Security Vulnerabilities in Virtual Reality (VR) Environments

Rashmi Elavazhagan, Amir Mohideen Basheer Khan, Taanish Alam,
Dr.Mohammad I Husain (Faculty Mentor), Nathan Lee (Peer Mentor)
California State Polytechnic University-Pomona

ABSTRACT

By providing an experience of the environment with a more real virtual reality (VR) technology that is also interactive, it has transduced fields such as healthcare, entertainment, and education. At the heart of this technology is Lab Streaming Layer (LSL), which enables synchronized real-time streaming of multiple sensory signals, e.g. eye tracking data, motion capture and physiological recordings. This makes LSL great for integrating these inputs, but enables security issues that represent notable privacy and system integrity risks. Critical vulnerabilities include data interception (attackers compromising low-strength encryption protocols) and session hijacking (preempted backups for maintaining the virtual reality sessions).

In this study, the research on these vulnerabilities is further contextualized with works for each of vulnerability, investigating attack surface which gets fuller when it comes to LSL-based functionalities. The research has outlined critical points in the data flow through which attackers can exploit the systems and some of the ways to secure them. The report suggests that key protections against such an attack would include end-to-end encryption, multi-factor authentication (MFA), and real-time monitoring to detect both system anomalies (such as large amounts of data being transferred) and user access behavior. 18], and should be a joint implementation of some or all of these security protocols to mitigate LSL exposure in VR environments.

OBJECTIVES

Identify Security Vulnerabilities:

The aim of this research is to (firstly) systematically list and classify the common vulnerabilities in any VR system using Lab Streaming Layer (LSL). It requires a deep study of the literature and case studies related to it to clock the highest risks. In particular, we highlight how hackers leverage data interception and session hijacking — two of the best known approaches in today's literature. The goal of the study is to provide a complete understanding on how different parts of these systems can be compromised, by mapping where such vulnerabilities would happen in the data flow. Another important goal is to determine the kind of attacks, like Man-in-the-Middle (MITM) that targets the unencrypted data stream and motion deception devices bring in fake data inside VR system. The vulnerability of each attack vector is reviewed based on its occurrence rates and possible effects for attacking not only the LSL architecture but also other SCADA protocols. In turn, the research lays the groundwork for designing impactful security countermeasures.

Propose Mitigation Strategies:

Complementary to the discovery of vulnerabilities, this work aims at proposing strong mitigation strategies that stand in the way of attackers looking for cracks into LSL-based VR systems. However, proposed solutions including end-to-end encryption to protect specific data streams like eye tracking and motion capture inputs are possible when ensuring the confidentiality is critical and using multi-factor authentication (MFA) to make sure that only authenticated users are allowed access into VR sessions. Additionally, this study examines the need for real-time monitoring in recognizing and reacting to strange behavior in VR environments. Systems that have rich monitoring capability can detect when low-level capture of the data stream, or injection of fake data is being attempted. Generally, all the focuses we intend to achieve in making this paper is good and usable strategies, VR developers can apply themselves in order to improve security of LSL based systems.

MATERIALS AND METHODS

1. **Literature Review:**

In the course of this endeavor, a thorough examination was carried out on the current resources in academic community with regards to security weaknesses within VR systems especially those utilizing Lab Streaming Layer (LSL). Literature was retrieved from the IEEE Xplore, ACM Digital Library and Google Scholar

Key areas of focus included:

- Finding attack vectors such as: session hijacking, data interception, Man-in-the-Middle (MITM) attacks and motion deception devices.
- Investigate possible mitigations like encryption, multi factor authentication (MFA) and real time monitoring tools to harden VR systems.

2. **Data Collection and Analysis:**

- It included a review of articles, research papers and similarly literature while paying special attention to studies that have verified particular vulnerabilities in VR based on LSL.
- This data was then classified in terms of the security threat and the adopted approaches mentioned in previous works, respectively.

We evaluated the attack vectors using two metrics, Frequency which indicates how many times an attack vector is reported in the selected papers, and Severity reflecting the potential impact of this UM in system security.

3. **Attack Vector Analysis:**

Based on literature an examination was made to categorize and analyze the identified attack vectors against VR systems in terms of how frequently they occurred as well as how severe These impacts could be. The identified key attack vectors:

- Data Interception: Attackers monitor clear–text sensory data streams, specifically for eye tracking and motion capture streams.
- Session Hijacking: Poor security protocols on the Part of the Authenticating system permits hackers to hijack VR program sittings as Legitimate users.
- Man-in-the-Middle Attacks (MITM): In this form, attackers sit between the pipelines of data between sensors and VR systems, which compromises the integrity of the data.
- Motion Deception Devices: Attackers feed rogue inputs into VR system to disturb real time feedback.

4. **Mitigation Strategy Evaluation:**

The potential mitigation strategies were evaluated based on their effectiveness in preventing or minimizing the impact of the attack vectors. These strategies include:

- Encryption: This makes it harder for data streams to be intercepted or modified by attackers.
- Multi-Factor Authentication (MFA): Requires more than one form of identity verification, which helps to curb session hijackings.
- Real-Time Monitoring: This system can detect abnormal behaviors, and as soon as it receives reports like motion deception or MITM attacks, it immediately send real time alerts.

RESULTS

1. Data Interception:
    1. Finding: Eye Tracking and Motion Capture data are highly vulnerable to interception by attackers who can exploit unencrypted data streams.
    2. Implication: Sensitive behavioral data from users can be exposed, leading to privacy breaches.
2. Session Hijacking:
    1. Environments allow attackers to take control of user sessions, impersonating legitimate users.
    2. Implication: Attackers can alter the VR environment, steal personal data, or disrupt user experiences.
3. Man-in-the-Middle (MITM) Attacks:
    1. Finding: Weak authentication protocols in VR Finding: Inadequately encrypted data streams make VR systems vulnerable to MITM attacks, where attackers intercept real-time sensory data.
    2. Implication: Attackers can modify or steal sensitive physiological and motion data, impacting user privacy and safety.
4. Motion Deception Devices:
    1. Finding: Motion deception devices can introduce false data into the VR system, disrupting real-time monitoring and preventing the detection of malicious behavior.
    2. Implication: These undetected manipulations can lead to compromised system integrity and user safety risks.

Mitigation Strategies:

3. Encryption: Suggested for encrypting all data streams with an end-to-end system, and especially those invasive streams (e.g., eye-tracking, motion-capture) to avoid unauthorized intrusion and hidden networks interception.
4. Multi-Factor Authentication (MFA):Best practice: MFA implementation ensures that only those users who are verified will be allowed to access VR sessions leading to a reduced risk of session hijack or spoofing.
5. Real-Time Monitoring: Real-time monitoring tools should have the capability of continual scanning over data streams where it is looking for unusual activity which could point to MITM attacks or motion deception attempts.

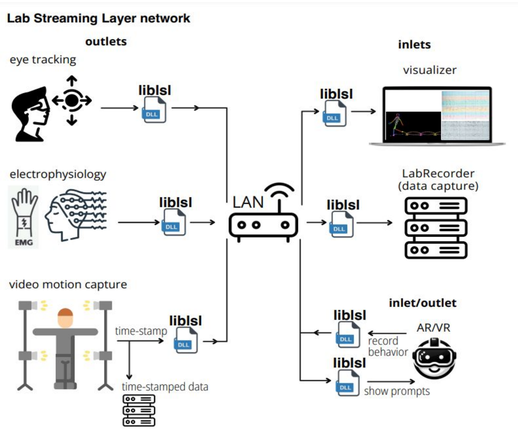

Diagram adapted from: Christian Kothe et al., 'The Lab Streaming Layer for Synchronized Multimodal Recording,' bioRxiv, 2024.

CONCLUSION

We find that **LSL** provides a compelling vision for transparently synchronizing sensory data in VR, but comes paired with a range of important security issues that need to be met. This report highlights that one of the leading attack vectors is the interception of **data predominantly unencrypted eye tracking and motion capture data.** Also, there is a high threat to the session hijacking yet as an outcome of insufficient authentication protocols that enables unethical users to fabricate VR results and get access to confidential information. These vulnerabilities can result in lethal effects such as data breaches, identity theft or exposure of the whole system.

The report points to the necessity of a comprehensive security approach to minimize these risks. **Man-in-the-Middle attacks are close to being impossible when data streams are end-to-end encrypted, and session hijacking can only succeed if multi-factor authentication is disabled.** Finally, real-time monitoring systems need to be deployed so that any anomalous usage and potential breaches can be identified, giving a pre-emptive way to protect the VR environment.

REFERENCES

1. Valluripally, S., Frailey, B., & Kruse, B. (2022). Detection of security and privacy attacks disrupting user immersive experience in virtual reality learning environments. IEEE Transactions on Learning Technologies.
2. Giaretta, A. (2022). Security and privacy in virtual reality--A literature survey. arXiv preprint arXiv:2205.00208.
3. Gulhane, A., Vyas, A., Mitra, R., & Oruche, R. (2019). Security, privacy and safety risk assessment for virtual reality learning environment applications. In Proceedings of the 16th IEEE Conference on Emerging Technologies (pp. 1-6).).
4. Somin, L., McKendrick, Z., Finn, P., & Sharlin, E. (2021). BreachMob: Detecting vulnerabilities in physical environments using virtual reality. In Proceedings of the ACM Symposium on Virtual Reality (pp. 54-58).

ACKNOWLEDGEMENTS

I would like to thank **Professor Dr. Mohammad I Husain** and **Nathan Lee** for their mentorship and support.

We also acknowledge **Christian Kothe et al.** for their work on the **Lab Streaming Layer for Synchronized Multimodal Recording**, from which the diagram in the **Results** section was adapted.

CONTACT

For further inquiries regarding this research, please contact:

•**Polysec Lab**
Email: mihusain@cpp.edu