

SoK: Authentication in Augmented and Virtual Reality

Sophie Stephenson[†], Bijeeta Pal[‡], Stephen Fan[†], Earlence Fernandes[†], Yuhang Zhao[†], Rahul Chatterjee[†]

[†]University of Wisconsin—Madison, [‡]Cornell University

Abstract—Augmented reality (AR) and virtual reality (VR) devices are emerging as prominent contenders to today’s personal computers. As personal devices, users will use AR and VR to store and access their sensitive data and thus will need secure and usable ways to authenticate. In this paper, we evaluate the state-of-the-art of authentication mechanisms for AR/VR devices by systematizing research efforts and practical deployments. By studying users’ experiences with authentication on AR and VR, we gain insight into the important properties needed for authentication on these devices. We then use these properties to perform a comprehensive evaluation of AR/VR authentication mechanisms both proposed in literature and used in practice. In all, we synthesize a coherent picture of the current state of authentication mechanisms for AR/VR devices. We draw on our findings to provide concrete research directions and advice on implementing and evaluating future authentication methods.

I. INTRODUCTION

Augmented reality (AR) and virtual reality (VR) head-mounted devices (HMDs) have recently become commercially viable for end-users [4], [5]. For example, VR devices have grown in popularity with the online gaming community, but their use extends to education [40], healthcare [66], the military [64], and beyond. AR devices, too, are becoming more prevalent; some, like Microsoft’s HoloLens, are geared towards a business environment, again with applications in healthcare, manufacturing, and education [4].

With the growing popularity of these devices, an increasingly common and critical task is secure and usable user authentication. It would be simplest for AR and VR to follow the paradigm of passwords as the *de facto* authentication mechanism. However, password entry does not easily translate to the novel interfaces of AR and VR. Instead of typical interaction methods like a keyboard and mouse or a smartphone touch screen, AR/VR users perform gestures (free-hand or with controllers) to interact with the device. Although such gestures *can* be used to enter text passwords, doing so is incredibly cumbersome; as a result, users choose weaker passwords, and the slow speed of entry leaves users vulnerable to external observer attacks (i.e., shoulder surfing).

Researchers have been actively working to improve text entry in AR/VR [26], [34], [38], [73]. However, existing works on improving text entry rely on language models to predict and correct errors [27]. Improving text entry in this way would not make password entry any more usable; secure passwords should be random and hard to guess, making it difficult to apply these error correction mechanisms. Further, more usable text entry will not solve the numerous security problems which have plagued passwords since their inception.

Prior work has considered authentication methods for wearables like smart watches (e.g., [53], [72]). However, the

authentication methods that work for wearables in general will not suffice for AR and VR. Unlike other wearables, AR and VR are trending towards being standalone, general-purpose computing devices, and thus typical authentication for wearables will not always work for AR/VR. Specifically, other wearables often require a paired device for authentication; e.g., Apple Watch users first log in by going to an app on their iPhone [11]. When AR/VR devices are standalone, users will not reliably have access to such a secondary device.

We believe AR/VR devices present an opportunity to look beyond password-based authentication and its long history of security problems. To enable richer user experiences, AR/VR devices come with a wide variety of sensors, such as front cameras for environment tracking, inward cameras for eye-tracking, inertial motion sensors, controllers, and touchpads. These sensors could also be used to provide smoother authentication experiences and enhanced security. For example, prior work has proposed shoulder-surfing-resistant PIN entry methods [50], [56], [57], [75], behavioral biometrics using eye, head, and controller movement [62], [67], and novel skull and ear biometrics [31], [70], among others. The myriad sensors provide opportunities for layered authentication as well; Mathis et. al’s RubikBiom, for example, implements a Rubik’s Cube-inspired PIN entry mechanism, then uses behavioral biometrics of the controller following successful PIN entry [55]. The possibilities are exciting.

The area of AR/VR authentication is still emerging. We argue that now is the right time to systematize existing work to inform the development and adoption of novel AR/VR authentication mechanisms, lest device designs become set in stone with possibly sub-optimal techniques (as is the case with web and mobile authentication).

We, therefore, perform the first systematization of knowledge of the authentication landscape on AR/VR devices. Rather than a conventional synthesis of knowledge, we adopt a more practical perspective which helps reveal the gap between research and real-world deployment of authentication. We survey users and developers of AR/VR devices to understand how they feel about the existing authentication mechanisms they (have to) use on these devices (Section III); we use insights from the user survey to derive a set of evaluation criteria for AR and VR authentication methods (Section IV); we analyze AR and VR applications on two popular devices to identify and evaluate the authentication methods being used in practice (Section V); and finally, we evaluate the novel authentication mechanisms being proposed in research and compare them to those used in practice (Section VI). Below, we highlight a few contributions that emerge from our comprehensive efforts.

Passwords have reached a breaking point on AR/VR. To date, passwords are the most prevalent form of authentication in popular AR and VR apps. However, our user study shows that entering passwords on AR and VR is overwhelmingly unusable. Users complain that using the virtual keyboard to enter a password is “cumbersome,” “difficult,” and “a pain,” and they emphasize that the lack of usability makes it inaccessible to users with physical disabilities. Some users are even forced to devise their own workarounds to make password entry easier for them. This finding highlights an urgent need to re-imagine authentication for AR/VR—a need that the varied sensors on AR and VR can hopefully solve.

Potential to unify the authentication stack via federated login. Multiple AR and VR devices require users to log into a paired account (e.g. Microsoft or Facebook) to unlock and use the device. In theory, this account could be used to bootstrap authentication for web services, providing the user with effortless app authentication. We analyze apps on a PC-tethered VR device (HTC Vive) and find that a few apps take advantage of this opportunity; however, on a standalone AR device (HoloLens 2), none take full advantage of it. With such compelling usability benefits, it is worth exploring why this authentication technique is not widely used.

The AR/VR OS will play a major role in driving the adoption of new authentication techniques. Although there is a growing body of work in AR/VR authentication, much of it is yet to see adoption. Our work, which includes a survey study of AR/VR developers, highlights a need to integrate these new authentication techniques with the OS so that developers can easily use them in applications. Developers and users point out that passwords are unusable and are looking for replacements, but they are limited by a lack of OS support.

Beyond supporting the implementation of new authentication methods, the OS will play a critical role in enabling the safe use of novel biometrics. Consider an inertial sensor that measures an individual’s unique head movements [67], [62]. A malicious app can get access to the same sensor for legitimate reasons (e.g., a game), record head movements, then leak them to an attacker. This issue of multi-use sensors needs OS arbitration and protection mechanisms to be useful in authentication. This might include trusted computing hardware, which could increase the power demands on an already energy-constrained device. Our work highlights this and other challenges to designing authentication for AR and VR devices.

II. BACKGROUND & RELATED WORK

A. Augmented and Virtual Reality Devices

AR and VR technology is maturing quickly. Current AR/VR devices support a wide range of input and output modalities, presenting unique opportunities for more secure and usable authentication mechanisms.

Augmented reality. AR glasses are expected to become the next generation of personal devices [45], [46], [60]. They strive

to be mobile, lightweight, and comfortable to wear, thus supporting long-term use everywhere throughout the day. Some AR glasses are powerful standalone devices (e.g., HoloLens, Magic Leap 1); others can only be used by connecting to smartphones (e.g., Google Glass, Vuzix Blade AR).

To recognize user behavior and support daily activities, AR glasses usually embed multiple input sensors. The most common sensors on AR glasses are RGB cameras and microphones. Inertial measurement units (IMUs) have also been incorporated into many AR glasses (e.g., Epson Moverio, HoloLens) to track the user’s head or body movements. Some AR glasses also have controllers (e.g., Magic Leap 1) or touchpads (e.g., Google Glass, Epson Moverio) to enable control of the glasses. More advanced AR glasses like the HoloLens 2 have outward depth cameras and inward cameras for eye tracking (and sometimes iris scanning, e.g., on HoloLens 2).

In terms of output, most AR glasses support both audio and visual feedback. Some provide 3D graphics via stereo displays, while some provide 2D visual feedback via a single display (e.g., Google Glass, Vuzix Blade). Magic Leap 1 also supports haptic feedback via its controller.

Virtual reality. VR devices are bulkier and more powerful than AR devices and are designed for at-home use. VR has been especially popular during the COVID-19 pandemic [22] since it provides immersive experiences for remote socializing and collaboration. While many VR headsets (e.g., Oculus Rift, Vive Pro) need to be connected to a PC, standalone VR headsets (e.g., Oculus Quest, Vive Cosmos) are also being released to support more flexible and comfortable experiences.

Audio and movement are the two most common inputs for VR devices. Most VR headsets come with a pair of controllers with buttons. Some controllers (e.g., Oculus, Vive Cosmos) also have touch sensors to detect the users’ holding gestures. The position and motion of the headset and controllers can be tracked either via external trackers in the environment (e.g., Vive Tracker [8]) or inside-out tracking techniques like IMU sensors. Some VR headsets have front cameras to enable users to see the real-world environment; these cameras are yet to be used to support VR interactions. The more advanced HTC Vive Pro Eye also incorporates eye tracking components. To generate immersive experiences, VR devices usually support realistic 3D graphics as visual output as well as spatial audio. VR controllers can also provide haptic feedback.

While most VR devices and applications focus on immersive gaming or social experiences, researchers have started envisioning the future of VR for productivity. For example, the VR office concept [35] suggests combining the VR headset with the conventional keyboard and mouse, so that a user can sit in front of their desk, wear their headset to join a virtual workspace, and use their keyboard and mouse to interact with the virtual environment more efficiently.

B. AR/VR Authentication

Although AR and VR are emerging technologies—and steadily gaining popularity—little work has tried to systematize the state-of-the-art of AR/VR authentication in research

and in practice. Early work [14], [68] focused on systematizing the functionalities of AR/VR technologies. For example, Rabbi et al. [68] looked into the different sensor-based tracking techniques in AR systems. Some recent work systematized the security and privacy challenges with AR/VR systems. For example, Roesner et al. [69] were the first to survey the security and privacy threats on augmented reality platforms. They note that a multi-application model, where AR systems are heading, would raise several security and privacy concerns. De Guzman et al. [25] provide a thorough survey of security and privacy in mixed reality systems; they consider authentication as a security property in mixed reality and mention some novel authentication strategies. Shrestha et al. [72] looked into the security and privacy of wearable computing devices, outlining a threat model around how to use them in offensive and defensive expositions. They discuss several authentication methods and evaluate these methods using the framework proposed by Bonneau et al. [16], but they do so in the context of wearables and focus mainly on the types of mechanisms proposed in research. In contrast, our study focuses specifically on *AR and VR devices* and evaluates the *properties* of the proposed methods. Overall, general security and privacy concerns of AR/VR technology are surveyed from multiple angles, but one of the key components of security—user authentication—has not been a focus of prior work.

Bonneau et al. [16] proposed an influential framework for evaluating authentication mechanisms. This framework is designed to compare authentication mechanisms for smartphones and laptops in “the quest to replace passwords.” Although the framework is quite generic and has been adapted for special cases including mobile authentication [74], [43], AR and VR devices have unique capabilities and limitations that are potentially not captured by this generic framework. For instance, many interactions with AR and VR require large, visible gestures. If an authentication method requires these gestures, users may not feel comfortable using it in public places. Bonneau et al. do not capture this notion of acceptability [16]. Thus, we exercise due diligence and propose a framework for evaluating authentication methods *specifically on AR and VR*. We take a holistic approach, using feedback from users and developers to create a framework that captures the unique needs of authentication on AR and VR devices.

C. Threat Model

The goal of the adversary is to impersonate a user to unlock the device or to log into an account. Based on authentication for personal general-purpose computing devices, we consider two adversaries for AR/VR: one without physical access to the device, and the other with physical access.

Adversaries without physical access. Since we expect users will use AR devices in public places, the first adversary we consider is an *external observer* (E). This adversary, also known as a shoulder-surfing adversary, can observe the user’s interactions with the device during authentication. This adversary is particularly important in an AR/VR context and

has been frequently considered by prior work, e.g., [57], [56], [62], [71]. We also consider an *internal observer* (I) who can monitor sensors on the device. For this threat, we assume the user accidentally installs a malicious app (controlled by the adversary) onto the device. Such a threat has been previously considered for smartphones, and laptops/desktops (e.g., [28], [39]), but for AR the threat is more pronounced since applications often have access to a myriad of available sensors which can be used for authentication. Finally, we consider a *credential stuffing* (S) adversary who has access to the user’s stolen credential from another verifier.

Adversaries with physical access. An adversary can steal an AR/VR device and launch more sophisticated software- and hardware-based attacks; we call this a *computation-bound adversary* (C). A similar but distinct adversary is one who already has access to the device, for example, in an intimate partner violence (IPV) scenario, or in the case of a curious colleague who wants to impersonate a user. We call this a *UI-bound adversary* (U) following the prior work [29]; such adversaries are UI-bound in the sense they have brief access to the device and can only interact with it via the provided user interface. The computation-bound and UI-bound adversaries are also known as offline and online guessing adversaries, respectively, in password attack literature.

Attacks can be made more effective by combining two or more adversarial settings discussed above. One common adversarial scenario, known as an *imitation attack* [71], involves the following steps: (1) gaining additional information about the user via external observation, followed by (2) a UI-bound attack when the device is accessible. However, as we will discuss in Section VI, some of the prior work does not consider even a single adversarial setting.

We record the threat models considered by researchers in prior works in Section VI. We begin our systematization by developing a set of coveted properties for authentication methods on AR/VR based on users’ and developers’ experiences with existing authentication methods.

III. USERS’ AND DEVELOPERS’ PERSPECTIVES TOWARDS AR/VR AUTHENTICATION

We surveyed users and developers about their experience with current authentication methods used on AR/VR. For users, we seek to understand their experiences, concerns, and needs when using the existing authentication mechanisms in off-the-shelf AR/VR devices; for developers, we explore whether they have incorporated authentication components into their AR/VR apps and how they chose those components. We use insights from this study to inform an evaluation of existing and proposed authentication methods for AR and VR in Sections V and VI.

A. Surveying AR/VR Users and Developers

Our survey contained five sections: screening, developer experiences, device usage, authentication experiences, and demographics/follow-up. Appendix A contains the full survey. Participants had to be over 18 and be familiar with AR or

VR devices, either as a user or as a developer (or both). We determined participant familiarity using a 7-point scale which ranged from “I have never used any [AR/VR] glasses” to “I own [AR/VR] glasses and use them often.” If the participant indicated that they had used AR glasses only a few times, or had never used AR glasses, we did not consider them familiar with AR for the purposes of the survey. We used the same criteria for VR. If the participant was familiar with neither AR nor VR, we terminated the survey.

Ethics. Our study was reviewed by our IRB and exempted as a human subject research study with minimal risk. We did not collect any personally identifiable information except for email addresses, which we only used for sending payments.

Survey promotion. We piloted the survey to ensure participants could interpret the questions as we intended. Then, we identified 24 online platforms where we would promote our survey, including relevant Slack channels (e.g., HoloDevelopers), university email lists, Twitter, Facebook groups (e.g., Oculus VR Community), and several relevant Reddit threads (e.g., r/hololens). We advertised the survey on each platform once on November 2, 2020, then once more on November 16, 2020, if applicable. We incentivized potential respondents with the chance to win a \$50 gift card for every 25 participants. If a participant’s responses were deemed incomplete (see below), they were not eligible for compensation.

Data filtering. We obtained 306 responses over the three weeks. We then discarded any incomplete (64) and poor quality (103) responses. For example, eight participants had clearly responded in relation to their experiences on *smartphone* AR, which was explicitly mentioned as out of scope for our study. One provided nonsense answers (e.g. “asdf”). Additionally, 94 appeared to be from a scam hive: they were submitted within a short time frame, with very similar email addresses and identical and/or nonsensical answers (e.g., “No one else can use it”). We discarded all such suspicious or irrelevant responses. After filtering, 139 responses remained.

Data analysis. To analyze the quantitative data, we focused on descriptive statistics only. For qualitative analysis, we collected participants’ free-text answers in the survey and performed thematic analysis [18]. There were 414 free-text comments across the 139 participants. Three researchers individually coded the first half of the free-text answers, then compared and discussed the codes together. This produced a codebook based on the agreement of the three researchers. One researcher then coded the remaining responses following the codebook and updated the codebook if new codes were found. Our final codebook contains 168 codes. We categorized the codes using multiple iterations of axial coding, then articulated twenty-one themes that emerged from the data. Fig. 1 presents notable themes and associated codes.

B. User Study Results

We received 139 valid responses to our survey (participants P001-139), including 49 developers (D01-D49). Appendix B










































Theme	Codes	#	Mechanisms
The virtual keyboard is unusable on AR and VR.	virtual keyboard	60	  
	auth speed	20	  
	difficult	8	  
	cumbersome	7	 
Difficulties with the virtual keyboard lead users to choose weak passwords.	tradeoff bw input effort / usability and pwd strength	12	
	symbols / capitalization	3	
Many users consider authentication on AR/VR to be just as secure as on other devices.	as secure as on other devices	28	  
	security depends on the pwd	12	
Users consider shoulder surfing, but disagree on whether it is possible on AR/VR.	observable actions / shoulder surfing	11	 
	screen hidden / safe from shoulder surfing	11	   
Users have concerns about privacy and using AR/VR devices in public.	privacy concerns	7	   
	safe at home / alone	5	 
	nothing private on device	4	 
	collect personal / sensitive data	3	 
Users are concerned about accessibility on AR/VR.	not accessible	4	
	physical disabilities	3	
	shaky hands	2	

Fig. 1. A selection of themes and associated codes from our qualitative analysis. The # column refers to the number of times the code appeared in user responses. The symbols in the “Mechanisms” column list the authentication mechanisms associated with the code:  = password,  = paired device,  = paired account,  = unlock pattern,  = iris scan.

contains a summary of participant demographics. We note that a majority of our participants are male; this may be partially explained by gender disparities in the adoption of AR and VR [24], in the gaming community (gaming is the most popular reason our participants use AR and VR) [23], and on Reddit (where many participants were referred from) [15].

Developers’ authentication decisions. Among the participants are forty-nine AR or VR developers. Twenty-one regularly develop for AR or VR, while the rest have developed for AR or VR in the past. We found that few AR/VR developers (29%) have ever deployed any authentication methods in their apps. There is a disparity between AR-only and VR-only developers: of twelve AR-only developers, six (50%) have deployed authentication, compared to just three out of eighteen developers (17%) who developed for VR only.

Of the fifteen developers who have deployed authentication in their apps, they have most frequently chosen to use passwords (42%) or paired accounts (36%). Below, we summarize the reasons for their authentication decisions. We acknowledge that this sample size is quite small, and thus our results may not reflect the decisions of most AR/VR developers.

Ease of implementation. Five developers cite ease of implementation as a reason that they chose to use passwords (3 participants), paired accounts (3), and iris scan (1). For example, D02 (gender: M, age range: 45-54) chose a paired account

because “Its [*sic*] built into the platform.” D40 (M,25-34) chose a password because it was straightforward to implement.

Consistency across platforms and services impacts developers’ decisions as well. D36 (M,35-44) shares that he chose a Google account because “It was the simplest and required for other [G]oogle services we were using.” Moreover, some developers emphasized the importance of integration with non-AR/VR versions of apps. D04 (M,25-34) describes that his VR app also has a desktop portal, and thus it made sense to use a password for both versions of the app.

Usability of the authentication mechanism. Five developers discuss how the usability of different authentication mechanisms—such as ease of use (3), efficiency (2), and speed (2)—impacts their choices. For example, D40 (M,25-34) mentions, “QR code was easy for the user (no input needed).” D33 (M,45-54) also associates ease of use with iris scan and paired accounts since they do not require the use of the cumbersome virtual keyboard. Evidently, developers consider usability when choosing authentication mechanisms.

Users’ exposure to authentication. Participants have experience with a variety of AR/VR devices (see details in Fig. 6 in Appendix B). However, we found that participants’ exposure to authentication mechanisms on AR/VR devices is fairly limited: twenty-one AR users (54%) have used authentication on AR devices, as have eighty VR users on VR devices (61%). This finding matches feedback from the developers that there are few authenticated apps on AR/VR devices. Other potential reasons for this limited exposure are that participants may not own the device and thus do not log in by themselves, or the device is shared and authentication is disabled for convenience.

We asked users which authentication methods they have used on AR and VR. Users have experience using passwords, unlock patterns, iris scan, paired devices, and paired accounts. By far, passwords are the most commonly used; passwords have been used by 81% of users with authentication experience on AR and 94% of users with authentication experience on VR. See Fig. 7 in Appendix B for more details.

Perceived security and privacy. Twenty-eight participants consider authentication on AR/VR to be just as secure as on any other devices. For example, P013 (M,18-14) mentions that passwords on VR are “No more or less secure than any other devices in my opinion.” These users are mainly concerned about preexisting vulnerabilities unrelated to the AR/VR platform (e.g., that passwords can be cracked).

Shoulder surfing is the major AR/VR-specific concern expressed in our survey. However, participants disagree on whether AR and VR are more or less vulnerable to shoulder surfing than other technologies. The seventeen users who believe AR/VR are *more* vulnerable to shoulder surfing are concerned about attacks on visible authentication actions (12) and the VR screen being visible on a secondary display (5). For example, P019 (F,25-34) explains her concerns about visible actions: “I think it could be possible to find out passwords by observing users typing them via holographic numpads, since the gestures are large and easy to see.”

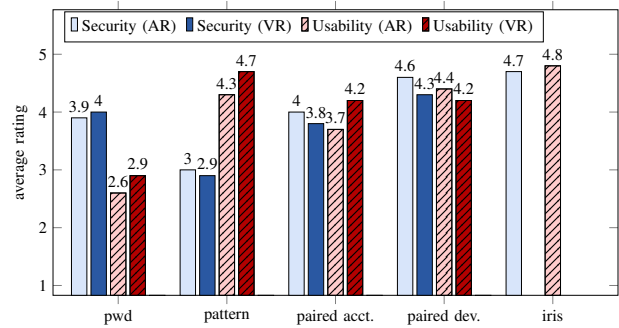


Fig. 2. Average user ratings of authentication methods on scale 1 to 5: 1=“Not secure at all” or “Very hard to use”; 5=“Very secure” or “Very easy to use”. Users only ranked methods they have used before on the specific type of device. No participants had used iris on VR.

On the other hand, the ten users who believe AR/VR are *less* vulnerable note that the screen on the head-mounted device is hidden from others, meaning traditional shoulder surfing attacks are not feasible. There is “no risk of someone looking over your shoulder to see what you are typing,” as P020 (M,25-34) notes. Moreover, some VR users are less worried about shoulder surfing because they don’t think VR devices will be used in public. Five participants comment that authentication on their devices is safe because they use the device only at home and/or alone. P011 (M,25-34) describes,

“[S]omeone could theoretically track your controller position to infer your password. But I use VR in my home alone, so I am not any more concerned about password entry than I would be for any other computer application.”

Users also have *privacy concerns* about authenticating on AR and VR devices. Though users believe iris scan to be the most usable authentication mechanism on AR, three users indicate concerns with the collection of their biometric data. Further, six users are worried about providing private account information and other private data to companies with poor reputations. For example, P139 vents about paired accounts: “[T]he lack of control over my own data is frustrating.”

Perceived usability. We summarize users’ most prevalent usability concerns about authentication on AR/VR devices.

Virtual keyboard woes. While a password is the most popular authentication mechanism on both AR and VR devices, it also receives the most negative feedback from our participants (Fig. 2). For usability, the mean score (out of five) for passwords is 2.6 for AR ($SD = 1.42$) and 2.9 for VR ($SD = 1.26$). The root of the problem for many users is the virtual keyboard. Fifty-nine responses indicate that using the virtual keyboard is challenging and takes too much physical effort. To type on a virtual keyboard in VR, users typically need to use the virtual laser extended from their controllers to point to the keys and press a button on the controller to select the key. “It usually requires slowly going through each character on a rendered keyboard and it is just zero fun” (P057: M,25-34). The typing experience in AR is even worse since it requires gesture interaction. To top it off, three users (P001, P016, P048) note that AR and VR have minimal support for password managers, meaning the user must type

their password every time they authenticate.

Accessibility issues. Four participants express accessibility concerns with the virtual keyboard: “Typing on a virtual keyboard is tolerable for the average user, but can be outright impossible for those with physical disabilities” (P109: gender not disclosed (ND), 18-24). Moreover, P078 (M,18-24) and P021 (M,18-24) specifically have difficulties typing with shaky hands. P021 explains his workaround: “Pointing and clicking at a keyboard without stable hands can make it difficult. I have my own work around involving stepping back, resetting my POV, and stepping closer to the keyboard.” These extra steps for adaptation add more effort to an already cumbersome process, and may even prevent some users from using AR/VR altogether. As P139 (M,25-34) explains, “Sometimes authentication itself feels like a barrier to entry.”

Perceived usability of non-password methods. Iris scan holds the highest usability scores for AR, while unlock pattern is the highest for VR (Fig. 2). AR users prefer to use a paired device—e.g., by scanning a QR code on their phone—over an unlock pattern for both usability and security. Paired accounts such as Facebook accounts have low usability scores (mean = 3.7, $SD = 1.25$) on AR devices; this is because paired accounts often require a user to enter a password associated with that account using the virtual keyboard. In contrast, users appreciate that the other methods require little to no user effort. As P054 (M,35-44) notes, using iris scan to authenticate is “easy, keeping your eyes open...” Moreover, users appreciate that paired accounts (3) or paired devices (1) require infrequent authentication. For example, after setting up a paired account, “I’m already logged into those accounts, so I don’t have to type my password in again” (P050: ND, 35-44).

IV. DERIVING PROPERTIES FOR AR/VR AUTHENTICATION METHODS

Our user survey provided key insights into users’ and developers’ experiences with AR and VR authentication. Here, we distill this information into a set of desired properties for AR and VR authentication mechanisms. In Sections V and VI, we leverage these properties to evaluate the AR/VR authentication methods used in practice and proposed in literature.

We combed through the responses, codes, and themes that resulted from our user survey to identify a list of *properties* desired by users and developers. We included any concern or topic that was noted by at least two respondents. We took a fairly generous approach to including properties; for example, because the code “Not accessible” appears in four responses, our evaluation considers accessibility for a range of disabilities. Through repeated discussion amongst the authors, we defined the requirements for a method to *offer* each desired property, as well as (in some cases) requirements for a method to *quasi-offer* the property.

A. Properties for Evaluation

In all, we identified twenty properties of interest to users and developers and organized them into four categories: deployment, usability, accessibility, and security & privacy. Where applicable, we took inspiration from Bonneau et al. [16] in

naming and organizing our desired properties. Appendix D contains precise definitions of each property and outlines our reasoning for including each property.

Deployability. Developers prefer authentication methods that are *OS-Supported* and *Platform-Agnostic*, characteristics which simplify the development experience. They also value efficiency, which we code as *Low-Power-Consumption*. Additionally, users feel more secure using *Mature* methods (ones that are well-tested and have a good security history).

Usability. Users mention several usability woes, usually regarding the virtual keyboard. From this, we identified that users value methods which have *Infrequent-Errors* and are *Efficient-to-Use*, *Physically-Effortless*, *Easy-to-Learn*, and *Acceptable-in-Public*. Multiple users mentioned how some methods require a secondary device, indicating that whether a method has *Nothing-to-Carry* is important to users. Finally, a method should be *Memorywise-Effortless* since several users mentioned the ease or difficulty of remembering secrets.

Accessibility. These arose from the concerns of four users (P021, P078, P109, P139). Though these users primarily mentioned physical disabilities, we extended their general concern for accessibility to cover five types of disability: *Accessible-Visual*, *Accessible-Hearing*, *Accessible-Speech*, *Accessible-Mobility*, and *Accessible-Cognitive*.

Security & privacy. Users worry that their passwords and PINs are guessable, or that their actions could reveal a secret to onlookers; thus, a method should be *Resilient-to-Guessing* and *Resilient-to-Physical-Observation*. Since users mention privacy concerns, particularly with iris scanning, it is best if a method *Protects-User-Privacy*. Finally, many users feel more secure if methods are *Multi-Factor*.

B. Properties Unique to AR/VR

Though all of these properties are valuable, some have particular importance on AR and VR devices. Our user study revealed five such properties. Importantly, these properties are *not* covered in Bonneau et al.’s seminal framework [16]. First, AR and VR devices are quite power-constrained—e.g., the HoloLens 2 has a battery life of just 2-3 hours [3]. Thus, a method must be *Low-Power-Consumption*, especially when these devices are used away from home. Similarly, as the future of personal devices, AR/VR will be used in public places and interactions with the devices will be visible to external observers. Thus, it is critical that methods are *Acceptable-in-Public* or users will be inclined to use other methods. For further deployability, it is crucial that AR and VR authentication mechanisms are *OS-Supported* so developers use them in practice. Finally, AR and VR can take advantage of myriad sensors for biometric authentication. This means they have the unprecedented opportunity to use *Multi-Factor* methods—as we show in Section VI, some prior work has already taken this leap [55], [76], [81]. However, it is also critical to consider whether these authentication methods *Protect-User-Privacy*. Bonneau et al. discuss the possibility

of combining methods, but do not consider methods that are multi-factor by design; AR and VR should be held to a higher standard and methods designed to be multi-factor should be encouraged. The emergence of these new properties, and their importance to an AR/VR context, validates our suspicion that a framework specific to AR and VR is needed.

We note that our participants surface several of the same properties as those in Bonneau et al.’s framework, indicating that these properties are still useful in evaluating AR and VR authentication methods. Importantly, though, we must interpret these properties from the perspective of AR and VR. Consider the property *Platform-Agnostic*. Bonneau et al. focus on whether methods are compatible with existing passwords; for AR and VR, the emphasis should be on whether a method can be used on other devices *at all*. This factor is important to take into consideration given the unique opportunity for biometric authentication on AR and VR. Similarly, Bonneau et al. consider a method quasi-*Nothing-to-Carry* if it requires a smartphone because the user likely carries a phone with them at all times; since the community envisions AR/VR to be standalone devices, we must consider an AR/VR authentication method that requires a smartphone as *Something-to-Carry*.

V. AUTHENTICATION IN EXISTING AR AND VR APPLICATIONS

We now explore the current state of AR and VR authentication mechanisms in practice—in particular, the authentication mechanisms used in current HoloLens 2 and HTC Vive apps. We first identify which authentication methods are in use, then evaluate these incumbent authentication methods using the criteria we derived in Section IV. In Section VI, we use this data as ground truth in our evaluation of recently-proposed authentication mechanisms for AR and VR.

A. Evaluating Incumbent Authentication Methods

We analyzed apps on the HTC Vive (a VR device) and the HoloLens 2 (an AR device) and evaluated the authentication methods they use according to our properties from Section IV.

For each device, we first reviewed the process of authenticating to the device itself. We then investigated the authentication mechanisms used in apps on these devices. On each device, we conducted two rounds of review to ensure good coverage of different types of apps and authentication methods available on the device. We first focused on the most popular apps available on the device by analyzing the top three apps in every category of the device’s app store. For HTC Vive, we used the top apps ranked by popularity on Viveport [9]; for HoloLens, we relied on the number of user ratings on the Microsoft Store.

The first round, as we will discuss, revealed that most popular apps on these devices do not use authentication. Thus, in our second round, we dug deeper into authentication-heavy categories. For each device, we created a shortlist of app categories that most frequently used authentication in the first round. For the HTC Vive, we randomly selected 8 apps in each of these categories and analyzed them just as we did in the first round. For the HoloLens, we specifically looked at

HoloLens-native apps, since we hypothesized that apps made for AR might leverage authentication methods better suited for AR. For each of the authentication-heavy categories, we analyzed *every* HoloLens-native application in that category. We summarize the types of authentication we found in Fig. 3.

Evaluation. We evaluated each incumbent method using the properties from Section IV. Two authors individually evaluated every mechanism we identified, then discussed to come to a consensus. Importantly, we focused on the implementation of each incumbent method *on AR/VR devices*. For example, using a password is not overwhelmingly error-prone on a computer or mobile device, but our user study showed that users experience frequent errors when entering a password on AR or VR (due to difficulties with the virtual keyboard). Thus, in our evaluation, passwords do not offer *Infrequent-Errors*.

B. Authentication on HTC Vive

Device authentication. A user first signs into their Steam account on a PC with a username and password. Then, the user launches SteamVR [7] on the PC to use the HTC Vive headset. The headset then prompts the user to log into their Viveport account on the PC using a username and password; once they do so, they are granted access to their Viveport library on both PC and headset and can start using apps.

App authentication. In round one, we analyzed three apps in each of the twenty categories on Viveport. Since apps can have multiple categories, this came out to thirty-six unique apps. Only eight apps (22%) use authentication: six use a password and two use a paired account (Fig. 3). Both apps which use a paired account are connected to the user’s Viveport account, which is already signed in when the user launches the app.

Our targeted analysis yielded similar results. In this round, we focused on four categories that had at least one app with authentication in round one or that we believed were likely to use authentication: Business, Video, Productivity, and Social. We randomly sampled eight apps from each category for a total of twenty-one unique apps. In this round, 52% of apps use authentication, a higher percentage than in the first round. However, the types of authentication we found are the same: five apps use passwords, five use paired accounts, and one app offers both a password and a paired account. Viveport is the only paired account offered. It is usually automatically signed in when the user starts the app, except for in one app [2], where the user has to log into their Viveport account again on the VR device after the app has launched.

C. Authentication on HoloLens 2

Device authentication. A user first signs into their Microsoft account on the headset using a username and password. To do this, HoloLens projects a virtual keyboard in view of the wearer, then the user moves their hand to “press” the virtual keys and enter their credentials. Upon initial setup, the user can set up iris scanning on the device; afterward, a user can unlock the device by simply putting it on, looking forward,

	HTC Vive		HoloLens 2		Total
	Popular	Targeted	Popular	Targeted	
Apps analyzed	36	21	76	45	178
Apps using auth	8	11	22	37	78
Mechanisms offered					
Password only	6	5	9	9	29
Paired account only	2	5	6	4	17
QR code only	-	-	-	9	9
Short code only	-	-	-	4	4
PIN only	-	-	-	1	1
Pwd & paired account	-	1	7	2	10
Pwd & QR code	-	-	-	6	6
Pwd & PIN	-	-	-	1	1
Pwd, PIN & paired acc.	-	-	-	1	1

Fig. 3. Summary of authentication mechanisms found in our analysis. A dash indicates no apps used the authentication mechanism.

and briefly waiting for the device to authenticate them.

App authentication. We analyzed seventy-six popular apps in twenty-five categories. The authentication landscape for these apps was again sparse and homogeneous, with only 29% requiring authentication. The only available authentication mechanisms on these apps are passwords and paired accounts, sometimes offered in tandem (Fig. 3). In contrast to the HTC Vive, most paired accounts on HoloLens require the use of a password to log into the paired account; thus, for popular HoloLens apps which use authentication, users must almost always enter a password. The most common paired account accepted is Facebook across eight apps, followed by Microsoft and Google with six each and Apple with three apps.

In the second round of review, we analyzed forty-five HoloLens-native apps in five authentication-heavy categories: Productivity, Personal Finance, Social, Security, and Business/Collaboration. While the other apps we analyzed use only passwords and paired accounts, apps that are tailored for HoloLens 2 use a wide variety of authentication mechanisms, including QR codes, short pairing codes, and PINs (see Fig. 3). In fact, 38% of the authenticated apps made for HoloLens 2 do not offer *any* methods that use a password. The contrast between authentication in HoloLens-native apps and generic apps indicates AR developers may be purposefully choosing authentication methods more suited for AR.

D. Evaluating Incumbent Authentication Mechanisms

From our exploration of authentication on current AR/VR devices, we identified a list of incumbent authentication mechanisms on AR and VR: password, paired account (both manually entered and automatically authenticated), PIN, short code, QR code, and iris scan. Now, we evaluate these mechanisms on the user- and developer-desired properties (Section IV). The gray rows of Fig. 4 summarize our evaluation.

Knowledge-based methods. Our analysis surfaced three knowledge-based methods: passwords, PINs, and paired accounts. Passwords are by far the most popular in our analysis and are thus the incumbent method to beat. They gain all of

the deployability benefits in our evaluation, which is likely a factor in their popularity (as suggested by our user survey, Section III)—however, they do quite poorly in the other categories. The primary issue with passwords on AR and VR is the requirement that users interact with the virtual keyboard. As we saw in our user survey, using the virtual keyboard is slow, difficult, and altogether unpleasant; thus, passwords are not *Efficient-to-Use*, *Physically-Effortless*, *Infrequent-Errors*, or *Accessible-Visual*, *-Mobility*, or *-Cognitive*. Further, we must assume that passwords are not *Resilient-to-Physical-Observation*, since the reverse has not been proven (and preliminary work shows they are indeed vulnerable [42]). Finally, we follow Bonneau et al. and neglect to grant passwords *Resilient-to-Guessing*, since users are historically bad at selecting passwords [16]. As the primary incumbent, passwords provide a low bar for novel authentication mechanisms to improve on. Traditional 4-digit PINs have the same benefits and drawbacks as passwords, but are additionally quasi-*Efficient-to-Use* and quasi-*Infrequent-Errors* since a small PIN pad is easier and faster to use than a full virtual keyboard.

Paired accounts are another common option. In many cases, they require the user to manually enter the username and password of the paired account to authenticate; this type of paired account has the same ranking as passwords, except it is quasi-*Memorywise-Effortless* since the user has to remember only a single secret for any app that uses this paired account. However, we also observed that some paired accounts utilize the account required to use the device, and thus are *automatically logged in* upon opening an app. This type of paired account is much more usable because the user does not have to perform any extra action when opening an app. In fact, automatic paired accounts gain nearly *all* usability properties, with the exception of *Memorywise-Effortless* and *Accessible-Cognitive* since the user must still remember the one secret for the paired account. For security, the lack of interaction means this method is *Resilient-to-Physical-Observation*. Automatic paired accounts are also quasi-*Resilient-to-Guessing*; the attacker would need to guess the credentials to unlock the device in the first place, which could be a password (not resilient), iris (resilient), or another method. Automatic paired accounts are thus a very promising option for authentication on AR and VR devices.

Token-based methods. The two token-based methods we saw are short code and QR code. For short code authentication, the user first goes to an app or logs into an account on a secondary device. Then, the headset displays a one-time code that the user enters on the secondary device. Short code is fully deployable and in general more usable than the knowledge-based methods because typing on a smartphone or laptop is quick and discreet in comparison to typing on AR and VR. Thus, short code is not *Physically-Effortless* or *Accessible-Visual*, *-Mobility*, or *-Cognitive*, but it is quasi-*Efficient-to-Use* and *Acceptable-in-Public*. Short code is also only quasi-*Memorywise-Effortless* since sometimes it requires the user to know the credentials for a paired account. For

Category	Name	Subtype	Threat Model	Deployability				Usability				Accessibility				Security							
				OS-Supported	Platform-Agnostic	Mature	Low-Power-Consumption	Efficient-to-Use	Physically-Effortless	Memorywise-Effortless	Easy-to-Learn	Nothing-to-Carry	Inrequent-Errors	Acceptable-in-Public	Accessible-Visual	Accessible-Hearing	Accessible-Speech	Accessible-Mobility	Resilient-to-Cognitive	Resilient-to-Guessing	Protects-User-Privacy	Multi-Factor	
Knowledge-based	password	🔑		●	●	●	●	-	-	-	●	●	-	-	-	●	●	-	-	-	-	●	-
	paired account (manual)	👤		●	●	●	●	-	-	○	●	●	-	-	-	●	●	-	-	-	-	●	-
	paired account (automatic)	👤		●	●	●	●	○	●	○	●	●	○	●	●	●	●	○	○	○	●	●	-
	PIN	...		●	●	●	●	○	-	-	●	●	○	-	-	●	●	-	-	-	-	●	-
	PIN [33]	...	E,U	●	●	●	●	○	-	-	●	●	○	-	-	●	●	-	-	-	-	●	-
	PIN [77]	...	E	●	●	●	●	-	-	-	●	●	†	-	-	●	●	-	-	-	-	●	-
	touch-based PIN [75]	...	E,U	-	●	○	-	-	-	-	●	●	-	○	-	●	●	-	-	-	-	●	-
	voice-based PIN [75]	...	E,U	-	●	○	-	-	○	-	-	-	-	-	-	-	-	○	-	-	-	●	-
	<i>gTalker</i> [49][50]	...	E,I,S,C,U	-	●	○	-	○	○	-	-	●	●	-	-	-	-	○	-	-	-	●	-
	<i>gTapper</i> [49][50]	...	E,I,S,C,U	-	●	○	●	○	-	-	-	●	●	○	-	●	●	-	-	-	-	●	-
	<i>gRotator</i> [49][50]	...	E,I,S,C,U	-	●	○	-	○	-	-	-	●	●	-	-	●	●	-	-	-	-	●	-
	<i>AugAuth</i> [79]	...	E	-	●	○	-	†	-	-	○	-	-	-	-	●	●	-	-	-	-	●	-
	<i>RubikAuth</i> [56][57]	...	E	-	●	-	●	○	○	-	-	●	○	○	-	●	●	○	-	○	●	●	-
	swipe pattern [33]	🖱️	E	●	●	●	●	○	-	-	●	●	○	-	-	●	●	-	-	-	-	●	-
	swipe pattern [63]	🖱️	E	●	●	●	●	○	-	-	●	●	○	-	-	●	●	-	-	-	-	●	-
	swipe pattern [77]	🖱️	E	●	●	●	●	-	-	-	●	●	†	-	-	●	●	-	-	-	-	●	-
<i>HoloPass</i> [37]	🖱️	E,C,U	-	●	●	●	†	-	-	●	●	†	-	-	●	●	-	-	●	-	●	-	
3D cubes [77]	🖱️	E	-	-	-	●	-	-	-	-	●	†	-	-	●	●	-	-	-	-	●	-	
3D cubes [78]	🖱️	E	-	-	-	●	-	-	-	-	●	†	-	-	●	●	-	-	-	-	●	-	
<i>LookUnlock</i> [30]	🖱️	E	-	-	-	●	-	-	-	-	●	†	-	-	●	●	-	-	-	○	●	-	
<i>RoomLock</i> [32]	🖱️	E	-	-	-	●	-	-	-	-	●	○	-	-	●	●	-	-	-	○	●	-	
<i>3DPass</i> [36]	🖱️	○	-	●	-	●	-	-	-	-	●	†	-	-	●	●	-	-	○	-	●	-	
Physical biometric	iris scan	👁️		●	-	○	●	●	●	●	●	●	●	○	●	●	●	●	●	●	○	-	
	iris & periocular [17]*	👁️	○	-	-	-	-	†	●	●	●	●	-	●	○	●	●	●	●	-	●	-	-
	periocular [41]	👁️	○	-	-	-	-	†	●	●	●	●	-	●	○	●	●	●	●	-	●	-	-
	visual stimulus [80]*	👁️	U	-	-	-	●	-	●	●	●	●	-	●	-	●	●	●	●	-	●	-	-
	<i>Brain Password</i> [52]	😊	○	-	-	-	-	-	●	●	●	-	○	-	-	●	●	●	●	○	●	○	-
	<i>SkullConduct</i> [70]	👂	○	-	-	-	-	●	●	●	●	○	○	●	●	●	●	●	●	○	●	-	-
	<i>EarEcho</i> [31]*	👂	○	-	○	-	-	●	●	●	●	○	○	●	●	●	●	●	●	○	●	-	-
	<i>ElectricAuth</i> [21]	⚡	E,U,S,I	-	-	-	-	○	●	●	●	-	●	-	●	●	●	●	●	○	●	-	-
Behavioral biometric	<i>Oculock</i> [54]	👁️	E,U	-	-	-	-	-	●	●	●	●	○	●	-	●	●	●	●	○	●	-	-
	virtual scene [61]	😊	U	-	-	-	-	○	●	●	○	●	-	●	-	●	●	●	●	-	●	-	-
	<i>Headbanger</i> [47]	😊	E,U	-	-	-	-	-	-	●	●	○	-	●	-	●	○	●	○	-	-	-	
	<i>GaitLock</i> [71]	👉	E,U	-	○	-	●	○	-	●	●	●	○	○	●	●	●	○	●	●	○	-	-
	Glass interactions [20]*	👉	○	-	-	-	●	○	○	○	●	●	○	○	-	●	●	○	●	-	-	-	-
	<i>GlassGuard</i> [65]*	👉👂	○	-	-	-	-	†	○	●	●	●	●	●	-	-	-	○	●	●	-	-	●
	throw trajectory [12][58]*	👉😊	○	-	-	-	-	-	-	●	○	●	○	-	-	●	●	-	●	○	-	-	●
	throw trajectory [59]	👉😊	○	-	-	-	-	○	-	●	○	●	○	-	-	●	●	-	●	○	-	-	●
	throw trajectory [44]	👉	○	-	-	-	-	○	-	●	○	●	○	-	-	●	●	-	●	○	-	-	-
	pointing [67]*	👉👁️😊	○	-	-	-	-	●	-	●	○	●	-	-	-	●	●	-	-	-	-	-	●
	grabbing [67]*	👉👁️😊	○	-	-	-	-	●	-	●	○	●	-	-	-	●	●	-	-	-	-	-	●
	walking [67]*	👉👁️😊	○	-	-	-	-	-	-	●	○	●	-	○	-	●	●	-	●	-	-	-	●
typing [67]*	👉👁️😊	○	-	-	-	-	-	-	●	○	●	-	-	-	●	●	-	-	-	-	-	●	
<i>BioMove</i> [62]*	👉👁️😊	○	-	-	-	-	-	-	●	○	●	-	-	-	●	●	-	-	●	○	-	●	
Token-based	short code	...		●	●	●	●	○	-	○	●	-	●	●	-	●	●	-	-	●	●	●	-
	QR code	📄		●	●	●	●	○	○	○	○	-	●	●	-	●	●	○	○	●	●	○	-
	<i>Glass OTP</i> [19]	📄	E,I,S,C,U	-	●	○	-	†	○	●	●	-	†	●	-	●	●	○	○	●	●	●	-
Multi-factor	<i>GlassGesture</i> [76]	?😊	E	-	○	-	-	†	-	●	●	●	-	-	●	●	-	-	●	●	○	●	
	<i>RubikBiom</i> [55]	...👉	○	-	○	-	-	○	-	-	-	●	●	-	●	●	-	-	●	●	○	●	
	<i>BlinkKey</i> [81]	...👁️	E,U,S	-	-	-	-	-	○	-	○	●	○	●	○	●	●	○	-	●	●	-	●

Names: If a name is in italics, that is the title of the mechanism as provided by the paper. Otherwise, it is a description of the method. * indicates the method is continuous.
 Threat Models: E = external observer, I = internal observer, S = credential stuffing, C = computation-bound adversary, U = UI-bound adversary, ○ = none.
 Subtypes: 📄 = password, 👤 = paired account, ... = PIN, 🖱️ = visual password, ? = security questions, 👉 = hand biometrics, 👁️ = eye biometrics, 👂 = voice biometrics, 😊 = gait/head biometrics, ⚡ = muscle stimulation, 👂 = ear biometrics; 📄 = QR code.
 Evaluation: ● = method fulfills criterion; ○ = method quasi-fulfills criterion; - = method does not fulfill criterion; † = not enough information.

Fig. 4. Systematization of authentication mechanisms from app analysis and collected papers. A gray row denotes an incumbent method used in current AR/VR apps. The Threat Model column is not applicable to incumbent methods.

security, since the code changes every time, it is *Resilient-to-Guessing* and *Resilient-to-Physical-Observation*. To conclude, short code provides some usability and security benefits over most knowledge-based methods—but with the important caveat that it is not *Nothing-to-Carry*.

Similar to short code, the QR code method expects the user to generate a QR code on some other device. Then, the user scans the QR code with the headset to authenticate. QR code is comparable to short code in our evaluation except for a few minor differences. To use a QR code, the user simply has to look at the QR code, rather than entering a short code on the other device; thus, QR code is quasi-*Physically-Effortless*, quasi-*Accessible-Mobility*, and quasi-*Accessible-Cognitive*. As before, we stress that QR code is not *Nothing-to-Carry*.

Physical biometrics (iris scan). Iris scan is only used for device authentication on HoloLens 2, but it is important to consider as the only biometric in our analysis. Unlike the other incumbent methods, iris scan is only quasi-*Mature*, since it is used in practice but not to a large extent. It is also not *Platform-Agnostic* though could theoretically become so in the future since most devices have user-facing cameras.

On the other hand, iris outshines the other methods in usability. Since the user does not have to do or remember anything, it gains *every* usability benefit and nearly all accessibility benefits (it is only quasi-*Accessible-Visual* since some users with visual impairments cannot open their eyes). Iris scan even does well in the security category, being both *Resilient-to-Guessing* (since Microsoft sets very strict requirements on the accuracy of its biometrics [10]) and *Resilient-to-Physical-Observation*. Importantly, iris scan only quasi-*Protects-User-Privacy*, since it uses biometric information locally on the device—this privacy/usability tradeoff is a point of contention not likely to be solved in the near future.

VI. EVALUATING PROPOSED AR/VR AUTHENTICATION MECHANISMS

Using these incumbent methods as ground truth, we now systematize recent research efforts in AR and VR authentication. First, we identify prior work which proposes new AR or VR authentication mechanisms. Then, we evaluate these newly-proposed authentication mechanisms using the properties from Section IV.

A. Identifying Prior Work

We collected papers which present new authentication methods for AR or VR. We queried Google Scholar on March 3, 2021 using the Scholarly Python library [6], running two queries for each of the 102 top venues we focused on. First, we searched for papers in that venue containing at least one of a set of authentication keywords. Then, we searched within the same venue with a set of keywords related to AR/VR. Appendix C gives more details about the venues and keywords we used. We only kept papers in the intersection of these two searches and published in or after 2010. This yielded 521 potential papers. Of these papers, we were only interested in those which presented *a new authentication mechanism specifically for AR or VR*. Surprisingly, only fourteen papers

fit this criterion. To ensure we captured all relevant papers, we then crawled the citations of each of the fourteen papers. If any citation was published in 2010 or later and presented a new authentication mechanism specifically for AR or VR, we included it in our list. After this second round of paper collection, we had our final list of thirty-eight papers which present forty-three unique authentication mechanisms in total.

B. Evaluating Proposed Methods

We evaluated the forty-three authentication mechanisms proposed in prior work. Two authors each evaluated half of the methods. Then, all authors participated in multiple rounds of discussion to ensure the evaluation was correct according to our definitions of each property (Appendix C).

For each mechanism, we relied on the information given in the associated paper. Most prior work does not report results for all evaluation properties; thus, in many cases, we used our best judgment when evaluating the mechanism. For some properties, we assumed a default value unless the paper proves otherwise. In particular, we assumed any method that requires signal processing does not have *Low-Power-Consumption*, and any method with visible actions is not *Resilient-to-Physical-Observation*. For *Efficient-to-Use* and *Infrequent-Errors*, we could not make any judgment in the absence of reported results. In Fig. 4, † indicates this absence of information.

C. Evaluation Results

We evaluate a variety of proposed authentication methods for AR and VR. Fig. 4 summarizes our results.

Knowledge-based methods. We evaluated 18 knowledge-based methods including PINs, obfuscated PINs, and visual/graphical passwords. Since automatic paired accounts are an outlier in this category, we compare proposed methods to the other incumbents: password, manual paired account, and PIN. Neither these incumbents nor the proposed methods appear to be the best choice for AR and VR devices.

Deployability. First, the proposed knowledge-based methods do well in deployability. Some methods—those that essentially re-implement incumbents [33], [77], [63]—achieve all deployment benefits, including *OS-Support*. Except for some 3D passwords which do not map to a traditional PIN [77], [78], [32], [30], all proposed knowledge-based methods are *Platform-Agnostic*. This is crucial to allowing developers to quickly adapt an existing app to an AR or VR context. Further, most of these methods are *Low-Power-Consumption* with the exception of methods that require speech [50], [49], [75], head movement [50], [49], or input from an external armband [79]. Finally, many proposed knowledge-based methods adapt existing methods (e.g., a classic PIN) to better suit AR/VR and are thus *Mature* or quasi-*Mature*. These deployability benefits make knowledge-based methods appealing to developers.

Usability. The cumbersome nature of entering a secret on AR/VR affects the usability of proposed methods. However, they occasionally do better than the incumbents. Some are quasi-*Efficient-to-Use*, taking three or fewer seconds to authenticate (e.g., [49], [50]); the rest take more than three

seconds to authenticate or do not report latency. Better, Li et al.'s three methods [50], [49] and George et al.'s PIN [33] have *Infrequent-Errors* with around 98% entry accuracy. Three methods [57], [56], [20], [65] are also quasi-*Acceptable-in-Public*, requiring only discreet touch gestures or gaze selection to enter the secret. Beyond that, proposed methods do not fare much better than the incumbents. For one property, they do worse: most proposed methods are not *Easy-to-Learn* since they complicate existing methods or are entirely unfamiliar.

Spoken PINs. Two methods [50], [49], [75], attempting to bypass the usability constraints of AR/VR interactions, allow a user to enter their PIN by speaking obfuscated digits. These methods do gain the benefits of being quasi-*Physically-Effortless* and quasi-*Accessible-Mobility* since no physical action is required besides speech. However, this comes at the cost of no longer being *Accessible-Hearing* or *-Speech*, and they do not gain the benefit of being *Accessible-Visual* since the user must still read the mapping of obfuscated digits. Additionally, these methods are no longer *Low-Power-Consumption*. Though speech-based methods avoid some pitfalls of other knowledge-based methods, they do not fare much better overall.

Shoulder surfing resilience. One key improvement these proposed methods offer over incumbent passwords is that obfuscated PIN methods [75], [50], [49], [79] are *Resilient-to-Physical-Observation*. Relatively simple changes like randomizing the layout of digits on the PIN pad can add this important security benefit while retaining existing benefits. RubikAuth [57], [56], a method that uses a Rubik's Cube-style PIN, is also proven to be *Resilient-to-Physical-Observation*, resisting 98.5% of attacks in a user study. In addition, some proposed methods are more *Resilient-to-Guessing* than incumbents due to larger password spaces; e.g., HoloPass boasts that user-chosen passwords require 306 billion guesses to crack. In accordance with these improvements, most methods consider an external observer in their threat model, and many consider UI-bound adversaries who attempt to guess the secret.

Summary. Besides automatic paired accounts, incumbent and proposed knowledge-based methods are on fairly equal (and unsatisfactory) footing. Promisingly, other methods offer benefits where knowledge-based methods cannot.

Physical biometrics. Improving upon many of the drawbacks of knowledge-based methods, physical biometrics achieve far better usability and accessibility across the board. However, this comes at the cost of deployability. In our evaluation, the seven proposed physical biometrics come close to the success of the incumbent, primarily suffering in terms of accuracy.

Deployability. No physical biometric, including iris scan, has perfect deployability. Zhang et al.'s method [80] is the only proposed physical biometric proven to be *Low-Power-Consumption* (a key metric, since all of the physical biometric methods require some form of signal processing). On the other hand, EarEcho [31], which measures the shape of the ear using sound through an earbud, is the only quasi-*Platform-Agnostic* physical biometric; its required earbud could feasibly be connected to any device. Though physical biometrics offer

usability upgrades from knowledge-based methods, this lack of deployment benefits may prevent widespread adoption.

Drawbacks. Compared to the incumbent, the key weaknesses of proposed physical biometrics are authentication time and accuracy. Only three proposed methods are *Efficient-to-Use*, taking less than a second to authenticate: Zhang et al.'s method [80], which measures a user's eye movement in response to visual stimuli, along with SkullConduct [70] and EarEcho [31], which measure the shape of the skull and ear, respectively. Since the incumbent is nearly instantaneous, extra seconds matter. Further, for biometric methods, accuracy impacts not only usability but also security. The accuracy of these proposed methods is not perfect, and as a result, many methods do not have *Infrequent-Errors* and are not *Resilient-to-Guessing*. Only ElectricAuth [21] gets full marks in these two categories. (Notably, ElectricAuth is also not *Nothing-to-Carry* or *Acceptable-in-Public* since it requires an arm-connected electronic muscle stimulation (EMS) device.)

Summary. Physical biometrics offer strong usability and accessibility guarantees. However, they lack certain deployability benefits, and they come at the cost of protecting user privacy. In theory, physical biometrics can be cancelable and quasi-*Protect-User-Privacy*—Brain Password, for example, is presented as a cancelable biometric since the visual stimuli can be changed [48]. However, these tradeoffs may still impede physical biometrics from being used in practice.

Behavioral biometrics. Several papers explore the feasibility of various behavioral biometrics for one-time and continuous authentication. Though their novelty is exciting, they generally achieve fewer benefits than physical biometrics.

Required movements. The primary difference between physical and behavioral biometrics is that, aside from two zero-effort methods based on eye and head movement [54], [61], most behavioral biometrics require active movement from the user. Two methods [20], [65] require only discreet actions to interact with Google Glass and are thus quasi-*Physically-Effortless* and *Acceptable-in-Public*. Others require large, but common actions, like walking [71], [67]; these methods are not *Physically-Effortless*, but are quasi-*Acceptable-in-Public* (they would be acceptable when the user is already walking, but not in other situations, e.g., a crowded bus). The remaining few methods require explicit actions that are not *Physically-Effortless* or *Acceptable-in-Public*, like throwing a virtual ball [12], [58], [59], [44]. Because of these explicit actions, behavioral biometrics have fewer accessibility benefits (most are not *Accessible-Visual* or *Accessible-Mobility*), and crucially, most lose the primary security benefit of physical biometrics: *Resilience-to-Physical-Observation*.

Multi-factor methods. While the physical biometrics are all single-factor, several proposed behavioral biometrics are *Multi-Factor*. GlassGuard [65] measures touch and voice behavior with Google Glass; others [12], [58], [59] measure head and hand movements while throwing a ball; and five methods [67], [62] combine head, eye, and hand movements during various activities. In theory, including multiple factors

could substantially improve behavioral biometrics’ resilience to shoulder surfing and guessing attacks. However, as with the proposed physical biometrics, these methods do not yet have the accuracy to be *Resilient-to-Guessing*, and most are not proven to be shoulder-surfing resistant.

Threat models. Most papers proposing biometrics do not consider an explicit threat model. This is likely because the focus for most proposed biometrics is making them feasible for authentication in the first place, rather than defending against an attacker. The behavioral biometric papers that do consider a threat model mainly consider imitation attacks on the visible actions required to authenticate.

Physical biometrics vs behavioral biometrics. Biometric methods perform best in usability and accessibility while doing poorly in deployability. Though behavioral biometrics are exciting and new—and are some of the only methods to be *Multi-Factor*—they lose points because they usually require explicit actions: they are less *Accessible* (particularly for mobility and vision), less *Physically-Effortless*, and less *Acceptable-in-Public* than their physical counterparts. Physical biometrics may therefore be a more promising option for AR/VR authentication in the long run.

Token-based methods appear only once in literature but achieve good marks in every category. The only proposed token-based method is Glass OTP [19], where the user scans a QR code on a companion Android app to unlock their Google Glass. Chan et al. evaluate Glass OTP on Bonneau et al.’s framework [16] (and therefore consider a robust threat model). By following our definitions carefully, our evaluation is slightly different than that reported in their paper.

Evaluating Glass OTP. Like the incumbent QR code and short code, Glass OTP does fairly well in all four categories of our evaluation. It has worse deployability: it does not have *OS-Support* and is not proven to be *Low-Power-Consumption*. Chan et al. assert that Glass OTP is not *Mature* since it is the first OTP method for Google Glass; we evaluate it as quasi-*Mature* because it adapts a mature mechanism (QR code). For usability, the authors report that Glass OTP has *Infrequent-Errors* but is not *Efficient-to-Use*. Since they did not perform a user study, we abstain from ranking Glass OTP on these two benefits. Glass OTP is also *Memorywise-Effortless* where the incumbents are not since it generates the QR code using a companion app. In all, token-based methods provide similar deployability to knowledge-based methods while offering improved usability, accessibility, and security.

Requirement of a secondary device. Though token-based methods do well in our evaluation, they have an important caveat: they are not *Nothing-to-Carry*. As long as AR and VR are used only in a select few environments, and generally in tandem with other devices, this is perfectly acceptable. However, as soon as these devices are standalone, the requirement of a secondary device will become a sizeable hurdle. Thus, we encourage designers to consider other methods that may be more compatible with the long-term direction of AR/VR.

Multi-factor methods are an intriguing solution. They in-

herit the deployment problems of biometrics and the usability/accessibility problems of knowledge-based methods, but they also achieve some of the highest security benefits in our evaluation. Multi-factor methods could be a practical way to add security to authentication on AR and VR.

Characterizing multi-factor methods. There are three multi-factor methods in our evaluation, all of which combine a knowledge-based method with a biometric. In GlassGesture [76], the user nods or shakes their head in response to displayed security questions, and their head movement biometrics are collected for multi-factor authentication. Mathis et al. present RubikBiom [55], [56], [57], which adds controller biometrics on top of a Rubik’s Cube-style PIN mechanism. Finally, Zhu et al.’s BlinKey [81] has a user blink in a remembered pattern (a quasi-PIN) and measures the physiological features of their blinks. Theoretically, GlassGesture and RubikBiom could be *Platform-Agnostic*—if the biometric layer is ignored on other platforms (as Mathis et al. propose), the knowledge-based layer could be used to authenticate the user anywhere. Notably, this would result in much lower security: GlassGesture would be reduced to “yes” or “no” security questions, and RubikBiom would map to a classic PIN. Even so, few other methods offer this important benefit.

Improved security. Since the extra biometric component is not obvious to the user, the usability and accessibility of multi-factor methods are no worse than that of knowledge-based methods. In stark contrast to knowledge-based methods, though, multi-factor methods do best in security. Requiring the user to enter a correct secret on top of passing a biometric layer means that multi-factor methods are both *Resilient-to-Guessing* and *Resilient-to-Physical-Observation*. They even quasi-*Protect-User-Privacy* in cases where the biometric component could be ignored on other platforms. No other type of authentication performs as well in security.

Summary. As previously discussed, the primary benefit of incumbent methods such as password and PIN is that they are *Platform-Agnostic*. Multi-factor methods could provide better security for these methods on AR and VR while remaining somewhat *Platform-Agnostic*. It is worth exploring ways to implement these methods in real systems so that we can achieve stronger security on AR and VR (including protection from shoulder surfing) without sacrificing deployability.

VII. DISCUSSION & OPEN CHALLENGES

We provide a three-way review of authentication on AR/VR devices from the viewpoint of users, developers, and researchers. Researchers are looking into developing new mechanisms, but this is not reflected in the deployed apps. Though users feel the pain of using traditional authentication methods and newly proposed methods can provide better usability and accessibility, most developers are still using passwords and PINs. Here, we highlight key findings, present open problems, and call for solutions that are practical, usable, and secure.

Improving the availability of usable authentication mechanisms. Our evaluation highlights the wide variety of authentication mechanisms proposed for AR and VR. Many new

methods offer usability and accessibility improvements over incumbent methods; however, most lack deployability. Though our study indicates that AR/VR developers are willing to tailor authentication methods to provide a better user experience, there is not enough support or incentive for them to choose these more usable options. We challenge creators of AR/VR authentication methods to think critically about how to put these new methods in the hands of developers.

Expectation of a companion device. Several apps use authentication methods that necessitate a companion device. For example, HTC Vive apps that use a Viveport paired account leverage the fact that the headset is tethered to a PC to provide automatic authentication. Here, the requirement of a companion device is trivial since the headset is designed to be connected to the PC at all times. However, we also see this requirement in apps on the HoloLens 2, an untethered device. The frequent use of these authentication methods indicates that AR devices may be perceived as a companion device to a computer or phone, rather than as a standalone device. To our knowledge, authentication is the only part of the apps requiring a companion device; with an alternative authentication mechanism, these apps would not require a companion device and could thus be used as a standalone personal device as the community envisions.

Need for comprehensive evaluation. As indicated by the number of † symbols in Fig. 4, many of the papers we looked at do not comprehensively test the methods they propose. In particular, several papers neglect to evaluate whether their methods are *Efficient-to-Use*, *Infrequent-Errors*, *Low-Power-Consumption* or *Resilient-to-Physical-Observation*, despite the importance of these considerations. We call on future AR/VR authentication designers to pay careful attention to our evaluation criteria when designing and evaluating new mechanisms.

Using biometrics safely. AR and VR, with their myriad built-in sensors, are poised to implement behavioral and physical biometrics. This is promising: biometrics tend to be more usable than other methods and have the potential to augment existing mechanisms or allow for continuous authentication. However, developers must be wary of the consequences of using biometric authentication on AR/VR.

Multi-use sensors. Biometric authentication should by default be handled by the platform and not individual apps. However, in AR/VR, this alone cannot protect biometric data from compromise because the same sensors used for authentication may also be used in an app. If malicious, these apps could easily collect the exact biometric information required for authentication just by using the available sensors.

Privacy implications. The use of biometrics requires private user data such as iris and fingerprint images. (In our evaluation, no biometric fully *Protects-User-Privacy*.) Thus, any biometric should be used only with the consent of users, and secure storage of this private data is critical. This is particularly important because biometrics are a “who-you-are” type authentication and cannot easily be replaced if compromised. If biometrics

are to be used in AR/VR, we must carefully understand the privacy implications of that decision and clearly communicate to users how their data is being used.

Unifying the authentication stack via federated login.

In Section V, we noted that several HTC Vive apps offer automatic authentication via a Viveport account. Four HoloLens 2 apps also offer authentication via a Microsoft account; however, for three of these apps, the user must fully log in to their Microsoft account again (using a username and password) despite having logged in to use the device in the first place. This is a missed opportunity. If HoloLens apps leveraged the Microsoft account already logged in on the device, they could gain the substantial usability benefits of automatic paired account authentication. Future work should explore the security/usability concerns of this approach and how to make federated login available to app developers.

Privacy concerns. Though unifying the authentication stack could improve usability, we caution that it could also have privacy implications. Consider Oculus devices, which users unlock using their Facebook account. If Oculus *required* the user to log in to apps with their Facebook account, then Facebook would know about all of the different kinds of accounts the user has on their Oculus device. Future work will need to consider the balance between effortless authentication and user consent when weighing this option for AR and VR.

Support for password managers. Password managers can greatly reduce the user’s burden to memorize and enter passwords. Unfortunately, in AR and VR, “There is no password management on the device (like LastPass) and worse, you cannot copy/paste a password from the LastPass vault” (P048: M,45-54). Without a password manager, users must use the virtual keyboard to manually input the password and thus are subject to the usability and security issues of the virtual keyboard. If password managers were available and functional on AR/VR, it could potentially mitigate complaints with passwords on AR/VR; however, password managers are historically hard to design properly for new platforms [51], [13]. Designing password managers for AR/VR is intriguing, but requires careful consideration.

Limitations. In Section III, we did not verify whether our survey participants have indeed used or developed on AR/VR devices; however, we carefully scrutinized the results for consistency and removed entries with clear evidence of a lack of experience on these platforms. Our survey results are also biased towards male respondents, which may affect the validity of our results. Additionally, in Section V, we only consider apps on the HoloLens 2 and HTC Vive, and thus cannot make inferences about other AR or VR devices from our app review. Finally, our literature survey Section VI considers papers from only top publication venues and references from those papers, meaning we could have missed some relevant prior work.

ACKNOWLEDGMENTS

We are grateful to the anonymous reviewers for their insightful comments. This work was partially supported by

the University of Wisconsin—Madison Office of the Vice Chancellor for Research and Graduate Education with funding from the Wisconsin Alumni Research Foundation, NSF Award CNS-2144376 and a gift from Facebook.

REFERENCES

- [1] CSRankings: Computer science rankings. <https://csrankings.org/>.
- [2] Engage. <https://www.viveport.com/1edbc9a7-1c11-4a5a-af97-8a486df647fd>.
- [3] Hololens 2 hardware. <https://docs.microsoft.com/en-us/hololens/hololens2-hardware>.
- [4] Microsoft hololens 2. <https://www.microsoft.com/en-us/hololens>.
- [5] Oculus quest 2. <https://www.oculus.com/quest-2/>.
- [6] Scholarly documentation. <https://scholarly.readthedocs.io>.
- [7] SteamVR on Steam. <https://store.steampowered.com/app/250820/SteamVR/>.
- [8] VIVE Tracker (3.0). <https://www.vive.com/us/accessory/tracker3/>.
- [9] Viveport — VR games, apps, & videos. <https://www.viveport.com/>.
- [10] Windows hello biometrics in the enterprise. <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise>, September 2021.
- [11] Set up your apple watch. <https://support.apple.com/en-us/HT204505,2022>.
- [12] AJIT, A., BANERJEE, N., AND BANERJEE, S. Combining pairwise feature matches from device trajectories for biometric authentication in virtual reality environments. In *Proceedings - 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality, AIVR 2019* (2019), pp. 9–16.
- [13] AONZO, S., MERLO, A., TAVELLA, G., AND FRATANTONIO, Y. Phishing attacks on modern android. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (2018), pp. 1788–1801.
- [14] AZUMA, R., BAILLOT, Y., BEHRINGER, R., FEINER, S., JULIER, S., AND MACINTYRE, B. Recent advances in augmented reality. *IEEE computer graphics and applications* 21, 6 (2001), 34–47.
- [15] BARTHEL, M., STOCKING, G., HOLCOMB, J., AND MITCHELL, A. Reddit news users more likely to be male, young and digital in their news preferences. Pew Research Center.
- [16] BONNEAU, J., HERLEY, C., VAN OORSCHOT, P. C., AND STAJANO, F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE Symposium on Security and Privacy 2012* (2012), IEEE.
- [17] BOUTROS, F., DAMER, N., RAJA, K., RAMACHANDRA, R., KIRCHBUCHNER, F., AND KUIJPER, A. Iris and periocular biometrics for head mounted displays: Segmentation, recognition, and synthetic data generation. *Image and Vision Computing* 104 (2020).
- [18] BOYATZIS, R. E. *Transforming qualitative information: Thematic analysis and code development*. sage, 1998.
- [19] CHAN, P., HALEVI, T., AND MEMON, N. Glass otp: Secure and convenient user authentication on google glass. In *International Conference on Financial Cryptography and Data Security* (2015), Springer, pp. 298–308.
- [20] CHAUHAN, J., ASGHAR, H. J., KAAFAR, M. A., AND MAHANTI, A. Gesture-based continuous authentication for wearable devices: the google glass case. *arXiv preprint arXiv:1412.2855* (2014).
- [21] CHEN, Y., YANG, Z., ABBOU, R., LOPES, P., ZHAO, B. Y., AND ZHENG, H. User authentication via electrical muscle stimulation.
- [22] CLEMENT, J. COVID-19: Impact on time spent using vr in the U.S. in 2020. <https://www.statista.com/statistics/1178715/coronavirus-impact-vr-usage/>.
- [23] CLEMENT, J. Distribution of computer and video gamers in the united states from 2006 to 2020, by gender. *Statista* (2021).
- [24] CLEMENT, J. Virtual reality (vr) and augmented reality (ar) device ownership and purchase intent among consumers in the united states as of 1st quarter 2017, by gender. *Statista* (2021).
- [25] DE GUZMAN, J. A., THILAKARATHNA, K., AND SENEVIRATNE, A. Security and privacy approaches in mixed reality: A literature survey. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–37.
- [26] DUBE, T. J., AND ARIEF, A. S. Text entry in virtual reality: A comprehensive review of the literature. In *International Conference on Human-Computer Interaction* (2019), Springer, pp. 419–437.
- [27] FASHIMPAUR, J., KIN, K., AND LONGEST, M. Pinchtype: Text entry for virtual and augmented reality using comfortable thumb to fingertip pinches. *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (2020).
- [28] FELT, A. P., FINIFTER, M., CHIN, E., HANNA, S., AND WAGNER, D. A survey of mobile malware in the wild. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (New York, NY, USA, 2011), SPSM '11, Association for Computing Machinery, p. 3–14.
- [29] FREED, D., PALMER, J., MINCHALA, D., LEVY, K., RISTENPART, T., AND DELL, N. “a stalker’s paradise” How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–13.
- [30] FUNK, M., MARKY, K., MIZUTANI, I., KRITZLER, M., MAYER, S., AND MICHAELLES, F. Lookunlock: Using spatial-targets for user-authentication on hmds. In *CHI'19 Extended Abstracts, May 4-9, 2019, Glasgow, Scotland UK* (2019), ACM.
- [31] GAO, Y., WANG, W., PHOHA, V. V., SUN, W., AND JIN, Z. Earecho: Using ear canal echo for wearable authentication. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 3 (2019), 1–24.
- [32] GEORGE, C., KHAMIS, M., BUSCHEK, D., AND HUSSMANN, H. Investigating the third dimension for authentication in immersive virtual reality and in the real world. *26th IEEE Conference on Virtual Reality and 3D User Interfaces, VR 2019 - Proceedings* (2019), 277–285.
- [33] GEORGE, C., KHAMIS, M., VON ZECHWITZ, E., BURGER, M., SCHMIDT, H., ALT, F., AND HUSSMAN, H. Seamless and secure vr: Adapting and evaluating established authentication systems for virtual reality. In *USEC 17, 26 February 2017, San Diego, CA, USA* (2017), Internet Society.
- [34] GROSSMAN, T., CHEN, X. A., AND FITZMAURICE, G. Typing on glasses: Adapting text entry to smart eyewear. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (2015), pp. 144–152.
- [35] GRUBERT, J., OFEK, E., PAHUD, M., AND KRISTENSSON, P. O. The office of the future: Virtual, portable, and global. *IEEE computer graphics and applications* 38, 6 (2018), 125–133.
- [36] GURARY, J., ZHU, Y., AND FU, H. Leveraging 3d benefits for authentication. *International Journal of Communications, Network and System Sciences* 10, 8 (2017), 324–338.
- [37] HADJIDEMETRIOU, G., BELK, M., FIDAS, C., AND PITSILLIDES, A. Picture passwords in mixed reality: Implementation and evaluation. In *CHI EA '19: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (2019), pp. 1–6.
- [38] HSIEH, Y.-T., JYLHÄ, A., ORSO, V., GAMBERINI, L., AND JACUCCI, G. Designing a willing-to-use-in-public hand gestural interaction technique for smart glasses. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 4203–4215.
- [39] KALIGE, E., BURKEY, D., AND DIRECTOR, I. A case study of eurograbber: How 36 million euros was stolen via malware. *Versafe (White paper)* 35 (2012).
- [40] KAMIŃSKA, D., SAPIŃSKI, T., WIAK, S., TIKK, T., HAAMER, R. E., AVOTS, E., HELMI, A., OZCINAR, C., AND ANBARJAFARI, G. Virtual reality and its applications in education: Survey. *Information* 10, 10 (2019).
- [41] KIM, S., AND LEE, E. Periocular biometric authentication methods in head mounted display device.
- [42] KREIDER, C. The discoverability of password entry using virtual keyboards in an augmented reality wearable: An initial proof of concept. In *SAIS 2018 Proceedings* (2018), vol. 23.
- [43] KUNDA, D., AND CHISHIMBA, M. A survey of android mobile phone authentication schemes. *Mobile Networks and Applications* (2018), 1–9.
- [44] KUPIN, A., MOELLER, B., JIANG, Y., BANERJEE, N. K., AND CHAP. *Task-Driven Biometric Authentication of Users in Virtual Reality (VR) Environments*. Springer International Publishing, 2018.
- [45] LESWING, K. The tech industry is looking to replace the smartphone — and everybody is waiting to see what Apple comes up with. *CNBC* (February 2021).
- [46] LEVY, S. AR is where the real metaverse is going to happen. *Wired* (November 2021).
- [47] LI, S., ASHOK, A., ZHANG, Y., XU, C., LINDQVIST, J., AND GRUTESER, M. Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns. In *IEEE International Conference on Pervasive Computing and Communications (PerCom)* (2016), IEEE.
- [48] LI, S., SAVALIYA, S., MARINO, L., LEIDER, A., AND TAPPERT, C. Brain signal authentication for human-computer interaction in virtual reality.

- Proceedings - 22nd IEEE International Conference on Computational Science and Engineering and 17th IEEE International Conference on Embedded and Ubiquitous Computing, CSE/EUC 2019* (2019), 115–120.
- [49] LI, Y., CHENG, Y., LI, Y., AND DENG, R. H. What you see is not what you get: Leakage-resilient password entry schemes for smart glasses. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (2017), pp. 327–333.
- [50] LI, Y., CHENG, Y., MENG, W., LI, Y., AND DENG, R. H. Designing leakage-resilient password entry on head-mounted smart wearable glass devices. Institutional Knowledge at Singapore Management University.
- [51] LI, Z., HE, W., AKHAWA, D., AND SONG, D. The emperor’s new password manager: Security analysis of web-based password managers. In *23rd USENIX Security Symposium (USENIX Security 14)* (San Diego, CA, Aug. 2014), USENIX Association, pp. 465–479.
- [52] LIN, F., CHO, K. W., SONG, C., XU, W., AND JIN, Z. Brain password: A secure and truly cancelable brain biometrics for smart headwear. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services* (2018), pp. 296–309.
- [53] LIU, S., SHAO, W., LI, T., XU, W., AND SONG, L. Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing* (2021), 103120.
- [54] LUO, S., NGUYEN, A., SONG, C., LIN, F., XU, W., AND YAN, Z. Oculock: Exploring human visual system for authentication in virtual reality head-mounted display.
- [55] MATHIS, F., FAWAZ, H., AND KHAMIS, M. Knowledge-driven biometric authentication in virtual reality. *Conference on Human Factors in Computing Systems - Proceedings* (2020).
- [56] MATHIS, F., WILLIAMSON, J., AND VANIEA, K. Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing.
- [57] MATHIS, F., WILLIAMSON, J., VANIEA, K., AND KHAMIS, M. Rubikauth: Fast and secure authentication in virtual reality. *Conference on Human Factors in Computing Systems - Proceedings* (2020).
- [58] MILLER, R., AJIT, A., BANERJEE, N. K., AND BANERJEE, S. Realtime behavior-based continual authentication of users in virtual reality environments. *Proceedings - 2019 IEEE International Conference on Artificial Intelligence and Virtual Reality, AIVR 2019* (2019), 253–254.
- [59] MILLER, R., BANERJEE, N. K., AND BANERJEE, S. 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)* (2020), pp. 311–316.
- [60] MUSSER, C. V. Smartphones are on their way out, and augmented reality is coming to replace them.
- [61] MUSTAFA, T., MATOVU, R., SERWADDA, A., AND MUIRHEAD, N. Unsure how to authenticate on your vr headset? come on, use your head! In *IWSPA’18, March 19–21, 2018, Tempe, AZ, USA* (2018), ACM.
- [62] OLADE, I., FLEMING, C., AND LIANG, H.-N. Biomove: Biometric user identification from human kinesiological movements for virtual reality systems. *Sensors* 20, 10 (2020), 2944.
- [63] OLADE, I., LIANG, H.-N., AND FLEMING, C. Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr). ACM.
- [64] PARKIN, S. How vr is training the perfect soldier. *Wearable* (2015).
- [65] PENG, G., ZHOU, G., NGUYEN, D. T., QI, X., YANG, Q., AND WANG, S. Continuous authentication with touch behavioral biometrics and voice on wearable glasses. vol. 47, IEEE, pp. 404–416.
- [66] PENSIERI, C., AND PENNACCHINI, M. *Virtual Reality in Medicine*. Springer International Publishing, Cham, 2016, pp. 353–401.
- [67] PFEUFFER, K., GEIGER, M. J., PRANGE, S., MECKE, L., BUSCHEK, D., AND ALT, F. 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* (2019), pp. 1–12.
- [68] RABBI, I., AND ULLAH, S. A survey on augmented reality challenges and tracking. *Acta graphica: znanstveni časopis za tiskarstvo i grafičke komunikacije* 24, 1-2 (2013), 29–46.
- [69] ROESNER, F., KOHNO, T., AND MOLNAR, D. Security and privacy for augmented reality systems. *Communications of the ACM* 57, 4 (2014), 88–96.
- [70] SCHNEEGASS, S., OUALIL, Y., AND BULLING, A. Skullconduct: Biometric user identification on eyewear computers using bone conduction through the skull. In *CHI ’16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 1379–1384.
- [71] SHEN, Y., WEN, H., LUO, C., XU, W., ZHANG, T., HU, W., AND RUS, D. Gaitlock: Protect virtual and augmented reality headsets using gait. vol. 16, pp. 484–497.
- [72] SHRESTHA, P., AND SAXENA, N. An offensive and defensive exposition of wearable computing. *ACM Computing Surveys (CSUR)* 50, 6 (2017), 1–39.
- [73] SPEICHER, M., FEIT, A. M., ZIEGLER, P., AND KRÜGER, A. Selection-based text entry in virtual reality. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–13.
- [74] THULLIER, F., BOUCHARD, B., AND MÉNÉLAS, B.-A. J. Exploring mobile authentication mechanisms from personal identification numbers to biometrics including the future trend. *Protecting Mobile Networks and Devices: Challenges and Solutions; CRC Press: Boca Raton, FL, USA* (2016), 1.
- [75] YADAV, D. K., IONASCU, B., ONGOLE, S. V. K., ROY, A., AND MEMON, N. Design and analysis of shoulder surfing resistant pin based authentication mechanisms on google glass. In *International conference on financial cryptography and data security* (2015), Springer, pp. 281–297.
- [76] YI, S., QIN, Z., NOVAK, E., YIN, Y., AND LI, Q. Glassgesture: Exploring head gesture interface of smart glasses. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications* (2016), IEEE, pp. 1–9.
- [77] YU, Z., LIANG, H., FLEMING, C., AND MAN, K. L. An exploration of usable authentication mechanisms for virtual reality systems. In *2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)* (2016), pp. 458–460.
- [78] YU, Z., OLADE, I., LIANG, H.-N., AND FLEMING, C. Usable authentication mechanisms for mobile devices: An exploration of 3d graphical passwords. In *2016 International Conference on Platform Technology and Service (PlatCon)* (2016), IEEE, pp. 1–3.
- [79] ZHANG, R., ZHANG, N., DU, C., LOU, W., HOU, Y. T., AND KAWAMOTO, Y. Augauth: Shoulder-surfing resistant authentication for augmented reality. In *2017 IEEE International Conference on Communications (ICC)* (2017), IEEE, pp. 1–6.
- [80] ZHANG, Y., HU, W., XU, W., CHOU, C. T., AND HU, J. Continuous authentication using eye movement response of implicit visual stimuli. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1 (2018).
- [81] ZHU, H., JIN, W., XIAO, M., MURALI, S., AND LI, M. Blinkkey: A two-factor user authentication method for virtual reality devices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 4 (2020).

APPENDIX A

CONTENT OF USER SURVEY

The questions used in our survey are listed below. We omit the possible responses for space; the full survey, including the possible responses, can be found in this GitHub repository: <https://git.doit.wisc.edu/srstephenso2/avrsec>.

A. Screening

- 1.1) How old are you? You must be at least 18 years old to participate in this study.
- 1.2) Please select the statement that best describes your familiarity with augmented reality (AR) glasses (e.g., Hololens, MagicLeap, Google Glass, etc.)
- 1.3) Please select the statement that best describes your familiarity with virtual reality (VR) devices (e.g., Oculus, HTC Vive, etc.)
- 1.4) Have you ever developed any applications for AR or VR devices?

B. Developers

- 2.1) Which AR or VR glasses have you developed applications for?
- 2.2) What types of applications have you developed for AR and VR glasses?
- 2.3) Have any of your apps used any form of authentication?
- 2.4) Why didn’t your apps require any authentication?

- 2.5) What form of authentication did you use in your applications?
- 2.6) Please describe the type(s) of authentication in more detail. For example, if it was a password, how did the user enter the password? If it was a biometric, which one was used?
- 2.7) Why did you choose that type of authentication over others?

Sections C and D were shown once for AR and once for VR.

C. Device usage

- 3.1) Select the device you have used the most often.
- 3.2) Do you own this device?
- 3.3) What is the major reason you use this device?

D. Authentication

Authentication is the process of proving your identity via a password, biometric, paired device, or any number of other methods.

- 4.1) Have you ever authenticated on a [AR/VR] device?
- 4.2) On which device(s) did you have to authenticate?
- 4.3) When did you have to authenticate on the device(s)?
- 4.4) What method of authentication did you use on the device(s)?

Questions 4.5-4.8 were repeated for each method used.

- 4.5) How secure do you feel using [method] for authentication on your [AR/VR] devices?
- 4.6) Please explain your reasoning for the above question.
- 4.7) How easy/hard is it to use [method] on [AR/VR] devices?
- 4.8) Please explain your reasoning for the above question.

E. Demographics & Followup

- 1) How do you identify your gender?
- 2) What is your highest education level?
- 3) What is your occupation?
- 4) Can we follow up with you for a short interview (30 minutes)? If so, please provide an email or phone number we can use to contact you.
- 5) If you are NOT accessing this survey through MTurk, please enter your email for a chance to win a \$50 Amazon Gift card. We will use the email for sending the gift card, if you are selected in the random draw. We will not use the email for any other purposes.

APPENDIX B ADDITIONAL DETAILS OF USER STUDY

Fig. 5 presents participant demographic information. Fig. 6 presents details about the popularity of each AR and VR device, as well as the reasons for use reported by users. Fig. 7 shows the number of participants who had experience authenticating with each authentication method.

Demographic item	N	%
Total	139	
Age		
18-24	55	39.6
25-34	33	23.7
35-44	35	25.2
45-54	11	7.9
55-64	3	2.2
More than 65 yrs.	2	1.4
Gender		
Female	8	5.8
Male	127	91.4
Prefer not to disclose	3	2.2
Prefer to self-describe	1	0.7
Highest education level		
High school diploma	21	15.1
Some college	33	23.7
Bachelor's degree	42	30.2
Some graduate school	9	6.5
Graduate or professional degree	34	24.5
Occupation		
Tech	55	39.6
Student	23	16.6
Business & marketing	11	7.9
Science & research	7	5.0
Arts	8	5.8
Manufacturing & Construction	5	3.6
Unemployed, self-employed	6	4.3
Other/no response	24	17.2

Fig. 5. Summary of participant demographics.

Device	Total	Reason for Use				
		Gaming	Productivity	Social	Education	Other
AR						
HoloLens	20	2	15	1	4	3
Google Glass	12	8	4	5	2	2
Magic Leap	5	1	2	0	1	1
Epson Moverio	1	1	0	0	0	0
Project North Star	1	0	0	0	0	1
# AR users	39	12	21	6	7	7
% AR users		31	54	15	18	18
VR						
Oculus Quest	50	43	8	11	4	3
Oculus Rift	27	24	7	6	4	4
HTC Vive	27	26	3	6	2	0
Valve Index	12	11	1	1	0	0
Oculus Go	10	9	1	3	1	1
Samsung Odyssey+	3	3	0	2	1	1
PlayStation VR	1	1	0	0	0	0
Dell Visor	1	1	0	0	0	0
HP Reverb G1	1	1	0	1	0	0
# VR users	132	119	20	30	12	9
% VR users		90	15	23	9	7

Fig. 6. Summary of device popularity and reasons for use. The "Total" column presents the total number of users who indicated the device was their primary device. Only primary users of a device could report their reasons for using the device, and they could select multiple reasons if desired.

APPENDIX C DETAILS OF IDENTIFYING PROPOSED AUTHENTICATION METHODS

Publication venues considered. Using Google Scholar metrics,¹ we gathered top Engineering & Computer Science

¹https://scholar.google.com/citations?view_op=top_venues

Authentication method	AR Users	VR Users
Password	17	75
Unlock pattern	4	7
Iris scan	6	0
Paired device	8	28
Paired account	3	38

Fig. 7. The number of users who have experience with each authentication method on AR and VR, respectively.

venues in five subcategories: Computer Security & Cryptography, for its relevance to authentication; Computer Vision & Pattern Recognition and Signal Processing, because of their relevance to biometric authentication techniques; Human Computer Interaction, because AR and VR are a focus of the HCI community; and Engineering & Computer Science (general), to ensure all top venues were considered. We considered the top 20 venues in each subcategory, then supplemented this list with venues from CSRankings [1] under the Computer Vision, Computer Security, Mobile Computing, and Human-Computer Interaction categories. We removed workshops from the list of venues. In total, we considered 102 top venues.

Keywords used. For authentication: “authentication”, “authenticate”, “authenticating”, “authenticated”, “user identification”, “password”, and “biometric”. For AR and VR: “virtual reality”, “augmented reality”, “mixed reality”, “smart glasses”, “smartglasses”, “head-mounted displays”, and “head-worn display”. We curated these keywords based on manual searches on Google Scholar for papers relevant to AR/VR authentication.

APPENDIX D DEFINITIONS OF EVALUATION CRITERIA

Fig. 8 shows why we included each criterion. Our definitions for each of the evaluation criteria are as follows.

Deployment criteria.

- (1) *OS-Supported*: The method is built into the SDK or similarly available for use by developers with close to no effort.
- (2) *Platform-Agnostic*: The method could also be used on a computer or smartphone with no additional hardware. For example, a method that requires the use of controllers is not platform-agnostic. Though computers and smartphones usually have user-facing cameras, we do not consider iris scanning or other eye biometrics to be platform-agnostic since most methods currently require external devices or are specific to AR/VR cameras. A scheme is quasi-*Platform-Agnostic* if The method only requires extra hardware which it is plausible the user will have (e.g. EarEcho requires an earbud), or the method is common across platforms but in a slightly different form (e.g. gait has been explored on smartphones and smart watches, but usually does not use head movement like in an HMD).
- (3) *Mature*: The scheme has been implemented and deployed

Criterion	Relevant codes (code frequency)
<i>OS-Supported</i>	Ease of implementation (4), Method built into SDK (2)
<i>Platform-Agnostic Mature</i>	Desktop interface/device portal (3) Security history (6), Well-tested (1)
<i>Low-Power-Consumption</i>	Efficiency of use (2)
<i>Efficient-to-Use Physically-Effortless</i>	Auth speed (20) Ease of use (10), Cumbersome (7), Difficult (8), Single click auth (11), etc. Difficult/Easy-to-memorize (3)
<i>Memorywise-Effortless Easy-to-Learn</i>	Get used to it (4), Not fluent with virtual keyboard (1)
<i>Nothing-to-Carry Infrequent-Errors Acceptable-in-Public</i>	Requires additional device (5) Error prone (6), Technical difficulties (2) Safe at home/alone (5), Not safe in public (1)
<i>Accessible-Visual Accessible-Hearing Accessible-Speech Accessible-Mobility</i>	Not accessible (4) Not accessible (4) Not accessible (4) Not accessible (4), Physical disabilities (3), Shaky hands (2)
<i>Accessible-Cognitive</i>	Not accessible (4)
<i>Resilient-to-Guessing Resilient-to-Physical-Observation Protects-User-Privacy</i>	Secret/Hard to guess (4), Easy to guess (1) Observable actions/shoulder surfing (11), Screen hidden/safe from shoulder surfing (11) Privacy concerns (7), Collect personal/sensitive data (3)
<i>Multi-Factor</i>	Multi-factor authentication (15)

Fig. 8. Reasons we included each criterion in our evaluation.

on a large scale for actual authentication purposes beyond research. A scheme is quasi-*Mature* if the foundational scheme is mature, but is implemented slightly differently (e.g., a classic PIN entered on a shuffled keyboard).

- (4) *Low-Power-Consumption*: The method does not perform any type of signal processing. The method may also fulfill the criterion if it performs signal processing but is proven to have a negligible effect on the battery life of the device. Incumbent methods are assumed to have *Low-Power-Consumption*.

Usability criteria.

- (1) *Efficient-to-Use*: The time the user must spend authenticating comparable to biometrics, i.e. nearly instantaneous. A scheme is quasi-*Efficient-to-Use* if the time the user must spend authenticating is comparable to using a PIN on a smartphone, i.e. 2-3 seconds.
- (2) *Physically-Effortless*: The authentication process does not involve explicit actions requiring physical effort. We consider eye movement to be effortless actions. A scheme is quasi-*Physically-Effortless* if the user’s effort is limited to a single movement comparable to a button press (e.g., one tap on the Google Glass touchpad), or involves only speech.
- (3) *Memorywise-Effortless*: Users of the scheme do not have to remember any secrets at all. A scheme is quasi-*Memorywise-Effortless* if users have to remember one secret for everything (as opposed to one per verifier).

- (4) *Easy-to-Learn*: The method is familiar and is not complicated to explain. Absent reported results for this metric, we identify the set of instructions needed to communicate the authentication mechanism to a user and use the number of instructions, plus a familiarity factor, to rank each mechanism. For example, AugAuth has two instructions: (1) read the shuffled digits, (2) enter your PIN [79]. It is also familiar to users as a PIN. In contrast, RubikAuth has three: (1) turn the cube to the correct face for the first digit of your PIN, (2) select the correct digit on that face, (3) repeat for each digit of your PIN [56], [57]. Since RubikAuth adds a lot of complexity to a traditional PIN, we consider it unfamiliar and increment the number of instructions to four. Using this method, we deem any method with zero or one instruction as *Easy-to-Learn*. Any method with two instructions is quasi-*Easy-to-Learn*. Though we recognize that this is a subjective process, we believe our results are internally consistent and thus provide a valid way to compare mechanisms on this criterion.
- (5) *Nothing-to-Carry*: Users do not need to carry an additional physical object (electronic device, mechanical key, piece of paper) to use the scheme. For example, a scheme that requires the use of electrodes is not nothing-to-carry. A scheme is quasi-*Nothing-to-Carry* if the object is one that they'd carry everywhere all the time anyway, such as their mobile phone, but not if it's their computer (including tablets).
- (6) *Infrequent-Errors*: The task that users must perform to log in usually succeeds when performed by a legitimate and honest user. In other words, the scheme isn't so hard to use or unreliable that genuine users are routinely rejected. This refers to both entry accuracy (for non-biometric methods) and model accuracy (for biometric methods). Specifically, we require 98% accuracy or above (or $\leq 1\%$ EER). A scheme is quasi-*Infrequent-Errors* if accuracy is at least 90% (or EER is $\leq 5\%$).
- (7) *Acceptable-in-Public*: A majority of users would feel comfortable using the scheme in any public place. The scheme therefore must not require large, visible actions or speaking. If the scheme only requires gestures the user would already do to interact with the device (like Glass commands), that also fulfills this criterion. A method is quasi-*Acceptable-in-Public* if the scheme requires only small, discrete gestures, such as placing a finger on the smart glasses frame or nodding one's head. Alternatively, the scheme requires gestures that would be completely acceptable in some situations, but not in others (e.g.
- (1) *Accessible-Visual*: The method does not require a user to be able to see or the use of eye biometrics. A scheme is quasi-*Accessible-Visual* if the scheme uses eye biometrics, but does not require the user to be able to see.

walking).

Accessibility criteria.

- (2) *Accessible-Hearing*: The method does not require a user to hear.
- (3) *Accessible-Speech*: The method does not require a user to speak.
- (4) *Accessible-Mobility*: The method does not require physical movements, besides speech. A scheme is quasi-*Accessible-Mobility* if the method requires only blinking or requires actions the user would already be doing to interact with the device (e.g. typical Google Glass interactions).
- (5) *Accessible-Cognitive*: The method does not require the user to memorize a secret. The method is also either completely passive or requires only movement that the user is likely to already be doing.

Security & privacy criteria.

- (1) *Resilient-to-Guessing* For knowledge-based methods, we consider the password space of the method. A password space equivalent to a four-digit PIN is not *Resilient-to-Guessing*, but a more complex password space is, as long as users choose from the entire space. For biometric methods, we consider the false accept rate (FAR) or the success rate of statistical attacks, whichever is reported. The FAR must be 5% or less for a method to be quasi-*Resilient-to-Guessing*, and it must be at most 1% to be fully *Resilient-to-Guessing*. If neither FAR nor statistical attack success rate is reported, we default to the same value as *Infrequent-Errors*.
- (2) *Resilient-to-Physical-Observation*: The method does not require the use of gestures which would be visible to observers. A method can also fulfill the criterion if it uses visible gestures but proves that gestures are resilient to physical observation (i.e., the attack success rate is less than 1%, or less than 5% to be quasi-*Resilient-to-Physical-Observation*).
- (3) *Protects-User-Privacy*: The scheme does not utilize any sensitive user data, i.e. biometric measurements. (Passwords are not considered sensitive user data.) We consider a scheme quasi-*Protects-User-Privacy* if it uses sensitive user data only locally on the device, or if it is promoted as a cancelable biometric.
- (4) *Multi-Factor*: The scheme involves multiple factors/authentication layers by design (e.g., a user entered PIN is combined with hand movement biometrics in RubikBiom). This includes biometrics from different body parts (e.g. head movement and hand movement).