SENTINEL-V2X

IDS/IPS for Connected and Automated Vehicles

TECHNOLOGY:

Vehicle-to-everything (V2X) technologies are a key component in the future development of highly automated driving systems. And while V2X communication methods provide channel security, limiting direct intrusion, they do not provide message content inspection for attacks from compromised devices.

Arilou's **Sentinel-V2X** mitigates this problem by combining **deep content inspection (DCI)** with **misbehavior detection (MD)** and sensor fusion. This ensures that received messages are in line with baseline expectations and other sources of vehicle data.

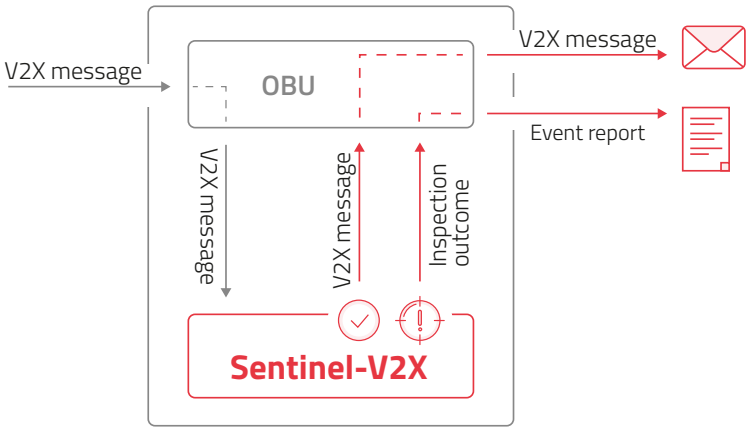
Sentinel-V2X inspects V2X messages as they are received by the vehicle's **onboard unit (OBU)**, screening them for attacks before further processing.

Solution

- **Inspect** traffic using DCI, MD, and sensor fusion for plausibility/deviation from allowed rules and baseline
- **Detect** messages that violate established baseline or expected vehicle behaviour determined from sensor fusion
- **Report** and convey detected cyber events for further analysis
- **Discard** events that are hazardous to safety or functionally

INTEGRATION ARCHITECTURE

Sentinel-V2X is an SDK that can be integrated into the OBU or nearby. Configurable as both an intrusion detection (IDS) and optional intrusion prevention system (IPS), Arilou offers flexible implementation modes tailored to meet OEM 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 V2X messages and other sensor data to generate a behavior profile and plausibility model.
- **Detect** attacks based on any deviation from the established profile and rules. Optional prevention discards divergent messages.

SECURITY MECHANISMS

Sentinel-V2X is designed to counter attackers manipulating data traffic via compromised V2X devices such as other vehicles, roadside transmitters or hacked command and control centers.

Features

- **Deep Content Inspection** of message payload validation and consistency vs. vehicle state, context and behavior
- **Misbehavior Detection** and **Plausibility** verification ensures messages are in line with expected system operations and do not constitute a potential cyber attack
- **Verification** of message format validity as per protocol specifications (message ID, Client ID, among others
- **Attack Mitigation** Denial–of–Service protection and whitelisting

Benefits

- **Rogue Message Protection** defends the vehicle from compromised V2X messages originating from other sources such as other vehicles, roadside equipment or mobile hackers
- **Propagation Mitigation** protects other V2X users from the spread of cyber-attacks by forwarding only inspected and validated messages

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