Ethernet network-security for on-board networks

Dr. Christian Meineck
Table of contents

1. Motivation and overview

2. Security measures (not only) for ethernet networks and ECUs

3. Outlook on possible architectural changes with regard to security

4. Summary
The car itself is a (more or less) closed ecosystem.
Software is modified in a controlled ecosystem.

We will add more connectivity to increase the functional spectrum including software updates.

Moving away from only automotive technologies towards including IT technologies.

Increasing amount of switched networks! There we can learn a lot from the IT community.
Ethernet != Ethernet

IT – CAT 5-7, 100Base-TX, 1000Base-T
- Pure networks
- QoS on IP-Level
- Packet loss is ok-ish
- Power over Ethernet
- Redundancy
- EMC?
- ...

Automotive – UTP, 100BaseT1, 1000BaseT1
- Mixed networks (Ethernet <-> CAN)
- QoS on Ethernet Level (802.1p)
- Packet loss might be critical
- Network management
- Centralized gateway
- EMC is very important
- ...

High Bandwidth (100 Mbit, 1 Gbit) + broadly field-tested standards allows a broad spectrum of interesting functions!
Attack Surface

**Goals**

- **Confidentiality**
  Protection against unauthorized access to functions and/or information

- **Integrity**
  Correctness of data and system functions

- **Availability**
  Functions and information’s are available whenever needed

- **Controllability**
  The system must remain in a state in which it can be controlled

- **Observability**
  The system state can be measured under any circumstances

- **Operability**
  The functionality of the system is ensured

- **Controllability**
  The system must remain in a state in which it can be controlled

- **Observability**
  The system state can be measured under any circumstances

- **Operability**
  The functionality of the system is ensured

**Confidentiality**
Protection against unauthorized access to functions and/or information

**Integrity**
Correctness of data and system functions

**Availability**
Functions and information’s are available whenever needed

**Controllability**
The system must remain in a state in which it can be controlled

**Observability**
The system state can be measured under any circumstances

**Operability**
The functionality of the system is ensured

---

**Confidentiality**
Protection against unauthorized access to functions and/or information

**Integrity**
Correctness of data and system functions

**Availability**
Functions and information’s are available whenever needed

**Controllability**
The system must remain in a state in which it can be controlled

**Observability**
The system state can be measured under any circumstances

**Operability**
The functionality of the system is ensured
Achieving the Goals

- **quality of security will decrease over time**
- we need **security updates**
- increase the **speed of releases**

- **scalable**
  - e.g. need **PKI with interaction points in production and after sales**
  - **management** of individual cars with individual functionality **over a long time**

- **fair market value**
  - $\frac{1}{x}$

- **security costs**
  - $\sim \frac{1}{x}$

- **time**
  - $\sim e^x$

---

This talk: Ethernet

“about 70 percent of all Porsches ever built are still on the road today”

- given a certain, desired functionality we have to **decide how much energy** we want to **spend** to secure it
- different goals: e.g. **security vs. controlling**

Dr. Christian Meineck | Porsche AG
Measures - Separation

- utilize tagged VLANs (IEEE 802.1Q) to separate traffic
  - Rule: Each frame has exactly one tag
- Build internal security zones
- separate internal from external traffic and minimize external connections
- need a layer-3 device for inter vlan communication
- minimize inter vlan communication
  - cyclic, multicast signal communication as known from the CAN world is somewhat problematic
- Separation shouldn’t end at the plug
Measures – Authentication, Encryption

- **No one** should be able to connect to the in-car network and participate

- **Looking** into **802.1X** and/or **MAC-Sec**
  Problem: after sales

- **Bus encryption** (i.e. TLS) for ethernet to ethernet communication is a very likely option

- **Embedded** and/or dedicated HSMs will be a standard requirement for ethernet ECUs

- **Two** (or even more) **processor architectures** for ECUs with more bus technologies might also become a standard requirement

- Make the net **static** e.g. **no ICMP + static neighbor cache**

Legend:
- ICMP: Internet control message protocol
- MAC-Sec: 802.1AE Mac security standard
- HSM: Hardware security module
- TLS: Transport layer security
Measures – Filter and Log

• Each network component needs a stateful firewall

• Communication is allowed based on a white-list

• DPI when possible and where needed e.g. on Ethernet <-> legacy bus devices

• Rate limiting
  Cyclic Multicast translates into \textbf{bit/s on port X}

• Most important: Logging!
  The \textbf{more information} is logged once a packet is discarded the easier it is to \textbf{find} the cause and distinguish between babbling idiot and a \textbf{possible attack}
 Measures – IDS and IPS

- We know at a very detailed level how the normal communication within the car should look like.

- We should use this to implement anomaly detection systems (IDS).

- Distributed or centralized approach.

- Hybrids of statistical methods (learning) and static approaches are thinkable.

- Reporting to backend important to detect attacks on a fleet.

- Cut links if suspicious communication is detected (IPS).

Legend:
IDS: Intrusion detection system
IPS: Intrusion prevention system
• Working towards a **decentralized architecture**: Domain oriented
• Establish link **redundancy** via broad-band (>= 1Gbit) Ethernet.
• Distribution of **functions** including failover
• Need for **more powerful ECUs**
• **Reduction** of ECUs
• POSIX/Linux is getting more and more **interesting**!
Summary

• A lot of „new“ functions will come to the car which are enabled by Ethernet

• Network Security is driven by Ethernet but will not stop there

• Embedded and dedicated HSMs will be an important building block

• We can learn a lot from the IT industry:
  Don’t reinvent the wheel! Adopt it!

• Decentralized gateway concept will gain momentum

• POSIX OS (or similar) will become more important
Thank you!

Dr. rer. nat. Christian Meineck

Dr. Ing. h.c. F. Porsche AG
Vernetzung / Diagnose und Gateways
Porschestraße 911
71287 Weissach
Telefon: +49 (0) 711 / 911-81921
E-Mail: Christian.Meineck@porsche.de