Sensor Security in Virtual Reality: Exploration and Mitigation

Tao Ni
City University of Hong Kong
taoni2-c@my.cityu.edu.hk

ABSTRACT

Virtual Reality (VR) technology, extensively utilized in gaming, social networking, and online collaboration, has raised significant security concerns due to the array of sensors integrated into VR headsets. This paper discusses several of our ongoing research that explore sensor vulnerabilities within VR headsets and proposes appropriate mitigation strategies. Specifically, we focus on three types of embedded sensors in VR headsets: unrestricted motion sensors, optical sensors, and eye-tracking sensors. Our investigation outlines the potential attacks exploiting these sensor vulnerabilities, which could result in privacy leakage and malicious signal injections. Furthermore, we detail the design and implementation of effective countermeasures to defend against these threats.

CCS CONCEPTS

• **Security and privacy → Embedded systems security**; **Side-channel analysis and countermeasures**.

KEYWORDS

Sensor Security, Virtual Reality, Attacks, Countermeasures

ACM Reference Format:
Tao Ni. 2024. Sensor Security in Virtual Reality: Exploration and Mitigation. In *The 22nd Annual International Conference on Mobile Systems, Applications and Services (MOBISYS '24), June 3–7, 2024, Minato-ku, Tokyo, Japan.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3643832.3661389

1 INTRODUCTION

Virtual Reality (VR) technologies have been growing exponentially over the past decade, attributed to their unparalleled ability to create immersive experiences without physical constraints. Beyond supporting a variety of VR games, VR technology brings innovations across a wide spectrum of fields, such as medical training, financial services, health and fitness, ecotourism, and online collaboration in virtual environments. These versatile functionalities suggest that VR plays an essential role as a next-generation mobile platform.

A typical VR system (*e.g.*, Meta Oculus Quest, HTC Vive, PICO) usually contains a head-mounted display (HMD) VR headset to render virtual scenes, and two controllers to facilitate interactions between the user and the virtual environments. Similar to smartphones, Figure 1 shows the VR system also integrates multiple sensors, *i.e.*, optical, motion, and eye-tracking sensors, to track the user's position and body movements. In particular, the newly-released Apple Vision Pro presents a controller-free manner in user-VR interactions by leveraging 12 cameras embedded on its headset to achieve accurate position tracking and gesture recognition.

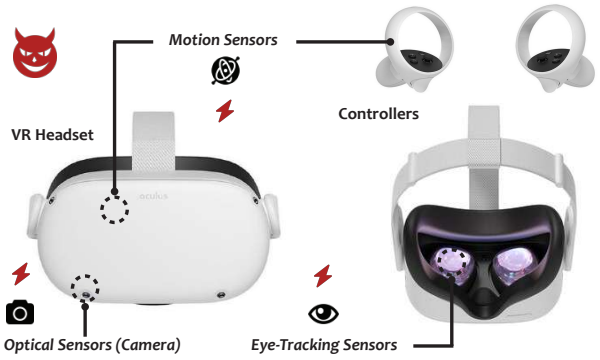

Figure 1: Illustration of embedded sensors in Meta Oculus Quest 2 VR headset and hand controllers.

However, the close relationship between VR and other mobile devices makes VR susceptible to similar sensor security issues and vulnerabilities. For instance, recent studies show motion sensors such as accelerometers and gyroscopes in VR headsets could be maliciously exploited to uncover user privacy like passwords [14, 16] and user's vital signals [15]. To take a further step in studying sensor security in VR platforms, we aim to comprehensively explore vulnerabilities in sensors embedded in VR devices and propose effective countermeasures to mitigate the threats. Specifically, we investigate security issues of embedded sensors in VR from two aspects: *(i)* privacy leakage from sensor-enabled functionalities, and *(ii)* potential attack surfaces for malicious injections.

- **Privacy Leakage.** Since multiple sensors are involved in users' interactions with the VR headset, physical signals leaked from the embedded sensors may carry privacy information that could be exploited for inferring user privacy, *i.e.*, electromagnetic (EM) signals used for image reconstruction [10], acoustic signals [5] and power traces [8] for keystroke inference.
- **Malicious Injection.** Sensor spoofing attacks are prevalent in mobile platforms, including VR devices. In these scenarios, attackers can manipulate sensor-enabled functionalities by injecting malicious signals. For instance, inaudibly manipulating voice assistants [7] or interfering with image transmissions [2].

2 EXPLORATION AND MITIGATION

Below, we summarize three of our ongoing works that aim to explore vulnerabilities of embedded sensors in VR devices, as well as the corresponding mitigation methods to protect user privacy.

(I) Unrestricted Motion Sensors. We investigate the motion sensors (*e.g.*, accelerometer, gyroscope) integrated into the VR headset

MOBISYS '24, June 3–7, 2024, Minato-ku, Tokyo, Japan

ACM ISBN 979-8-4007-0581-6/24/06…$15.00
https://doi.org/10.1145/3643832.3661389

and controllers for position-tracking on three mainstream VR development platforms (*e.g.*, OpenVR [13], Oculus [12]), where we find the user permission of these motion sensors is unrestricted [14]. Attackers could compromise the VR headset and install malware to access data from these unrestricted motion sensors to further infer sensitive user privacy, *i.e.*, passwords through the virtual keyboard [14], videos playing in the virtual scenes [6], and even spatial mesh of surrounding environments [16].

We propose two countermeasures to mitigate threats from unrestricted motion sensors. *(i) Permission-based and Privacy-aware Sensor Management:* One potential countermeasure is to implement a permission-based and privacy-aware framework in VR platforms with a customized sensor access policy that requires the VR user to grant permission to the usage of these motion sensors when installing specific apps [14]. *(ii) Shuffling Virtual Keyboard:* Another approach is to implement shuffling virtual keyboards with random layouts in VR applications, which could obfuscate keystroke inference attacks from these motion sensor data.

(II) Optical Sensors. To track the position and movements of the two controllers, a VR headset usually integrates with multiple optical sensors (*e.g.*, cameras), *i.e.*, Apple Vision Pro features a total of 12 cameras. In particular, we discover that these embedded cameras are vulnerable to side-channel attacks, leading to potential privacy leakage and malicious injections. For instance, cameras usually convert digital images to current traces for transmitting to processing units, and this process inevitably emits electromagnetic (EM) emanations that can be captured by adversaries to reconstruct high-quality image streams [4]. Furthermore, attackers can also leverage intentional electromagnetic interference (IEMI) to inject modulated EM signal to interfere with the image transmission [2].

To defend against attacks on VR headset cameras, we summarize two directions from both hardware and software perspectives. *(i) Shielding EM Emanations:* VR device manufacturers could redesign the headset by adding extra shields [9, 11] on cameras to create a Faraday cage to prevent the EM emanations from being captured by adversaries. *(ii) Random Noise Obfuscations:* VR system dynamically generates random EM noise from other components (*e.g.*, sensors, CPU/GPU) to obfuscate the EM emanations from cameras.

(III) Eye-Tracking Sensors. Commodity VR headsets contain eye-tracking sensors to monitor the trajectory of gaze points to support gaze interactions with virtual scenes. Nevertheless, real-time gaze movements are sensitive biometric information of the VR user. Attackers could exploit malware to obtain gaze data to infer user identity and uncover fine-grained visual behaviors [3].

To prevent privacy leakage from eye-tracking sensors, we also propose two effective approaches. *(i) Second-factor Authentication.* We can design and implement a second-factor authentication mechanism in VR systems to validate the authorization of the user [1], *i.e.*, leveraging biometric characteristics like the auditory-pupillary response [17]. *(ii) Gaze Encryption.* We propose an encryption/decryption to prevent meta-data leakage from the gaze information.

3 CONCLUSIONS AND FUTURE WORKS

In this paper, we introduce security concerns of embedded sensors in commodity VR devices. Specifically, we have revealed vulnerabilities in unrestricted motion sensors, optical sensors, and eye-tracking sensors integrated with VR headsets and propose corresponding countermeasures to mitigate their threats.

Here we discuss some future work. *First*, we will explore different attacks that exploit side-channel information, such as vibrations and acoustic signals from the VR headset. *Second*, we will design and implement privacy-preserving countermeasures from the software-defined aspect to achieve a more general defense. *Finally*, we will share our findings with VR manufacturers and users to raise public awareness of the potential risks of embedded sensors in VR devices.

REFERENCES

[1] Yongliang Chen, Tao Ni, Weitao Xu, and Tao Gu. 2022. SwipePass: Acoustic-based second-factor user authentication for smartphones. *Proceedings of the ACM IMWUT* (2022).

[2] Qinhong Jiang, Xiaoyu Ji, Chen Yan, Zhixin Xie, Haina Lou, and Wenyuan Xu. 2023. GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI. In *Proceedings of USENIX Security*.

[3] Guohao Lan, Bailey Heit, Tim Scargill, and Maria Gorlatova. 2020. GazeGraph: Graph-based few-shot cognitive context sensing from human visual behavior. In *Proceedings of ACM SenSys*.

[4] Yan Long, Qinhong Jiang, Chen Yan, Tobias Alam, Xiaoyu Ji, Wenyuan Xu, and Kevin Fu. 2024. EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. In *Proceedings of ACM NDSS*.

[5] Shiqing Luo, Anh Nguyen, Hafsa Farooq, Kun Sun, and Zhisheng Yan. 2024. Eavesdropping on Controller Acoustic Emanation for Keystroke Inference Attack in Virtual Reality. In *Proceedings of NDSS*.

[6] Anh Nguyen, Xiaokuan Zhang, and Zhisheng Yan. 2024. Penetration Vision through Virtual Reality Headsets: Identifying 360 Videos from Head Movements. In *Proceedings of USENIX Security*.

[7] Tao Ni, Yongliang Chen, Weitao Xu, Lei Xue, and Qingchuan Zhao. 2023. XPorter: A Study of the Multi-Port Charger Security on Privacy Leakage and Voice Injection. In *Proceedings of ACM MobiCom*.

[8] Tao Ni, Guohao Lan, Jia Wang, Qingchuan Zhao, and Weitao Xu. 2023. Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting. In *Proceedings of USENIX Security*.

[9] Tao Ni, Jianfeng Li, Xiaokuan Zhang, Chaoshun Zuo, Wubing Wang, Weitao Xu, Xiapu Luo, and Qingchuan Zhao. 2023. Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning. In *Proceedings of ACM MobiCom*.

[10] Tao Ni, Xiaokuan Zhang, and Qingchuan Zhao. 2023. Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel. In *Proceedings of ACM CCS*.

[11] Tao Ni, Xiaokuan Zhang, Chaoshun Zuo, Jianfeng Li, Zhenyu Yan, Wubing Wang, Weitao Xu, Xiapu Luo, and Qingchuan Zhao. 2023. Uncovering user interactions on smartphones via contactless wireless charging side channels. In *Proceedings of IEEE S&P*.

[12] Meta Quest. 2023. https://www.oculus.com/experiences/quest.

[13] Valve Software. 2023. OpenVR SDK. https://github.com/ValveSoftware/openvr.

[14] Yi Wu, Cong Shi, Tianfang Zhang, Payton Walker, Jian Liu, Nitesh Saxena, and Yingying Chen. 2023. Privacy leakage via unrestricted motion-position sensors in the age of virtual reality: A study of snooping typed input on virtual keyboards. In *Proceedings of IEEE S&P*.

[15] Tianfang Zhang, Zhengkun Ye, Ahmed Tanvir Mahdad, Md Mojibur Rahman Redoy Akanda, Cong Shi, Yan Wang, Nitesh Saxena, and Yingying Chen. 2023. FaceReader: Unobtrusively Mining Vital Signs and Vital Sign Embedded Sensitive Info via AR/VR Motion Sensors. In *Proceedings of ACM CCS*.

[16] Yicheng Zhang, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh. 2023. It's all in your head (set): Side-channel attacks on AR/VR systems. In *Proceedings of USENIX Security*.

[17] Huadi Zhu, Mingyan Xiao, Demoria Sherman, and Ming Li. 2023. SoundLock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response.. In *Proceedings of NDSS*.

SHORT BIO

Tao Ni is currently a Ph.D. candidate at the Department of Computer Science, City University of Hong Kong. His research interests are focused on exploring security and privacy in cyber-physical systems (CPS), uncovering potential side-channel attacks, and developing privacy-preserving defense mechanisms.