High Level Design Document for Intrusion Detection System (IDS) Components in Automotive

|  |  |  |
| --- | --- | --- |
| Version | Date | Description |
| 1.0 | 19/03/2025 | Initial Draft |

# Introduction

This document outlines the high-level design for the Intrusion Detection System (IDS) components in automotive applications. The IDS aims to enhance the security of automotive systems by detecting and mitigating potential intrusions.

# Objective

The primary objective of the IDS is to identify and respond to malicious activities, unauthorized access, and anomalies in the automotive network, ensuring the safety and reliability of the vehicle's operation.

# Scope

This document covers the design of IDS components, including their architecture, functionality, and interactions within the automotive environment. It focuses on both hardware and software aspects, ensuring comprehensive coverage of the system.

# System Architecture

The IDS architecture for automotive applications consists of several key components:

## 1. Sensors

## Sensors are responsible for collecting data from various parts of the vehicle's network, including CAN (Controller Area Network) bus, LIN (Local Interconnect Network) bus, and other communication channels. These sensors monitor traffic, identify anomalies, and send data to the IDS for analysis.

## 2. IDS Engine

## The IDS engine is the core component that processes the data received from sensors. It employs various detection techniques, such as signature-based detection, anomaly-based detection, and specification-based detection, to identify potential threats.

## 3. Data Aggregator

## The data aggregator collects and consolidates data from multiple sensors and sources within the vehicle. It ensures that the IDS engine receives comprehensive information for accurate analysis.

## 4. Alert Manager

## The alert manager handles the generation and management of alerts triggered by the IDS engine. It prioritizes alerts based on severity, mitigates false positives, and ensures that critical alerts are promptly communicated to the vehicle's control system and, if necessary, to the user.

## 5. Response System

## The response system is responsible for executing predefined actions in response to detected threats. It can isolate compromised components, reconfigure network settings, and activate countermeasures to mitigate the impact of an intrusion.

## 6. Logging and Reporting

## This component maintains detailed logs of IDS activities, including detected threats, generated alerts, and response actions taken. It also generates periodic reports for analysis and review, enabling continuous improvement of the IDS.

# 5. Functional Requirements

## 1. Real-time Monitoring

The IDS must continuously monitor network traffic and system activities in real-time to detect potential threats promptly.

## 2. Threat Detection

The IDS should employ multiple detection techniques to identify a wide range of threats, including known attacks, unknown anomalies, and protocol violations.

## 3. Alert Management

The system must prioritize and manage alerts effectively, ensuring that critical threats are addressed immediately while minimizing false positives.

## 4. Response Capabilities

The IDS should have the capability to execute automated responses to mitigate detected threats and protect the vehicle's systems.

## 5. Logging and Reporting

Comprehensive logging of IDS activities and periodic reporting are essential for analysis, audit, and improvement of the system.

# 6. Non-functional Requirements

## 1. Performance

The IDS must operate with minimal latency to ensure real-time threat detection and response without affecting the vehicle's performance.

## 2. Reliability

The system should be highly reliable, with redundancy and fault-tolerance mechanisms to ensure continuous operation even in the event of component failures.

## 3. Scalability

The IDS should be scalable to accommodate future expansion, including additional sensors, new detection algorithms, and enhanced response capabilities.

## 4. Security

The IDS itself must be secure against tampering and attacks, ensuring the integrity and confidentiality of the data it processes.

# 7. Component Interaction

The IDS components interact in the following manner:

* The sensors continuously monitor network traffic and system activities, sending collected data to the data aggregator.
* The data aggregator consolidates sensor data and forwards it to the IDS engine for analysis.
* The IDS engine processes the data using various detection techniques and identifies potential threats.
* Upon detecting a threat, the IDS engine triggers an alert, which is managed by the alert manager.
* The alert manager prioritizes the alert based on severity and communicates it to the response system.
* The response system executes predefined actions to mitigate the threat, ensuring the vehicle's safety.
* All activities, including detected threats, alerts, and responses, are logged by the logging and reporting component for analysis and review.

# 8. Conclusion

This high-level design document provides an overview of the IDS components for automotive applications, outlining their architecture, functionality, and interactions. The IDS aims to enhance vehicle security by detecting and mitigating potential threats, ensuring the safety and reliability of automotive systems.