Agenda

• Automotive System
• Vulnerability and Threat
• Security Engineering
  • Process and Method
  • Security Technology
• Summary
Automotive System

E/E system

Electrical and/or electronic system (E/E) system

- system that consists of electrical and/or electronic elements, including programmable electronic elements

- EXAMPLE Power supply; sensor or other input device; communication path; actuator or other output device.

- ISO 26262
Automotive System
Vulnerabilities

Features controlled by computers
Attack surface
Architecture

- Security vulnerabilities
  - Coding error
    - Improper implementation
    - Buffer overflow
    - Improper input validation
  - Design error
    - Architecture
    - Cryptographic protocols
    - Weak crypto
  - Legacy systems
    - CAN standard
    - No proper protection of crypto keys
  - Supply chain
    - Undocumented features & services
  - Backend error
  - Debug interfaces
Automotive System Threats

Comprehensive Experimental Analyses of Automotive Attack Surfaces

Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno.


An earlier version of this paper was prepared as a report for the National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration, March 3–4, 2011.

The full paper is available in PDF form here: [PDF](#).

Experimental Security Analysis of a Modern Automobile

Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage.


The full paper is available in PDF form here: [PDF](#).

Remote Exploitation of an Unaltered Passenger Vehicle

Dr. Charlie Miller ([cmiller@openrice.org](mailto:cmiller@openrice.org))

Chris Valasek ([cvalasek@gmail.com](mailto:cvalasek@gmail.com))

August 13, 2015

0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars

Zhijiang Cai, Aohui Wang, Wenkai Zhang

(zhijiangcai, aohuiw, wenkaizhang)@tencent.com

with contributions from: Michael Gruflke, Hendrik Schuppe

(michael.gruflke, hendrik.schuppe)@bmwgroup.com

[https://electrek.co/2019/08/22/tesla-stolen-keyfob-hack-camera-how-to-prevent-it/](https://electrek.co/2019/08/22/tesla-stolen-keyfob-hack-camera-how-to-prevent-it/)
Where do we go from here?
Automotive Security Engineering
Product Cyber Security Program

Cyber Security Culture

- Threat Analysis and Risk Assessment
- Security Goals
- Security Concept
- Security Implementation
- Security Validation
- Security Case
- Security in Production, Operations and Maintenance
- Incident Response Update

https://github.com/zhendongma/ISO-SAE-21434
Automotive Security Engineering

Security Dimensions

Backend/Cloud

V2X communication

E/E Architecture

ECU

uController

Communication from/to Backend

Interfaces / Gateway

On-board communication

µC and HSM

Figure 1: Message Authentication and Freshness Verification

Specification of Secure Onboard Communication AUTOSAR CP Release 4.3.1

AUTOSAR Specification of crypto driver release 4.3.1

EVITA hardware security module
## Automotive Security Engineering

### Security Technologies

<table>
<thead>
<tr>
<th>Feature</th>
<th>2018</th>
<th>2023+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Separation</td>
<td>Seldom</td>
<td>Common</td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>Seldom</td>
<td>Many</td>
</tr>
<tr>
<td>Hardware Trust Anchor (e. g., HSM)</td>
<td>Seldom</td>
<td>Many</td>
</tr>
<tr>
<td>AUTOSAR Modules</td>
<td>Seldom</td>
<td>Many</td>
</tr>
<tr>
<td>Signed Software Updates</td>
<td>Seldom</td>
<td>Many – Common</td>
</tr>
<tr>
<td>Secure Diagnostic Services</td>
<td>Seldom (with weaknesses)</td>
<td>Many</td>
</tr>
<tr>
<td>Secure Boot</td>
<td>Seldom</td>
<td>Many</td>
</tr>
<tr>
<td>Authenticated Boot</td>
<td>Seldom</td>
<td>Many</td>
</tr>
<tr>
<td>Secure Communication with Backend</td>
<td>Many</td>
<td>Common</td>
</tr>
<tr>
<td>Secure Onboard Communication</td>
<td>None</td>
<td>Many</td>
</tr>
<tr>
<td>Firewall</td>
<td>Many</td>
<td>Common</td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td>None</td>
<td>Seldom - Many</td>
</tr>
<tr>
<td>Wi-Fi/Bluetooth Security</td>
<td>Common (with weaknesses)</td>
<td>Common</td>
</tr>
</tbody>
</table>

M Ring, D Frkat, M Schmiedecker, “Cyber security Evaluation of automotive E/E Architectures,” ACM CSCS, 2018
Automotive Security Engineering

Security Features

- Secure Access
- Secure Flashing
- Secure Boot
- Secure Data Storage
- Hardware Interface Protection
- Secure In-Vehicle Communication
- Software Encryption
- Secure Logging
Automotive cyber security is catching up
Product security starts top-down
Security engineering best-of-class solutions