The Unconcealed Network of OVR Voice Assistant: A Cyber Attack Prospect

Arpita Dinesh Sarang
SysCore Lab, Department of Information Security, and Convergence Engineering for Intelligent Drone,
Sejong University,
Seoul 05006, South Korea
arpitasarang98@gmail.com

Sang-Hoon Choi
SysCore Lab,
Sejong University,
Seoul 05006, South Korea
csh0052@gmail.com

Ki-Woong Park*
Department of Information Security, and Convergence Engineering for Intelligent Drone,
Sejong University,
Seoul 05006, South Korea
woongbak@sejong.ac.kr

***Abstract*—The Metaverse is a socially influential platform that offers XR (Extended Reality) users access to multitudinous applications such as a website, a web application, or a desktop program. The handheld controllers, gestures, or voice commands are typically used by the XR-Users to navigate and access these applications. Considering voice commands are the fastest, they are used the most these days. We undertook an attempt to evaluate the security of voice commands for navigating browsers in the Metaverse to access websites. We studied the network analysis trends in depth for virtual environments. We observed URL (Uniform Resource Locator) whitelisting when performing tests on the Oculus Quest 2 voice assistant. We conducted partial network analysis on the network traffic collected during the URL voice command request processing using the OVR (Oculus Virtual Reality) device. With this partial network analysis of the network traffic, we propose a threat model for the OVR voice assistant for processing URLs. We convey, whether voice commands are secure even though they utilize URL whitelisting as a disguise through our research.**

Keywords—Metaverse, Speech Recognition, Network Analysis, Cyber Security, IoT(*Internet of Things****), AI(****Artificial Intelligence****)***

I. INTRODUCTION

Metaverse that we access using IoT(Internet of Things) devices such as the Head Mounted Display(HMD) or the VR(Virtual Reality) glasses has allowed the XR Users to gain unrealistic experiences. These experiences have been a luxury for users as they made the tasks over the computer fascinatingly pleasurable by taking the user to an artificial self-designed world through IoT devices. The term "Metaverse" describes a collective space developed from the merging of the digital and virtually enhanced real worlds for XR users. There is multifaceted research that provides an overview of definitions of the metaverse, the ideologies and underlying technologies required for the metaverse, and how and where the metaverse is employed for specific domains [1]. This multiple employment of the metaverse requires a combination of multiple technologies, especially the newly released technologies to make it more advanced for the future of virtual reality. This adds newer components to the metaverse infrastructure which raises concerns for the security and data privacy of the virtual world and XR users. These security concerns are highly discussed in the SARANG(Simplified Avatar Relationship Association with Non-linear Gradient) framework and tend to increase over time [2]. A proposed security architecture focuses on three crucial elements: intrusion detection systems (IDS), user authentication, and digital asset security, with a particular focus on blockchain technology and non-fungible tokens (NFTs) [13]. An investigation of metaverse threat vectors, such as cross-reality attacks, social engineering, decentralised application vulnerabilities, and synthesised media, is based on a security architecture that is presented [14]. With the incline in cybercrimes and cyber warfare in the metaverse, new cyber threats have appeared [15]. Two such latest components, the AI(Artificial Intelligence) technologies and the 6G(Sixth Generation) Network are hyped for consumption in the metaverse by challenges and research gaps [3]. The Network component plays an important role in the metaverse for connecting the components of the Metaverse infrastructure and the resources. The exchange of all kinds of data occurs through the network such as user to application, and application to application. Having a secure network transmission of data that includes user-sensitive or environment sustainability information is a necessity.

In our scenario, we examine the network transmission that occurs when a user utilises voice commands to traverse and access browser websites. When compared to alternative methods like gestures or portable devices, voice commands are typically the most convenient way to navigate the metaverse. However, in order to increase its usability, different voice assistant architectures are introduced [4]. Therefore, we examine the network's security while interpreting voice commands as it is novice to the metaverse infrastructure. We conducted a thorough investigation of packet data decryption, packet payload exploitation, and network packet sniffing. We contributed by outlining the threat model to ensure that no packets are being sniffed and to prevent cyber-attacks and other future breaches. We performed our tests on the OVR(Oculus Virtual Reality) device Quest 2 version.

The following is the remaining paper flow: Background information and current developments in network-based exploitation and network analysis are presented in Section II. In Section III, we illustrate our threat model for using voice commands in Metaverse to access the browser. In Section IV,

* Corresponding author

we conclude our research regarding the security of the Metaverse.

II. Related Work

The 5G(fifth generation) network technology, which offers high bandwidth and low latency, is now being utilized in the Metaverse. Additionally, it will function with recently developed 6G networks. This high-speed network will provide efficient data transmission and performance between Metaverse infrastructure components. High-speed data transmission and processing have evolved these networks, yet security standards are neglected in favour of performance. The Confidentiality, Integrity and Availability(CIA) of Networks have shown low preference in the development of Metaverse. This will result in network-based cyberattacks against the metaverse.

URLs are exploited to attack users, systems, and networks, including spam, malware and phishing. Through URLs, data is requested and malware is shared in response over the Network [5]. By extracting motion data from network packets and plotting it to keystroke records, attacks like remote keylogging have proven feasible [6]. Blind message attacks may be possible when network packet data is exposed, even in partial on Metaverse[7]. We determine Metaverse to be a potential target for cyber-attacks that lead to poor experience, exploitation of data privacy and unauthorised access to XR user resources.

A. *Network Traffic Analysis*

In the event that the network packet data is not properly encapsulated, network-based attacks could occur on Metaverse. There are multiple network classification techniques based on Machine Learning(ML) that help us perform network packet analysis [11]. On the contrary, detecting the imbalance in network traffic i.e. monitoring malicious behaviour is also being researched [12]. The payload and packet data are the two components that make up a network packet. In Figure 1, the Decoded Network packet structure is depicted for voice command through OVR. In this network packet, cells that are coloured orange to green are the payload for the packet. It consists of the packet's source and destination IP(Internet Protocol) and transmission port number, protocol, identification number, and timestamp. Whereas, the yellow cells depict the data or query of the user. As the query or data may contain sensitive user information or metaverse sustainability data. Figure 2, shows source destinations to which network packets traverse during communication with other servers for a voice command request. An attacker with packet sniffing skills can analyze and use cyber-attacks by using network packet data.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
02	A5	54	E8	3F	32	80	F3	EF	3C	FC	1B	08	45	00	00
00	40	85	76	40	00	40	11	21	D8	C0	A8	89	0C	C0	A8
89	01	DC	D4	00	35	00	2C	2A	BF	01	2C	01	00	00	01
00	00	00	00	00	00	05	67	72	61	70	68	08	66	61	63
65	62	6F	6F	6B	03	63	6F	6D	00	00	01	00	01		

Fig 1. Network Packet for OVR Voice Command

B. *URL Whitelisting for Voice Command*

The practice of whitelisting URLs is not something novel. The corporate firm devices still utilise URL whitelisting, for example, to prevent employees from visiting banned websites and to limit their access to whitelisted URLs.

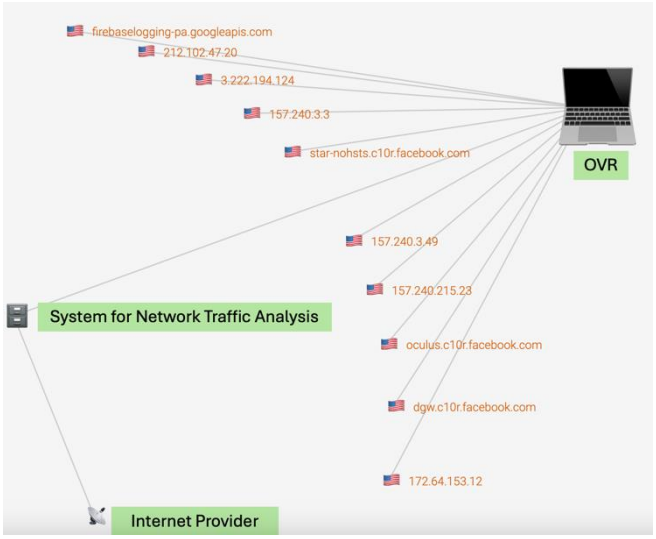

Fig 2. OVR Network Packet communication with other servers

We can combine URL features to prevent other URL use once a URL has been whitelisted [8]. The OVR Quest 2, tends to follow URL whitelisting to intercept the voice assistant application misinterpreting voice command. We observed only the whitelisted commands were accessible through voice assistant and redirected to browser webpages. Whereas the exclusive URLs were not redirected to the browser instead led to Horizon App and prompted as "Not found". Consumption of this technique increased the Voice Assistant's efficiency in Speech Recognition and reduced the chances of unexpected malicious website access. Manual search in the browser allows access to excluded sites.

Therefore, we examine the OVR Voice Assistant by providing both a whitelisted URL and a Non-whitelisted URL. When the whitelisted URL is accessible we performed network analysis to inspect the security of data transmitted.

III. Proposed Threat Model for OVR Voice Assitant

To make the threat model more facile to understand, we have divided this part into two subsections. We embark on test setup and observation in subsection A. Additionally, we explain our threat model in subsection B.

A. *Methodology*

We constructed a virtual network environment and connected OVR Quest 2 to conduct our testing in order to demonstrate that the attack is feasible by taking advantage of the network packet data for URLs accessed with voice commands.

We attempted to use the voice commands to retrieve the URLs, which were supposed to direct users to the browser and provide the web pages they had requested. Rather than

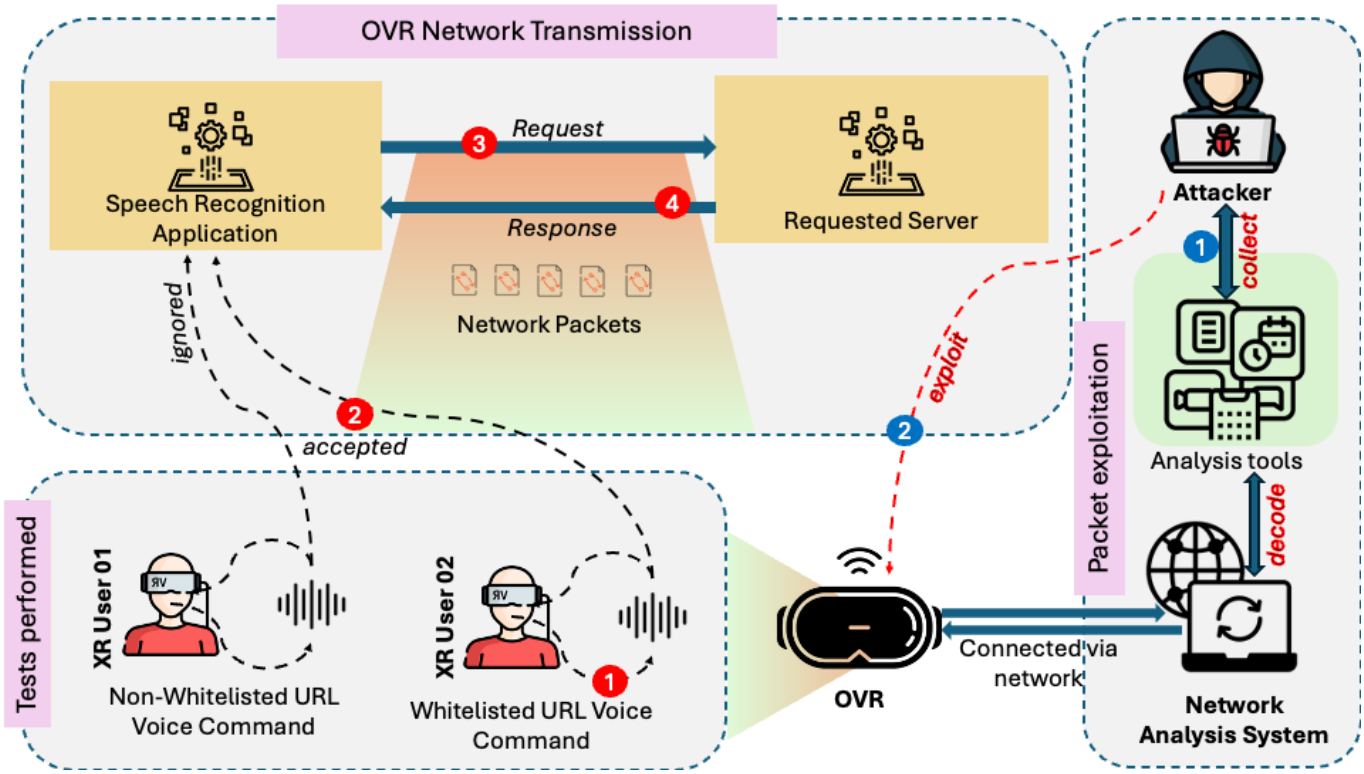

Fig 3. OVR voice assistant-based URL access network security

responding to the voice commands, the HTTP (Hyper Text Transfer Protocol) URL queries were ignored. Phishing websites like "Pacebook.com" and dangerous URLs like "torrent.com" were ignored too. The XR user was redirected to Horizon Finder and prompted “This is what we found” with no search result when tried accessing these URLs. However, to legitimate and secure URLs such as "facebook.com" or "Youtube.com" through voice commands the XR user was redirected to the browser. During these tests, we developed the assumption that the OVR Voice Assistant used a list of URLs whitelisted in order to prevent XR users from navigating to malicious or insecure websites and to improve the efficiency of speech recognition software in processing URL voice command requests by preventing misinterpretations that lead to malicious websites.

In order to assess the security of the voice assistant technology used in the OVR, we attempted to record the network traffic for this situation. The voice command requests and responses to network traffic for OVR URLs were recorded. We conducted a partial analysis of the network packet payload using tools such as Wireshark, Hex decoder and A-packets, assuming that additional decryption of the data may be achieved through the use of a framework like OVRseen [9], which bypasses the SSL/TLS certification for websites in favour of network analysis tools. This will assist us in fully decoding a network packet.

The attacker can use the ability to decode network packets and conduct a thorough analysis to obtain data and patterns in an identical way they would attack XR users.

B. Proposed Threat Model

Our Proposed Threat Model in Figure 3, depicts the OVR voice assistant-based URL access network security. In which we partially evaluate the attack scenario by learning the workflow and performing a network packet analysis. The red coloured points, numbered from 1 to 4 in the model state the workflow of accessing the URL using a voice command. Firstly, point 1 in the workflow stage where the user gives URL access voice command. Point 2 is the acceptance of commands by the voice assistant app when found amongst the whitelisted URLs. Point 3, is when the voice command is processed by the voice assistant app to open a website requested example, “Open facebook.com”. This URL is requested by Facebook’s server through network packets. Finally, point 4 is when the remote Facebook server responds with network packets that open the Facebook webpage in the browser. The blue colour points in the model determine the attacker’s strategy to exploit the network packets in the workflow. Point 1, the attacker tries to perform packet sniffing but monitoring and analysing the packet. When the attacker acquires sufficient it is possible to execute point 2, which is a cyber-attack. By performing the attack the attacker gains access to user-sensitive data and the data linked to the Metaverse. The Attacker will be able to achieve this as suggested in the Section 2A. The availability of the Network packet data which can be decoded and analysed for flow. Whereas the network packet data can also be decrypted for OVR Quest 2 based on the OVRseen Application developed recently [9]. This further leads to security vulnerabilities and privacy leaks widely in VR apps [10].

Based on network analysis and the proposed threat model, we estimate that the OVR Voice Assistant being novel is vulnerable to cyber-attacks.

IV. Conclusion

In order to emphasize the significance of cyber security, we endure further into network analysis for the metaverse as we conclude our study. When novice technologies are added to Metaverse, performance is prioritized above cyber security. This highlights the vulnerabilities in the Metaverse infrastructure that can result in loss of capital, unpleasant experiences, and data privacy exploitation. We assert that, although being whitelisted, Voice Command access to URLs is susceptible to packet sniffing and cyber assaults through our suggested threat model. Since this study was only partially assessed, in subsequent research, we will fully assess it by utilising Packet Analysis and Analytics to decrypt data from network packets.

Acknowledgement

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Ministry of Science and ICT (Project No. RS-2024-00438551, 50%; 2021-0-01816, 20%), and the Ministry of Science and ICT grant through the Information Technology Research Center (ITRC) Program (Project No. RS-2023-00228996, 30%)

References

[1] H. Gao, A. Y. L. Chong, and H. Bao, "Metaverse: Literature review, synthesis and future research agenda," Journal of Computer Information Systems, vol. 64, no. 4, pp. 533–553, 2024.

[2] A. D. Sarang, M. A. Alawami, and K. W. Park, "MV-Honeypot: Security threat analysis by deploying avatar as a honeypot in COTS metaverse platforms," CMES-Computer Modeling in Engineering & Sciences, vol. 141, no. 1, 2024.

[3] M. Zawish, F. A. Dharejo, S. A. Khowaja, S. Raza, S. Davy, K. Dev, and P. Bellavista, "AI and 6G into the metaverse: Fundamentals, challenges and future research trends," IEEE Open Journal of the Communications Society, vol. 5, pp. 730–778, 2024.

[4] J. Lin, Y. Xu, W. Guo, L. Cui, and C. Miao, "XIVA: An intelligent voice assistant with scalable capabilities for educational metaverse," in CAAI International Conference on Artificial Intelligence, Cham, Switzerland: Springer Nature, Aug. 2022, pp. 559–563.

[5] K. Nguyen and Y. Park, "Detecting malicious websites by using deep Q-networks," in 2024 Silicon Valley Cybersecurity Conference (SVCC), June 2024, pp. 1–10.

[6] Z. Su, K. Cai, R. Beeler, L. Dresel, A. Garcia, I. Grishchenko, Y. Tian, C. Kruegel, and G. Vigna, "Remote keylogging attacks in multi-user VR applications," arXiv preprint arXiv:2405.14036, 2024.

[7] K. Yan, X. Zhang, and W. Diao, "Stealing trust: Unraveling blind message attacks in Web3 authentication," arXiv preprint arXiv:2406.00523, 2024.

[8] A. Maci, N. Tamma, and A. Coscia, "Deep reinforcement learning-based malicious URL detection with feature selection," in 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), Feb. 2024, pp. 1–7.

[9] 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), Aug. 2022, pp. 3789–3806.

[10] 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 Proc. IEEE/ACM 46th Int. Conf. Software Engineering, Apr. 2024, pp. 1–13.

[11] A. Azab, M. Khasawneh, S. Alrabaee, K. K. R. Choo, and M. Sarsour, "Network traffic classification: Techniques, datasets, and challenges," Digital Communications and Networks, vol. 10, no. 3, pp. 676–692, 2024.

[12] S. B. Divya and S. P. Mary, "A comparative analysis of using deep learning and machine learning technologies for intrusion detection for effective network traffic analysis," in 2024 7th Int. Conf. Circuit Power and Computing Technologies (ICCPCT), vol. 1, Aug. 2024, pp. 563–569.

[13] A. Awadallah, K. Eledlebi, J. Zemerly, D. Puthal, E. Damiani, K. Taha, T. Y. Kim, P. D. Yoo, K. K. R. Choo, M. S. Yim, and C. Y. Yeun, "Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities," IEEE Communications Surveys & Tutorials, 2024.

[14] M. Alauthman, A. Ishtaiwi, A. Al Maqousi, and W. Hadi, "A framework for cybersecurity in the metaverse," in 2024 2nd Int. Conf. Cyber Resilience (ICCR), Feb. 2024, pp. 1–8.

[15] S. Saharan, S. Singh, A. K. Bhandari, and B. Yadav, "The future of cyber-crimes and cyber war in the metaverse," in Forecasting Cyber Crimes in the Age of the Metaverse, IGI Global, 2024, pp. 126–148.