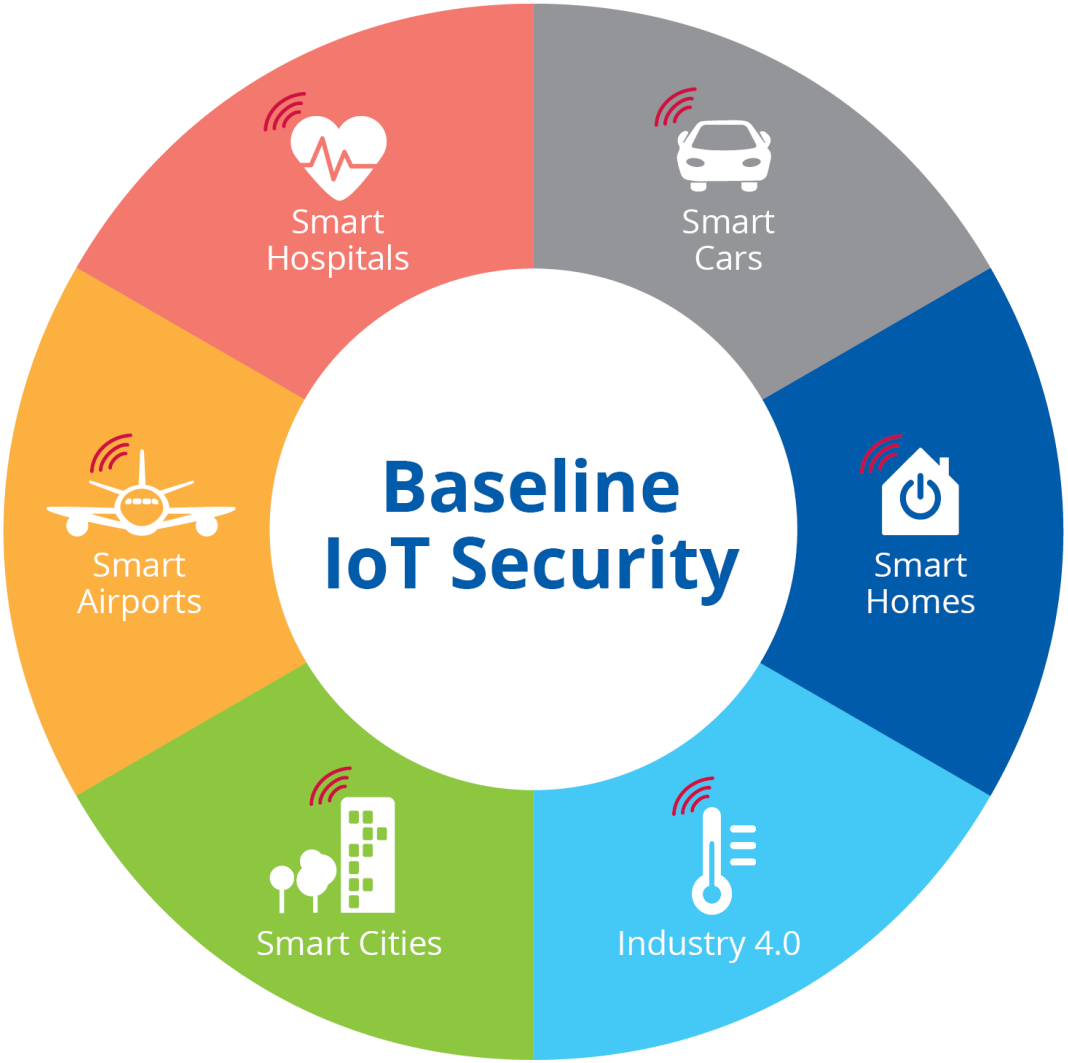
EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA EFFORTS ON AUTOMOTIVE CYBERSECURITY

Dr. Apostolos Malatras
Network and Information Security Expert, ENISA

13 | 09 | 2019

HOW DO WE SECURE IOT?



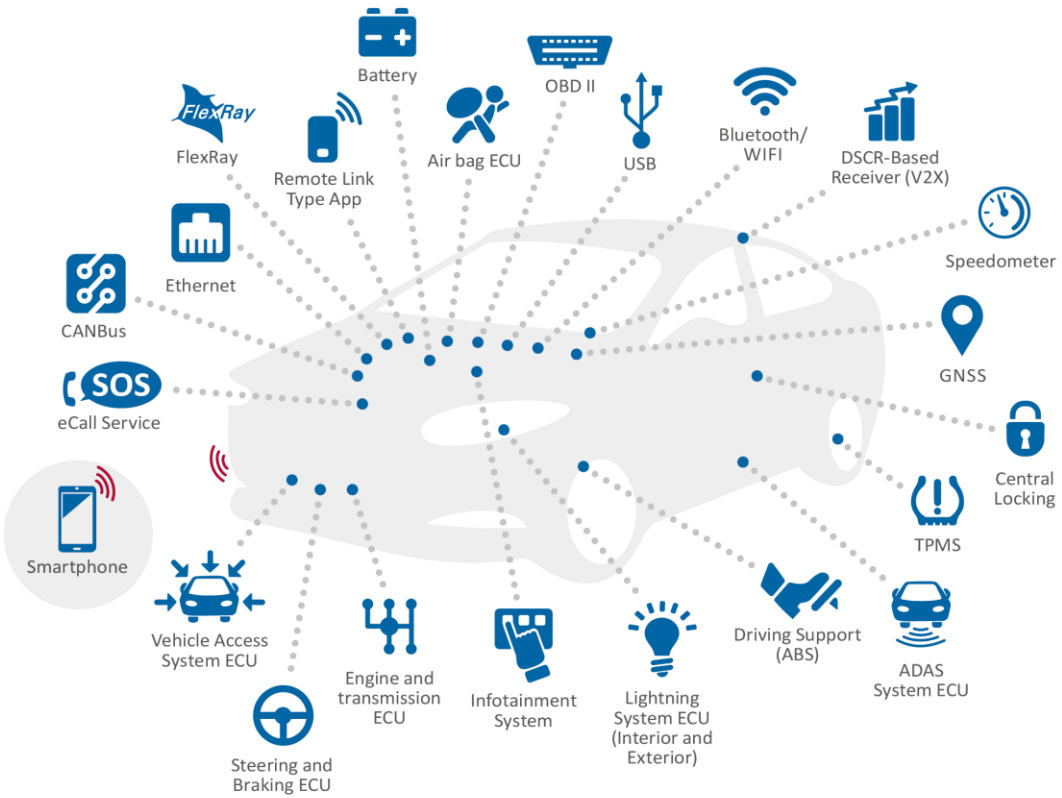
ENISA ACTIVITIES ON AUTOMOTIVE

- **Support the implementation of the NISD in the Road Transport sector**
- **Good practices for cybersecurity of smart cars**
  - 2016 ENISA study on Securing Smart Cars
  - 2019 work on **(semi-) autonomous vehicles**
- **Collaboration with DG MOVE, GROW & CONNECT via CCAM Platform**
- **Engagement with industrial stakeholders, e.g. OEMs, Tier 1 and Tier 2 suppliers**

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

AUTOMOTIVE SECURITY CHALLENGES

- **Increased attack surface**
- **Insecure development in today's cars**
- **Security culture**
- **Liability**
- **Safety and security convergence**
- **Supply chain**



THREAT TAXONOMY

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

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

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 adaption

PHYSICAL THREATS

Fault injection / glitching
Side channel
Access to HW debug ports

THREATS

ADVANCED PERSISTENT THREATS

NEFARIOUS ACTIVITY / ABUSE

Denial of service
Malicious code / software activity
Manipulation of hardware & software
Manipulation of information
Unauthorised 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)

NETWORK OUTAGE

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

SMART CARS SECURITY MEASURES

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

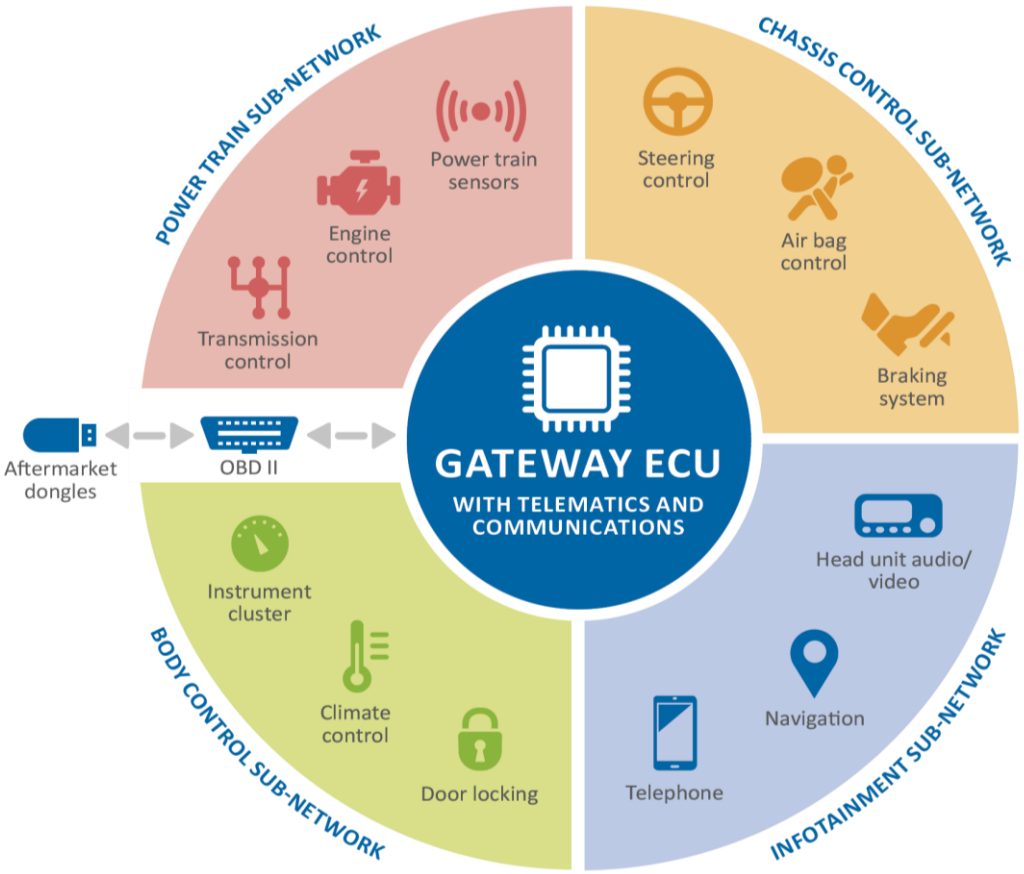
- GP-SF-07 – Do not create proprietary cryptographic schemes, but use state-of-the-art standards instead
- GP-SF-08 – Rely on an expert in cryptography
- GP-SF-09 – Consider using dedicated and independently audited, hardware security modules
- GP-SF-10 – Cryptographic keys should be securely managed

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

SMART CARS RECOMMENDATIONS

- Cybersecurity by design
- Improve information sharing amongst industry actors
- Promote consensus on technical standards & good practices
- Clarify cyber security liability among industry actors



Secure Smart Cars today
for safer autonomous vehicles tomorrow

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 FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu