How Security Mechanisms Can Protect Cars Against Hackers

Christoph Dietachmayr, CIS Solution Manager
EB USA Techday, Dec. 3rd 2015
Driver’s Fears Are Being Fueled by Recent News

Connected Cars, new opportunities for hackers

IAA: New Autonomous Driving Concepts
Connected Car Offers New Business Models for Hackers?
Autonomous Theft?
How Security Mechanisms Can Protect Cars Against Hackers

Agenda

• Electronic Control Unit (ECU) Security
• On-board Network Security
• Excursion: Security Issues in a Safety Environment
• Vehicle Security
• The Connected Car
How Security Mechanisms Can Protect Cars Against Hackers

Agenda

• Electronic Control Unit (ECU) Security
• On-board Network Security
• Excursion: Security Issues in a Safety Environment
• Vehicle Security
• The Connected Car
ECU Security

- Secure update
- Secure boot
- Hardware security module
- Software as a product
Secure ECU Software Architecture
Software and Hardware Security Modules

```
data = "42mil/h";
key = 0x1234;
secure(data, key);
...
```

CryShe

Software implementation

Security Hardware peripheral

AUTOSAR

Csm

Interface layer

Csm

Implementation layer

Cry
Software and Hardware Security Modules

EB supports the algorithms you need!
How Security Mechanisms Can Protect Cars Against Hackers

Agenda

• Electronic Control Unit (ECU) Security
• On-board Network Security
• Excursion: Security Issues in a Safety Environment
• Vehicle Security
• The Connected Car
On-Board Network Security

- Theft protection
- Anomaly detection
- Intrusion detection
- Secure communication
How Security Mechanisms Can Protect Cars Against Hackers

Agenda

• Electronic Control Unit (ECU) Security
• On-board Network Security
• Excursion: Security Issues in a Safety Environment
• Vehicle Security
• The Connected Car
How Security Mechanisms Can Protect Cars Against Hackers

Security Issues in a Safety Environment

- **Security**: Protection against external access, e.g. hacks
- **Safety**: Reliable execution environment for ECUs. “knowing what the system does”

Security protects Safety

There is no safety without security and vice versa

© Elektrobit (EB) 2015
How Security Mechanisms Can Protect Cars Against Hackers

Agenda

• Electronic Control Unit (ECU) Security
• On-board Network Security
• Excursion: Security Issues in a Safety Environment
• Vehicle Security
• The Connected Car
Vehicle Security: Various Access Points

- Car2Infrastructure
- Bluetooth connection
- Car2Car
- Wireless key
- eCall
- Internet connection
- WiFi Hotspot
- Remote HVAC
- Remote start
- Tire pressure monitor
How Security Mechanisms Can Protect Cars Against Hackers

Current Vehicle Systems Architecture
How Security Mechanisms Can Protect Cars Against Hackers

Future Vehicle Systems Architecture
Use Case: Smart Antenna
How Security Mechanisms Can Protect Cars Against Hackers

Smart Antenna

Concentrate Wireless access
Secure Separation
Threat monitoring
Denial of Service prev.

© Elektrobit (EB) 2015
Vehicle Security
Agenda

- Electronic Control Unit (ECU) Security
- On-board Network Security
- Excursion: Security Issues in a Safety Environment
- Vehicle Security
- The Connected Car
The Connected Car
The Connected Car
The Connected Car
The Connected Car
How Security Mechanisms Can Protect Cars Against Hackers

Over the Air Functionality

- Secure Backend Channel
- SW storage
- Over the Air:
  - SW update agent
  - Remote Diagnostics agent
  - ...
- Secure COM

100% security is an illusion
- Secure OTA update
- Remote diagnostics
- Identity vs. privacy

EB Software

© Elektrobit (EB) 2015
EB Security Platform

EB Security Portfolio

- Secure separation
  - Hypervisor
  - Virtualisation

- Secure HW
  - HSM firmware
  - Future Security HW
  - Security architecture

- Security applications
  - Unlock / Download
  - SW as Product
  - Secure Com...

- Key management
  - Sym/Asym
  - Key Derivation
  - Initial / Update

- Crypto
  - Algorithms
  - SHE drivers
  - HSM drivers

- OTA
  - Secure Connection
  - Update strategies
  - Implementation
  - Backend

- Secure Communication
  - Firewall
  - Intrusion-/Anomaly detection

- Testing & Certification
  - Functional
  - Penetration Testing
  - FIPS / Com. Criteria

- Security Consulting
  - Architecture
  - Solutions
  - How-To

- Car2X
  - Consulting
  - Implementation
  - Testing
Summary

• **Security is necessary on all levels**
  – In ECUs and between ECUs
  – In the vehicle and between vehicles
  – In the backend

• **A big challenge, but you are not alone**
  – Existing and approved mechanisms available
  – EB secures vehicles for more than 15 years

• **Security needs constant care**
  – Monitoring on all levels
  – Update over the air is key to keep cars secure

• **Visit us at:** [https://www.elektrobit.com/security](https://www.elektrobit.com/security)
Thank you

Christoph.Dietachmayr@elektrobit.com
automotive.elektrobit.com