Enhancing automotive cybersecurity in Europe

Liveri Dimitra | OECD Workshop on Digital Security and Resilience in Critical Infrastructure and Essential Services | 16.02.18, Paris

European Union Agency for Network and Information Security
Positioning ENISA activities

**CAPACITY**
- Hands on activities

**POLICY**
- Support MS & COM in Policy implementation
- Harmonisation across EU

**COMMUNITY**

**EXPERTISE**
- Recommendations
- Independent Advice
Secure Infrastructure and Services

www.enisa.europa.eu/topics
Smart Cars Security Landscape
Smart cars security

- Connected and Autonomous Vehicles cybersecurity
  - C-ITS Platform
    - Certificate Policy
    - Security Policy

- What about cars of today?
  - Day 1 (and 1+) will see CAD coexisting with today’s cars
  - It’s becoming more and more frequent headlines item
  - Cybersecurity concerns of today’s cars need to be examined
What could possibly go wrong?

Car hackers:
Model S

Hackers exploited connected "smart" devices for massive cyberattack

U.S. investigators are still trying to figure out who was behind the cyberattack Friday that crippled some of the biggest sites on the internet, from Amazon to Twitter.

Researchers blind autonomous cars by tricking LIDAR

As I was on the motorway, I saw a man who wasn't there. Then things went pear-shaped.
Securing Smart Cars
Securing Smart Cars

- Increased attack surface
- Insecure development in today’s cars
- Security culture
- Liability
- Safety and security process integration
- Supply chain and glue code
REGULATING INTELLIGENT VEHICLES
EU issued a directive (2010/40/EU) on intelligent transport systems, this being one of the first efforts of the EU in the direction of regulating security for smart cars.

C-ITS DEPLOYMENT PLATFORM
DG MOVE sets up (November 2014) the C-ITS deployment platform with a focus on connected and autonomous cars. Dedicated working group on security. Overall goal is to reach consensus among stakeholders on C-ITS deployment issues.

2010

2013

2014

JUNE
FIRST AUTO ISAC
With the aim to facilitate sharing of information on cyber security threats in the automotive field, carmakers set up the Auto ISAC.

INTERNET-BASED ATTACKS ON THE RISE
In one of the most widely reported attacks, C. Miller and C. Valasek hacked a Jeep Cherokee via the Internet. They were able to take control of a series of features and led to a recall of 1.4 million cars in order to patch the vulnerability.

FEBRUARY
ENISA JOINS THE FIELD
ENISA, the EU cyber security agency commences work on smart car cyber security. ENISA also sets up the CARSEC expert group on car security. ENISA’s aims to engage with stakeholders, propose recommendations and raise awareness.

2015

SEPTEMBER
ADDRESSING HACKING GOES GLOBAL
G7 transport ministers reach an agreement to join forces to fight the increasing threat of car hacking. They issued a related declaration on automated and connected driving.

MAY
ATTACKS BECOME MAINSTREAM
In another case of a cyber attack, researchers were able to hack the Mitsubishi Outlander over Wi-Fi, and thus gaining control of the alarm. This allowed them to drain the car’s battery and to gain access to the lights.

2016

JULY
EU FUNDS RELATED RESEARCH
A cybersecurity research scheme is launched by the European Commission. The goal is to trigger funding of €1.8 billion.

NIS DIRECTIVE
The NIS Directive comes into force, aiming at increased cybersecurity in critical infrastructure. Amongst other sectors, it will mandate security requirements for road transport operators of essential services.

AUGUST
MILLER AND VALASEK STRIKE AGAIN
In a new attack, the two researchers exposed a series of novel hacks that when exploited can provide access to the steering wheel, the acceleration/braking system. Said attacks required that the computer be plugged into the dashboard.

JULY
ATTACK ON CAR KEYS
A vulnerability allowed security researchers to attack Volkswagen’s keyless ignition system. It enabled igniting the car engine without actually using the keys. Volkswagen sued the researchers, who published an academic paper two years later.

FURTHER ATTACKS
Another attack on smart cars involved the Ford Escape, on which hackers were able to disable the brake system and have access to the horn via their computer.
Smart cars Perimeter

Secure Smart Cars today
for safer autonomous cars tomorrow
Smart Cars Assets

**BODY CONTROL**
- Protocols: CAN, LIN/SAE J2602, RF...
- Services: Keyless/passive entry...

**INFOTAINMENT CONTROL**
- Protocols: MOST, Bluetooth, Wifi...
- Services: entertainment (audio/video), driving services: traffic information, maps...
- Infotainment subnetwork (e.g. MOST), Ad-hoc internal networks (e.g. Bluetooth, Wifi...)

**POWERTRAIN CONTROL**
- Protocols: CAN...
- Services: Powertrain control

**CHASSIS CONTROL**
- Protocols: CAN, FlexRay, RF...
- Services: Drive- or brake-by-wire, lane assist, collision control...

**DIAGNOSTIC AND MAINTENANCE SYSTEMS**
- Protocols: OBD II, Ethernet...
- OBD II ports, Aftermarket dongles, Garage or maintenance equipment

**COMMUNICATIONS CONTROL**
- Protocols: 3G, Wifi...
- Services: eCall services

Legend:
- Components
- Networks

**Assets**

- Body control subnetwork
- Diagnostic subnetwork
- Power train subnetwork
- Chassis control subnetwork
- External communication networks
Smart Cars Threats

**DAMAGE / LOSS (IT ASSETS)**
- Loss of information in the cloud
- Loss of (integrity of) sensitive information
- Damage caused by a third party
- Loss from DRM conflicts
- Information leakage

**PHYSICAL THREATS**
- Fault injection / glitching
- Side channel
- Access to HW debug ports

**NEFARIOUS ACTIVITY / ABUSE**
- Denial of service
- Malicious code / software activity
- Manipulation of hardware & software
- Manipulation of information
- Unauthorized access to information system / network
- Compromising confidential information
- Identity fraud
- Abuse of information leakage
- Unauthorized use of administration of devices & systems
- Unauthorized use of software
- Unauthorized installation of software
- Abuse of authorizations
- Malicious software
- Remote activity (execution)

**FAILURES / MALFUNCTIONS**
- Failures / malfunctions of devices or systems
- Failures or disruptions of the power supply
- Software bugs
- Failures / malfunctions of parts of devices
- Failures or disruptions of communication links
- Failures or disruptions of main supply

**NETWORK OUTAGE**

**UNINTENTIONAL DAMAGES (ACCIDENTAL)**
- Information leakage or sharing
- Erroneous use or administration of devices and systems
- Using information from an unreliable source
- Unintentional change of data in an information system
- Inadequate design and planning or lack of adoption

**ADVANCED PERSISTENT THREATS**

**EAVESDROPPING / INTERCEPTION / HIJACKING**
- Interception of information
- Replay of messages
- Interfering radiations
- Man in the middle / session hijacking
- Network reconnaissance and information gathering
- Repudiation of actions

**LEGEND:**
- Threats perceived as significant by ≥80% answers
- Threats perceived as significant by ≤60% answers
Attacks scenarios

ENVIRONMENT: VEHICLE PASSENGER COMPARTMENT

1. Get a direct connection to car components

1bis. Obtain a legitimate or illegitimate access to diagnostic equipment

Access to CAN via OBD-II port or direct access to TCU/ECU

VEHICLE CAN NETWORK

2. From the access gained onto the TCU/ECU, obtain an access to vehicle systems

Targeted ECU

ENVIRONMENT: INTERNET/CELLULAR CARRIER

1. Use a vulnerability of an external interface to identify a vulnerable car

VEHICLE CAN NETWORK

2. Use a vulnerability of an external interface to gain access to internal services

TCU

3. From the access gained onto the TCU/ECU, obtain an access to vehicle systems

Targeted ECU
POLICY AND STANDARDS
- GP-PS-01 – Adherence to regulation
- GP-PS-02 – Liability

GOOD PRACTICES

ORGANISATIONAL MEASURES
GENERAL
- GP-OM-01 – Designate a dedicated security team
- GP-OM-02 – Define a dedicated ISMS

SECURE DEVELOPMENT
- GP-OM-03 – Assess the threat model and use cases
- GP-OM-04 – Provide security and privacy by design
- GP-OM-05 – Implement and test the security functions

SECURITY UNTIL THE END-OF-LIFE
- GP-OM-06 – Assess the security controls and patch vulnerabilities
- GP-OM-07 – Define a security update policy
- GP-OM-08 – Perform a vulnerability survey
- GP-OM-09 – Check the security assumptions regularly during life-time
- GP-OM-10 – Protect the software update mechanism
- GP-OM-11 – Raise user awareness

TECHNICAL

COMMUNICATION PROTECTION
- GP-SF-03 – Provide end-to-end protection in confidentiality and integrity
- GP-SF-04 – Mitigate vulnerabilities or limitations of standard security library
- GP-SF-05 – Consider denial of service as a usual threat to communication infrastructures
- GP-SF-06 – Protect remote monitoring and administration interfaces

IDENTIFICATION, AUTHENTICATION, AUTHORIZATION
- GP-SF-16 – Use mutual authentication for remote communication
- GP-SF-17 – Use multi-factor authentication for use authentication
- GP-SF-18 – Implement access control measures to separate the privileges of different users as well as the privileges of different applications
- GP-SF-19 – Allow and encourage the use of strong passwords
- GP-SF-20 – Enforce session management policies to avoid session hijacking
- GP-SF-21 – Provide the user with mechanisms to securely erase their private data

SECURITY AUDIT
- GP-SF-01 - Security events must be securely logged
- GP-SF-02 – Users must be informed of security events

SELF-PROTECTION
- GP-SF-22 – Define a consistent policy for self-protection
- GP-SF-23 – Implement Hardware self-protection
- GP-SF-24 – Implement Software self-protection
- GP-SF-25 – Protect Non-user data
- GP-SF-26 – Perform Hardening
- GP-SF-27 – Isolate components

CRYPTOGRAPHY
- GP-SF-07 – Do not create proprietary cryptographic schemes, but use state-of-the-art standards instead
- GP-SF-08 – Rely on an expert in cryptography
- GP-SF-09 – Consider using dedicated and independently audited, hardware security modules
- GP-SF-10 – Cryptographic keys should be securely managed

USER DATA PROTECTION
- GP-SF-11 – Identify personal data
- GP-SF-12 – Implement transparency measures
- GP-SF-13 – Design the product/service with legitimate purpose and proportionality in mind
- GP-SF-14 – Define access control, anonymity and unlinkability measures to enforce the protection of private data
- GP-SF-15 – Define measures to ensure secure deletion of user data in case of a change of ownership
Secure Smart Cars today for safer autonomous cars tomorrow
https://www.enisa.europa.eu/road
The road ahead
The Network and Information Security Directive
NIS Provisions

• Obligations for all MS to adopt a national NIS strategy and designate national authorities.

• Creates first EU cooperation group on NIS, from all MS.

• Creates a EU national CSIRTs network.

• Establishes security and notification requirements for operators of essential services and digital service providers.
### NIS Directive and Road transport

**Operators of Essential Services**

<table>
<thead>
<tr>
<th>(d) Road transport</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 (11) responsible for traffic management control</td>
</tr>
<tr>
<td>— Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council (12)</td>
</tr>
</tbody>
</table>
## NIS directive - TIMELINE

<table>
<thead>
<tr>
<th>Date</th>
<th>Duration</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2016</td>
<td>-</td>
<td>Entry into force</td>
</tr>
<tr>
<td>February 2017</td>
<td>6 months</td>
<td>Cooperation Group starts its tasks</td>
</tr>
<tr>
<td>August 2017</td>
<td>12 months</td>
<td>Adoption of implementing on security and notification requirements for DSPs</td>
</tr>
<tr>
<td>February 2018</td>
<td>18 months</td>
<td>Cooperation Group establishes work programme</td>
</tr>
<tr>
<td>9 May 2018</td>
<td>21 months</td>
<td>Transposition into national law</td>
</tr>
<tr>
<td>November 2018</td>
<td>27 months</td>
<td>Member States to identify operators of essential services</td>
</tr>
<tr>
<td>May 2019</td>
<td>33 months (i.e. 1 year after transposition)</td>
<td>Commission report - consistency of Member States' identification of OES</td>
</tr>
<tr>
<td>May 2021</td>
<td>57 months (i.e. 3 years after transposition)</td>
<td>Commission review</td>
</tr>
</tbody>
</table>
ENISA activities 2018-2019

- Support the implementation of the NISD in the Road Transport sector
- Good practices for cybersecurity of smart cars
- Collaboration with DG MOVE through C-ITS Platform
- Engagement with industrial stakeholders, e.g. ACEA, Tier 1 and Tier 2 suppliers
ENISA CaRSEC Expert Group

Join us and apply

• Contribute to ENISA efforts and reports
• Exchange knowledge and expertise
• Review ENISA studies and participate in workshops
• Platform for discussion on automotive cybersecurity

https://resilience.enisa.europa.eu/carsec-expert-group
Thank you,

Dimitra Liveri

resilience@enisa.europa.eu

https://www.enisa.europa.eu/