Date: 2023.05.28

Auditor: H.I.M. Samaranayaka

Organization: Sri Lanka Institute of Information Technology

System: Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles

Executive Summary:

The purpose of this audit report is to assess the security posture and effectiveness of the Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles developed by SLIITThe audit was conducted based on the OWASP Framework to identify potential vulnerabilities, weaknesses, and areas of improvement within the system.

Scope:

The audit focused on the following areas of the Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles:

1. Architecture and design
2. Network communication
3. Data encryption and integrity
4. Authentication and access controls
5. Intrusion detection capabilities
6. Logging and monitoring mechanisms

Findings:

The audit revealed the following findings:

3.1 Architecture and Design:

Recommendation: The system's architecture and design demonstrate a solid foundation for security. However, it is recommended to conduct periodic architecture reviews to ensure its effectiveness against emerging threats and evolving attack vectors.

3.2 Network Communication:

Finding: The communication channels between the components of the system lack proper encryption, making them susceptible to eavesdropping and man-in-the-middle attacks.

Recommendation: Implement secure communication protocols, such as Transport Layer Security (TLS), to protect the confidentiality and integrity of data exchanged between system components.

3.3 Data Encryption and Integrity:

Finding: The system does not provide end-to-end encryption for sensitive data transmitted between vehicles and the central monitoring infrastructure.

Recommendation: Implement strong encryption mechanisms, such as symmetric and asymmetric encryption, to ensure the confidentiality and integrity of data throughout the system.

3.4 Authentication and Access Controls:

Finding: The system lacks robust authentication mechanisms for vehicle identification and access control.

Recommendation: Implement strong authentication protocols, such as two-factor authentication, and enforce strict access controls to prevent unauthorized access to the system and its components.

3.5 Intrusion Detection Capabilities:

Finding: The system's intrusion detection capabilities are not comprehensive enough to detect sophisticated attacks targeting Internet of Vehicles.

Recommendation: Enhance the system's intrusion detection capabilities by incorporating machine learning algorithms and anomaly detection techniques to identify and respond to advanced threats effectively.

3.6 Logging and Monitoring Mechanisms:

Finding: The system lacks adequate logging and monitoring mechanisms for capturing and analyzing security events.

Recommendation: Implement robust logging and monitoring mechanisms to record and analyze security events, enabling timely detection and response to potential security incidents.

Conclusion:

In conclusion, the Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles developed by [Insert Organization Name] exhibits several vulnerabilities and areas that require improvement to ensure the security and integrity of the system. By addressing the identified findings and implementing the recommended measures, the system's security posture can be significantly enhanced.

The organization is advised to promptly address the recommendations outlined in this report to mitigate potential risks and protect the Multi-Tiered Hybrid Intrusion Detection System for Internet of Vehicles from unauthorized access, data breaches, and other security incidents.

Disclaimer:

This audit report is based on the assessment conducted by H.I.M.Samaranayaka within the defined scope and timeframe. While every effort has been made to ensure the accuracy of the findings, it is important to note that security is an ongoing process, and new vulnerabilities may arise over time. Therefore, it is recommended to conduct regular security audits and maintain a proactive approach to secure the system effectively.

Signed: Isuru Samaranayaka

H.I.M. Samaranayaka

Undergraduate (Cyber Security SOC Analyst)

2023.05.28