaze pointing, which sometimes results in pointing at the following target before confirming selection of the prior target using the trigger. This occurs less often when switching surfaces (Figure 5).

Some users leak information by slightly moving their heads along with their eye movements. This is how the experimenter uncovered one RubikAuth password entered by gaze. This is because gaze and head movements are closely associated under natural conditions [9, 10] and is in line with what Sidenmark et al. [117] suggested: eye gaze should be treated as multimodal input that combines eye, head, and body movement.

However, Collins and Barnes experiments [20] showed that under certain circumstances gaze and head movements can be controlled independently. Future longitudinal studies of RubikAuth should confirm how likely it is that users move their head and body when interacting using gaze. Such head and body movements when providing input on RubikAuth may eliminate the security benefits of using gaze-based authentication in the long run. A further question to consider is whether users can leverage conflicting head and eye movements to trick attackers.

Furthermore, a comprehensive review of knowledge-based authentication schemes highlighted the need of schemes that adapt to the overall context of use [66]. Future systems can detect head movements and either warn the user or take precautions (e.g., rotating the cube to confuse attackers) in situations where they are at stake of being observed. Although gaze and head movements are closely associated, they *can be* controlled independently [20] and can therefore enable users to trick attackers when providing gaze-based input on RubikAuth.

6.4.2 Employing Suitable Threat Models. Existing work focused mostly on one-time shoulder surfing attacks, and video attacks recorded using a stationary camera [39, 41, 42, 100]. We employed three threat models that simulate 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 (Findings 11 and 12). We argue that evaluations of authentication schemes should employ advanced threat models like the ones considered in this paper to ensure realistic results. This is particularly important for VR where the user is often unaware of their surroundings [40, 88], which in turn allows observers to inconspicuously optimise their attacks by, for example, recording videos or using support material.

6.4.3 Users' Perception vs Reality. Previous work found that users' perceptions of what makes passwords secure do not always match reality [51, 130]. In our evaluation, we found that users have a basic understanding of what makes a RubikAuth password more secure against observations. This is in line with what Katsini et al. [68] found when exploring different image grid visualisations and the creation of strong graphical passwords on a desktop computer. For example, when asked to set strong passwords, participants selected passwords with multiple surface switches, and reported they prefer using eye gaze and believe it is the most secure (Finding 8 and 14).

We found that increasing the number of cube manipulations significantly improves observation resistance, and that using gaze for pointing results in the least accurate guesses by attackers. Further, our participants used their knowledge from other authentication schemes to inform their decisions

related to password strength. For example, some participants used "1234" as the weak password [7]. This raises further interesting questions for future work: to what extent do users transfer their knowledge of other schemes? and how does this impact the security and usability of novel authentication mechanisms? Future work can gain insights into habituation when using an authentication scheme like RubikAuth over a longer period of time. Prior work indeed showed that habituation can affect the way users authenticate and interact with a system [101, 126]. Furthermore, prior work by Katsini et al. [67, 69] found that the user's likelihood to create weak graphical passwords can be predicted from their gaze behaviour. Future work can explore if gaze behaviour can predict the creation of weak RubikAuth passwords and nudge the user accordingly.

6.4.4 Manipulate the Cube to Manipulate the Attacker? Some participants mentioned that RubikAuth allows them to apply fake cube rotations to trick attackers. 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. While these findings indicate that users *can* go an extra mile for additional security, it is not clear if users would indeed do that. Previous work showed that sometimes users know what would constitute secure behaviour, but refrain from doing it due to usability issues [130]. An interesting next step would be to investigate the extent to which users of RubikAuth adapt their behaviour to improve security even more. While we encourage future work in studying cases where users introduce randomness to their input (e.g., fake rotations, personalised visual design), we strongly advise against having the system introduce randomness by, for example, randomising the layout of digits. Previous work has shown repeatedly that randomising authentication interface elements reduces usability significantly [1, 25, 133].

During our experiments, a few participants already mentioned that fake rotations could be applied to trick potential attackers and that a more frequent usage would result in even faster entry times and establish some kind of muscle memory. We believe that practice also benefits attackers. In particular, we expect that attackers will come up with more advanced observation attacks over time.

Another way to complicate attacks is by dynamically switching pointing methods during authentication as suggested by one participant. However, it is necessary to investigate to what extent a seamless transition between multiple pointing methods can be provided and how it affects usability.

6.4.5 RubikAuth: A Personalised Authentication Scheme? Although users are in full control of RubikAuth's position and orientation in the virtual environment, some may also prefer a smaller-sized cube or alternative arrangements of RubikAuth's password elements. Prior work suggests that the representation of authentication schemes (e.g., the size) can have a noticeable impact on usability and security [42]. In RubikAuth, users could "personalise" the authentication scheme to meet individual requirements. For example, users could come up with different cube sizes. Note that we strictly distinguish between *personalised* and *randomised*: with *personalised* we refer to a RubikAuth that is designed individually by the user and does not introduce a random factor.

Our qualitative analysis regarding users' most frequent recall strategies in Section 4.4 revealed that users rely on spatial proximities, visual patterns, and physical movements and rotations when recalling a RubikAuth password. This suggests that introducing any kind of randomisation would break their strategy or force users coming up with alternative approaches. The most frequent voiced recall strategies suggest that users remembered the spatial arrangement of their individual passwords rather than the digits and surface colours. This is in line with guidelines for designing graphical authentication mechanism interfaces [108]: people are particularly good at remembering spatial source positions [43], which is also supported by the pictorial superiority effect [96] and dual

encoding [18]. This also emphasises the strengths of a secure and easy-to-use authentication system as presented with RubikAuth.

Compared to graphical authentication schemes that use personalised pictures, e.g., faces from family members or friends [13, 32], a personalised setting of RubikAuth (in terms of cube size and/or arrangement of the numbers) would not necessarily decrease security. For example, one could think of an individual arrangement of RubikAuth's password elements (e.g., swapping the position of the "1" with the "9") , a 90° rotation of specific RubikAuth surfaces or of the entire cube at the beginning of an authentication. If users are in full control of such authentication scheme characteristics, they are still able to apply above-mentioned recall strategies or even enhance them if the system allows it.

6.5 Concluding Remarks: RubikAuth and the Recent Trend of Continuous Authentication in Virtual Reality

Unlike continuous authentication schemes, RubikAuth is an entry point scheme that does not require continuous sensor data (e.g., human body movements). RubikAuth is still capable of securing entire VR interaction sessions, and even improving continuous authentication schemes that rely on behavioural biometrics.

6.5.1 Securing the Entire VR Interaction Session. Ensuring that an intruder cannot take over a VR system after the user has authenticated can be achieved in two ways: 1) via continuous authentication, or 2) by requiring the user to authenticate again whenever they take off their VR HMD.

Continuous authentication can be achieved using behavioural biometrics. Although there are several recent works that propose this in VR (e.g., [78, 86, 90, 91, 103]), Miller et al.'s work is the first that explores cross-system behavioural biometric authentication in VR [91], which is essential in a world where users may have multiple VR systems in the foreseeable future. Indeed, 21.7% of millennial respondents to a questionnaire claim to already own such a VR device [30] and, similar to the increased adoption of other technologies such as smartphones [16], it is expected that households will have multiple VR devices in the near future. The recent increasing interest in consumer VR devices (e.g., Oculus Quest's sell-through shipments [31]) and the wide-spread adoption of VR devices underscore the need for authentication schemes that are generalisable across different devices. To build generalisable VR authentication schemes, contextual factors such as the hardware of the different VR HMDs should be considered [66]. The work by Miller et al. [91] is an example of generalising an authentication scheme across different VR HMDs with different hardware specs.

Interacting with RubikAuth involves lots of movements and rotations: head, gaze, non-dominant hand, and dominant hand movements that could be used to establish an additional behaviour-based security layer on top of a knowledge-based authentication scheme. While we consider such an approach still to be an entry point authentication, it would not require long-term or permanent access to sensor data [110], but still has the potential to make authentications more secure [86]. Given that VR sessions are considered to be rather long (*M=38 minutes* [29]) compared to, for example, smartphone sessions (*M=5.12 minutes (307 seconds))* [57], sensors (e.g., the proximity sensor in the Oculus Quest [111]) could be used to log off users when they step out of the VR experience (i.e., when taking off the HMD) to prevent malicious users from accessing sensitive data after authentications. However, we have to keep in mind that such an approach would require users to explicitly re-authenticate; thus, users may not make use of such a feature [130].

6.5.2 RubikAuth as a Fallback for Biometric Authentication. There are situations where biometric systems are not functional enough anymore; thus, alternative fallback authentication mechanisms are required. For example, when VR devices are used in situations with restricted freedom of movements (e.g., using VR during air travel [132]) human-behavioural movements may not be feasible anymore for continuous authentication. In such scenarios it is vital to provide equally usable and secure

fallback authentication mechanisms. Biometric authentication oftentimes relies on knowledge-based authentication as a fallback method [8] and it is unlikely to change in the foreseeable future [56]. An authentication scheme is only as strong as its weakest link, and if fallback authentication methods are insecure, then even the most secure biometric authentication scheme is insecure [127]. Although RubikAuth is not primarily designed as a fallback authentication method, it is also capable of acting as a fast and highly secure fallback method, especially in situations where behavioural biometric authentication is ineffective and not possible given the context a user is in.

6.6 Learned Lessons for Designing Authentication for Virtual Reality

To summarise, we draw the following lessons learned for designing and evaluating novel authentication schemes in VR:

(1) The use of manipulable 3D objects in VR greatly improves authentication speed and observation resistance.

(2) Increasing the number of manipulations (e.g., surface switches in RubikAuth) improves security further and presents opportunities to trick observers, but could negatively influence usability (e.g., increases input time).

(3) Using gaze improves security but requires longer authentication time and might be insecure if users inadvertently move their heads.

(4) Leveraging additional characteristics of novel authentication schemes, e.g., physical movements when authenticating, is a promising direction to support memorability and enable users to consolidate a specific motor task into memory through repetition.

(5) Studying threat models beyond classical one-time observations by, for example, including real-world 3D replicas and smartphones with HD cameras to record and playback the authentications, improves our understanding of the security of VR authentication systems.

7 CONCLUSION

We investigated authentication in virtual reality (VR) using an environment-independent manipulable 3D cube. We compared pointing at targets on the cube using eye gaze, head pose, and controller tapping. We conducted three within-subjects experiments, a usability study (N=23), a follow-up memorability study (N=21), and a security study (N=15). Across three studies, we showed how an environment-independent manipulable 3D authentication scheme improves authentications in VR in terms of usability and observation resistance. First, in our usability study we found that entering a four-symbol password on RubikAuth using controller tapping is significantly faster (2.60 s) than head pose (3.44 s) and eye gaze (3.60 s). In terms of usability and security our participants preferred gaze-based interaction for authentications on RubikAuth. Second, our memorability study revealed that users tried to memorise their RubikAuth passwords with the help of spatial positions of the digits and by recalling physical movements and rotations. Third, our security study highlighted the high resistance of RubikAuth to observation attacks, even under classical and enhanced threat models. Gaze-based interaction on RubikAuth outperformed head pose and controller tapping in terms of resistance to observation attacks. Observation resistance is 96% for controller tapping, 97.79% for head pose, and 99.55% for eye gaze. Finally, our results suggest that providing attackers with support material contributes to more critical security evaluations. We concluded with five lessons learned for the design and evaluation of authentication schemes for virtual reality.

8 ACKNOWLEDGEMENTS

We thank all participants for taking part in this research. We also thank our editor and all anonymous reviewers whose reviews and input improved this manuscript significantly. We also thank our colleagues from the Glasgow Interactive Systems research group (GIST) and the Technology Usability Lab in Privacy and Security (TULiPS) for their feedback. Special thanks to Mark McGill. This publication was supported by the University of Edinburgh and the University of Glasgow jointly funded PhD studentships, by the Erasmus+ internship grant from the LMU Munich, and by the Royal Society of Edinburgh (award number #65040).

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. https://doi.org/10.1145/3314111.3319837

[2] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 906–918. https://doi.org/10.1145/3025453.3025961

[3] Ashwin Ajit, Natasha Banerjee, and Sean Banerjee. 2019. Combining Pairwise Feature Matches from Device Trajectories for Biometric Authentication in Virtual Reality Environments. In *2019 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE Computer Society, Los Alamitos, CA, USA, 9–97. https://doi.org/10.1109/AIVR46125.2019.00012

[4] Tepljakov Aleksei Alessandro, Mirani and Hayretdin Bahsi. 2020. User Behavior Analysis for Predictive Virtual Reality Applications: An Ethical and Data Security Perspective. (2020).

[5] Hassoumi Almoctar, Pourang Irani, Vsevolod Peysakhovich, and Christophe Hurter. 2018. Path Word: A Multimodal Password Entry Method for Ad-hoc Authentication Based on Digits' Shape and Smooth Pursuit Eye Movements. In *Proceedings of the 20th ACM International Conference on Multimodal Interaction (ICMI '18)*. ACM, New York, NY, USA, 268–277. https://doi.org/10.1145/3242969.3243008

[6] Sean Andrist, Michael Gleicher, and Bilge Mutlu. 2017. Looking Coordinated: Bidirectional Gaze Mechanisms for Collaborative Interaction with Virtual Characters. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 2571–2582. https://doi.org/10.1145/3025453.3026033

[7] Nick Berry. 2013. *PIN analysis*. http://www.datagenetics.com/blog/september32012/index.html accessed 30 June 2020.

[8] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. In *In Proc. USEC*. https://doi.org/10.1.1.725.2698

[9] B. Biguer, M. Jeannerod, and C. Prablanc. 1982. The coordination of eye, head, and arm movements during reaching at a single visual target. *Experimental Brain Research* 46, 2 (01 May 1982), 301–304. https://doi.org/10.1007/BF00237188

[10] Emilio Bizzi, Ronald E. Kalil, and Vincenzo Tagliasco. 1971. Eye-Head Coordination in Monkeys: Evidence for Centrally Patterned Organization. *Science* 173, 3995 (1971), 452–454. https://doi.org/10.1126/science.173.3995.452

[11] Joseph Bonneau. 2012. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP '12)*. IEEE Computer Society, USA, 538–552. https://doi.org/10.1109/SP.2012.49

[12] Miguel Borges, Andrew Symington, Brian Coltin, Trey Smith, and Rodrigo Ventura. 2018. HTC Vive: Analysis and Accuracy Improvement. In *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*. 2610–2615. https://doi.org/10.1109/IROS.2018.8593707

[13] Sacha Brostoff and M. Angela Sasse. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *People and Computers XIV — Usability or Else!* Springer London, London, 405–424. https://doi.org/10.1007/978-1-4471-0515-2_27

[14] William Buxton and Brad Myers. 1986. A Study in Two-handed Input. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '86)*. ACM, New York, NY, USA, 321–326. https://doi.org/10.1145/22627.22390

[15] Kelly Caine. 2016. Local Standards for Sample Size at CHI. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 981–992. https://doi.org/10.1145/2858036.2858498

[16] Pew Research Center. 2017. *A third of Americans live in a household with three or more smartphones*. https://www.pewresearch.org/fact-tank/2017/05/25/a-third-of-americans-live-in-a-household-with-three-or-more-smartphones/ accessed 29 June 2020.
[17] Kathy Charmaz and Linda Liska Belgrave. 2015. *Grounded Theory*. American Cancer Society. https://doi.org/10.1002/9781405165518.wbeosg070.pub2
[18] Sonia Chiasson, Alain Forget, Elizabeth Stobert, Paul C Van Oorschot, and Robert Biddle. 2009. Multiple password interference in text passwords and click-based graphical passwords. In *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 500–511. https://doi.org/10.1145/1653662.1653722
[19] Jacob Cohen. 1973. Eta-Squared and Partial Eta-Squared in Fixed Factor Anova Designs. *Educational and Psychological Measurement* 33, 1 (1973), 107–112. https://doi.org/10.1177/001316447303300111
[20] C. J. S. Collins and G. R. Barnes. 1999. Independent control of head and gaze movements during head-free pursuit in humans. *The Journal of Physiology* 515, 1 (1999), 299–314. https://doi.org/10.1111/j.1469-7793.1999.299ad.x
[21] VALVE Corporation. 2019. *SteamVR Plugin*. https://assetstore.unity.com/packages/tools/integration/steamvr-plugin-32647 accessed 29 August 2019.
[22] Lynne Coventry, Antonella De Angeli, and Graham Johnson. 2003. Usability and Biometric Verification at the ATM Interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*. Association for Computing Machinery, New York, NY, USA, 153–160. https://doi.org/10.1145/642611.642639
[23] Charles Benedict Davenport and Albert Gallatin Love. 1921. *Army Anthropology: Based on Observations Made on Draft Recruits, 1917-1918, and on Veterans at Demobilization, 1919*. Vol. 15. US Government Printing Office.
[24] 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). https://doi.org/10.1136/bmjstel-2017-000295
[25] 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. https://doi.org/10.1145/1556262.1556312
[26] 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. https://doi.org/10.1145/2556288.2557097
[27] Alexander De Luca, Emanuel Von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2389–2398. https://doi.org/10.1145/2470654.2481330
[28] 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. https://doi.org/10.1145/2470654.2481331
[29] Statista Research Department. 2018. *Virtual reality and augmented reality (VR and AR) devices average session time in the United States as of 2018*. https://www.statista.com/statistics/831819/us-virtual-augmented-reality-device-average-session-time/ accessed 29 June 2020.
[30] Statista Research Department. 2019. *Share of respondents who own a virtual reality headset computing device in the United Kingdom in 2019, by generation*. https://www.statista.com/statistics/1044070/uk-virtual-reality-headset-ownership/ accessed 29 June 2020.
[31] Statista Research Department. 2020. *Oculus Rift and Oculus Quest sell-through shipments worldwide in 2016 and 2019*. https://www.statista.com/statistics/936099/global-oculus-rift-oculus-quest-sales/ accessed 03 July 2020.
[32] Rachna Dhamija and Adrian Perrig. 2000. Déjà Vu: A User Study Using Images for Authentication. In *Proceedings of the 9th Conference on USENIX Security Symposium - Volume 9 (SSYM'00)*. USENIX Association, USA, 4.
[33] DVPR. 2016. *DPVR M2 PRO - A standalone virtual reality headset*. http://dpvr.net/m2pro.html accessed 29 August 2019.
[34] Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. 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 (CHI '17)*. ACM, New York, NY, USA. https://doi.org/10.1145/3025453.3025636
[35] Sascha Fahl, Marian Harbach, Yasemin Acar, and Matthew Smith. 2013. On the Ecological Validity of a Password Study. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, Article 13, 13 pages. https://doi.org/10.1145/2501604.2501617
[36] Misahael Fernandez, Florian Mathis, and Mohamed Khamis. 2020. GazeWheels: Comparing Dwell-time Feedback and Methods for Gaze Input. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction (NordiCHI*

'20). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3419249.3420122

[37] 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. https://doi.org/10.3389/fpubh.2018.00044

[38] FOVE. 2016. *FOVE 0 - virtual reality headset with eye-tracking technology*. https://www.getfove.com/ accessed 29 August 2019.

[39] 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. https://doi.org/10.1145/3290607.3312959

[40] 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. https://doi.org/10.1145/3322276.3322363

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

[42] 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. https://doi.org/10.14722/usec.2017.23028

[43] Bradley S. Gibson, Libo Li, Emily Skow, Kimberly Brown, and Lauren Cooke. 2000. Searching for One Versus Two Identical Targets: When Visual Search Has a Memory. *Psychological Science* 11, 4 (2000), 324–327. https://doi.org/10.1111/1467-9280.00264 PMID: 11273393.

[44] Barney G Glaser and Anselm L Strauss. 2017. *Discovery of grounded theory: Strategies for qualitative research*. Routledge. https://doi.org/10.4324/9780203793206

[45] Gene V Glass, Percy D Peckham, and James R Sanders. 1972. Consequences of failure to meet assumptions underlying the fixed effects analyses of variance and covariance. *Review of educational research* 42, 3 (1972), 237–288. https://doi.org/10.2307/1169991

[46] Google. 2014. *Google Cardboard - Experience virtual reality in a simple, fun, and affordable way.* https://vr.google.com/cardboard/ accessed 29 August 2019.

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

[48] 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. https://doi.org/10.1016/S0166-4115(08)60623-8

[49] Jonathan Gurary, Ye Zhu, and Huirong Fu. 2017. Leveraging 3d benefits for authentication. *International Journal of Communications, Network and System Sciences* 10, 08 (2017), 324. https://doi.org/10.4236/ijcns.2017.108B035

[50] 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. https://doi.org/10.1145/3290607.3313076

[51] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security (SOUPS '14)*. USENIX Association, USA, 213–230.

[52] Sandra G Hart. 2006. NASA-task load index (NASA-TLX); 20 years later. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 50. Sage publications Sage CA: Los Angeles, CA, 904–908. https://doi.org/10.1177/154193120605000909

[53] Michael R Harwell, Elaine N Rubinstein, William S Hayes, and Corley C Olds. 1992. Summarizing Monte Carlo results in methodological research: The one-and two-factor fixed effects ANOVA cases. *Journal of educational statistics* 17, 4 (1992), 315–339. https://doi.org/10.3102/10769986017004315

[54] Eiji Hayashi and Jason Hong. 2011. A Diary Study of Password Usage in Daily Life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2627–2630. https://doi.org/10.1145/1978942.1979326

[55] Eiji Hayashi, Oriana Riva, Karin Strauss, A. J. Bernheim Brush, and Stuart Schechter. 2012. Goldilocks and the Two Mobile Devices: Going Beyond All-or-nothing Access to a Device's Applications. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, Article 2, 11 pages. https://doi.org/10.1145/2335356.2335359

[56] Cormac Herley and Paul Van Oorschot. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security Privacy* 10, 1 (2012), 28–36. https://doi.org/10.1109/MSP.2011.150

[57] Daniel Hintze, Philipp Hintze, Rainhard D. Findling, and René Mayrhofer. 2017. A Large-Scale, Long-Term Analysis of Mobile Device Usage Characteristics. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 1, 2, Article 13 (June 2017), 21 pages. https://doi.org/10.1145/3090078

[58] Teresa Hirzle, Jan Gugenheimer, Florian Geiselhart, Andreas Bulling, and Enrico Rukzio. 2019. A Design Space for Gaze Interaction on Head-mounted Displays. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 625, 12 pages. https://doi.org/10.1145/3290605.3300855

[59] HTC. 2016. *HTC VIVE Pro Eye*. https://www.vive.com/uk/product/vive-pro-eye/ accessed 29 August 2019.

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

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

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

[63] Paul Kabbash, William Buxton, and Abigail Sellen. 1994. Two-handed input in a compound task.. In *CHI*, Vol. 94. 417–423. https://doi.org/10.1145/191666.191808

[64] Maurits Kaptein and Judy Robertson. 2012. Rethinking Statistical Analysis Methods for CHI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. Association for Computing Machinery, New York, NY, USA, 1105–1114. https://doi.org/10.1145/2207676.2208557

[65] Christina Katsini, Yasmeen Abdrabou, George Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions.. In *Proceedings of the 38th Annual ACM Conference on Human Factors in Computing Systems (CHI '20)*. ACM, New York, NY, USA, 21. https://doi.org/10.1145/3313831.3376840

[66] Christina Katsini, Marios Belk, Christos Fidas, Nikolaos Avouris, and George Samaras. 2016. Security and Usability in Knowledge-based User Authentication: A Review. In *Proceedings of the 20th Pan-Hellenic Conference on Informatics (PCI '16)*. ACM, New York, NY, USA, Article 63, 6 pages. https://doi.org/10.1145/3003733.3003764

[67] Christina Katsini, Christos Fidas, George E. Raptis, Marios Belk, George Samaras, and Nikolaos Avouris. 2018. Influences of Human Cognition and Visual Behavior on Password Strength During Picture Password Composition. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 87, 14 pages. https://doi.org/10.1145/3173574.3173661

[68] 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. https://doi.org/10.1145/3206505.3206546

[69] Christina Katsini, George E. Raptis, Christos Fidas, and Nikolaos Avouris. 2018. Towards Gaze-based Quantification of the Security of Graphical Authentication Schemes. In *Proceedings of the 2018 ACM Symposium on Eye Tracking Research & Applications (ETRA '18)*. ACM, New York, NY, USA, Article 17, 5 pages. https://doi.org/10.1145/3204493.3204589

[70] Jiro Kawakita. 1991. The original KJ method. *Tokyo: Kawakita Research Institute* 5 (1991).

[71] 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. https://doi.org/10.1145/2851581.2892314

[72] Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 2017. They are all after you: Investigating the Viability of a Threat Model that involves Multiple Shoulder Surfers. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia (MUM '17)*. ACM, New York, NY, USA, 5. https://doi.org/10.1145/3152832.3152851

[73] 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. https://doi.org/10.1145/3136755.3136809

[74] Mohamed Khamis, Carl Oechsner, Florian Alt, and Andreas Bulling. 2018. 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. https://doi.org/10.1145/3206505.3206522

[75] Mohamed Khamis, Ozan Saltuk, Alina Hang, Katharina Stolz, Andreas Bulling, and Florian Alt. 2016. TextPursuits: Using Text for Pursuits-Based Interaction and Calibration on Public Displays. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '16)*. ACM, New York, NY, USA, 12. https://doi.org/10.1145/2971648.2971679

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

[77] 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. https://doi.org/10.1016/j.nedt.2018.08.002

[78] Alexander Kupin, Benjamin Moeller, Yijun Jiang, Natasha Kholgade Banerjee, and Sean Banerjee. 2019. Task-Driven Biometric Authentication of Users in Virtual Reality (VR) Environments. In *MultiMedia Modeling - 25th International Conference, MMM 2019, Thessaloniki, Greece, January 8-11, 2019, Proceedings, Part I*. 55–67. https://doi.org/10.1007/978-3-030-05710-7_5

[79] Mikko Kytö, Barrett Ens, Thammathip Piumsomboon, Gun A. Lee, and Mark Billinghurst. 2018. Pinpointing: Precise Head- and Eye-Based Target Selection for Augmented Reality. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. ACM, New York, NY, USA, Article 81, 14 pages. https://doi.org/10.1145/3173574.3173655

[80] Timothy R. Levine and Craig R. Hullett. 2006. Eta Squared, Partial Eta Squared, and Misreporting of Effect Size in Communication Research. *Human Communication Research* 28, 4 (01 2006), 612–625. https://doi.org/10.1111/j.1468-2958.2002.tb00828.x

[81] Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu, Janne Lindqvist, and Macro Gruteser. 2016. Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns. In *2016 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. 1–9. https://doi.org/10.1109/PERCOM.2016.7456514

[82] Lisa M Lix, Joanne C Keselman, and HJ Keselman. 1996. Consequences of assumption violations revisited: A quantitative review of alternatives to the one-way analysis of variance F test. *Review of educational research* 66, 4 (1996), 579–619. https://doi.org/10.2307/1170654

[83] Shiqing Luo, Anh Nguyen, Chen Song, Feng Lin, Wenyao Xu, and Zhisheng Yan. 2020. OcuLock: Exploring Human Visual System for Authentication in Virtual Reality Head-mounted Display. In *Network and Distributed System Security Symposium (NDSS 2020) (USEC '20)*. NDSS. https://doi.org/10.14722/ndss.2020.24079

[84] Joseph Masling. 1966. Role-related behavior of the subject and psychologist and its effects upon psychological data.. In *Nebraska symposium on motivation*. University of Nebraska Press.

[85] Florian Mathis, John Williamson, Vaniea Kami, and Mohamed Khamis. 2020. RubikAuth: Fast and Secure Authentication in Virtual Reality. In *Proceedings of the 38th Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '20)*. ACM, New York, NY, USA, 9. https://doi.org/10.1145/3334480.3382827

[86] Florian Mathis, John Williamson, Kami Vaniea, and Mohamed Khamis. 2020. Knowledge-driven Biometric Authentication in Virtual Reality. In *Proceedings of the 38th Annual ACM Conference on Human Factors in Computing Systems (CHI EA '20)*. ACM, New York, NY, USA. https://doi.org/10.1145/3334480.3382799

[87] Alex Turner Jesse McCulloch Matt Zeller, Brandon Bray. 2019. *HoloLens Gestures*. https://docs.microsoft.com/en-us/windows/mixed-reality/gestures/ accessed 01 March 2020.

[88] 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. https://doi.org/10.1145/2702123.2702382

[89] Dominik Meyer, Jan Haase, Marcel Eckert, and Bernd Klauer. 2016. A threat-model for building and home automation. In *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*. 860–866. https://doi.org/10.1109/INDIN.2016.7819280

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

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

[92] Mark R Mine. 1995. Virtual environment interaction techniques. *UNC Chapel Hill CS Dept* (1995).

[93] 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. https://doi.org/10.1145/3290605.3300707

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

[95] Tahrima Mustafa, Richard Matovu, Abdul Serwadda, and Nicholas Muirhead. 2018. Unsure How to Authenticate on Your VR Headset?: Come on, Use Your Head!. In *Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics (IWSPA '18)*. ACM, New York, NY, USA, 23–30. https://doi.org/10.1145/3180445.3180450

[96] Douglas L Nelson, Valerie S Reed, and John R Walling. 1976. Pictorial superiority effect. *Journal of experimental psychology: Human learning and memory* 2, 5 (1976), 523. https://doi.org/10.1037/0278-7393.2.5.523

[97] Diederick C. Niehorster, Li Li, and Markus Lappe. 2017. The Accuracy and Precision of Position and Orientation Tracking in the HTC Vive Virtual Reality System for Scientific Research. *i-Perception* 8, 3 (2017), 2041669517708205. https://doi.org/10.1177/2041669517708205 PMID: 28567271.

[98] Oculus. 2016. *Oculus Rift*. https://www.oculus.com/rift/ accessed 03 February 2020.

[99] Ilesanmi Olade, Charles Fleming, and Hai-Ning Liang. 2020. BioMove: Biometric User Identification from Human Kinesiological Movements for Virtual Reality Systems. *Sensors* 20, 10 (2020), 2944. https://doi.org/10.3390/s20102944

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

[101] Nikhil Palaskar, Zahid Syed, Sean Banerjee, and Charlotte Tang. 2016. Empirical Techniques to Detect and Mitigate the Effects of Irrevocably Evolving User Profiles in Touch-Based Authentication Systems. In *Proceedings of the 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE) (HASE '16)*. IEEE Computer Society, USA, 9–16. https://doi.org/10.1109/HASE.2016.39

[102] Anjul Patney, Marco Salvi, Joohwan Kim, Anton Kaplanyan, Chris Wyman, Nir Benty, David Luebke, and Aaron Lefohn. 2016. Towards Foveated Rendering for Gaze-tracked Virtual Reality. *ACM Trans. Graph.* 35, 6, Article 179 (Nov. 2016), 12 pages. https://doi.org/10.1145/2980179.2980246

[103] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. ACM, New York, NY, USA, Article 110, 12 pages. https://doi.org/10.1145/3290605.3300340

[104] Nick Pino. 2019. *HTC Vive review*. https://www.techradar.com/reviews/wearables/htc-vive-1286775/review accessed 29 August 2019.

[105] Alexander P. Pons and Peter Polak. 2008. Understanding User Perspectives on Biometric Technology. *Commun. ACM* 51, 9 (Sept. 2008), 115–118. https://doi.org/10.1145/1378727.1389971

[106] Tobii Pro. 2018. *Tobii Pro VR Integration*. https://www.tobiipro.com/product-listing/vr-integration/ accessed 29 August 2019.

[107] Yuan Yuan Qian and Robert J. Teather. 2017. The eyes don't have it: An Empirical Comparison of Head-based and Eye-based Selection in Virtual Reality. In *Proceedings of the 5th Symposium on Spatial User Interaction (SUI '17)*. ACM, New York, NY, USA, 91–98. https://doi.org/10.1145/3131277.3132182

[108] Karen V. Renaud. 2009. Guidelines for designing graphical authentication mechanism interfaces. *International Journal of Information and Computer Security* 3, 1 (2009), 60–85. https://doi.org/10.1504/IJICS.2009.026621

[109] John T.E. Richardson. 2011. Eta squared and partial eta squared as measures of effect size in educational research. *Educational Research Review* 6, 2 (2011), 135 – 147. https://doi.org/10.1016/j.edurev.2010.12.001

[110] Franziska Roesner, Tadayoshi Kohno, and David Molnar. 2014. Security and Privacy for Augmented Reality Systems. *Commun. ACM* 57, 4 (April 2014), 88–96. https://doi.org/10.1145/2580723.2580730

[111] 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.* https://www.wired.com/review/oculus-quest accessed 19 January 2020.

[112] Chris Salter, O. Sami Saydjari, Bruce Schneier, and Jim Wallner. 1998. Toward a Secure System Engineering Methodology. In *Proceedings of the 1998 Workshop on New Security Paradigms (NSPW '98)*. Association for Computing Machinery, New York, NY, USA, 2–10. https://doi.org/10.1145/310889.310900

[113] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the Design Space of Graphical Passwords on Smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 11, 14 pages. https://doi.org/10.1145/2501604.2501615

[114] Reza Shadmehr and Thomas Brashers-Krug. 1997. Functional stages in the formation of human long-term motor memory. *Journal of Neuroscience* 17, 1 (1997), 409–419. https://doi.org/10.1523/JNEUROSCI.17-01-00409.1997

[115] Yiran Shen, Hongkai Wen, Chengwen Luo, Weitao Xu, Tao Zhang, Wen Hu, and Daniela Rus. 2019. GaitLock: Protect Virtual and Augmented Reality Headsets Using Gait. *IEEE Transactions on Dependable and Secure Computing* 16, 3 (May 2019), 484–497. https://doi.org/10.1109/TDSC.2018.2800048

[116] Adam Shostack. 2014. *Threat Modeling: Designing for Security* (1st ed.). Wiley Publishing.

[117] Ludwig Sidenmark and Hans Gellersen. 2019. Eye, Head and Torso Coordination During Gaze Shifts in Virtual Reality. *ACM Trans. Comput.-Hum. Interact.* 27, 1, Article Article 4 (Dec. 2019), 40 pages. https://doi.org/10.1145/3361218

[118] Marco Speicher, Anna Maria Feit, Pascal Ziegler, and Antonio Krüger. 2018. Selection-Based Text Entry in Virtual Reality. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article Paper 647, 13 pages. https://doi.org/10.1145/3173574.3174221

[119] 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. https://doi.org/10.1145/2470654.2470695

[120] William G. Stillwell, David A. Seaver, and Ward Edwards. 1981. A comparison of weight approximation techniques in multiattribute utility decision making. *Organizational Behavior and Human Performance* 28, 1 (1981), 62 – 77. https://doi.org/10.1016/0030-5073(81)90015-5

[121] Elizabeth Stobert and Robert Biddle. 2013. Memory Retrieval and Graphical Passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 15, 14 pages. https://doi.org/10.1145/2501604.2501619

[122] Elizabeth Stobert and Robert Biddle. 2014. The Password Life Cycle: User Behaviour in Managing Passwords. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 243–255. https://www.usenix.org/conference/soups2014/proceedings/presentation/stobert

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

[124] Shridatt Sugrim, Can Liu, and Janne Lindqvist. 2019. Recruit Until It Fails: Exploring Performance Limits for Identification Systems. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 3, Article 104 (Sept. 2019), 26 pages. https://doi.org/10.1145/3351262

[125] Shridatt Sugrim, Can Liu, Meghan Mclean, and Janne Lindqvist. 2019. Robust Performance Metrics for Authentication Systems. https://doi.org/10.14722/ndss.2019.23351

[126] Zahid Syed, Sean Banerjee, Qi Cheng, and Bojan Cukic. 2011. Effects of User Habituation in Keystroke Dynamics on Password Security Policy. In *Proceedings of the 2011 IEEE 13th International Symposium on High-Assurance Systems Engineering (HASE '11)*. IEEE Computer Society, USA, 352–359. https://doi.org/10.1109/HASE.2011.16

[127] Christian Tiefenau, Maximilian Häring, Mohamed Khamis, and Emanuel von Zezschwitz. 2019. "Please enter your PIN" – On the Risk of Bypass Attacks on Biometric Authentication on Mobile Devices. arXiv:cs.HC/1911.07692

[128] Tobii. 2019. *Tobii Pro VR Integration*. https://www.tobiipro.com/product-listing/vr-integration/ accessed 29 August 2019.

[129] Outi Tuisku, Päivi Majaranta, Poika Isokoski, and Kari-Jouko Räihä. 2008. Now Dasher! Dash Away! Longitudinal Study of Fast Text Entry by Eye Gaze. In *Proceedings of the 2008 Symposium on Eye Tracking Research & Applications (ETRA '08)*. Association for Computing Machinery, New York, NY, USA, 19–26. https://doi.org/10.1145/1344471.1344476

[130] Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, New York, NY, USA, 3748–3760. https://doi.org/10.1145/2858036.2858546

[131] 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. https://doi.org/10.1145/2702123.2702212

[132] Julie R. Williamson, Mark McGill, and Khari Outram. 2019. PlaneVR: Social Acceptability of Virtual Reality for Aeroplane Passengers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300310

[133] Christian Winkler, Jan Gugenheimer, Alexander De Luca, Gabriel Haas, Philipp Speidel, David Dobbelstein, and Enrico Rukzio. 2015. 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 (CHI '15)*. ACM, New York, NY, USA, 1407–1410. https://doi.org/10.1145/2702123.2702316

[134] J. D. Woodward. 1997. Biometrics: privacy's foe or privacy's friend? *Proc. IEEE* 85, 9 (1997), 1480–1492. https://doi.org/10.1109/5.628723

[135] Chun Yu, Yizheng Gu, Zhican Yang, Xin Yi, Hengliang Luo, and Yuanchun Shi. 2017. Tap, Dwell or Gesture?: Exploring Head-Based Text Entry Techniques for HMDs. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 4479–4488. https://doi.org/10.1145/3025453.3025964

[136] 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. https://doi.org/10.1109/APCCAS.2016.7804002