2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct) | 979-8-3315-0691-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISMAR-Adjunct64951.2024.00017

Breaking the Virtual Barrier of Exploit Chain Attacks in XR Systems

Asif Uz Zaman Asif*
Colorado State University,
Fort Collins, CO 80523,
USA

Meera Sridhar†
University of North Carolina,
Charlotte, NC 28223,
USA

Indrakshi Ray‡
Colorado State University,
Fort Collins, CO 80523,
USA

Francisco R. Ortega§
Colorado State University,
Fort Collins, CO 80523,
USA

Abstract

Extended Reality (XR) is an emerging technology that will soon be a ubiquitous part of daily life. However, the security of these systems remains a major concern as attackers can target these systems and get vital information about the user. XR systems integrate advanced sensors that are capable of collecting identifiable data of a user which can have devastating effects. One particularly concerning threat is exploit chain attacks are attacks that use chains of multiple exploits to compromise a system. Given the history of similar attacks on Android systems and the fact that a lot of XR headsets run some version of Android, this vulnerability is especially relevant. In this position paper, we examine the potential problems associated with exploit chain attacks on XR headsets.

Index Terms: Extended Reality, Augmented Reality, Virtual Reality, Exploit Chain Attacks

1 Introduction

Exploit chain attacks are chains of multiple exploits that compromise a system's vulnerabilities by linking multiple exploits to target specific components of the system itself in a specific order. These attacks are different from regular exploits that target a single system vulnerability because they use exploit chains to launch attacks that target multiple small vulnerabilities in the system, ultimately compromising the entire system and taking control of it [2]. These kinds of attacks typically use the trust relationship within a system to get beyond security measures and use exploit primitives, which are specialized methods that work best when combined with other exploits or in a particular setting. Since this kind of attack is still in its early stages, not much information about it is known to the general public [17]. However, protection mechanisms must be implemented immediately because these attacks, if launched, will have catastrophic repercussions. In our position paper, we examine the impact of exploit chain attacks on XR, which includes augmented and virtual reality (AR,VR) systems.

The largest question regarding security is that XR head-mounted displays (HMDs) provide a different set of larger challenges in terms of security compared to phones, computers, and other existing systems. One of the reasons is that the user is actively wearing them (e.g., it is very likely in the future that AR glasses will be used for long periods of time if not all day). Another reason is that attacks could affect perception and degrade performance without the user even knowing it. This may be especially true if Social VR (e.g., Meta New Horizons) becomes as popular with young kids as Roblox is today [12, 14, 1]. This position XR-HMDs create new security challenges. Our position paper describes one attack, and it hopes to bring awareness and discussion to the attack described in this paper but also the larger set of challenges facing XR security.

*e-mail: asif09@colostate.edu
†e-mail: msridhar@charlotte.edu
‡e-mail: indrakshi.ray@colostate.edu
§e-mail: f.ortega@colostate.edu

2 Current Software stack of XR devices

Four parts make up the XR headset's current software stack as shown in Fig. 1: Software Development Kit (SKD), Game Engine, Application Programming Interfaces (API), and Runtime and Compositors. SDKs, which offer frameworks, APIs, and resources for building VR applications, are crucial tools for XR development. OpenVR SDK (which supports the HTC Vive), Oculus SDK (which supports the Oculus Rift and Quest devices), Google VR SDK (which supports Google Cardboard), and PlayStation VR Dev Kit (which supports the Sony PlayStation VR) are a few of the well-known SDKs. Unity and Unreal Engine are two well-known game engines that developers can use to create immersive XR games. Game engines are an essential component of XR experiences. These game engines are integrated SDKs to offer interactive 3D environment creation tools. Conversely, APIs enable various XR headset components to connect with one another. Two well-known APIs are OculusAPI (for Oculus devices) and OpenAPI (developed for SteamVR). Lastly, platform elements like safety borders, system menus, and handling numerous XR apps are managed by the Runtime and Compositors.

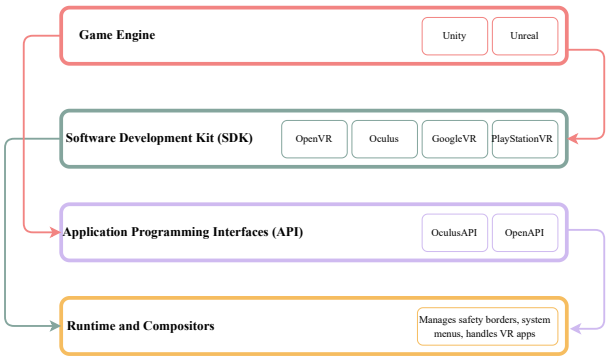

Figure 1: Software stack for XR devices with four major components: Game Engine, SDK, API, and Runtime and Compositors.

3 Security concerns

In this section, we will describe our approach to generating exploits for XR research, as well as investigate the exploit chain for Android devices and some of the current Common Vulnerabilities and Exposures (CVE)s that exist for XR devices.

3.1 Exploits for AR Research

Our work is inspired by the work done by Yang et al. [20] where they cloned two legitimate apps by doing that the authors were able to alter the data that was displayed in the HMDs as well as eavesdrop on live communication. The authors in this work replicated the user environment to avoid detection. Therefore, we want to first develop an exploit for man-in-the-middle (MITM) for the XR system and then identify the vulnerabilities that can be used to prepare exploit chains for XR-HMDs.

2771-1110/24/$31.00 ©2024 IEEE
DOI 10.1109/ISMAR-Adjunct64951.2024.00017

Developing a MITM [7] exploit entails intercepting and alternating the communication between two parties. By doing this, we seek to gain a deeper understanding of the system's security and strategies for enhancing it. To take control of the session, we will use Packet Sniffing and Session Hijacking to intercept and alter the two parties' communication. We can perform this export in a controlled environment with the help of a program called Wireshark. A network protocol that can gather and show packet data makes it crucial for packet sniffing. Additionally, OVRseen [18] can be used to capture and decrypt network traffic.

3.2 Exploit Chains in Android

Since Android (or a flavor of it) is the operating system used by the majority of XR mobile devices (e.g., Quest 3), XR systems are also susceptible to vulnerabilities that are now present in Android systems. Since Android systems have been in use for so long, there are many known vulnerabilities in them, some of which have already been fixed, but with each new update, new vulnerabilities are introduced that have not been found yet. Attacks on XR systems have the potential to be extremely damaging, especially when they target VR systems where the user is fully submerged in the virtual world and is, therefore, unaware of their surroundings. Should an attacker gain access to the system, they might initiate attacks that could cause motion sickness in the user or even relocate them to a new location, which could put the user in danger. Attackers can also decrease the frame rate of the user, which can impair the task that a user is accomplishing in the VR environment.

3.3 Prior CVEs in XR

There are existing vulnerabilities that are present within the XR systems CVE-2024-21625 [10], CVE-2019-3562 [8], CVE-2021-24038 [9], and CVE-2024-27812 [11] to name a few.

A high-severity vulnerability known as CVE-2024-21625 affects the SideQuest desktop program which is required to download virtual reality apps for Oculus Quest. This vulnerability results from deep link URLs in versions earlier than 0.10.35 which did not have been properly sanitized. These deep links can take action inside the application from web content by utilizing the custom sidequest:// protocol.

On the other hand, CVE-2019-3562 affects Oculus Browser versions 5.2.7 to 5.7.11 because of this flaw the user interface of a browser can be altered by a remote web page to inject arbitrary HTML code into the browser's user interface. An attacker might therefore be able to execute malicious code and impersonate the user interface.

Furthermore, CVE-2021-24038 was discovered in Oculus Desktop software versions that came out after 1.39 and before 31.1.0.67.507. A bug in the management of handles OOVRServiceLauncher.exe causes this vulnerability. Local privilege escalation may occur as a result of this bug which allows an attacker to have higher-level privileges than they should have which could jeopardize the security of the system.

Additionally, CVE-2024-27812 is the vulnerability with Apple's visionOS specifically affecting the Apple Vision Pro. The WebKit component was found to be the source of the problem where processing specially crafted web content could result in a denial-of-service (DoS) event. Because of how the WebKit framework handles some file operations incorrectly this vulnerability exists.

4 Related Work

In this section, we will look at the privacy concerns, and vulnerabilities present in the XR-HMDs as well as the prior research done in the field of Android devices.

4.1 Common Privacy Concerns with XR-HMDs

Bystander privacy [15], which refers to the privacy of someone who is not actively participating in an XR environment but is present in the same room as someone else wearing an XR-HMD, is a major issue with XR systems that is challenging to address. This is because the sophisticated sensors on the XR-HMDs have the ability to record and capture sensitive information that is present in the surrounding environment [13]. When someone wears a headset, the privacy of others may ultimately be compromised because these devices have the ability to record audio and video streams and upload the sensitive to the cloud. Thus, when attackers compromise cloud storage, they can access the data and exploit the information they have discovered.

4.2 Vulnerabilities present XR-HMDs

Numerous issues with the current system have been brought to light by this area of research. Guo et al. [4] found problems with the Oculus VR applications' security and privacy policies. Excessive permissions were requested by programs that were not required for their operation. Examples of insufficient data security protocols were also noted, raising the possibility of unauthorized access to user information. In this field, another intriguing study by Luo et al. [6] showed that it is feasible to accurately deduce keystrokes from the sound emissions of gaming controllers to a considerable extent. The methods used entailed recording the sound waves generated when buttons on different (Xbox and PlayStation) game controllers were pressed. After that, the researchers used machine learning techniques to evaluate these signals in order to detect and classify particular keystrokes. Kumarapeli et al. [5] looked at the potential privacy hazards associated with leveraging behavioral data for user identification in VR environments. The integration of state-of-the-art tracking sensors into contemporary VR technology has significantly enhanced user immersion and data richness. This study investigated the accuracy with which machine learning algorithms recognize VR users across a range of tasks and sessions, including scenarios in which users deliberately alter their behavior to evade detection. It also examined how users' physical characteristics impact the accuracy of these algorithms. The results of the study show that, using behavioral data, VR users may be reliably recognized.

4.3 Exploit Chain in Android Devices

Because exploit chains are a new concern, researchers are already looking into the potential effects that these kinds of attacks may have on a system. A prototype system named AppChainer is offered by Xiang et al. [19], which explores the idea of chaining several vulnerabilities within Android applications. AppChainer seeks to determine and assess the payload's chainability. This system looks for possible attack surfaces and assesses whether the payload that enters them can be combined with other payloads to create an exploit chain. Guang [3] showed that even with the notable advancements in security for contemporary Android systems, it is feasible to create an exploit chain by taking advantage of several vulnerabilities. The authors concentrate on the TiYunZong exploit chain, which circumvents conventional exploitation strategies like return-oriented programming (ROP) by employing different approaches such data attacks and the use of JavaScript interfaces.

From the literature, we have found evidence that in the current state, the XR-HMDs have security vulnerabilities, and therefore there is a need to make this space more secure and robust for the end user. The current lack within this field motivated us to look at the vulnerabilities present in the realm of the XR ecosystem.

5 Position: Security concerns for exploit chains in future AR systems

XR researchers and related fields (e.g., optics) continue to improve XR-HMDs that one day will become as pervasive as the smartphone has become. Assuming that people would be wearing glasses with AR capabilities for their day-to-day activity for long periods of time and with ubiquitous VR for different types of immersive experiences (which is a lot closer than AR glasses), the security challenges will rise and can have major impacts. The authors of these position papers believe that XR will continue to get smaller, lighter, and more capable, becoming a true multi-purpose device, as the phone is today. The devices are expected to follow a model where the HMD is the edge node, the edge, and the cloud, all working at different capabilities, with AI being the center of these devices. If security, such as the one described, is not addressed for the particular use cases that XR has and for the future of general-purpose XR, it may have unintended consequences with great risks for users. In the words by Dr. Alan Kay, "The best way to predict the future is to invent it," [16], let's invent an XR ecosystem with security and privacy in mind.

References

[1] eMarketer Editors. Meta's horizon worlds opens to teens, sparking debate. 2023. 1

[2] GitHub Security Lab. One day short of a full chain: Real world exploit chains explained. https://github.blog/2021-03-24-real-world-exploit-chains-explained/, 2021. Accessed: July 28, 2024. 1

[3] G. Guang. An exploit chain to remotely root modern android devices. https://github.com/secmob/TiYunZong-An-Exploit-Chain-to-Remotely-Root-Modern-Android-Devices/blob/master/us-20-Gong-TiYunZong-An-Exploit-Chain-to-Remotely-Root-Modern-Android-Devices-wp.pdf, 2021. 2

[4] H. Guo, H.-N. Dai, X. Luo, Z. Zheng, G. Xu, and F. He. An empirical study on oculus virtual reality applications: Security and privacy perspectives. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, pp. 1–13, 2024. 2

[5] D. Kumarapeli, S. Jung, and R. W. Lindeman. Privacy threats of behaviour identity detection in vr. *Frontiers in Virtual Reality*, 5:1197547, 2024. 2

[6] S. Luo, A. Nguyen, H. Farooq, K. Sun, and Z. Yan. Eavesdropping on controller acoustic emanation for keystroke inference attack in virtual reality. In *The Network and Distributed System Security Symposium (NDSS)*, 2024. 2

[7] A. Mallik. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2(2):109–134, 2019. 2

[8] National Vulnerability Database. Cve-2019-3562: Vulnerability detail, 2019. Accessed: 2024-07-29. 2

[9] National Vulnerability Database. Cve-2021-24038: Vulnerability detail, 2021. Accessed: 2024-07-29. 2

[10] National Vulnerability Database. Cve-2024-21625: Vulnerability detail, 2024. Accessed: 2024-07-29. 2

[11] National Vulnerability Database. Cve-2024-27812: Vulnerability detail, 2024. Accessed: 2024-07-29. 2

[12] M. News. Meta opens horizon worlds to children - a risky move. 2024. 1

[13] T. Ni. Sensor security in virtual reality: Exploration and mitigation. In *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services*, pp. 758–759, 2024. 2

[14] W. Oremus. Kids are flocking to facebook's "metaverse." experts worry predators will follow. *The Washington Post*, 2022. 1

[15] S. Pahi and C. Schroeder. Extended privacy for extended reality: Xr technology has 99 problems and privacy is several of them. *Notre Dame J. on Emerging Tech.*, 4:1, 2023. 2

[16] I. Piumarta and K. Rose, eds. *Points of View: A Tribute to Alan Kay*. Viewpoints Research Institute, Inc., Glendale, California, 2010. 3

[17] TechOne IT. What is a zero-day exploit chain?, 2024. Accessed on July 28, 2024. 1

[18] R. Trimananda, H. Le, H. Cui, J. T. Ho, A. Shuba, and A. Markopoulou. {OVRseen}: Auditing network traffic and privacy policies in oculus {VR}. In *31st USENIX security symposium (USENIX security 22)*, pp. 3789–3806, 2022. 2

[19] X. Xiang, Y. Jiang, Q. Guo, X. Zhang, X. Gong, and B. Liu. Appchainer: investigating the chainability among payloads in android applications. *Cybersecurity*, 6(1):16, 2023. 2

[20] Z. Yang, C. Y. Li, A. Bhalla, B. Y. Zhao, and H. Zheng. Inception attacks: Immersive hijacking in virtual reality systems. *arXiv preprint arXiv:2403.05721*, 2024. 1