Augmenting Security and Privacy in the Virtual Realm: An Analysis of Extended Reality Devices

Derin Cayir and Abbas Acar | Florida International University
Riccardo Lazzeretti and Marco Angelini | Sapienza University of Rome
Mauro Conti | University of Padua
Selcuk Uluagac | Florida International University

We present a device-centric analysis of security and privacy attacks and defenses on extended reality (XR) devices. We present future research directions and propose design considerations to help ensure the security and privacy of XR devices.

Extended reality (XR) technologies stand at the forefront of a new digital revolution in an era of constant technological innovations. Nowadays, XR technology is much more than a device that produces 3D visuals. With new devices released each year and additional manufacturers getting involved in this field, XR devices are considered for different application domains, from entertainment to education to health care. The emerging metaverse realm offers a bright future, with capabilities ranging from assisting astronauts on their mission, to making hearing-impaired individuals “see” the conversations via subtitles.

XR devices are versatile in their functionality, equipped with an array of advanced sensors, communication capabilities, and hardware specifications. As these technologies evolve, our perception of reality seamlessly blends with the virtual world. However, the exponential growth of XR technologies raises concerns about whether these devices are secure and the users’ sensitive information is kept private. The increasing number of users will naturally attract attackers attempting to exploit these devices. The challenge arises from the diverse sectors currently utilizing these technologies and the unique properties of the devices themselves. This heterogeneity of the devices aggregates the potential attacks, and complicates the examination of current devices. Thus, it is vital for the research community in this field and the developers of these devices to consider what the current technologies propose and the vulnerabilities that the attackers can exploit.

In this article, we study possible attacks on XR devices that could compromise the security and privacy of users and their environment in a device-centric approach. We highlight our key findings from detailed literature analysis, discuss the current attack vectors of

Digital Object Identifier 10.1109/MSEC.2023.3332004
Date of current version: 4 December 2023

XR devices, and present the security and privacy attacks with their corresponding defenses proposed in the literature. We analyze the attacks performed on the virtual environments (VEs) separately, emphasizing the need for a further focus on this topic. Finally, we point to new research opportunities and propose design considerations, which can serve as valuable guidance for developers and the metaverse community.

Methodology

Literature Review

To find the articles that perform security and privacy attacks or defenses on XR devices, we queried Google Scholar, ACM, and IEEE libraries on 1 February 2023. From 319 articles, we have restricted our selection to 41 articles listed in Table 1, testing practical attacks and their defenses that target XR devices' security and privacy. For interested readers, we detail our literature review methodology and the PRISMA 2020 guidelines followed further in the GitHub repository.[3]

Device Search

From the selected articles, we gathered the devices used for the experiments. We also added to our device dataset other XR devices from the same companies that produced the devices mentioned in the articles. At the end of this process, in total, we identified 30 XR devices. The full list can also be found in the GitHub repository.[3]

Security and Privacy Analysis

We examined the devices' security and privacy by analyzing their documentation websites, manufacturer posts, articles, and blogs, the links of which are given in the GitHub repository.[3] In addition to the on-device properties, we analyzed the literature to find information about the security and privacy vulnerabilities of the devices and which types of attacks were seen on them. The questions we discuss in privacy policies are "Which type of data are collected, and where are they stored?", "Why are these data collected?", "With whom are the data shared?", "What are the users' rights on their data?" and "What are the privacy requirements of the apps on the devices?".

Security and Privacy Mechanisms in XR Devices

In this section, we examine some general properties of XR devices. Then, we highlight XR devices' security and privacy mechanisms using their security documentation and privacy policies.

General Properties of XR Devices

Virtual reality (VR) aims to replace the real world with a digital world, fully separating the user from their surroundings. On the other hand, augmented reality (AR) overlays virtual objects onto physical objects in the real world. Mixed reality (MR) combines AR and VR, allowing interactive integration between the two worlds. XR encompasses AR, VR, and MR, containing all the devices that merge the virtual and real worlds, as shown in Figure 1. To seamlessly integrate the virtual world with the real world, XR devices strive to stimulate as many senses as possible (vision, hearing, smell, touch, and taste) through their sensors and actuators. Some general properties of XR that enhance realism are discussed in the following sections.

Positional-Tracking Features. XR devices offer six degrees of freedom (6 DoF) or 3 DoF, inside-out, or nonpositional tracking. With 3 DoF, the device can only track the rotational movement of the user, whereas with 6 DoF it tracks the user's rotation and position. These are achieved by built-in sensors such as the gyroscope, magnetometer, accelerometer, cameras, infrared sensors, and inertial measurement units.

Tracking Sensors. Tracking sensors play a crucial role in XR devices and span from tracking the user's motions and interactions to their environment.

User Motion Tracking. XR devices have a head-mounted display (HMD) that contains accelerometer, gyroscope, and magnetometer sensors to understand the head movements of users. Similarly, hand controllers are equipped with these motion sensors to track the position and orientation of a user's hands or even their finger movements. Many devices on the market, such as Meta Quest 2 and Microsoft HoloLens, support hand tracking, where users can use their hands instead of a cursor. This is possible with inside-out cameras on the headsets.[4] XR devices can also detect a user's body motions, tracking different body parts to translate these movements into avatars. For example, HTC sells Vive Trackers, external devices that users can attach to their bodies to integrate their movements into VR with more precise accuracy.[5]

User Interaction Tracking. Alongside translating body movements into the virtual realm, XR devices are equipped with eye- and speech-tracking technologies, which could be used to enhance the avatars, fully mimicking a user's speech and eye movements, and also developing more realistic simulations for medicine, missions, and much more. Microsoft HoloLens, Meta Quest Pro, and HTC Vive devices have eye-tracking sensors on the HMDs. With Vive Focus's eye tracker, users need only gaze in a certain direction to open/close tabs or select objects.[6] Meta Quest Pro

Table 1. A list of articles (additional references).

Number	Reference
P1	M. E. Mahan, “ Exploring ransomware on the oculus quest 2,” Ph.D. dissertation, Louisiana Tech University, 2022.
P2	S. Valluripally et al., “Modeling and defense of social virtual reality attacks inducing cybersickness,” *IEEE Trans. on Dep. and Secure Comput.*, vol. 19, pp. 4127-4144, Oct. 2021.
P3	J. Happa et al., “Cyber security threats and challenges in collaborative mixed-reality.” *Frontiers in ICT 6*, Apr. 2019.
P4	Ü. Meteriz-Yıldıran et al. “A keylogging inference attack on air-tapping keyboards in virtual environments.” in *IEEE Conf. on VR and 30 User lnterf.*, 2022, pp. 765-774.
P5	S. R. K. Gopal et al., “Hidden reality: caution, your hand gesture inputs in the immersive virtual world are visible to all!” presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.
P6	A.Arafat et al., “Vr-spy: A side-channel attack on virtual key-logging in vr headsets.”in *IEEE Conf on VR and 30 User lnterf.*, 2021, pp. 564-572.
P7	Z. Ling et al., “I know what you enter on gear vr,” presented at IEEE Conf. on Comm. and Network Sec., Jun. 10-12, 2019.
P8	C. Slocum et at. “Going through the motions:AR/VR keylogging from user head motions.” presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.
P9	Y. Zhang et al., “It’s all in your head (set) : Side-channel attacks on ar/vr systems,” presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.
P10	R. Miller et al., “Using external video to attack behavior-based security mechanisms in virtual reality (vr),” in *IEEE Conf on VR and 30 User lnterf.*, 2022, pp. 684-685.
P11	H. Khan, U. Hengartner, and D. Vogel, “Augmented reality-based mimicry attacks on behavior-based smartphone authentication,” in *16th Ann. Int. Conf on Mobile Sys.*, 2018, pp. 41-53.
P12	A. J. Bose and P. Aarabi, “Virtual fakes: Deepfakes for virtual reality,” in *IEEE Workshop on Multi. Signal Proc.*, 2019, pp. 1-1.
P13	D. Maloney, S. Zamanifard, and G. Freeman, “Anonymity vs. familiarity: Self-disclosure and privacy in social virtual reality.” in *ACM Symp. on VR Software and Tech.*, 2020, pp. 1-9.
P14	B. Falk et al., “Poster: reavatar: virtual reality de-anonymization attack through correlating movement signatures,” in *ACM SIGSAC Conf. on Comp. and Comm.* Sec., 2021, pp. 2405-2407.
P15	P. P. Tricomi et al., “You can’t hide behind your head-set: User profiling in augmented and virtual reality,” in *IEEE Access*, vol 11, pp. 9859-9875, 2022.
P16	V. Nair et al., “Unique identification of 50,000+ virtual reality users from head & hand motion data.” presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.
P17	J. Li et al., “Kalεido: Real-Time privacy control for Eye-Tracking systems.” presented at the 30th USENIX Sec. Symp., Aug 11-13, 2021.
P18	B. David-John et al. “Towards gaze-based prediction of the intent to interact in virtual reality.” in *Proc ACM Sym. on Eye Track. Res. and App.*, 2021, pp. 1-7.
P19	B. David-John, et al. “A privacy-preserving approach to streaming eye-tracking data.” *IEEE Trans. on Vis. and Comp. Graph.*, pp. 2555-2565, Mar. 2021.
P20	J.Steil et al. “Privacy-aware eye tracking using differential privacy.” in *Proc. ACM Symp. on Eye Track. Res. and App.*, 2019, pp. 1-9.
P21	A. Liu et al. “Differential privacy for eye-tracking data.” in Proc. *ACM Symp. on Eye Track. Res. and App.*, 2019, pp. 1-10.
P22	E.Bozkir et al. “Differential privacy for eye tracking with temporal correlations.” *Plos one* 16.8, no. 8, 2021.
P23	Y.Kim et al. “Erebus:Access Control for Augmented Reality Systems.” presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.

(*Continued*)

Table 1. (*Continued.*) A list of articles (additional references).

P24	C. Shi et al., "Face-mic: inferring live speech and speaker identity via subtle facial dynamics captured by ar/vr motion sensors," in Proc. of 27th Ann. Int. Cont. on Mobile Comp. and Net., 2021, pp 479-490.
P25	R. Trimananda et al., "OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR." presented at the 31st USENIX Sec. Symp., Aug 10- 12, 2022.
P26	T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies." in Proc. SIGCHI Cont. on Human Fae. in Comp. Sys., 2014, pp. 2377-2386.
P27	Lebeck, Kiron, et al. "Towards security and privacy for multi-user augmented reality: Foundations with end users." in *IEEE Symp. on Sec. and Privacy*, 2018, pp. 392-408.
P28	J. O'Hagan et al., "Privacy-Enhancing Technology and Everyday Augemented Reality: Understanding Bystanders" in *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2023, pp. 1-35.
P29	H. Farrukh, et al. "Locln: Inferring Semantic Location from Spatial Maps in Mixed Reality." presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.
P30	Y. Zhaoe et al., "Privacy-preserving Reflection Rendering for Augmented Reality.", in *Proc. ACM Int. Conf. on Multimedia*, 2022, pp. 2909-2918.
P31	J. De Guzman et al., "Security and privacy approaches in mixed reality: A literature survey." *ACM Computing Surveys*, vol. 52, no. 6, pp. 1-37, 2019.
P32	P. Casey et. al, "Immersive virtual reality attacks and the human joystick," *IEEE Trans. on Dep. and Secure Comp.*, vol. 18, no.2, 2019, pp. 550-562.
P33	F. Roesner, T. Kohno, and D. Molnar, "Security and privacy for augmented reality systems," *Commun. ACM*, vol. 57, no.4, pp. 88-96, 2014.
P34	K. Lebeck et al., " How to safely augment reality: Challenges and directions," in Proc. 17th. Int. Workshop on Mobile Comput. Sys. and App., 2016, pp. 45-50.
P35	K. Ruth, T. Kohno, and F. Roesner, "Secure Multi-User content sharing for augmented reality applications." presented at the 28th USENIX Sec. Symp., Aug 14-16, 2019.
P36	S. Rajaram et al., "Eliciting Security & Privacy-Informed Sharing Techniques for Multi-User Augmented Reality." in *Proc. 2023 CHI Conf on Human Factors in Comput. Sys.*, pp. 1-17.
P37	M. Vondrek, et al., "Rise of the metaverse's immersive virtual reality malware and the man-in-the-room attack & defenses," in *IEEE Comp. & Sec.*, 2022, p. 102923.
P38	K. Cheng et al., "Exploring user reactions and mental models towards perceptual manipulation attacks in mixed reality." presented at the 32nd USENIX Sec. Symp., Aug 9-11, 2023.
P39	H. Lee et al., "AdCube : WebVR Ad Fraud and Practical Confinement of Third-Party Ads." presented at the 30th USENIX Sec. Symp., Aug 11-13, 2021.
P40	Y.Abdrabou et al. "Understanding shoulder surfer behavior and attack patterns using virtual reality." in *Proc. 2022 Int. Conf. on Adv. Visual Int.*, 2022, pp. 1-9.
P41	F. Mathis, K. Vaniea, and M. Khamis. "Can i borrow your aim? using virtual reality for (simulated} in situ authentication research." in IEEE Conf. on VR and 30 User lnterf., 2022, pp. 301-310.

also captures and stores the raw face image of users to extract the user's natural facial expressions to create more natural-looking avatars.[7]

Environmental Tracking. XR devices have outward-facing cameras that track everything within the user's environment and facilitate the precise rendering of 3D objects in the user's environment. Proximity sensors detect the presence of objects, while depth sensors enable the devices to create a 3D map of the user's environment. Although VR devices are not primarily designed to integrate real-world and virtual-world objects as AR/MR devices are, many contemporary VR devices, including Meta Quest 2, Pico 4, PlayStation (PSVR) 2, and Magic Leap, still incorporate these sensors and pass-through cameras to enable room-scale inside-out tracking. Meta apps can also use pass-through cameras to blend the physical and VE of users, a purpose that goes beyond merely viewing, and not processing, the real environment's data.[8]

Audio and Speakers. Audio/speakers are integrated into the devices, and some devices have 3D spatial audio so that users can physically locate the sounds they are experiencing in their virtual world. Meta Quest 2 and HTC Vive are examples of devices that use 3D spatial audio.

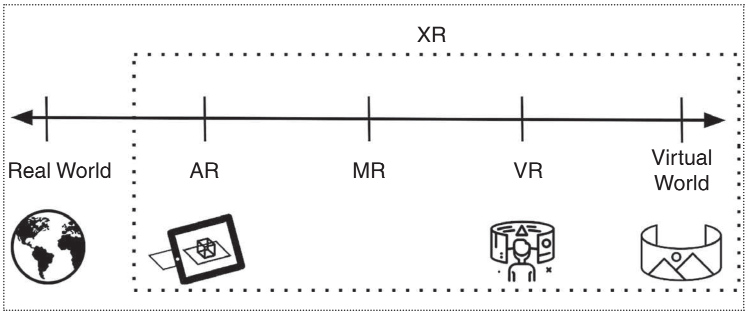

Figure 1. The spectrum of XR technologies.

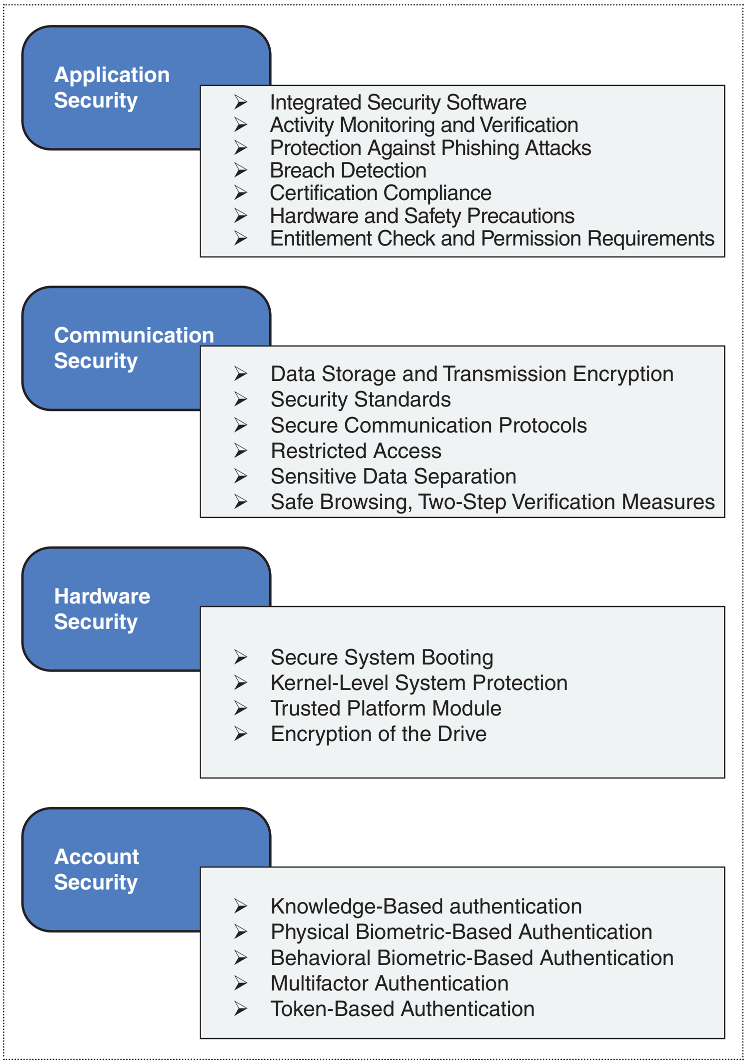
Application Security
➢ Integrated Security Software
➢ Activity Monitoring and Verification
➢ Protection Against Phishing Attacks
➢ Breach Detection
➢ Certification Compliance
➢ Hardware and Safety Precautions
➢ Entitlement Check and Permission Requirements
Communication Security
➢ Data Storage and Transmission Encryption
➢ Security Standards
➢ Secure Communication Protocols
➢ Restricted Access
➢ Sensitive Data Separation
➢ Safe Browsing, Two-Step Verification Measures
Hardware Security
➢ Secure System Booting
➢ Kernel-Level System Protection
➢ Trusted Platform Module
➢ Encryption of the Drive
Account Security
➢ Knowledge-Based authentication
➢ Physical Biometric-Based Authentication
➢ Behavioral Biometric-Based Authentication
➢ Multifactor Authentication
➢ Token-Based Authentication

Figure 2. The security properties of XR devices.

Haptic Feedback. Haptic feedback is an essential part of the VR experience to incorporate users' senses into their virtual world. Different software development kits support haptics for developing immersive apps, such as vibrating the controllers[9] and applying force to simulate touch. There are also additionally sold suits and gloves, designed to make the metaverse experience even more realistic.

Communications. XR devices include Wi-Fi and Bluetooth communication so that users can collaborate with other users or connect to their other gadgets. Each device has a compatibility requirement and can run on different operating systems (OSs). For app development platforms, the devices are compatible with different graphic cards and random-access memories.

Security Properties of XR Devices

The impact of security and privacy attacks is high on XR devices as they are complex technologies that collect potentially user-identifiable information. Due to the immersive nature of these devices, attacks can manipulate users' perception of reality, potentially leading to physical harm. To ensure the security and privacy of the devices, vendors apply different methods that aim to meet the challenges of the modern cyber threats landscape, as summarized in Figure 2.

Application Security. Applications are essential for delivering different functionalities to users. As applications have access to users' sensitive data, securing them against exploitation of sensitive information is a high priority. Device vendors adopt various measures to achieve this goal. Microsoft HoloLens relies on Microsoft Defender SmartScreen, integrated into the OS, warning users of dangerous websites and applications that can perform phishing and malware delivery. Meta monitors and verifies account activity to prevent malicious acts and policy violations. Vuzix safeguards users' information from phishing attacks by preventing third-party apps from asking for users' sensitive information. Sony uses the information collected from the user to detect breaches, such as unauthorized access to the apps. Pico Neo 4 uses "ETSI EN 303 645"-based security certification, which includes regular security updates and key management practices.

Communication Security. Device vendors use different encryption standards to prevent attackers from accessing sensitive user information. For instance, HTC has data processing or altering, anonymization, pseudonymization, encryption during transmission using Transport Layer Security (TLS), and access restriction.

However, as stated in their policy, HTC does not take responsibility for threats from independent third-party applications. Microsoft HoloLens 2 secures data transfer between itself and the cloud using Azure integration. Furthermore, Dynamics 365 Remote Assist helps when deploying to external clients, separating sensitive device vendor data and resources. Google devices ensure continuous encryption to keep data private while in transit and have security features like Safe Browsing, Security Checkups, two-step verification, physical security measures, and restricted access to personal information. Quest's VR messenger app prioritizes security, testing end-to-end encryption and specific apps' access control with its latest updates.

Similarly, Meta devices have end-to-end encryption. For digital audio and video content encryption, Epson Moverio supports High-Bandwidth Digital Content Protection-encrypted content. Additionally, the data in transit is protected through TLS by many other manufacturers, such as Magic Leap, Pico, Samsung, and Vuzix.

Hardware Security. Devices employ various hardware security measures to guard against unauthorized access and physical attacks. For instance, Microsoft HoloLens 2 uses the Trusted Platform Module, a hardware-level security technology that generates and stores cryptographic keys and authenticates the device using unique Rivest–Shamir–Adleman keys. Furthermore, BitLocker provides another level of security by encrypting the drive, employing AES-XTS-256 encryption, and safeguarding the data with multifactor authentication, including read-only media and privacy protection of writable data. Similarly, Pico devices use secure system booting, kernel-level system protection, and a trusted environment.

Account Security. We note different authentication methods deployed on different devices. For instance, HTC Vive Cosmos and Epson Moverio use pin/password authentication. Quest Pro and Meta devices, on the other hand, use unlock patterns, also providing users with privacy-customization options. Furthermore, some devices use accounts for logging in. Pimax, for instance, links its authentication to a Steam account; Samsung authenticates through an Oculus login; and Magic Leap relies on its ID system, where a code verification is sent to a registered e-mail address. Similarly, PSVR devices use a QR code for the initial device sign-in, and then four-digit passwords with two-step verification for the remaining entries. Microsoft HoloLens supports iris-based authentication, but the users can also choose password entry to log in to their devices. Some third-party apps utilize biometrics, such as PalmID, which stores encrypted biometric signatures in Epson Moverio devices. On the other hand, the Pico Neo 3 Pro only requires a login for the Pico App Store due to its business-focused purpose, where setup and access to files and apps must be quick.

Privacy Policies of XR Devices

Built-in sensors in XR devices collect data during or after use of the gadgets. Many of today's devices collect and share this information according to their privacy policies. So, in this section, we discuss the privacy of the devices in the current market by examining their policies and summarizing their properties.

Which type of data are collected and how? The data collected by XR devices are highly sensitive, including information about users' physical properties, movements, environment, gender, age, gestures, and biometric information. If an attacker targets these data, the consequences can be damaging. Hence, users must be aware of the type of data the device vendors collect and where and how these data are stored. As stated in the privacy policies of Meta and HTC, the devices collect data in three ways: user-provided, sensor-collected, and third-party obtained. The information users give while using devices may be about their transactions, social interactions, communications, e-mail addresses, phone numbers, gender, location, physical features, avatar, content, and social media accounts. The automatically collected data may be about the people, games, apps, and features with whom users interact. Through cookies, the data are linked to the user, including information about product access, device type, Internet Protocol address, unique identifiers, Wi-Fi network, web traffic, environment, physical dimensions (e.g., height and head size), play area, hand size, and movement. The information gathered from third parties may be from apps, developers, content providers, and marketing partners.

Where are the data stored? Data storage practices vary among devices. Meta stores the data in the device in their raw form. Similarly, Magic Leap 2 has no cloud nor centralized server connection and stores the data on the device. HTC stores the data on the user's phone or HTC's servers (encrypting the data and not transmitting them to anywhere other than the device and the connected PC).

Why are these data collected? Device vendors collect data for many purposes, including improving user experience, providing better-personalized services, communicating with the user, and protecting the manufacturers, their users, and the public (e.g., analyzing data to detect abuse, such as spam or illegal content). The data may also be used to enhance realism, such as using controllers, HMD movements, and audio to make the avatar more realistic.

With whom are these data shared? Data collected by the devices can be shared without users' knowledge. It is crucial for users to understand what is done with their data and for the developers of these devices to know how other vendors handle the data they collect. Generally, the data are shared with domain administrators, advertisement network providers, affiliated companies, other users, and third parties, with the users' consent. Many vendors state that the data may be transferred to, stored in, and processed in any other country where the device manufacturers' business has less protective privacy laws.

What rights do users have over their data? Users have the right to manage, update, limit, and delete their data as well as to oppose and withdraw consent for data collection and marketing messages, as stated in Pico's, HTC's, and Vuzix's privacy policies. The user can do this by contacting the e-mail provided on the website. Deleting a Meta account results in deleting posts, entities, and apps, but not other users' posts about that user. With PSVR devices, users can adjust the amount of shared data through the settings.

What are the privacy requirements of the apps on the devices? Most of the devices analyzed in this article are programmable, where at-home users can create their own apps for their needs. However, this freedom comes with the cost of compromising the security and privacy of the devices. Developers should set basic app requirements to ensure a coherent experience and prevent malicious apps. Meta suggests VR check guidelines for app developers in its privacy policy and requires the apps to follow its privacy policies, linking to the policy and clearly explaining collected data and use. Similarly, Google proposes general rules that app developers must follow for users' safety. They define what can be collected from users and how the apps should form their own privacy and content policies. Moverio prohibits collecting any information without users' consent and any phishing to gain sensitive information about its users.

Security Attacks and Defenses

In this section, we categorize security attacks into two categories: 1) attacks on XR devices and 2) attacks via XR devices. Our attack categorizations are shown in Figure 3. Articles presenting the attacks are listed in Table 1.

Attacks on XR Devices

Malware Attacks. In malware attacks, an attacker plants viruses, or worms, on users' devices without their knowledge. An example of a malware attack observed on VR devices is Big Brother, proposed by ReasonLabs.[10] The malware can infect VR devices with an Android-based OS. With this, the attacker can remotely connect to an Android-based VR device and record the headset screen. This malware infects the user's computer, and once the malware enters the PC, it waits for a developer-mode-enabled VR device to connect. Upon connection, it opens a TCP port to record the user's headset whenever the PC and VR device share the same Wi-Fi network.

Also, ransomware can target XR devices, limiting users' access until a ransom amount is paid.[11] An

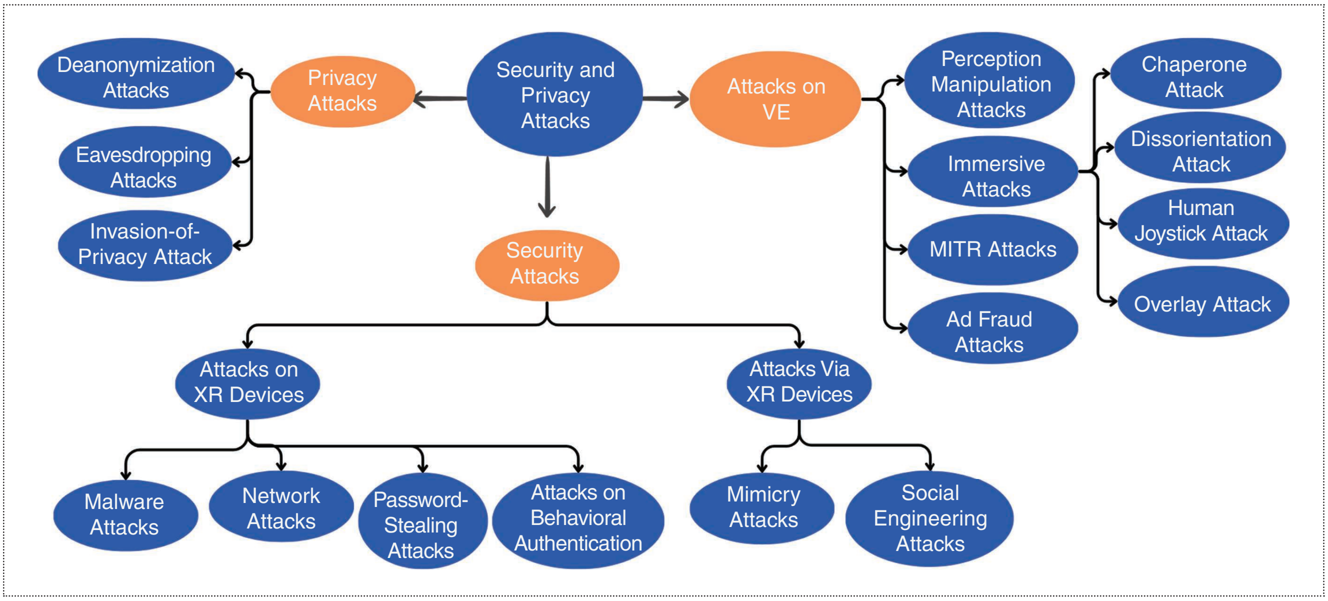

Figure 3. Security and privacy attacks in the literature.

Android ransomware sample was tested on Meta Quest 2 by integrating Simple Ransomware Sample (SRS) on the device, which is developed as a standard Android application (see [P1] in Table 1). The goal was to get read-and-write data permissions through SRS and encrypt the data with a function that uses Java Crypto and Security libraries. Researchers concluded that the attack surface of Meta Quest 2 includes essential elements that can be leveraged for effectively carrying out ransomware attacks.

Network Attacks. In network attacks, attackers exploit vulnerabilities of the target network and bypass the security mechanisms in place. For instance, Valluripally et al. (see [P2] in Table 1) showed that a denial-of-service (DoS) attack was executed via packet tampering, duplication, and dropping, resulting in a crash of the VR environment's server. Another study (see [P3] in Table 1) also showed that DoS attacks resulting in frame-rate drops in devices may lead to nausea and dizziness and create cybersickness attacks.

Password-Stealing Attacks. Password-stealing attacks target the authentication of devices and can lead to unauthorized access and sensitive information leakage. Key-logging attacks can be performed by capturing users' hand traces to identify their passwords while using an in-air tapping keyboard for input (see [P4] in Table 1). An adversary could plant hand-tracker devices or videotape the user's text entry processes to obtain the victim's hand-trace patterns and reconstruct inputs like passwords. This was also evident in a recent study where researchers retrieved graphical pattern lock inputs, passwords, e-mails, and pin entries of the users with VR HMDs, all from a video of the user interacting with the XR device (see [P5] in Table 1).

Moving beyond visual observations, other studies explored nonvisual approaches to identify key-logging (see [P6] in Table 1). These methods utilize a range of techniques, from analyzing network signals to leveraging device sensors, further highlighting the significance of this threat. For instance, Ling et al. (see [P7] in Table 1) performed vision-based and motion-based side-channel attacks on Samsung Gear VR devices using sensors. The motion-based side-channel attack, in particular, utilized Samsung Gear VR's user motion-tracking sensors by tricking the user into downloading a malicious app, which collected orientation angles, hence giving information about where a key click occurs, leading to leakage of the user's password. Similarly, HMD's motion sensors from any XR devices with virtual keyboards revealed characteristics of users' typing behavior, enabling them to segment motion signals and determine typed words (see [P8] in Table 1). Moreover, a recent article further exploited side-channel information, such as thread times to differentiate digit inputs using a spy program on Microsoft HoloLens 2 and Meta Quest 2 devices (see [P9] in Table 1).

Attacks on Behavioral Authentication. Due to usability considerations, behavioral authentication systems are considered ideal for AR/VR devices. Miller et al. (see [P10] in Table 1) analyzed a ball-throwing task for authentication, where they could extract the 2D motion trajectories from captured videos and match them to the 3D enrollment trajectories of users using HTC Vive, Vive Cosmos, and Meta Quest devices. Thus, they demonstrated that behavior-based authentication approaches could also be susceptible to attacks by obtaining the 2D video of users.

Attacks Via XR Devices

Mimicry Attacks. AR devices can facilitate successful mimicry attacks on keystroke dynamics-like behavioral biometrics. Khan et al. (see [P11] in Table 1) proposed an AR-based approach to mimic the touch dynamics used for smartphone authentication. The results showed that 87% of the attacks can bypass the authentication method.

Social Engineering Attacks. Extensive data collected from the advanced sensors of XR devices also pose security concerns through impersonation and social engineering attacks, such as deep fakes. With deep fakes, an attacker could trick people into believing they are someone else. For instance, it has been shown that by creating deep fakes, where the face and body of the user are physically altered to a digital form, attackers can mimic users and how they appear (see [P12] in Table 1). To prevent deep-fake audios, Maloney et al. (see [P13] in Table 1) suggest that developers can make a layer to modulate the voice input obtained from the HMD so that the user's personal information is not identifiable.

Privacy Attacks and Defenses

Privacy attacks focus on violating the users' right to exploit their personal information. In this section, we review privacy attacks and defenses on XR devices.

Deanonymization Attacks

XR devices have many sensors that help navigate the user's environment, seamlessly blending real and virtual worlds. Naturally, these sensors collect information on the user's surroundings and personal information. Such information can be highly private as devices may record unique user movement data, potentially compromising anonymity. For instance, in a deanonymization attack called *ReAvatar* (see [P14] in Table 1), users are identified by their virtual avatar via correlating specifically recorded movements. Remarkably, users' movement remains unique even when using multiple avatars so that attackers can also deanonymize them across multiple avatars. Moreover, Tricomi et al. (see [P15] in Table 1) show that AR (Microsoft HoloLens) and VR (HTC Vive Pro) platforms are vulnerable to deanonymization attacks by identifying the users from basic physical actions like walking and pointing. In a more recent study (see [P16] in Table 1), HMDs and controllers' motion sensor data revealed user behavior patterns, making potential attackers reidentify users across different sessions of popular games.

Other types of highly sensitive data are biometric data. Many XR devices, such as PSVR2, Magic Leap 2, Pimax Vision 8k, Microsoft HoloLens 2, and HTC Vive Pro Eye, have widely adopted eye-tracking technology for different purposes ranging from authentication to understanding users' interests for advertising. Given the rich information content eyes offer, this raises critical privacy concerns. For example, pupil size can be used to understand someone's interests, while eye movements can be analyzed to infer mental disorders, cognitive states, gender, and age (see [P17] in Table 1). Researchers also found that the natural gaze dynamics from eye-tracking sensors could be used to predict users' interaction with virtual objects (see [P18] in Table 1), and also by attackers for user identification (see [P19] in Table 1).

Several strategies can be employed to safeguard user privacy, including the use of differential privacy, which involves the addition of random noise to obfuscate individual data without undermining overall data utility (see [P17], [P20], [P21], and [P22] in Table 1). Currently, independent content developers can directly access the raw data collected by XR devices' sensors. Hence, to protect users' privacy, researchers have proposed designing application programming interfaces that would add Gaussian noise to raw data while also implementing temporal and spatial downsampling (see [P19] in Table 1). Furthermore, to prevent overprivileged malicious apps from accessing raw sensor data, Kim et al. (see [P23] in Table 1) have proposed an access control scheme for AR that allows users to limit access to sensor data.

Eavesdropping Attacks

An eavesdropping attack tested in HTC Vive Pro and Meta Quest devices is the Face-Mic approach, which derives sensitive information by exploiting motion sensors (see [P24] in Table 1). Speech-associated facial movements, bone-borne vibrations, and airborne vibrations of the user are collected, permitting determination of personal information such as the user's gender. This attack utilizes zero-permission sensors (i.e., motion sensors) and reveals the user's protected information without the user's consent.

Invasion-of-Privacy Attacks

Invasion-of-privacy attacks involve the unauthorized collection and use of personal information. For instance, researchers realized that side-channel information could also be used for concurrent app fingerprinting on Microsoft HoloLens 2 devices (see [P9] in Table 1), identifying which app the user is currently using. Furthermore, several academic works found that the traffic flow from XR devices revealed user-identifiable information, especially when users were using social applications (see [P25] in Table 1).

Moreover, with outward-facing, always-on cameras, users themselves can record their environment in every detail without any notice, compromising bystanders' privacy. Especially, AR glasses could be harder to notice in public settings, where bystanders might not expect to be recorded (see [P26] in Table 1). Several articles conducted user studies to test bystander privacy experiences in crowded public spaces (see [P26], [P27], and [P28] in Table 1), showing users' concerns about bystander privacy violations and invasive applications on their devices. In Zhang et al. (see [P9] in Table 1), researchers found that environmental events created additional rendering, which was identifiable from the performance counter analysis of the devices. From this, researchers identified the existence of a bystander by analyzing the CPU frame rates of Microsoft HoloLens, and they also calculated the distance of the bystander from the device.

AR and MR devices capture spatial maps of the users' environment to overlay virtual content in the users' surroundings by depth sensors and always-on cameras, which introduce privacy concerns. Researchers found that this can reveal information about the location of the users (see [P29] in Table 1). With a tailored malicious app, researchers extracted the 3D spatial map of the user's environment using Microsoft HoloLens and identified the user's indoor location from a model trained with 3D objects present in an environment. Another study (see [P30] in Table 1) found that inputs captured by AR devices during object rendering can contain sensitive objects, which will be translated onto reflective AR objects. This reflection-based privacy attack results in the user's physical environment information being recovered by the attacker.

The literature suggests implementing defenses such as an intermediate layer between the sensor interfaces and the apps like input sanitization (see [P31] in Table 1). This way, sensitive information can be protected by the input access control system. This can be achieved in the following two different ways:

1. *Negotiating permission*: Developers can include an option where the bystanders have a right to opt out if they feel their privacy is compromised (see [P31] in Table 1). For instance, physical switches that block the cameras or push–pull notifications, where the bystanders near an XR device receive an option not to get recorded, can be implemented (see [P26] in Table 1).
2. *Blurring*: Developers can add a protection layer where sensitive objects (e.g., faces and license plates) in the captured images can be blurred (see [P26] in Table 1).

Attacks and Defenses in VEs

With XR devices, security and privacy concerns are not limited to the physical world. This section discusses security and privacy issues in the VE.

Immersive Attacks

Immersive attacks target the unique properties of VR devices and are categorized into chaperone, disorientation, human joystick, and overlay attacks. An article (see [P32] in Table 1) shows that this is possible in HTC Vive and Oculus Rift devices by simply modifying VE parameters in a JavaScript Object Notation file.

Chaperone Attack. In a chaperone attack, the attacker modifies the virtual boundaries of the victim (see [P32] in Table 1). In situations where the user's confidence in the boundaries that are no longer valid is high, the attacker might do physical harm to the user by altering the boundaries. A proof-of-concept attack was performed, and HTC Vive and Oculus Rift devices were found to be vulnerable against all tested OpenVR and SteamVR applications (see [P32] in Table 1). To perform the chaperone attack, researchers obtained the artifacts, such as the location of the VR boundaries, system settings, and executable path location, by exploiting SteamVR's vulnerability of storing the data in plain text without any integrity checks.

Disorientation Attack. In a disorientation attack, the user's location and rotation were adjusted by making minor changes in the player's orientation through yaw and translation parameters (see [P32] in Table 1). In cases where users are immersed in VEs and subject to visual motion cues without physical motion, visually induced motion sicknesses are seen. This way, the player's orientation is controlled, forming a seasick sensation. Smaller fluctuations in the artifacts resulted in stronger seasick sensations. These attacks were performed through Steam, and the success of this attack was similar to the chaperone attack as the same artifacts were targeted.

Human Joystick Attack. Human joystick attacks are designed to alter the direction or location of a user within the VE without their awareness (see [P32] in Table 1). These attacks aim to manipulate the user's movement, potentially leading to physical harm, such as the user hitting an object. For instance, the VE was shifted continuously to move the user to an attacker-defined location.

To solve these attacks, some countermeasures are suggested: intrusion detection, where an attack is flagged if it detects any patterns different from the expected timing model, or securing timing information, where the modulation frequency of the optical signal is changed.

Overlay Attack. Attackers can superimpose images (such as inappropriate or alarming content) onto the user's screen to potentially cause harm or distress or block the user's view. Loud songs can be played, and bright, flashing lights can be displayed on the XR device, which may harm users physically. These attacks can be particularly dangerous because users may not realize that the overlaid content is not a part of the XR experience and may react to it as if it were real. An unlimited number of images was overlayed on Oculus Rift and HTC Vive devices [P32]. Furthermore, it is also found that packet-sniffing attacks can be used to capture users' physical location parameters illegally to perform overlay attacks (see [P2] in Table 1).

Overlay attacks are also a valid concern for AR devices that are designed to overlay computer-generated visual, audio, and haptic signals onto the real world (see [P33] in Table 1). In immersive AR applications, users must trust the app and, if it is targeted by the attacker, users can be deceived about the real world. As a possible solution, windowing the display regions is suggested, where the OS gives the applications separate windows corresponding to the bounded regions of the display (see [P34] in Table 1). With this solution, the applications' outputs are isolated from one another. Furthermore, Lebeck et al. (see [P34] in Table 1) propose managing the outputs of AR devices as fine-grained objects, made of first-class OS primitives, which make the OS capable of controlling when and where objects are placed. This method yields better flexibility and output control than windowing the displays.

Security risks in AR do not just come from the apps themselves but also from users, who might intentionally spam others with disturbing virtual objects, or manipulate their virtual objects without permission. As a possible defense, Ruth et al. (see [P35] in Table 1) propose an app-level library or an OS interface tailored for AR multiuser application developers. They consider users' expectations, who may have different expectations about how AR content should be shared.

Their proposed framework sets security objectives for controlling other users' permission to access shared (outbound) content and managing the incoming (inbound) content and owned physical space. They introduce "ghost" objects, where certain sensitive parts of the object are not shared with other AR users, and they suggest policies on physical space ownership in AR. Furthermore, Rajaram et al. (see [P36] in Table 1) pairs AR and security and privacy experts to find solutions to AR overlay attacks. This study highlights that virtual menus and proximity-based interactions were suggested for content sharing and access control techniques.

Man-in-the-Room Attacks

Man-in-the-room (MITR) attacks represent a specific threat targeting the VE where users are known to share private information (see [P37] in Table 1). These attacks often exploit users' immersion within the VE, benefiting from their tendency to assume the same privacy norms that are valid in the real world also hold in the virtual world. For example, a private virtual room that users may use to communicate with each other may be targeted by an MITR attacker as users would feel secure in a virtual room and would not expect an outsider to join without their consent. However, via an MITR attack, the attacker can exploit this perception and know everything happening inside a private VR room without the victim's knowledge or authorization (see [P37] in Table 1).

An example of MITR attacks was performed on the Bigscreen VR app on Steam, which is supported by HTC Vive, Oculus Rift, and Windows MR devices (see [P37] in Table 1). The Bigscreen app is used for communication in a VR environment. The attackers found a loophole where they exploited app vulnerabilities that caused a self-replicating infection (worm) without the user installing anything malicious. With the MITR attack, attackers could eavesdrop in the virtual room without other users noticing them. The attackers could turn on the users' microphones to listen to their conversations and observe their actions.

Perception Manipulation Attacks

As XR devices are designed to be highly immersive, many concerns have been expressed about the impacts of attacks on XR devices on the users. In Cheng et al. (see [P38] in Table 1), researchers created three attack scenarios targeting visual, auditory, and situational awareness perceptions.

With the visual attacks, the researchers overlay an adversarial virtual object, observing that the participants were fooled into believing that the overlayed content was real, and their reaction times were significantly slowed. Interestingly, after the presence of the attacks, the participants started becoming hesitant and getting triggered by nonadversarial content. Imagine a real-world scenario where a user uses an XR device to get real-time guidance when driving and an adversary overlays incorrect speed limits and traffic signs. The user will be deceived by these overlays and have a reduced reaction time, which is a valid concern while driving. The issue is that these attacks' impact continues even after the attack is finished as users will lose their trust in the device and become hesitant with each traffic sign encountered.

Auditory attacks were performed while users were concentrating on memorizing a sequence of elements. The immersive nature of XR audio led the users to treat the audio cues as a real-world stimulus. Finally, the researchers displayed notifications on a screen that is in the background and realized that participants were not quick to notice real-world instructions while using their XR devices, showing that users are more focused in the metaverse than the real world.

Ad Fraud Attacks

Web-based VEs can be targeted by adversaries to create ad frauds that generate unintended ad traffic involving ad impressions or clicks (see [P39] in Table 1). In XR technologies, the 3D world is rendered on an HTML canvas document object model to create immersive experiences for users and help them interact with the web page they are browsing. There are currently no primitives to separate the execution of an ad-serving JavaScript (JS), enabling researchers to launch different attacks. One of these attacks was called a *gaze and controller jacking* attack, where a fake gaze and controller cursor was created to make users intentionally click on the malicious VR objects. Furthermore, with a blind spot tracking attack, researchers exposed the limited visual awareness of users during 360° views by placing malicious promotional objects in the blind spots of users' views. Similarly, with the abuse of an auxiliary display attack, researchers could block users from seeing their immersive world by displaying ads. As a potential solution, the researchers propose AdCube, which sandboxes the ad-serving JS and suggests that ad entities should be given a confined area. The researchers also suggest that publishers specify DOMs that interact with a confined third-party ad script and generate access control policies on write-and-read permissions for DOMs.

Future Research Directions

In this section, we leverage the insights gleaned from our study.

Authentication is the leading defense method. The current literature proposes unique ideas for user authentication, ranging from behavioral methods such as throwing a virtual ball, to biometrics that utilize almost every part of the human body. Although authentication methods are the basis for securing the device from outsiders because none of the devices have adopted the proposed authentication methods, it is clear that authentication offers only a partial panacea for device security.

Future Research Direction 1

Authentication alone cannot guarantee complete security, and it is important to consider multiple layers of security to address all possible attack vectors. Therefore, researchers must propose additional defense strategies that tackle a broader range of security threats and vulnerabilities.

XR Devices as Virtual Testbeds

Alongside XR devices serving as tools for various security attacks, they can also be used to create realistic virtual testbeds. This idea is explored in academia by generating scenes in XR devices to understand attacker behaviors (see [P40] in Table 1) and test the proposed methods' usability (see [P41] in Table 1). VR-generated test environments provide remarkable similarities to real-world scenarios while addressing the shortcomings of in-person studies, such as overcoming ethical and legal constraints. Given their inherent flexibility, VEs are easily modifiable, making them ideal for such testing and educational scenarios.

Future Research Direction 2

Professionals across diverse disciplines can utilize the extended reality devices to generate realistic testbeds and evaluate their algorithms within a remarkably authentic, yet controlled, environment. Additionally, virtual environments can facilitate testing the usability and efficiency studies of the defense solutions on users.

Device Diversity in Security Testing

Researchers predominantly utilize the same devices to apply their findings. The most used products were HTC Vive and Meta Quest 2 due to their wide accessibility and general public use. Although we cannot assert that other devices not mentioned in this article are fully secure, we recommend that readers focus on OS characteristics or examine root causes of the vulnerabilities when understanding whether a type of attack is also applicable to their devices.

Future Research Direction 3

Future research should conduct security assessments using several devices, beyond just the popular ones. This way, more attack vectors can be uncovered, identifying new potential vulnerabilities in a rapidly developing field.

Design Considerations

This section presents practical guidelines from our study to help developers create safer, more secure XR devices.

Protection of Sensitive Data

The immersive experience XR technologies provide is made possible through the advanced sensors with which they are equipped. However, our findings highlight that XR devices pose security and privacy risks by collecting intrusive sensor data, which can also expand the attack surface for other devices.

Design Consideration 1

The accessibility of raw sensor data within extended reality device app development environments has established a notable threat model. Therefore, we recommend that developers of commonly used app development platforms (e.g., Unity and Unreal Engine) incorporate a default setting that limits the accessibility of users' raw data to independent app developers. Implementing such differential privacy measures would protect user data without compromising the app's performance.

Physical Input Methods

Input methods for sensitive data (e.g., passwords, text messages, and e-mails) are highly physical as users point their hands to a predefined location on a virtual keyboard. This opens up XR devices to numerous attacks, wherein an attacker will potentially extract users' key presses, or replicate the authentication method by observing their actions.

Design Consideration 2

To prevent attackers from inferring users' inputs, developers should utilize nonphysical input methods. Eye-tracking technologies could be used for users to enter their passwords, where they will enter their keys by looking at a key for a predetermined amount of time. Additionally, developers might consider methods like shuffling the keys of the keyboards to avoid virtual keyboard password-stealing attacks.

VE as a New Attack Vector

Security and privacy issues such as MITR attacks or inferring user passwords through user motions are specific to targeting the VE of a user.[5] While using XR devices, a user must continuously trust the environment generated by the devices. Hence, when an attacker targets the VE, the user who is fully immersed will be drastically affected.

Design Consideration 3

In the design phase of virtual environments (VEs) of virtual reality and mixed-reality devices, developers and device manufacturers should incorporate user feedback mechanisms. Utilizing insights from user studies on VEs, such as the one conducted by Lebeck et al. (see [P27] in Table 1), can provide an understanding of users' needs and expectations from VEs. Additionally, direct features like in-app surveys can be done to further enhance user security.

Vague Privacy Policies

Several vendors' privacy policies are not explicitly tailored to individual devices and fail to distinguish between the data collected when using an HMD and other scenarios. Moreover, in current privacy policies, there is no explicit identification of with whom among the partners, developers, domain administrators, or affiliated manufacturers the data are shared.

Design Consideration 4

Sensitive data collection by extended reality devices requires clear communication and transparency from developers and manufacturers to users. Therefore, manufacturers should make their privacy policies easily accessible and understandable, communicating transparently about data collection and management processes. Features like opt-out options and data collection indicators should be added.

In this article, we focused on the emerging technology of XR, conducting a comprehensive analysis of the security and privacy mechanisms of the devices currently dominating the market. Specifically, we provided an evidence-based approach where we analyzed the literature for security/privacy attacks on XR devices. We also highlighted the critical need to analyze attacks and defenses in the VE. Finally, we provided the lessons learned, which discussed the topics that could be further explored as future research, and suggested some design considerations for developers to improve the security and privacy of their applications. Overall, this article aims to help researchers understand what is currently needed as future defense directions and take appropriate measures. ■

Acknowledgment

We thank the anonymous reviewers and special issue editors for their helpful feedback and time. This research was supported, in part, by 1) the U.S. National Science Foundation (Award 2039606 and Award 2219920), Cyber Florida, Microsoft; 2) La Sapienza University of Rome within the 2020 Bando Ricerca project "Secure ANd PrivatE Information" sharing; and 3) Project "SERICS" (PE00000014) under the NRRP MUR program funded by the European Union-NGEU. The views expressed by the authors in this article are their own, not the funding entities.

References

1. "CSRankings: Computer science rankings," CSRankings, USA, Sep. 2023. [Online]. Available: https://csrankings.org/#/index?all&us
2. S. Stephenson et al., "SoK: Authentication in augmented and virtual reality," in *Proc. IEEE Symp. Security Privacy*, 2022, pp. 267–284, doi: 10.1109/SP46214.2022.9833742.
3. "Methodology of 'augmenting security and privacy in the virtual realm: An analysis of extended

reality devices'." GitHub. Accessed: Sep. 28, 2023. [Online]. Available: https://github.com/cslfiu/Augmenting_Security_and_Privacy_in_the_Virtual_Realm-Methodology

4. "Hand tracking privacy notice," *Meta*, Sep. 2023. Accessed: Sep. 21, 2023. [Online]. Available: https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/hand-tracking-privacy-notice/
5. "Introducing Vive tracker," *Vive*, Sep. 2023. Accessed: Sep. 21, 2023. [Online]. Available: https://www.vive.com/us/accessory/tracker3/
6. "Vive focus 3 eye tracker," *Vive*, Sep. 2023. [Online]. Available: https://business.vive.com/eu/product/vive-focus-3-eye-tracker/
7. "Natural facial expressions privacy notice," *Meta*, Sep. 2023. Accessed: Sep. 21, 2023. [Online]. Available: https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/natural-facial-expressions-privacy-notice/
8. "Use passthrough on meta quest," *Meta*, Sep. 2023. Accessed: Sep. 21, 2023. [Online]. Available: https://www.meta.com/help/quest/articles/in-vr-experiences/oculus-features/passthrough/
9. "Haptic feedback," *Meta*, Sep. 2023. Accessed: Sep. 21, 2023. [Online]. Available: https://developer.oculus.com/documentation/unity/unity-haptics/
10. Research Team. "'Big Brother': A new attack vector affecting metaverse security." ReasonLabs. Accessed: Sep. 21, 2023. [Online]. Available: https://reasonlabs.com/research/big-brother
11. H. Oz et al., "RøB: Ransomware over modern web browsers," presented at the 32nd USENIX Secur. Symp., Aug. 9–11, 2023.
12. F. Roesner, T. Kohno, and D. Molnar, "Security and privacy for augmented reality systems," *Commun. ACM*, vol. 57, no. 4, pp. 88–96, 2014, doi: 10.1145/2580723.2580730.
13. K. Ruth, T. Kohno, and F. Roesner, "Secure multi-user content sharing for augmented reality applications," presented at the 28th USENIX Secur. Symp., Aug. 14–16, 2019.
14. S. Rajaram et al., "Eliciting security & privacy-informed sharing techniques for multi-user augmented reality," in *Proc. CHI Conf. Human Factors Comput. Syst.*, 2023, pp. 1–17, doi: 10.1145/3544548.3581089.
15. T. Denning, Z. Dehlawi, and T. Kohno, "In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies," in *Proc. SIGCHI Conf. Human Factors Comput. Syst.*, 2014, pp. 2377–2386, doi: 10.1145/2556288.2557352.

Derin Cayir is pursuing her Ph.D. at Florida International University, Miami, FL 33174 USA, where she is currently a graduate research assistant in the Cyber-Physical Systems Security Lab. Her research interests include privacy/security systems for extended reality devices. Cayir received her bachelor's degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey. She is a Student Member of the IEEE Computer Society. Contact her at dcayi001@fiu.edu.

Abbas Acar is a postdoctoral associate in the Cyber-Physical Systems Security Lab at Florida International University, Miami, FL 33174 USA. His research interests include privacy-aware technologies, alternative authentication methods, and security/privacy issues related to the Internet of Things. Acar received his Ph.D. in electrical and computer engineering from Florida International University, USA. Contact him at aacar001@fiu.edu.

Riccardo Lazzeretti is an associate professor in engineering in computer science at Sapienza University of Rome, 00185 Rome, Italy. His research focuses on security and privacy, with a particular focus on the Internet of Things. Lazzeretti received his Ph.D. in information engineering from the University of Siena, Italy. He is a Senior Member of IEEE. Contact him at lazzeretti@diag.uniroma1.it.

Marco Angelini is an assistant professor of engineering in computer science at Sapienza University of Rome, 00185 Rome, Italy. His research interests include visual analytics, applied in the cybersecurity domain. Angelini received his Ph.D. in computer engineering from Sapienza University of Rome, Italy**.** Contact him at angelini@diag.uniroma1.it.

Mauro Conti is a full professor at the University of Padua, Padua, Italy, and he is also affiliated with the Delft University of Technology, Delft, The Netherlands, and the University of Washington, Seattle, USA. His main research interest is in the area of security and privacy. Conti received his Ph.D. in computer science from Sapienza University of Rome, Italy. He is a Fellow of IEEE, Asia-Pacific Artificial Intelligence Association, and Young Academy of Europe, and a senior member of the Association for Computing Machinery. Contact him at mauro.conti@unipd.it.

Selcuk Uluagac is an eminent scholar chaired professor in the Knight Foundation School of Computing and Information Science at Florida International University, Miami, FL 33174 USA, where he leads the Cyber-Physical Systems Security Lab. His research focuses on cybersecurity and privacy with practical and applied aspects. Uluagac received his Ph.D. in electrical and computer engineering from the Georgia Institute of Technology. Contact him at suluagac@fiu.edu.