SENTINEL-ETH

IDS/IPS for Automotive Ethernet

TECHNOLOGY:

Automotive Ethernet is soon to become the core in-vehicle network. Ethernet brings greater bandwidth and enables new functionality, but it also brings new challenges and legacy-risks from the IT domain.

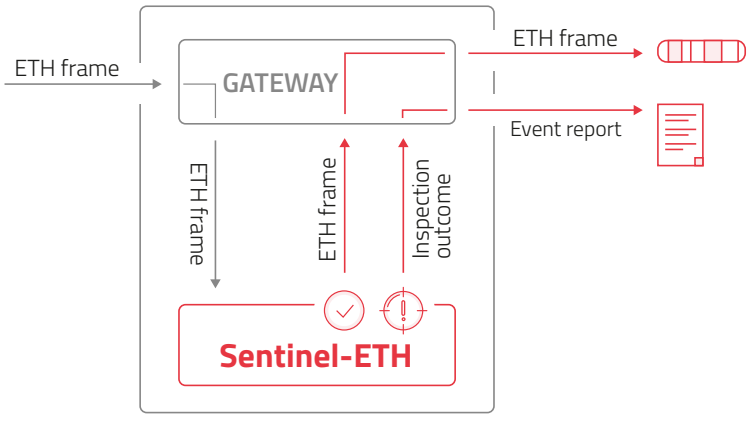
Sentinel-ETH overcomes these issues by incorporating intrusion detection, firewalling, and an optional prevention system directly into automotive Ethernet networks.

Solution

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

INTEGRATION ARCHITECTURE

Sentinel-ETH 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 Ethernet network. 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 examination of ethernet 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-ETH is designed to counter attackers manipulating network traffic via compromised ECUs or other controllers.

Features

- **Basic Layer (1-4) Inspection** (physical, data link, network and transport) – only designated MAC addresses per physical port, MAC-IP binding, TCP/UDP verified tuples, ARP poisoning, ICMP type & code
- **Deep Content Inspection** of message payload validation and consistency vs. vehicle state, context and behavior

- **Verification** of message format validity as per protocol specifications (message ID, Client ID, among others
- **Anomaly Detection** using the designated baseline and allow/deny ruleset preventing zero-day attacks
- **Signature based** blacklist detection for known attack scenarios
- **Deep Packet Inspection** of IT and automotive protocols (SOME/IP, DoIP, AVB, among others)
- **Stateful Protocol Inspection** for completeness of transactions of procedures
- **Attack Mitigation** Denial–of–Service protection and whitelisting

BENEFITS

- High performance processing of frames using optimized hardware and software
- Implementation options:
  - Integrated in a switch on a secured gateway, functioning as firewall
  - Independent entity as NIDS or NIPS
  - Distributed - ECU endpoint protection as HIDPS
- Can manage extremely rare cases such as reckless driving, emergency braking, etc., and can exclude false-alarm generation
- Optional Prevention function (firewalling) discards frames identified as attacks
- Logs detected events and statistics for inspected traffic
- The only dedicated and objective cyber-security component in the vehicle
- Event reporting options:
  - Telematics (over CAN bus)
  - Cellular SMS
  - Cellular/any IP network using Syslog
  - Other options can be added per customer request

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