Security areas and modular IDPS architecture design elements protecting Automotive Ethernet Networks

2019 IEEE-SA Ethernet & IP @ Automotive Technology Day – Detroit
Dr. Georg Gaderer & Dr. Michael Ziehensack, Elektrobit
Motivation

• Classical Dependability is a well known and throughout the automotive industry well mastered topic

• Nowadays we see several needs raising
  – Raising data-rate of communication (CAN, LIN, FR vs. GBit Ethernet)
  – Raising computing effort (simple logic vs. High Performance, multicore computing)
  – Raising complexity (window control vs. Piloted driving)
  – Rase of connectivity to outside world (simple OBD connector vs. Update over the air)

*This increases the focus on security, yet strengthening the safety aspect (Integrity, Availability)*
Protecting Automotive Ethernet Networks

Automotive System Security Layers

- Secure Environment
- Secure Ext. Comm. & Interfaces
- Secure Network Segmentation
- Secure OnBoard Comm.
- Secure Platform (HW, Boot, Update, Separation)

Multi-Level Communication Security Architecture

- **Level 1**: restrict access to the network
- **Level 2**: secure onboard communication
- **Level 3**: apply data usage policies
- **Level 4**: detect anomalies and defend

Focus of presentation
Security Areas

What to separate?

– **Vehicle Functions according to criticality and trust level** grouped in security areas
– For example,
  • security area with highly critical functions (breaking, steering, ...)
  • security areas with HMI functions ...
  • security area with functions that contain external interfaces (mobile connection, remote key, WLAN, V2G, ...)

How to separate?

– **Physical**: Domain E/E Architecture (physical)
– **Logical**: VLANs, IP Subnets for new E2E architectures with mixed topology (e.g., centralized architecture with no physical separation or zonal E/E arch.)
– **Gateways**: Traffic between the security areas is only possible between adjacent areas via a gateway
Security Areas

Level of Separation?

- **Goal**: increase the number of borders to cross between security areas
  - Like an onion skin, the **security areas are nested into each other**, with the innermost security area offering the highest level of protection, e.g., a frame from the cloud must never reach a breaking ECU directly.
  - End nodes can only be part of a single security area.

- **Gateways** (Security Area Crossings)
  - Communication between areas only via dedicated gateways such as, **VLAN Bridges, IP routers, Application Level Gateways**
  - Dedicated gateways shall provide a **Firewall with deep packet inspection** (e.g., check of VLAN, MAC/IP-addresses, port numbers, L5+ protocol type, ...)

Variant A:
- Separation based on domains
- no hierarchy beside external connection
- Max. 2 borders
- Comparison with IT: Sec Area 0 = public network Sec Area 1 = DMZ Sec Area 2 = private network

Variant B:
- Separation based on criticality
- multiple hierarchy levels
- Max. 3 borders
Example for a Security Area Crossing

**IP Router with Firewall**

- **Switch Hardware**
  - CPU
  - Eth Ctrl
  - Switch Core

- **EB Switch Firmware**
  - OS
  - IP Router
  - IP Stack
  - Eth Driver
  - Firewall

**Service Proxy (application level gateway)**

- **Network 1**
  - Client (C)
  - Server (S)
  - **DPI** (Deep Packet Inspection)

- **Network 2**
  - Client (C)
  - Server (S)

- **Firewall**
  - **VM** (Virtual Machine)
  - **Net 1**
  - **Net 2**

- **One to three VMs depending on security level**

- **Service 1**
  - Client on Net1 uses Server on Net2

- **Service 2**
  - Client on Net2 uses Server on Net1

**Efficient application data exchange (blocks network frames)**
Intrusion deduction and prevention System (IDPS)

Intrusion Detection
- Traffic Monitoring
  - Location: Host
  - Layer: Application
- IP Security Events
  - Location: Host
  - Layer: UDP/TCP
- IP Traffic
  - Location: Host, Switch, Firewall, Router
  - On demand mirroring
- IP Statistics
  - Location: Host, Router
  - Layer: IP
- Port Statistics
  - Location: Switch
  - Layer: MAC, Phy

Network Stack
- Frame Header
- Frame Data
- IP Header
- IP Data
- TCP/UDP Header

Intrusion prevention
- Traffic Monitoring
  - Location: Host
  - Layer: context aware Application
  - Plausibilisatoin in Application
- IP Security Events
  - Location: Host
  - Layer: UDP/TCP
  - Firewall, stateful firewall
  - IP Traffic limitation, whitelists
- IP Traffic
  - Location: Host, Switch, Firewall, Router
  - Layer: all, network setup
  - IP Traffic limitation, whitelists
- IP Statistics
  - Location: Host, Router
  - Layer: IP
  - VLANs, Port Whitelists
- Port Statistics
  - Location: Switch
  - Layer: MAC, Switch Config
  - Port Checking, VLANs
## IDS types

<table>
<thead>
<tr>
<th>Host IDS</th>
<th>Network IDS</th>
<th>Hybrid IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analyzes</strong></td>
<td>• internals of a computing system and • Host network interfaces on a ingress packet level</td>
<td>• Packets in the network to detect suspicious activities • Can be on a packet or packet statistics level</td>
</tr>
<tr>
<td><strong>Pros</strong></td>
<td>One can instrument on every layer • Can monitor encrypted communication if directed to the host</td>
<td>• Independent from target system</td>
</tr>
<tr>
<td><strong>Cons</strong></td>
<td>• Depends on protocol stack of the host • Cannot detect anomalies in the whole network</td>
<td>• A full coverage would require mirroring of all packets • Unefficient, thus usually not done • Cannot monitor encrypted packets</td>
</tr>
</tbody>
</table>
# Attack Patterns and detection mechanisms

<table>
<thead>
<tr>
<th>Attack Pattern</th>
<th>Host IDS</th>
<th>Network IDS</th>
<th>Hybrid IDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Scan from one host</td>
<td>Most cases detectable</td>
<td>Difficult to detect but possible</td>
<td>Additional data from Network IDS may improve Host IDS</td>
</tr>
<tr>
<td>Distributed port scan</td>
<td>Difficult to detect</td>
<td>Many cases detectable</td>
<td>Additional data from Host IDS may improve Network IDS</td>
</tr>
<tr>
<td>Buffer overflow attack</td>
<td>Many techniques for detection exist</td>
<td>undetectable</td>
<td>Same as Host IDS</td>
</tr>
<tr>
<td>Denial of service attack (non distributed)</td>
<td>Detectable</td>
<td>Detectable and easy to isolate</td>
<td>Additional Data from Host IDS may improve Network IDS</td>
</tr>
<tr>
<td>Denial of service attack (distributed, e.g., gateway)</td>
<td>Detectable, difficult to isolate</td>
<td>Difficult to detect</td>
<td>Detectable, difficult to isolate</td>
</tr>
<tr>
<td>Man in the middle</td>
<td>Difficult to detect</td>
<td>May be detected</td>
<td>May be detected</td>
</tr>
</tbody>
</table>
### IDS Sensor Examples

#### Where, what and How

<table>
<thead>
<tr>
<th>Location</th>
<th>Data</th>
<th>Type*</th>
<th>Implementation</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network IDS (Switch)</td>
<td>Port Statistics</td>
<td>(M)</td>
<td>Traffic statistics per port</td>
<td>Hardware supported ingress sampling needed</td>
</tr>
<tr>
<td>Host IDS (Host Ethernet Interface, Switch firmware, router)</td>
<td>IP Statistics</td>
<td>(M)</td>
<td>Table statistics per flow (Layer 4) Sampling of configuration interface data</td>
<td>Hardware supported ingress sampling needed</td>
</tr>
<tr>
<td>Network IDS (Switch, Switch Firmware, Router)</td>
<td>IP Traffic duplication</td>
<td>(D)</td>
<td>Duplicate matching packets acc. To a filter</td>
<td>Layer 2 filtering support needed</td>
</tr>
<tr>
<td>Host IDS (Host Ethernet Interface, Firewall)</td>
<td>IP security Events</td>
<td>(D)</td>
<td>Forward dropped frames (or metadata)</td>
<td>e.g., frames out of spec (comm. Matrix)</td>
</tr>
</tbody>
</table>

*Sensor Type:
- (M)etadata (Port, protocol statistics)
- (D)eepl Packet Inspection (Frame by frame inspection, flow analysis)
Modular IDPS Architecture

Sensors, actuators and controllers

- Sensors and actuators are usually paired
- Each sensor/actuator needs unified interface (CONN)
- Sensors and actuators for VM internal parts are not shown
- SOC* Platform is connected via gateway
- Controller do an anomaly detection based on sensor data
The Impact-Automatism-Latency tradeoff

Influencing factors of IDSPs reactions

Intrusion detection might end up in extensive decisions. Those are dependent on level

- The Latency of decision: from a certain level on one might want to have human in the loop (e.g., grounding of a whole fleet)

- The Authority of an automatism: on a low level decisions can be taken easier (e.g., discard packets with security violation)

- The Impact: on a higher level decisions influence a bigger portion of the system
Summary

• Protect automotive networks is important, because of safety, legal and commercial requirements
• Security areas have been defined to restrict the attack surface
• Crossing Security areas are limited to gateways with firewalls and deep packet inspection
• EB’s modular IDPS consists of sensors, actuators and controllers for efficient intrusion detection
• Anomaly detection is done on different levels considering latency, automation level and impact

Thank you for your attention!

Author information

Dr. Georg Gaderer, Elektrobit
Senior Manager, Car Infrastructure Software
greg.gaderer@elektrobit.com

Dr. Michael Ziehensack, Elektrobit
VP, Car Infrastructure Software
michael.ziehensack@elektrobit.com
Get in touch!

sales@elektrobit.com
www.elektrobit.com

Restricted Network Access
Secure Onboard Communication
Data Usage Policies
Detection & Defense