Cybersecurity Challenges in the Automotive Industry

Dr. Csilling Ákos

Robert Bosch Kft.

BOSCH

Cybersecurity Challenges
The car as a rolling computer centre

- Originally, cars were designed as closed systems. Cyber-security was not an issue.
- Many different! electronic control units (ECUs) on an inhomogeneous network.
- Strong cost incentive – smallest possible controller, least possible memory, no complex calculations.
- Start up in seconds, reaction time is often critical, many real-time constraints.
- External connectivity to cloud services, infrastructure, peers and user devices.
- CANbus – designed for a closed environment, no inherent protection.
- Automotive Ethernet – designed as an open environment, no inherent protection.
- Physically accessible
  - Almost open access while parked.
  - Third-party repair shops need diagnostic and repair access.
  - Uncontrolled spare parts.
  - Side-channel attacks on legitimate HW.
- The owner may have an incentive: tuning, odometer tampering.

Cybersecurity Challenges
Real-Life Examples

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

Hackers Remotely Kill a Jeep on the Highway—With Me in It

source: wired.com

ANDY GREENBERG SECURITY 11.23.2020 07:00 AM

This Bluetooth Attack Can Steal a Tesla Model X in Minutes

The company is rolling out a patch for the vulnerabilities, which allowed one researcher to break into a car in 90 seconds and drive away.

source: wired.com

Cybersecurity Challenges
Stealing a Toyota RAV4 in 2022

Ian Tabor
@mintynet

No fcuking point having a nice car these days, came out early to find the front bumper and arch trim pulled off and even worse the headlight wiring plug had been yanked out, if definitely wasn't an accident, kerb side and massive screwdriver mark. Breaks in the clips etc. C&#ts

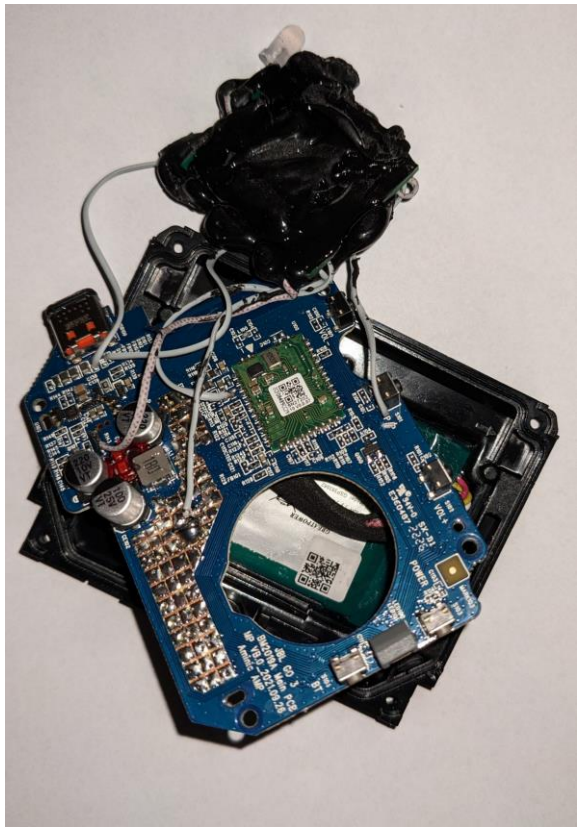
6:03 PM · Apr 24, 2022

Ian Tabor @mintynet · Jul 21, 2022
I know what they were doing, the car is gone! My @ToyotaUK app shows it's in motion. I only filled the tank last night. FCUK!

> **Ian Tabor** @mintynet · Jul 19, 2022
> Why do I bother having a nice car? I know it's a first world problem but can who ever it is just leave my fcuking car alone. No lights on the way to work this morning and even more gashes in the paint work and the moulding has no clips any more. Not happy. twitter.com/mintynet/statu...

Source: https://kentindell.github.io/2023/04/03/can-injection/

Cybersecurity Challenges
Stealing a Toyota RAV4 in 2022



Source: https://kentindell.github.io/2023/04/03/can-injection/

Cybersecurity Challenges
Attacker Motivations in the Automotive Industry

- Terrorism / causing accidents
  - Is it easier to hack a car than to place a bomb under it?
    Not necessarily, but…
    - It can be done at a distance (safer)
    - It can be scalable (can hack many cars after breaking one)
    - It can be shared (other actors may use it)

Image: © 2017 ESCRYPT. Exemplary attack demonstration only. This is NOT a real attack/vulnerability!

- Ransomware / theft
  - „Pay to Drive”
  - Stealing the vehicle, its components, or the data stored in it

- (Self-)Tuning
  - Restrictions from OEMs (e.g., enable paid features for free)
  - Restrictions from regulations (e.g., disable speed limit or emissions control)

Cybersecurity Challenges
Example Attack Surfaces in Vehicles

- External connectivity interfaces (GSM, WiFi, Bluetooth, GPS)
  - Replay attack, lack of authentication, over the air (OTA)
  - Mobile car application being hacked/attacked allowing access to the car
  - Communication jamming, Denial-of-Service (DoS)
- Sensor fooling
  - Placing false road signs, or modifying real ones (e.g., speed limit)
- Physical access
  - Access via On-Board Diagnostic (OBD) port
  - Uncontrolled spare parts may be installed (they may be malicious)
- Human factor: the owner may – willingly or not – compromise security

source: shutterstock.com

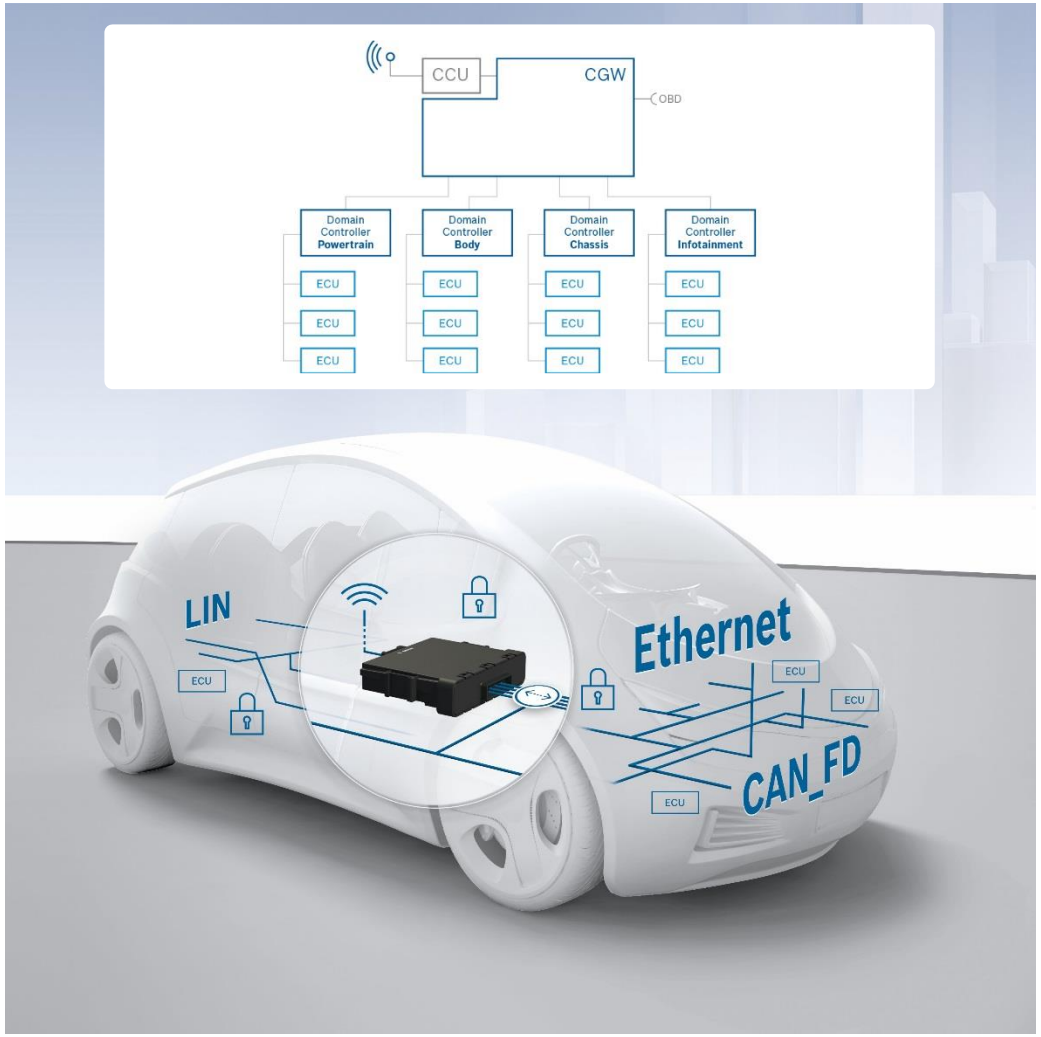
Cybersecurity Challenges
Regulations and technical standards

- UN ECE R155
  Cyber security and cyber security management system
  - Supply chain management
  - Risk assessment
  - Cybersecurity measures
  - Detect and respond to attacks
  - Log data to support forensics
  - Testing

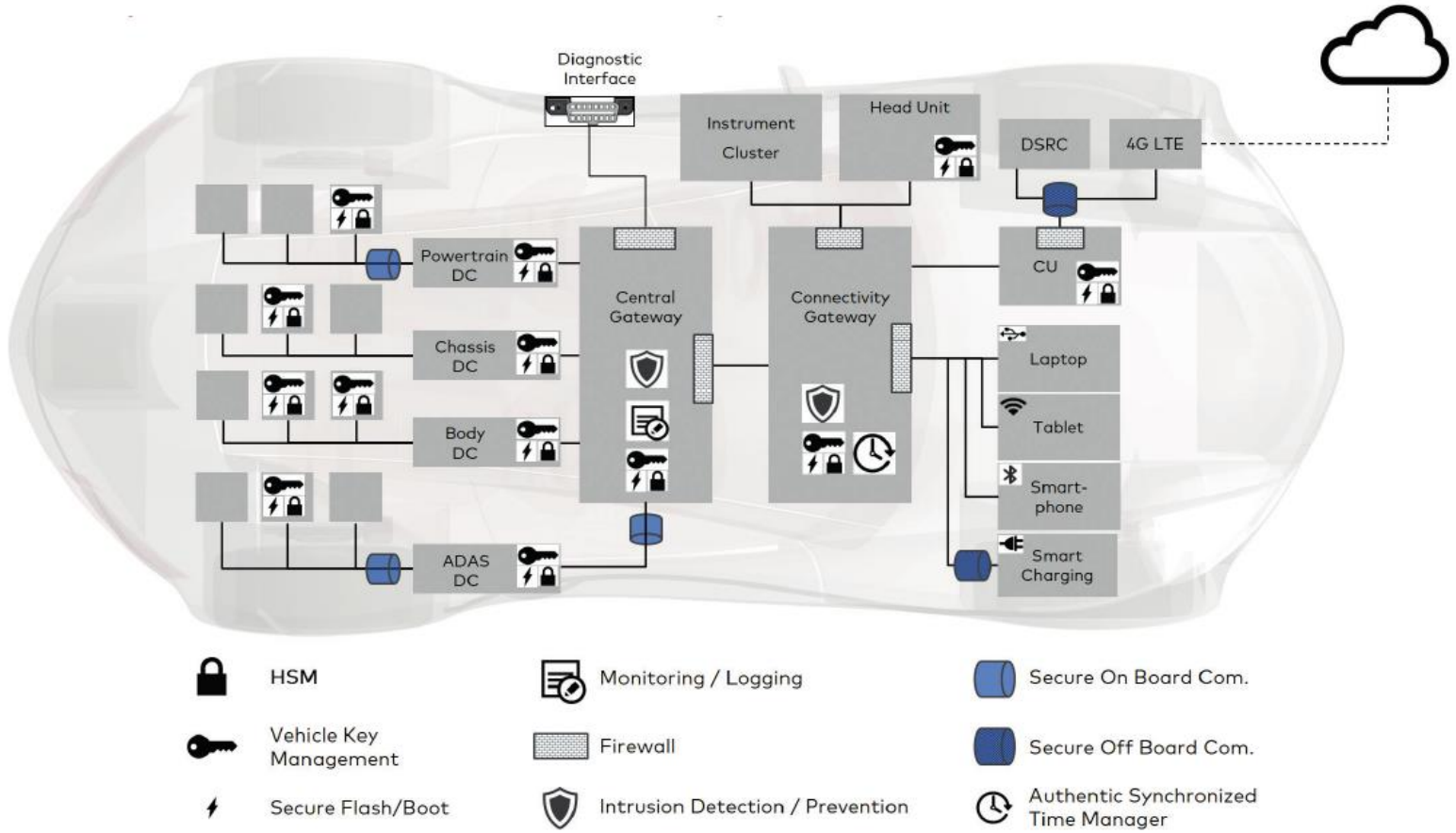
- ISO/SAE-20434
  Road vehicles: cybersecurity engineering
  - Organizational & project-dependent cybersecurity management
  - Supply chain management
  - Full lifecycle covered: from concept to decommissioning
  - Threat and risk analysis (TARA)
  - Continuous monitoring & response

Cybersecurity Challenges
Domain-based architecture

- Each domain has a separate controller
  - Domain controllers isolate critical functions
- Central gateway connects the various domains
  - controls external connectivity, diagnostics port
  - implements firewall
  - manages virtual networks (VLAN)
- Automotive Ethernet used between domains
  - Point-to-point connections, managed switches
- Hardware security module (HSM)
  enables sophisticated security features at low cost



Cybersecurity Challenges
Secure Vehicle Architecture



Source: https://assets.vector.com/cms/content/know-how/automotive-cyber-security/Security_Solution_FactSheet_EN.pdf

Cybersecurity Challenges
Conclusions

- Vehicles are subject to cybersecurity attacks
- Legacy technology not designed for security
- Conflicts with functional requirements
- Limited supply of qualified professionals

- Regulation is in place to enforce the systematic management of cybersecurity
- Technical standards are available to provide guidelines on how to comply

- Growing awareness in the industry
- Development processes are being updated