Automotive Cybersecurity Regulations

Dr. Kai Frederik ZASTROW
Senior Fellow Regulation Certification Standards, Stellantis
Chairman of OICA Cluster 4 Cybersecurity and Software Updates
Why cybersecurity regulation?

- **Risk of cyberattacks**
  - **Safety/Security impact:**
    - Hacker may get access to *private data* or may *manipulate* existing vehicle software
    - Hacker may use vehicle as weapon for *criminal actions* / terrorist attacks
  - **Economic impact:**
    - Automotive cybersecurity market: about 683 M € in 2023 (IHS Markit)
    - Economic risk for vehicle manufacturer, e.g. for recalls

- **Objective of the regulation**
  - *Protect the vehicle from cyber-attacks*
Why SW update regulation?

- Update software on vehicles during the whole vehicle life in order to:
  - **Ensure safety/security** of the vehicle (bug fixes, cybersecurity updates, etc.)
  - Maintain functionality and **compliance with legal acts** (traffic rules, etc.)
  - **Add new functions** (e.g. infotainment) **without** impact on type approved characteristics.
  - **Add new functions** (e.g. ADAS functionalities) **with** impact on type approved characteristics that are covered by new/extended type approvals.

- Objective of the regulation
  - Ensure that the SW on a vehicle is and stays **compliant with vehicle homologation**
Global Automotive Standards and Regulations to address Cybersecurity and SW updates

**UN / WP.29 – World Forum for Harmonization of Vehicle Regulations**
- UN Regulation 155 on Cyber Security
- UN Regulation 156 on SW updates

**ISO TC22/SC32/WG11 - Cybersecurity**
- ISO/SAE 21434 Cybersecurity Engineering

**ISO TC22/SC32/WG12 – Software update**
- ISO 24089 Software Update Engineering

**National Discussions**
- Germany VDA QMC
- UK BSI PAS 1885:2018
- ...  

**European Union**
- Cybersecurity Act
- General Data Protection Regulation
- NIS Directive (Network and Information Security)

**China**
- Cybersecurity Law & Data Security Law
- Personal Information Protection Law
- Information Security: SAC/TC 260
- Automotive: SAC/TC 114/SC 34/WG Cyber

**USA**
- NHTSA Cybersecurity Guidelines

**UN Regulations (adopted in June 2020) are worldwide consensus:**
Developed under GRVA (chaired by Germany, Japan and China) / TF Cybersecurity & OTA issues (chaired by UK, Japan and USA).
Cybersecurity concerns the whole vehicle

Example for risks of unsecured access:

⇒ Cybersecurity cannot be covered by certification of only some specific components
Split approach for the cybersecurity assessment:

i) Assessment and certification of vehicle manufacturer **Cyber Security Management System**

ii) Assessment and certification of **vehicles**

**Organizational structure & processes**

**Design of the vehicle EE architecture, risk assessment and implementation of mitigations**
## Annex 5, Part A: List of threats

<table>
<thead>
<tr>
<th>High level and sub-level descriptions of vulnerability/threat</th>
<th>Example of vulnerability or attack method</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1 Threats regarding back-end servers related to vehicles in the field</td>
<td></td>
</tr>
<tr>
<td>1. Back-end servers used as a means to attack a vehicle or extract data</td>
<td></td>
</tr>
<tr>
<td>1.1 Abuse of privileges by staff (insider attack)</td>
<td></td>
</tr>
<tr>
<td>1.2 Unauthorized internet access to the server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)</td>
<td></td>
</tr>
<tr>
<td>1.3 Unauthorized physical access to the server (conducted by for example USB sticks or other media connecting to the server)</td>
<td></td>
</tr>
<tr>
<td>2. Services from back-end server being disrupted, affecting the operation of a vehicle</td>
<td></td>
</tr>
<tr>
<td>2.1 Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on</td>
<td></td>
</tr>
<tr>
<td>3. Vehicle related data held on back-end servers being lost or compromised (“data breach”)</td>
<td></td>
</tr>
<tr>
<td>3.1 Abuse of privileges by staff (insider attack)</td>
<td></td>
</tr>
<tr>
<td>3.2 Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers</td>
<td></td>
</tr>
<tr>
<td>3.3 Unauthorized internet access to the server</td>
<td></td>
</tr>
</tbody>
</table>
### Annex 5, Part B: Mitigations on vehicles

#### Table B1
Mitigation to the threats which are related to "Vehicle communication channels"

<table>
<thead>
<tr>
<th>Table A1 reference</th>
<th>Threats to &quot;Vehicle communication channels&quot;</th>
<th>Ref</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation</td>
<td>M10</td>
<td>The vehicle shall verify the authenticity and integrity of messages it receives</td>
</tr>
<tr>
<td>4.2</td>
<td>Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)</td>
<td>M11</td>
<td>Security controls shall be implemented for storing cryptographic keys (e.g., use of Hardware Security Modules)</td>
</tr>
<tr>
<td>5.1</td>
<td>Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream</td>
<td>M10</td>
<td>The vehicle shall verify the authenticity and integrity of messages it receives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M6</td>
<td>Systems shall implement security by design to minimize risks</td>
</tr>
<tr>
<td>5.2</td>
<td>Communication channels permit manipulation of vehicle held data/code</td>
<td>M7</td>
<td>Access control techniques and designs shall be applied to protect system data/code</td>
</tr>
</tbody>
</table>
Annex 5, Part C: Mitigations outside the vehicle

Table C1
Mitigations to the threats which are related to "Back-end servers"

<table>
<thead>
<tr>
<th>Table A1 reference</th>
<th>Threats to &quot;Back-end servers&quot;</th>
<th>Ref</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 &amp; 3.1</td>
<td>Abuse of privileges by staff (insider attack)</td>
<td>M1</td>
<td>Security Controls are applied to back-end systems to minimise the risk of insider attack</td>
</tr>
<tr>
<td>1.2 &amp; 3.3</td>
<td>Unauthorised internet access to the server (enabled for example by backdoors, unpatched system</td>
<td>M2</td>
<td>Security Controls are applied to back-end systems to minimise unauthorised access. Example Security Controls can be found in OWASP</td>
</tr>
<tr>
<td></td>
<td>software vulnerabilities, SQL attacks or other means)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3 &amp; 3.4</td>
<td>Unauthorised physical access to the server (conducted for example by USB sticks or other media</td>
<td>M8</td>
<td>Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data</td>
</tr>
<tr>
<td></td>
<td>connecting to the server)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Attack on back-end server stops it functioning, for example it prevents it from interacting</td>
<td>M3</td>
<td>Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP</td>
</tr>
<tr>
<td></td>
<td>with vehicles and providing services they rely on</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Loss of information in the database</td>
<td>M4</td>
<td>Security Controls are applied to minimise risk</td>
</tr>
</tbody>
</table>
UN Regulation 156 on SW updates

Split approach:

i) Assessment and certification of vehicle manufacturer **Software Update Management System**

ii) Assessment and certification of **vehicles**

iii) Implementation of **software identification numbers** for specific regulations

- Organizational structure & processes, incl. management of SW identification
- Requirements for safe execution of SW updates and user information
- Implementation of SW identification numbers (RXSWIN) in specific regulations
R155 Cybersecurity & R156 SW update implementation

- Jan 2021: Entry into force: legal acts are available for application by UN Contracting Parties.
- UN Contracting Parties require them in their national vehicle type approval:
  - Japan
    - R155 & R156
      • Immediately for automated vehicles SAE level 3 or higher
      • July 2022 for new whole vehicle types & July 2024 for new registrations if SU affecting type approval and OTA capability
      • Jan 2024 for new whole vehicle types & May 2026 for new registrations: R155 & 156 if SU affecting type approval and no OTA capability; R155 in all other cases
  - European Union
    - R155: 6 July 2022 for new whole vehicle types & 7 July 2024 for new registrations
    - R156: under preparation (via delegated act amending EU 2018/858)
  - Other countries may follow
“Recommendations on uniform provisions concerning cyber security and software updates”

- Document produced by UN Task Force is as much as possible aligned with R155 and R156 for countries that have no type approval regime.
  - Covers both: cyber security and software update processes
  - Covers the whole life cycle of a vehicle model (from design to post-production)
  - Lists technical requirements for the vehicle and for the management system
  - Considers the concept of SW identification numbers (RXSWIN)

- Recommendation WP.29/GRVA/2022/5 adopted by GRVA in January 2022

- Need to follow next steps
Opportunities for global harmonization

- Make sure that the **54 signatory countries** of the UN Geneva 1958 Agreement **apply the UN Regulations** (and do not invent national requirements)

- Make sure that countries that do not apply directly R155 and R156 **apply at least the Recommendations** on uniform provisions

- **Harmonize the Chinese draft national standards** under development by SAC/TC 114/SC 34/WG Cyber **with ISO and UN**.
THANK YOU FOR YOUR INTEREST!
Link to UN documents