Automotive Anomaly Monitors and Threat Analysis in the Cloud

Dr. André Weimerskirch

Vector Automotive Cyber Security Symposium – October 12, 2017
Cybersecurity Components

Secure Internal & External Communications
1. Block access to vehicle networks (Firewall)
2. Isolate security sensitive ECUs via gateway
3. Authenticate and/or encrypt comm.

Protect Computing Platform
1. Secure microcontroller (e.g. HSM)
2. Secure boot and hypervisor
3. Secure environment & integrity monitoring

Remote Updates and Analytics
1. Record and maintain history
2. Cloud-based analytics
3. OTA security updates

Information Sharing
1. Auto-ISAC and information monitoring
2. Incident response
3. Monitoring throughout product lifecycle

Development Process
1. Secure development and production processes
2. Threat analysis & penetration testing
3. Industry standards (e.g. SAE J3061)

Monitor Vehicle Network and ECUs
1. Monitor and protect ECU computing platforms
2. Anomaly detection & prevention of in-vehicle network
3. Plausibility checks of content
Multi-Layered Cybersecurity Architecture

**Cell Phone**
- Secure Phone Environment
- Secure Virtual Car Key

**Cloud Computing**
- Security Operations Center
- Threat Analytics
- SOTA backend

**V2V / V2I**

**Keyless and Passive Entry Systems**

**Battery Charging Systems**

**Security Architecture & Integration**
- Secure Development Process
- Testing and Validation
- Over-The-Air Software Architecture
- Modular Security Architecture
- Connectivity and Gateway Experts
- Automotive Software Integration Expertise

**Vehicle Security Services**
- Software Over-The-Air (SOTA) Updates
- Anomaly Management and Reporting
  - Secure Environment Management & Reporting
  - CAN & Ethernet Network Traffic

**Wireless Communication Security**
- Secure Server Communications / TLS
- V2X IEEE 1609.2
- WiFi WPA2
- Bluetooth Security
- Security Protocol for Virtual Car Key

**Vehicle Network Security (Gateway)**
- CAN Anomaly Detection (SOTA Supported)
- Dynamic Firewall (SOTA supported)
- Network Isolation from External Interfaces
- Secure CAN / Ethernet

**ECU Platform Security**
- Hypervisor
- Secure Boot
- Hardened OS
- Secure Environment
Secure Computing Platforms – Separation and Protection

- Secure Platform
  - Secure boot
  - Hardened OS
- Separation
  - Hypervisor
  - Separate uC
- Secure Communication
  - Interface firewall/filter
  - Secure CAN / Ethernet
- FOTA to fix security flaws

Diagram:
- Secure Boot
- Adaptive AutoSar
- Vehicle VM
- Security VM
- Application VM's
- Secure Boot
- Certificate Mgmt
- Crypto
- Secure Logging
- Vehicle Abstraction API
- Network Anomaly Detection
- Diagnostics
- Power Mgmt
- Flasher
- Application VM's
- V2X/V2I
- Safety Applications
- Traffic Efficiency
- Infotainment
- Application VM's
- ETSI DENM, CAM
- US Standard BSM-I, BSM-II, SPaT, MAP, TIM
- Vehicle Abstraction API
- Events
- Cell Talker
- Web Server
- OTA (DM & Policy)
- CarKey API
- System Monitor
- GPS-MON
- WiFi AP/Client
- eCall
- Secure Boot
- Hypervisor / Software Container
- 4G cellular
- Bluetooth
- V2V/ V2I
- GPS
- WIFI

Legend:
- LEAR Corporation
- 100 Years
- Secure Platform
- Secure boot
- Hardened OS
- Separation
- Hypervisor
- Separate uC
- Secure Communication
- Interface firewall/filter
- Secure CAN / Ethernet
- FOTA to fix security flaws
Monitors

1. Network anomaly detection
   - ‘smart filtering’
   - Intelligent monitoring

2. ECU monitors (control flow, whitelist of executables, hardware monitors, ...)

3. Content monitor (plausibility)
Network and ECU Monitor

- Protect computing platforms and network architecture in vehicle
  - Smart firewall
  - Network separation
  - Secure CAN/Ethernet
  - Secure platform
- Modules in vehicle run local monitors
  - Network monitor
  - ECU monitor
  - Content monitor
- Run analysis in cloud
- Update software

This loop will continuously improve the defense capabilities
In-vehicle anomaly detection systems (ADS) monitor the on-board communication bus (e.g. CAN and Ethernet) to detect anomalous messages.

Attackers will try to inject malicious messages to modify vehicle’s behavior (e.g. by a local or remote attack).

Anomalous on-board messages are an indication of an anomalous event.
- Sensor defect
- Cyber attack

It seems there are two levels of anomaly detection:
1. All deterministic, or highly reliable mechanisms, should be incorporated in a ‘Smart Firewall’. Anomalies are discarded.
2. Non-deterministic and statistical methods are usually used for intelligent monitoring. These messages are only flagged.

➢ #1 is clearly needed and usually deployed in a central gateway.
➢ #2 covers prognostics, monitors all anomalies, and might be needed to detect advanced, context related attacks.

ADS sends reports about anomalies to a Security Operations Center (SOC) in the cloud where they are analyzed.
Network ADS: Lear/Honeywell Architecture

- Used for prognostics and cybersecurity
1. Attack
2. Observe
3. Monitor and Detect
4. Mitigate via OTA
5. Verify OTA action
6. Block further attack

Network ADS: Lear/Honeywell Demonstrator

Secured!
ECU Monitor

- ECU Monitor components include:
  - Secure Environment
  - OS & Application Logs
  - Self-tests
  - DTCs

- Secure Environment extends secure boot and validates the integrity of the computing environment during run-time.
  - Whitelists of binaries
  - Software attestation
  - Control flow integrity

- Secure Environment mechanisms detect an attack and can react based on a policy to restart suspected processes, restrict features, or reboot an entire platform.

- Upon detection, the ECU Monitor sends reports about anomalies to a Security Operations Center (SOC) in the cloud where they are analyzed.
1. Attack

2. Monitor and block attack

3. Secured!
It is likely that the input of exposed interfaces will be used by in-vehicle control applications:

- Lidar/radar/...
- V2X/802.11p/pWLAN
- Slow-down on curves

Exposed interfaces must be separated from ADAS/powertrain via firewall/filter, e.g., located in a gateway.

The gateway will filter all direct attacks, e.g., attacks that inject forged messages to impact the powertrain.

- This will avoid that a successful hacker can inject control commands.
• So, the attacker can still inject valid messages with forged content to mislead the receiver control application.
  ➢ It seems hard to deploy an application context firewall in the gateway
  ➢ Need a plausibility check in each relevant ECU and/or application

➢ Resilient applications are required that can handle false content input

• Plausibility checks are necessary to support cybersecurity
  • Redundancy: different sensor types (e.g., camera and radar) or different sensors (e.g., two wheel speed sensors) can provide redundant input
  • Redundancy II: different implementations can provide redundant input
  • Logical tests: based on physical properties
  • ...

• Upon detection, the Content Monitor sends reports about anomalies to a Security Operations Center (SOC) in the cloud where they are analyzed.
Next Step: System Integration

ECU 1
- Content Plausibility Monitor
- ECU Monitor

... ECU n
- Content Plausibility Monitor
- ECU Monitor

Gateway / Domain Controller

Combine

ECU Monitor
Network ADS

Security Operations Center

Software Over-the-Air

100110001110
111101010101

Content Plausibility Monitor
ECU Monitor
...
Next Big Step: Resilient Architecture – Local Reaction

- Use monitors to detect anomalies.
- If monitor detection confidence level is deterministic or above a certain threshold (99.9...9%), then there is the possibility to react

**Network anomaly detection:**
- Smart filtering in a central gateway to discard malicious packets
- Upon discarding messages, gateway could trigger turning-off external communication completely, or switch to a stricter firewall filter

**ECU monitor:**
- Upon any alarm, could kill virtual machines, processes, interfaces, etc.
- Then jump to a fail-operational software module

**Content monitor:**
- Jump to fail-safe or fail-operational mode
• A variety of security mechanisms is available today to protect vehicle architectures.

• The next step is to use monitors:
  1. Network anomaly detection
     • ‘smart filtering’
     • Intelligent monitoring
  2. ECU monitors (control flow, whitelist of executables, hardware monitors, ...)
  3. Content plausibility monitor

• Monitoring can be used to support a resilient architecture by detecting an attack and jumping to a fail-operational mode

Each monitor also allows prevention, if it can deterministically detect at real-time in the vehicle.
Dr. André Weimerskirch
VP Cyber Security
Lear Corporation

Ann Arbor, Michigan, USA

Email: aweimerskirch@lear.com