SENTINEL-TRK

IDS/IPS for Heavy-Duty Vehicles (SAE J1939)

TECHNOLOGY:

Heavy-duty vehicles use the **SAE standard J1939** protocol for control area networks (CAN). This protocol can be exploited to commit cyber-attacks on the vehicle's, frequently interoperable, electronic control units (ECUs).

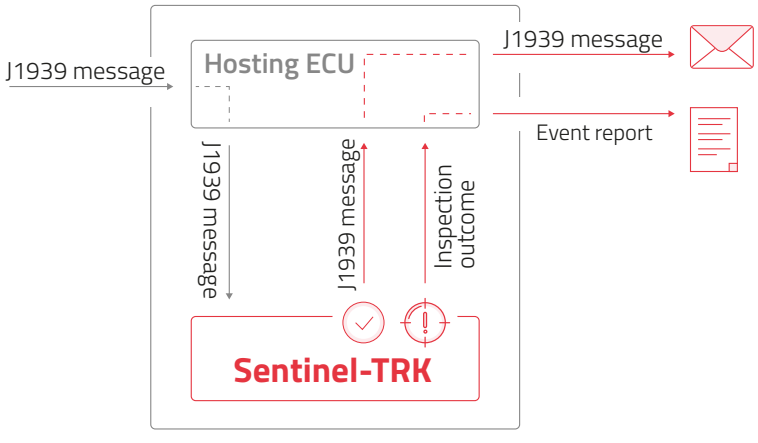
Arilou's **Sentinel-TRK** overcomes these issues by incorporating intrusion detection (IDS) with an optional intrusion prevention (IPS) mechanism for heavy-duty vehicles using the SAE J1939 protocol.

Solution

- **Inspect** traffic for deviation from allowed rules and baseline
- **Detect** messages that violate established baseline or expected vehicle behaviour
- **Report** detected cyber-events for further analysis
- **Discard** events that are hazardous to safety or functionally

INTEGRATION ARCHITECTURE

Sentinel-TRK is an SDK integrated into an ECU. It may be an existing ECU such as a gateway or TCU, or a dedicated ECU attached to the J1939 CAN Bus. Arilou offers flexible implementation modes tailored to meet OEMs needs and architectural environments.



- **Learn** and define a normal **communication profile and rules** based on available data, machine learning, and user customization.
- **Monitor** and examine the SAE J1939 traffic routing functions of gateway rules.
- **Detect** attacks based on any deviation from the established profile and rules. Optional prevention discards divergent frames.

SECURITY MECHANISMS

Sentinel-TRK is designed to counter attackers manipulating network traffic via compromised ECUs or other controllers.

Features

- **Network Baseline** establishment using machine learning from traffic recordings and DBC files
- **Anomaly Detection** Context aware, stateful operation
- **Message Inspection** formality and plausibility (signal ranges, rate changes)
- **Protocol Flow Validation** based on timing and order among other variables
- **Attack Mitigation (Configurable)** Denial-of-Service prevention, whitelisting and firewalling capabilities
- **Maintenance** Secure updates
- **Reporting** Advanced event logging, both cloud-based and local
- **Rogue Message Drop** in optional IPS mode

Benefits

- **Easy Integration** fully configurable, no architecture changes are required.
- **Reduces Costs** improves reliability and increases profitability
- **Platform Agnostic** supports multiple real-time and higher-level environments
- **Available as Software-Only** integrates with existing ECU hardware

ABOUT ARILOU:

Arilou Automotive Cybersecurity, part of NNG Group, believes in an automotive future secured against cyber-attack. A leading provider of pioneering cybersecurity solutions for the automotive industry, Arilou was the first to introduce CAN (**Sentinel-CAN, Sentinel-TRK**) and automotive Ethernet (**Sentinel-ETH**) in-vehicle network security.

Winner of **Frost & Sullivan's** 2019 Technology Innovation award, and independently tested by **UMTRI**, with perfect results, Arilou's **Sentinel-CAN** software intrusion detection and prevention system and **Sentinel-PHY** electronic fingerprint authentication offer supreme detection and prevention rates with zero false alarms.

With its holistic approach and low-cost multi-layered solutions, **Arilou** is making full protection for vehicles a reality.

V2020_10