DESIGN AND IMPLEMENTATION OF IDS FOR AVB/TSN NETWORKS

Rodrigo Alves (UFPE/BOSCH)
Michael Buchalik (BOSCH)
Divanilson R. Campelo (UFPE)
Timo Lothspeich (BOSCH)
Design and Implementation of IDS for AVB/TSN Networks

Agenda

- Intrusion Detection Systems (IDS)
- Motivation
- Threat Scenarios
- Evaluation & Measurements
- Conclusion and Future Work
INTRUSION DETECTION SYSTEMS (IDS)
Design and Implementation of IDS for AVB/TSN Networks

Automotive Security - Overview

In recent history, the automotive industry has spent significant effort to secure its products. Security can be found on different layers.

- **Individual ECU**: ECU software and data integrity protection
- **In-vehicle network**: Integrity protection of critical in-vehicle signals and messages
- **E/E-Architecture**: Protected and separated domains by E/E architecture and gateway
- **Connected Vehicle**: Vehicle firewall and security standards for external interfaces
- **Intrusion Detection System**: Network communication behavior is monitored and analyzed

**Key Terms**
- **ECU**: Electric Control Unit
- **ADAS**: Advanced Driver Assistance System
- **BCM**: Body Control Module
- **PT**: Power Train
- **GW**: Gateway
- **HU**: Head Unit
- **OBD**: On-Board Diagnostics

© Robert Bosch GmbH 2019. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.
Design and Implementation of IDS for AVB/TSN Networks

Intrusion Detection System

A strong push from the U.S. government for “timely detection and rapid response” of potential vehicle cyber security incidents in the field.
MOTIVATION
### Design and Implementation of IDS for AVB/TSN Networks

**Audio Video Bridging / Time Sensitive Networking**

<table>
<thead>
<tr>
<th></th>
<th>Synchronization</th>
<th>Stream Reservation</th>
<th>Shapers</th>
<th>Reliability</th>
<th>Prioritization Enhancements</th>
<th>Security</th>
<th>Transport</th>
<th>Network Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AVB</strong></td>
<td>802.1AS-2011</td>
<td>802.1Qat-2010</td>
<td>802.1Qav</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1722-2011</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(gPTP)</td>
<td>(SRP)</td>
<td>(Credit Based Shaper)</td>
<td></td>
<td></td>
<td></td>
<td>(Audio/Video)</td>
<td></td>
</tr>
<tr>
<td><strong>TSN</strong></td>
<td>P802.1AS-Rev</td>
<td>802.1Qca-2015</td>
<td>802.1Qbv-2015</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1722-2016</td>
<td>1722.1-2013 (AVDECC)</td>
</tr>
<tr>
<td></td>
<td>(Reliable gPTP)</td>
<td>(Path Reservation)</td>
<td>(TT Shaper)</td>
<td></td>
<td></td>
<td></td>
<td>(Additional Automotive encapsulation for: CAN, LIN, FlexRay, etc.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.1Qcc-2018</td>
<td></td>
<td>802.1Qch-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Enhanced SRP + Network Configuration)</td>
<td></td>
<td>(Cyclic Scheduling)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>P802.1Qcr</td>
<td></td>
<td>802.1CB-2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Async Traffic Shaper)</td>
<td></td>
<td>(Redundant Paths)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>802.1Qbu-2016</td>
<td></td>
<td>802.1Qci</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Frame preemption)</td>
<td></td>
<td>2017 (Ingress Filtering and Policing)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1722-2016</td>
<td></td>
<td>1722.1-2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

▶ A set of standards to add deterministic features to the network like precise timing, bounded latency, guaranteed bandwidth, fault tolerant, etc.
Design and Implementation of IDS for AVB/TSN Networks

Motivation: Ethernet TSN Stack

"If you want to protect your network, know your network"
Design and Implementation of IDS for AVB/TSN Networks

Motivation: One Header, Three Protocols
Design and Implementation of IDS for AVB/TSN Networks

Motivation: Complex Header e.g. AVTP
Design and Implementation of IDS for AVB/TSN Networks

AVB/TSN IDS Focus

- Monitor Time Synchronization (AS)
- Monitor Stream Reservation (Qat)
- Traffic Shaping (Qbv, Qch)
- Network configuration (AVDECC)
- Transport Protocols (AVTP)
Design and Implementation of IDS for AVB/TSN Networks

Threats and Anomaly Detection - Example 1

Man-In-the-Middle

- Usual Follow-up Interval
- Sync Interval
- Missing Follow-up
- Follow-up messages
- Sync messages
Design and Implementation of IDS for AVB/TSN Networks

Threats and Anomaly Detection - Example 2

Rogue Grandmaster

ECU 1 - Grandmaster

ECU 1 - Grandmaster

ECU 2

ECU 3

ECU 2

ECU 3

Malicious ECU

Malicious ECU

I am the Grandmaster!

I am a better Grandmaster!
Design and Implementation of IDS for AVB/TSN Networks
Threats and Anomaly Detection - Example 3

Spoofed streams

Flooding attacks

Deviations from protocol specification

Valid Stream 1

Invalid Stream 1

Malicious ECU

ECU 1

Switch

ECU 2

ECU 3

Flooding

Malicious ECU

ECU 1

Switch

ECU 2

ECU 3

Version PTP 2

Version PTP 1

Malicious ECU

ECU 1

Switch

ECU 2

ECU 3

Flooding attacks

Deviations from protocol specification

Spoofed streams
Design and Implementation of IDS for AVB/TSN Networks
Threats and Anomaly Detection - Example 4

Denial of Service
EVALUATION & MEASUREMENTS
Design and Implementation of IDS for AVB/TSN Networks
PoC Implementation – Preliminary Results
Design and Implementation of IDS for AVB/TSN Networks

Test Case 1: Latency

1.) RFC 2544: Benchmarking Methodology for Network Interconnected Devices
Design and Implementation of IDS for AVB/TSN Networks
Test Case 2: gPTP Synchronization – Offset and P2P-Delay
Design and Implementation of IDS for AVB/TSN Networks

Test Case 3: CPU Throughput for IPS

Throughput [frame/s]

Throughput [Mbit/s]
CONCLUSION AND FUTURE WORK
Design and Implementation of IDS for AVB/TSN Networks

General Considerations

- No considerable difference for IDS compared to normal switch operation
- IPS use-case adds considerable overhead
  - Packet Loss and Jitter are also affected
- CPU processing power becomes relevant for IDS/IPS performance
- More throughput for bigger packets
- Network configuration is a key factor
  - One step sync vs Two step sync
  - Time Synchronization and Path Delay Calculation intervals
  - Number of devices on the network
  - Switch configuration (Number and size of RX buffers) need to fit network characteristics
Design and Implementation of IDS for AVB/TSN Networks
Future work: IEEE 802.1CB

- Distributed IDS on multiple devices?
- Other protocols → MACsec, YANG
- Performance comparison between different devices
- Take safety considerations into concern
  - E.g. Rate limiting and drop malicious packets
- Performance improvements
  - Take more advantages on HW features
  - Required processing power for higher bandwidth networks:
    → 2.5Gb/s, 5Gb/s, 10Gb/s +
- Interfacing with other Anomaly Detector components, e.g. CAN
Thank you for your attention

Please visit us at our booth for further discussion!

#LikeABosch
BACKUP
Design and implementation of IDS for AVB/TSN networks

Firewall vs IDS

1. **Firewall**
   - Little/No-Delay
   - No logging
   - Individual Components

2. **In-Vehicle Networking**
   - Integrity protection of critical in-vehicle signals and messages

3. **EE Architecture**
   - Protected and separated domains by E/E architectures and gateways

4. **Connected Vehicle**
   - Vehicle firewall and security standards for external interfaces

5. **Connected Fleet**
   - IDS monitors and analysis of fleet data to prevent attacks

**Intrusion Detection System**

- Deeper Inspection
- Traffic History
- Logging
- Part of bigger System

---

Little/No-Delay

Individual Packets

No logging

Individual Components

Deeper Inspection

Traffic History

Logging

Part of bigger System