Assessing Security in Virtual Reality: Forensics, Privacy and Perception

Fall 2023 Poster Showcase

Students: Evan Anspach , Mason Coco, Oluwatosin Falebita, and Ethan Myers
Faculty: Dr. Francisco R. Ortega, Professor Indrakshi Ray

Objective

- Assess Vulnerabilities in Augmented and Virtual Realities to determine risks to data privacy, user safety and user trust in the system.
- Asses what Data is being stored on VR headsets as well as how it is being stored.

Background

- AR/VR systems face many unique challenges and vulnerabilities, the impact of many of these vulnerabilities on user's is not yet understood.

Data Security in AR/VR

- **Data collection:** includes user biometrics, financial data, usage history, voice recordings, advertising data, and personal stats.
- **Data storage:** Data is stored in Meta Servers, on the device itself, and within the Oculus app of any paired device.
- **Data safety:** Data is stored on the device use AES-256 XTS standard encryption.
- **Data transmission:** Data is encrypted using TLS 1.2 and 1.3 protocols.
- **Privacy**: Users have the option to adjust privacy settings on their Oculus Quest 2.

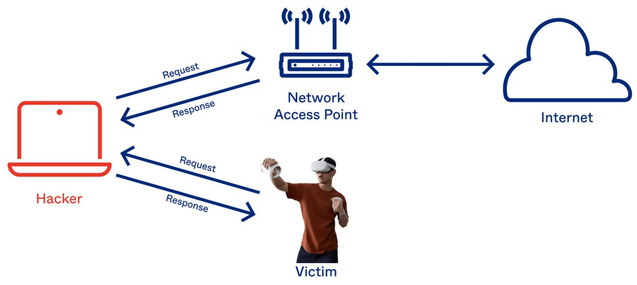
VR/AR Security Vulnerabilities

- Limited information regarding security vulnerabilities is available.
- A significant challenge we face is the device limitation, restricting users to access only store-specific applications.
- We are examining a range of devices including the Meta Quest series, PICO Neo Eye, Microsoft HoloLens, and the upcoming Apple Vision Pro
- Initiate our own penetration tests to uncover potential security vulnerabilities.
- The niche adoption of these devices, in comparison to smartphones poses less incentive for cybercriminals, leading to lower risk exposure.

Proposed Experiments

- Virtual/Augmented Reality environment to manipulate the user's perception using ARP Poisoning.
- Attack must go unnoticed as the victim would just take the headset off.
- Target practice like application to test the effectiveness of virtual/augmented reality has on our perception and how different factors of the application can be changed to affect user performance.
- The detectability of the manipulation will be measured using a Think Aloud protocol as well as both pre and post surveys of user perception of the application.
- These studies work to understand the ways manipulative behavior could be introduced into an application through hardware and software vulnerabilities, and assess its impact on users and the Just Noticeable Difference point for certain perception attacks.

ARP Poisoning/Spoofing

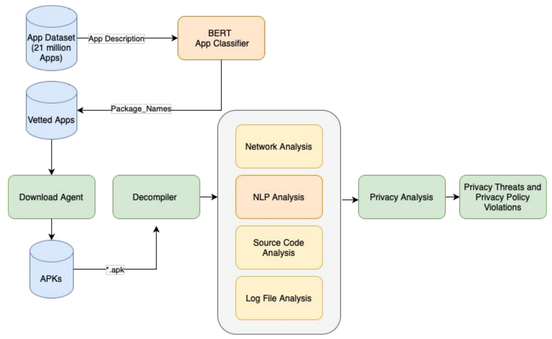


VR Digital and Network Forensics

- **Is data secure?** We would conduct digital forensics examination of Oculus Quest 2 and Oculus Go device partitions
- **Is the transmission of data secure?** We would perform network forensics to determine the extent of user and security.

Connected Apps and Privacy Analysis

- **Why Apps?:** VR/AR headsets and apps often work together to provide a seamless user experience. Studying them in conjunction is critical to understand how they complement each other in terms of functionality, data sharing, and user interactions.
- **Privacy Concerns:** AR/VR apps can collect a wide range of user data, including location, biometric information, and interaction patterns. Privacy threat analysis is essential to identify how this data is collected, stored, and shared.
- **NLP Analysis:** Analyzes textual data to detect privacy policy violations and consent and data handling descriptions.
- **Log Analysis:** Identify PII's in logged in production and track data access and processing, ensuring compliance with privacy regulations.
- **Network Analysis:** Monitors network traffic to detect unlawful data sharing and tests data security and user consent compliance.
- **Source Code Analysis:** Scans source code for vulnerabilities, potential data breaches, and lacking security protocols.



References

1. Adams, D., Bah, A., Barwulor, C., Musabay, N., Pitkin, K., & Redmiles, E. (2018). Perceptions of the privacy and security of virtual reality. *iConference 2018 Proceedings*.
2. *Meta information collection*. Meta. (n.d.-a). https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/oculus-information-collection/
3. *Meta Quest Move Information Storage*. Meta. (n.d.-b). https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/oculus-move-information-storage/
4. *Security & Privacy for Enterprise-Level VR: Oculus for business*. Security & Privacy for Enterprise-Level VR | Oculus for Business. (n.d.). https://business.oculus.com/security/
5. Odeleye, B., Loukas, G., Heartfield, R., Sakellari, G., Panaousis, E., & Spyridonis, F. (2023). Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers & Security*, *124*, 102951.