“Automotive Security: Challenges, Standards and Solutions”

Alexander Much
12 October 2017
Driver’s fears are being fueled by recent news
New business models for hackers?

Pied Piper of Hamelin
Autonomous theft?
WORLD You GUESS THIS WEIGHS AS MUCH AS A SMALL ADULT?
WHAT?
 Uh, PROBABLY.

GREAT!

*THUMP*
PLEASE FASTEN YOUR SEAT BELT.
*CLICK*
TAKE ME TO ANCHORAGE, ALASKA.
NAVIGATING.

*SLAM*

I LOVE SELF-DRIVING CARS.
...WHOSE CAR WAS THAT?
DUNNO, BUT THEY SHOULDN'T HAVE LEFT IT RUNNING.

© xkcd.com, https://xkcd.com/1559/
From: Bill Gates  
Sent: Tuesday, January 15, 2002 5:22 PM  
To: Microsoft and Subsidiaries: All FTE  
Subject: Trustworthy computing

When we face a choice between adding features and resolving security issues, we need to choose security. We must lead the industry to a whole new level of Trustworthiness in computing. [...]

Trustworthy Computing is the highest priority for all the work we are doing. [...]

Key aspects include: [...] Availability, [...] Security, [...] Privacy.

Do we have similar challenges now in Automotive?
Dependability?

Important:
• safety != reliability
• safety != security
• safety != availability

The challenge: balancing „ilities“.

Security is arriving fast!

Safety << Security!

Standards, Norms and Activities

- ISO/SAE AWI 21434 - Road Vehicles -- Cybersecurity engineering (Under development)
- NIST, FIPS, etc.
- CERT ([coding standards and more](#))
- MISRA (coding standard)
- ISO 27000 ([wikipedia](#))
- RTCA/DO-326 (avionics)
- IEC 62443 (primarily automation)
- CMMI ([Security by Design with CMMI v1.3](#), from Siemens)
- Microsoft SDL ([Security Development Lifecycle](#))
- EVITA ([research project](#))
- Automotive OEM standards
- SAE J3061
- OpenSAMM ([Software Assurance Maturity Model](#))
  (4 additional processes, similar to e.g. ISO 15504-10)
- and many, many more …
Defining the system boundaries is complex in development as well as during operations.

Systems are dynamic: assumptions made during development may be false during operations.

© Nancy Leveson, Engineering a Safer World (free download)
OTA & Quality: A “Warning”

• OTA offers many opportunities, including business models, etc.
• OTA will fundamentally change how we look at function deployment.

• OTA partially lowers SOP “pressure”:

  “we’ll add / fix it later”

• Easy updates have lead to crappy software in other domains.

The quality community needs to be aware of this fact!
Defense-in-Depth Strategy

Level 1: Restrict access to the network
Level 2: Secure onboard communication
Level 3: Apply data usage policies
Level 4: Detect anomalies and defend
Entry Points

- Car2Infra
- Car2Car
- eCall
- WiFi Hotspot
- Remote HVAC
- Remote start
- Tire pressure monitor
- Bluetooth connection
- Wireless key
- Internet connection
- CDROM, USB
- OBD, Diagnosis
Level 1: Restrict access to the network (I)

- **Limit the number** of ECUs with **off-board connections** (WLAN, bluetooth, cellular, wireless key, DAB, OBD plug, PLC), e.g. via
  - central network access point with stateful firewall
  - diagnostic communication from external tester to ECUs via central gateway (communication between tester and central gateway via TLS)
Level 1: Restrict access to the network (II)

- Divide network into security zones, e.g. extern, “demilitarized”, internal. And restrict traffic between zones: Physical split or separation via VLANs
- Not only extern-intern, but also intern-intern, e.g. infotainment to powertrain
Level 1: Restrict access to the network (III)

- static **Ethernet Switch** Forwarding tables OR MAC learning only during learning mode (e.g. end-of-line)

- static ARP tables **at nodes** OR Address Resolution Protocol only during learning mode (e.g. end-of-line)

- **device authentication/authorization**

- **deactivation** of unused (non authorized) ports

Source: AUTOSAR 4.2 EthSwt SWS
Multi-Level 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
### Level 2: Secure onboard communication

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Standard</th>
<th>Type/Layer</th>
<th>Authent.</th>
<th>Encryption</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACsec</td>
<td>IEEE 802.1AE</td>
<td>Hop-by-hop Data-Link</td>
<td>X</td>
<td>X</td>
<td>Requires crypto/keys at each network node</td>
</tr>
<tr>
<td>IPsec AH</td>
<td>IETF RfC 4302</td>
<td>End-to-End IP</td>
<td>X</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>(Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Header)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPsec ESP</td>
<td>IETF RfC 4303</td>
<td>End-to-End IP</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>(Encapsulating</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Payload)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>IETF RfC 5246</td>
<td>End-to-End TCP</td>
<td>X</td>
<td>X</td>
<td>Does not work with UDP</td>
</tr>
<tr>
<td>(Transport Layer Security)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecOC</td>
<td>AUTOSAR</td>
<td>End-to-End PDUs</td>
<td>X</td>
<td>-</td>
<td>supports MACtruncation (works also with CAN / FlexRay)</td>
</tr>
</tbody>
</table>
Multi-Level 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
Level 4: Detect anomalies and defend

- **Anomalies:** deviations to specified communication matrices

- **Detection:** via central device or at the receiver
  e.g. plausibility check based on diverse input data or data sequence, failed integrity checks

- **Defend:** report (e.g. DTC, involvement of driver, …) and start mitigation
  - mask (e.g. block messages from infotainment ECU, block messages from “babbling idiot” by enforcing bandwidth limitation at switches) or
  - reconfigure (e.g. deactivation of critical functions, initiate hand-over in case of autonomous driving, request change of session key …)
Levels protecting against attacks violating the **availability**, **integrity** and **confidentiality**:

<table>
<thead>
<tr>
<th>Level</th>
<th>Availability</th>
<th>Integrity</th>
<th>Confidentiality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1: restrict access to the network</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Level 2: secure onboard communication</td>
<td>No (DoS attacks)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Level 3: apply data usage policies</td>
<td>No (DoS attacks)</td>
<td>Yes</td>
<td>No (eavesdropping)</td>
</tr>
<tr>
<td>Level 4: detect anomalies and defend</td>
<td>Yes (Yes)</td>
<td>(Yes)</td>
<td>No (eavesdropping)</td>
</tr>
</tbody>
</table>
Standardization for security similar to ISO 26262 is needed, which forms a **consensus** in the automotive domain.

Safety, security, reliability are system aspects that need to be balanced. → They are all part of the “quality” of the product.

We need assessors who are technical experts of the systems they assess. → “Simple” process and document checking won’t be enough.

The community needs to co-ordinate specialty engineering audits.

Systems engineering needs to be established within organizations.
Questions?