Holger Zeltwanger

“Machines” on wheels
Standardizing cyber security in commercial vehicles

headquarters@can-cia.org
Presentation outline

- Cyber security is nothing new
- Experiences in automotive applications
- EC regulation on securing the measured load
- DIN 4630: Secured telematics
- Cyber-security engineering

Takeaway: “The whole is greater than the sum of the parts.” (Aristotle)
**Security and duty vehicles**

*Takeaway:* Automated and autonomous machines need secure networks.
Cyber security is nothing new

Takeaway: Do not re-invent the wheel.
Cyber crimes and defense

- Value of cyber crimes will increase to US-$ 8 billion in 2020 (source: Juniper Research). In 2016, it was the second most reported kind of crime (source: PWC).
- The WannaCry ransomware attack affected more than 200,000 systems including industrial control systems.
- An attacker resides within a network for an 146-days average before detection (source: Microsoft).
- Most network intrusions (63 %) are the result of weak or “stolen” passwords.
- Microsoft checks per month 400 billion e-mails and 450 billion app log-ins on phishing attacks. Bing search engine observes 18 billion indexed web pages on malicious software.

Takeaway: Cyber crime is a big business like illegal drugs.
Vulnerabilities and attacks

- **Direct-access attack**: Unauthorized user gaining physical access
- **Backdoor**: Bypassing normal authentication or security checks
- **Denial-of-service (DoS) attacks**: Making the machine or network unavailable
- **Eavesdropping**: Listing to a private conversation (e.g. monitoring electro-magnetic transmissions)
- **Spoofing**: Masquerading as a valid entity
- **Tampering**: Malicious modification of products
- **Phishing**: Acquiring sensitive information (e.g. passwords, keys)
- Etc.

**Takeaway**: The weakest link in the chain breaks.
Denial-of-service attacks

ICS-ALERT-17-209-01: DoS vulnerability reported by Italian researchers (adding a CAN error frame producing unit)

Takeaway: Protect your properties. Limit the access.
Limit the access

Do not map the JTAG protocol unsecured to the CAN interface, for example.

Takeaway: Protect all (!) “doors” and “windows”.

© CiA
Automotive experiences

Takeaway: Lock doors, windows, hood, trunk, and all other interfaces!
Why cyber security matters

FCA recalled 1.4 million cars after the Jeep hack.
Security researchers detected a series of vulnerabilities in in-vehicle network designs, in particular maleficent CAN-based messages could be injected causing for example brake ECUs to enter service mode or to disable the brake system.
The carmakers are very concerned about “fleet” attacks, because they make them to be susceptible to blackmails.

Takeaway: Recalling of cars can be costly, to be blackmailed, too.
The chosen approach complies with Autosar SecOS:
- Client (test tool) requests the “seed” from the server (car ECU),
- Server sends the “seed”,
- Client sends the “key” (appropriate for the “seed” received),
- Server responds that the “key” is valid and that it is unlocked.

**Takeaway:** The OBDII is secured on application level and transport layer.
**Cryptography options**

ISO 14229-1 authentication service \( (29_{16}) \)

- Authentication with PKI* Certificate Exchange (APCE)
- Authentication with Challenge-Response (ACR)

Asymmetric cryptography

Symmetric cryptography

Costs

*PKI: public key infrastructure

**Takeaway:** Generic external test tools need to implement all options.
ISO 26021 series: Password

Takeaway: Do not use “weak” passwords, add other security provisions.
ISO 16844 series: Tachograph

Scope

The Digital Tachograph is a recorder of the professional drivers’ activities (rest and driving hours). It provides trustworthy information to EU enforcers controlling compliance with Social Regulation (EC) No 561/2006. The digital tachograph was introduced to:

Objectives

- Increase road safety, by controlling the activity of the drivers (limiting daily driving hours)
- Ensure minimum working conditions standards for professional drivers
- Guarantee fair competition between EU transport companies

Technical Requirements

In order to fulfill these objectives the digital tachograph requires a motion sensor paired with it and smartcards which are used to control secure access to the device and its data for drivers, law enforcers, companies and workshops.

Takeaway: Start with securing the sensor data.
**Takeaway:** Cyber security is a system design issue.
On-board weighing system

ISO 11992-2-to-CiA-413 gateway

CiA 413

CiA 459

On-board weighing device IF
On-board weighing controller IF

CiA 461 series

Secured and sealed

Takeaway: Use securely connected sensors.
The OBW* controller writes the same Trivium key to all devices in the weighing system before sealing it in a secure environment.

Takeaway: Sealed sensors/controllers do not need further authentication.
**Takeaway:** There are different security requirements (e.g. geo-fencing).
Agriculture hacking

- FBI warns agriculture industry about increasing cyber risk, in particular in relation to “precision farming”.
- Many agriculture vehicles are using the not cyber-secured CAN-based ISO 11783 series network connecting tractors and so-called implements (harvesting machines and other add-on equipment such as sprayers).
- Market-leading agriculture equipment supplier use EULAs (end-user license agreements) to force farmers to update software only in the suppliers’ workshops, due to security reasons.
- Farmers fight back for their right-to-repair their agriculture machinery by themselves.

**Takeaway:** There could be conflicts between suppliers and end-users.
ISO/SAE 21434 series

- Experts from ISO and SAE are developing jointly a cyber security process framework standard series.
- This framework is tailored from the ISO 26262 functional safety process framework.
- This framework includes a common language for communicating and managing cyber security risk among stakeholders.
- This framework does not prescribe specific technology or solutions related to cyber security.

Takeaway: Standardizing cyber security engineering is necessary.
IEC 62443 series

IEC 62443-1: Terminology, concepts and models

IEC 62443-2: Establishing an industrial automation and control system security program

IEC 62443-3: Operating an industrial automation control system security program

IEC 62443-4: Specific security requirements for industrial automation and control systems

IEC 62443-5: Security technologies for industrial automation and control systems

Takeaway: Should be ISO/SAE 21434 and IEC 62443 harmonized?
HLP* (“data link”) security

- It is based on cryptographic methods that include encryption, digital signatures, and message authentication codes (MACs).
- It provides a description of services to establish ECUs as trusted parties in respect of one another and to protect against specific threats.
- It is applicable to all network technologies between pairs of ECUs capable of storing and processing secret data so that unauthorized third parties are denied access to it.
- Parameters are provided to select the desired level of security.
- It is used for example by the ISO 16844 tachograph standard.

* HLP: higher-layer protocol

Takeaway: ISO 15764 is a proven generic encryption standard.
CiA 602-2, CAN FD for commercial vehicles – Part 2: Application layer

<table>
<thead>
<tr>
<th>CAN-ID</th>
<th>CAN FD data field (up to 64 byte)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-bit or 29-bit*</td>
<td>Multi-PDU</td>
</tr>
<tr>
<td>C-PDU 1</td>
<td>C-PDU 2</td>
</tr>
</tbody>
</table>

* Includes the SAE J1939 Source Address

“Autosar” PDU short header (4 byte) ─ Payload

<table>
<thead>
<tr>
<th>24-bit ID</th>
<th>AD (e.g. J1939 PG)</th>
<th>(Safety/security) trailer</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS</td>
<td>TL</td>
<td></td>
</tr>
<tr>
<td>3 bit</td>
<td>3 bit</td>
<td>2 bit</td>
</tr>
<tr>
<td>Data page</td>
<td>PDUF</td>
<td>8 bit</td>
</tr>
<tr>
<td>PDUS</td>
<td>PL length</td>
<td>8 bit</td>
</tr>
<tr>
<td>1 to 60 byte</td>
<td></td>
<td>0, 4 or 8 byte</td>
</tr>
</tbody>
</table>

LEGEND
TL = trailer length

**Takeaway:** CAN FD provides sufficient payload length for security.
CAN data link security

CAN supports security out-of-the-box for initial key exchange

◆ Everybody can transmit but nobody knows, who it is.
◆ Diffie-Hellman (DH) key exchange* can be speed-up.

* The initial key can be used to encrypt subsequent communications using a symmetric key cipher (prior to public key methods like DH, cryptographic keys had to be transmitted in physical form such as key lists for the Enigma).

Takeaway: A CAN node fingerprint can only be identified by oscilloscopes.
Takeaway: Security in hardware can improve the overall security.
Summary

- The whole is greater than the sum of the parts: Cyber security is a system design issue.

- Each cyber security case is unique: Individual assessments are necessary.

- Cyber security is highly political: Laws and regulations should protect the “weakest” stakeholders (e.g. the right-to-repair).

- Do not re-invent the wheel: Laws and regulations can be simplified by referencing the appropriate cyber security related standards.
Questions and answers

If you enjoyed my presentation tell it to others; if not, keep it to yourself.