Cyber security in V2X communications

Gilles Ampt – 5 December 2017
Chairman of Security Community
Smart Mobility Standards & Practices
Cyber security in V2X communications

Gilles Ampt
security@ditcm.eu

5 December 2017
Topics to be discussed today

• What is Vehicle Security?
• What is V2X Security?
• What are the main risks in V2X?
• WHEN and HOW to address V2X risks?
• How about a trusted V2X communications network?
Dutch Smart Mobility Community for Standards & Practices

• Objective: acceleration of the implementation and large scale deployment of Smart Mobility.
• Central place in the Netherlands for knowledge sharing and decision making.
• Involvement of experts and policy makers from governments, industry and research institutions.
• National governance connected to international platforms.
Security Experts Say That Hacking Cars Is Easy

by Jonathan Vanian       ©JonathanVanian       JANUARY 20, 2016, 01:17 PM EDT

It’s Now Legal to Hack Your Car’s Many Computers

Sensitive vehicle data could be easily manipulated, altered or distributed - undetected - if these changes are implemented.

New car features come at a cost

Automobiles may be getting more advanced, but that
What is Security?

Being in Control of Risks

• Risks of Connected Vehicles
  – Vehicle theft (digital attack)
  – Motor management manipulation (unauthorized remote control)
  – Data loss (incl. loss of personal data/privacy)
  – Software updates (reliability, authorization)

• Application interests at risk:
  – Integrity of data
  – Confidentiality of data
  – Availability of data
  – Authorised Access and Authenticated Access
Connected driving part of Autonomous driving

- Emergency Vehicle
- Green Light Optimal Speed Advisory
- Hazardous Location Warning
- Warning Lights on
- Avoidance of traffic jams
- Local Road Works Warning
### Initial risks in V2X communications

<table>
<thead>
<tr>
<th>Threats</th>
<th>Likelihood/Impact/Risk assessment</th>
<th>(ETSI) design requirement/ Organisation Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>GNSS jamming and spoofing</td>
<td>critical</td>
<td>Monitoring, Robust design e.g. dGPS</td>
</tr>
<tr>
<td>Radio signal jamming</td>
<td>critical</td>
<td>Radio frequency agility and control</td>
</tr>
<tr>
<td>Message saturation</td>
<td>critical</td>
<td>Message frequency control and Authentication</td>
</tr>
<tr>
<td>Replay of expired/old messages</td>
<td>critical</td>
<td>Message timestamps</td>
</tr>
</tbody>
</table>

When and how to address risk?

- Risk ownership
  - delegation of risk would be window dressing
- Risk assessment
  - repeatedly needed as risk landscape is evolving

- Legal compliance
  - New EU privacy law (GDPR) demands risk based approach
- Security baselines
  - Stakeholders require organisations to be in control

- V2X communications
  - Security by design

Risk is a management process

Risk is a choice of management
Security by Design

- EU trust framework for V2X communications
- Authentication and authorisation of ITS stations
  - Commercial vehicles
  - Special purpose vehicles
  - Road side units
Cyber security in V2X communications

Gilles Ampt
security@ditcm.eu

5 December 2017