# Automotive Security

CoRE Group

Milena Hippler

22.05.2017

# Agenda

1. Einleitung – Warum Security?
2. Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks
   - In-Vehicle Netzwerk
   - Klassifizierung von Angriffen
   - Schutz Mechanismen
3. A Survey of Security and Privacy in Connected Vehicles
   - Vernetzte Fahrzeuge
   - Klassifizierung von Sicherheitsaspekten
   - Bedrohungen
4. Konferenzen
5. Ausblick hinsichtlich Penetrationstest
6. Fazit
7. Quellen

# 2. Warum Security?

- Zunächst interne Netzwerke nicht zugreifbar von außerhalb des Autos, daher spielten Security Mechanismen keine große Rolle

- Trend
  - Moderne Autos besitzen häufig Interfaces, die Wired- und/oder Wireless-Kommunikation mit der Außenwelt ermöglichen
  - Embedded Computing Systems in modernen Autos sind nicht länger ein Closed Network

# 3. Survey on security threats and protection mechanisms in embedded automotive networks

Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaniche, Youssef Laarouchi (2015) [1]

- Konzentration auf das In-Vehicle Netzwerk

# In-Vehicle Netzwerk

[2]

- ECU (Electronic Control Unit)
- kontrolliert eine oder mehrere Funktionen eines Fahrzeuges
- ECUs formen ein automobiles In-Vehicle Netzwerk
- ECUs verbunden mit Bussystem, Übermittlung aller Nachrichten per Broadcast
- Anforderungs-abhängige Nutzung mehrerer Protokolle zur Kommunikation zwischen ECUs

→ ein Fahrzeug besteht also aus mehreren Subnetzwerken vernetzt durch Gateway ECUs

# In-Vehicle Netzwerk Protokolle - CAN

- CAN (Controller Area Network)
- Meistgenutzte Protokoll in Automobil Netzwerken
- Multi-Master: Jeder Knoten kann sofort Nachricht auf CAN Bus übermitteln, falls zu dem Zeitpunkt keine Nachricht via Bus übermittelt wird
- Entscheidungsregelwerk bei Konflikten: Vergleich von Frame Identifiern, der mit dem höchsten MSB hat höchste Priorität
- Struktur eines CAN Frame:

| SOF | Identifier | Control | Data | CRC | ACK | EOF |
|---|---|---|---|---|---|---|
| 1 bit | 12/30 bits | 6 bits | 0 - 64 bits | 16 bits | 2 bits | 7 bits |

[1]

# In-vehicle Netzwerk Protokolle

- SAE (Society for Automotive Engineers) klassifiziert Kommunikationsprotokolle in 4 Kategorien
  - in Bezug auf ihre Raten und angegebenen Features:

| Class | Rate | Use | Examples |
|---|---|---|---|
| A | <10kb/s | Body control | LIN |
| B | 10kb/s → 125kb/s | Non critical generic data transfer | CAN-B (Low-speed CAN) |
| C | 125kb/s → 1Mb/s | Critical real-time communications | CAN-C (High-speed CAN) |
| D | >1Mb/s | Multimedia or X-by-wire | MOST, FlexRay |

[1]

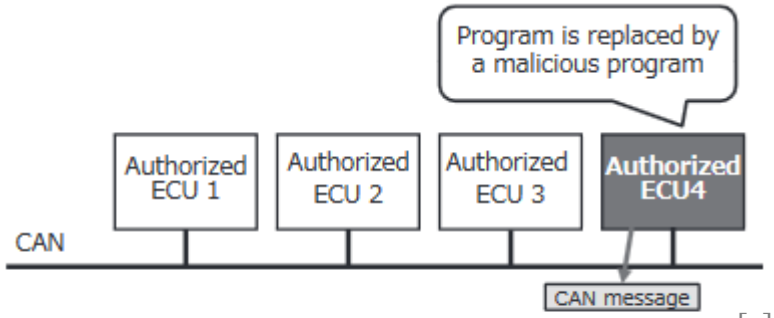
# Interne Angriffe

- Schwachstellen in aktuellen Netzwerkprotokollen
- CAN kann folgende Eigenschaften der Security nicht garantieren:
  - Vertraulichkeit
  - Authentizität
  - Verfügbarkeit
  - Integrität
  - Nachweisbarkeit

# Lokale Angriffe

- Angriff über OBD (On-Board-Diagnostics) Port mittels OBD Dongles
- Szenarien:
  - ECUs updaten und reflashen
  - Anvisierte ECU kann sich sogar auf anderen Bus befinden

→Sobald Angreifer Kontroller über 1 Knoten, machen es ihm aktuelle Protokolle möglich die Kontroller über alle weiteren ECUs des Fahrzeuges zu erhalten




[3]

**Fig. 1.** Replacement of authorized ECU program by malicious program

# Entfernte Angriffe

1. Indirekter Zugang: CD-Player, USB-Port
2. Short Range Angriffe:
   - Wireless Pairing von mobilen Geräten
   - Car-to-Car Kommunikation
   - Wireless Entriegeln
3. Long Range Angriffe:
   - Web Browsing
   - AppStore

# Schutz Mechanismen - Beschränkungen

- *Hardware*:

  Speicher und Rechenleistung beschränkt, daher aufwendige kryptographische Funktionen oft nicht möglich

- *Echtzeit*:

  Je komplexer die Anweisung, desto länger die Laufzeit

- *Physikalische Beschränkungen*

- *Kompabilität*:

  Kostenreduzierung wenn kompatibel mit aktuellen System und Kompabilität mit externen Geräten muss möglich sein

# Schutzvorkehrungen des CAN Busses

Drei Kategorische Lösungsansätze für die Kommunikationssicherheit von CAN:

1. *Kryptografie*:

   HSM (Hardware Security Module) konzipiert vom EVITA Projekt zur Entlastung der ECU

2. *Anomalien Erkennung*:

   Überwachung der Daten die zwischen ECUs übermittelt werden und auf Legitimität prüfen

3. *ECU Software Integrität*:

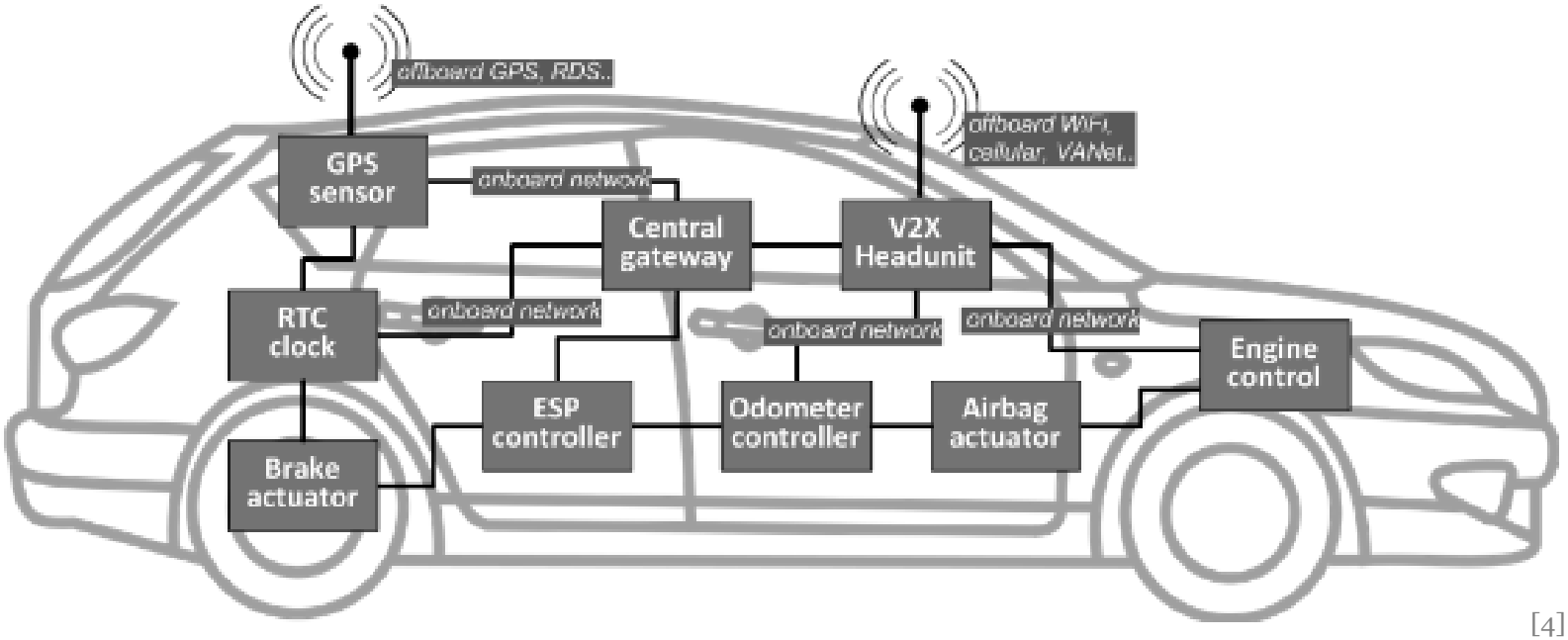
   Validierung der Sicherheit von ECU Code

# 4. A Survey of Security and Privacy in Connected Vehicles

Lotfi ben Othmane, Harold Weffers, Mohd Murtadha Mohamad, and Marko Wolf
(2015) [4]

- Konzentration auf vernetzte Fahrzeuge

# Vernetzte Fahrzeuge



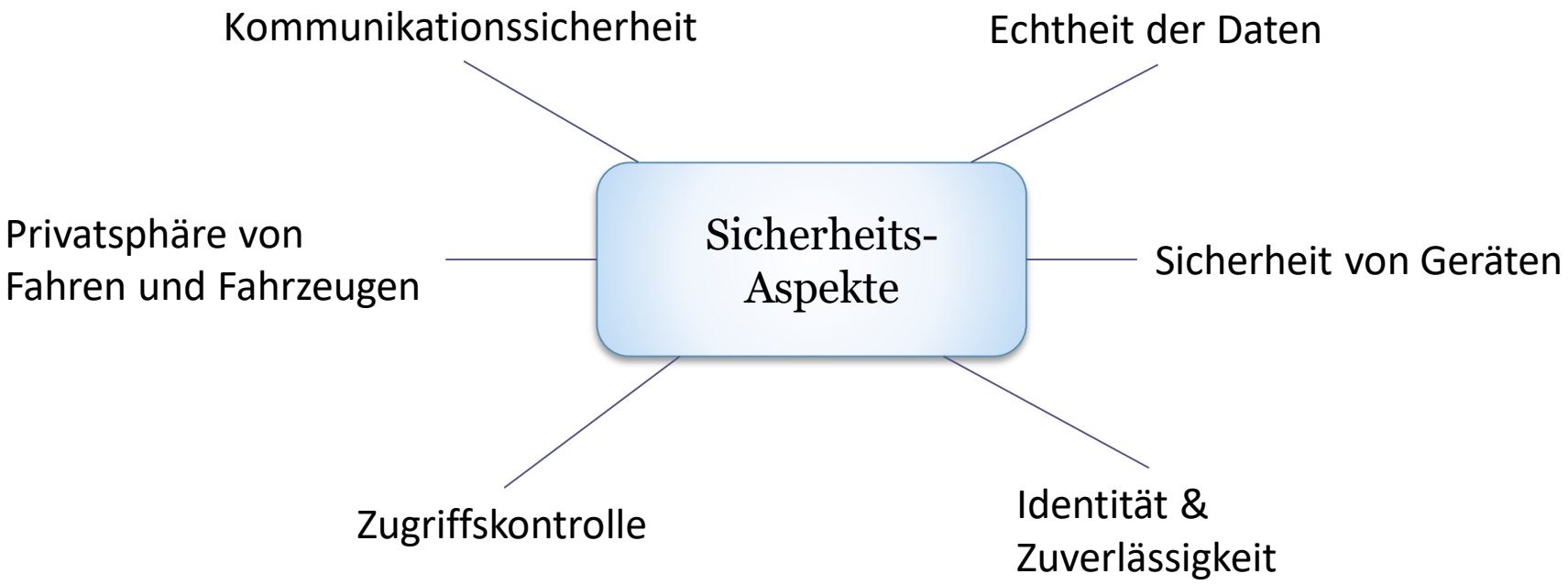

[4]

# Netzwerke vernetzter Fahrzeuge

[5]

- *In-vehicle Netzwerk:*
  - Kommunikation zwischen ECUs
- *VANets (vehicular ad hoc network):*
  - Kommunikation mit anderen Fahrzeugen (V2V) und mit RSUs (Road Side Units) (V2I)
  - Mitglieder des VANets tauschen Informationen aus um ein gemeinsames Wissen über den Verkehr zu haben
- *WPAN (wireless personal area network):*
  - Kommunikation mit persönlichen Geräten mittels Wireless Technologien wie Bluetooth
- *Mobilfunknetz:*
  - Kommunikation mit Service Providern (SP) und Service Center (SC)

# Klassifizierung von Sicherheitsaspekten eines vernetzten Fahrzeuges



# Bedrohungen in Bezug auf einigen der Sicherheitsaspekte

*Bedrohungen der …*

*… Kommunikation*:

- Nachrichtenunterdrückung
- Erzeugung falscher Nachrichten
- Wiederholungs-Angriff

*… Echtheit der Daten*:

- Wurmloch-Angriff
- Verbreitung falscher Nachrichten

*… Sicherheit der Geräte*:

- Denial of Service Attacke (DoS)

*… Privatsphäre*:

- Spionage durch Sammeln von Daten

# 5. Konferenzen

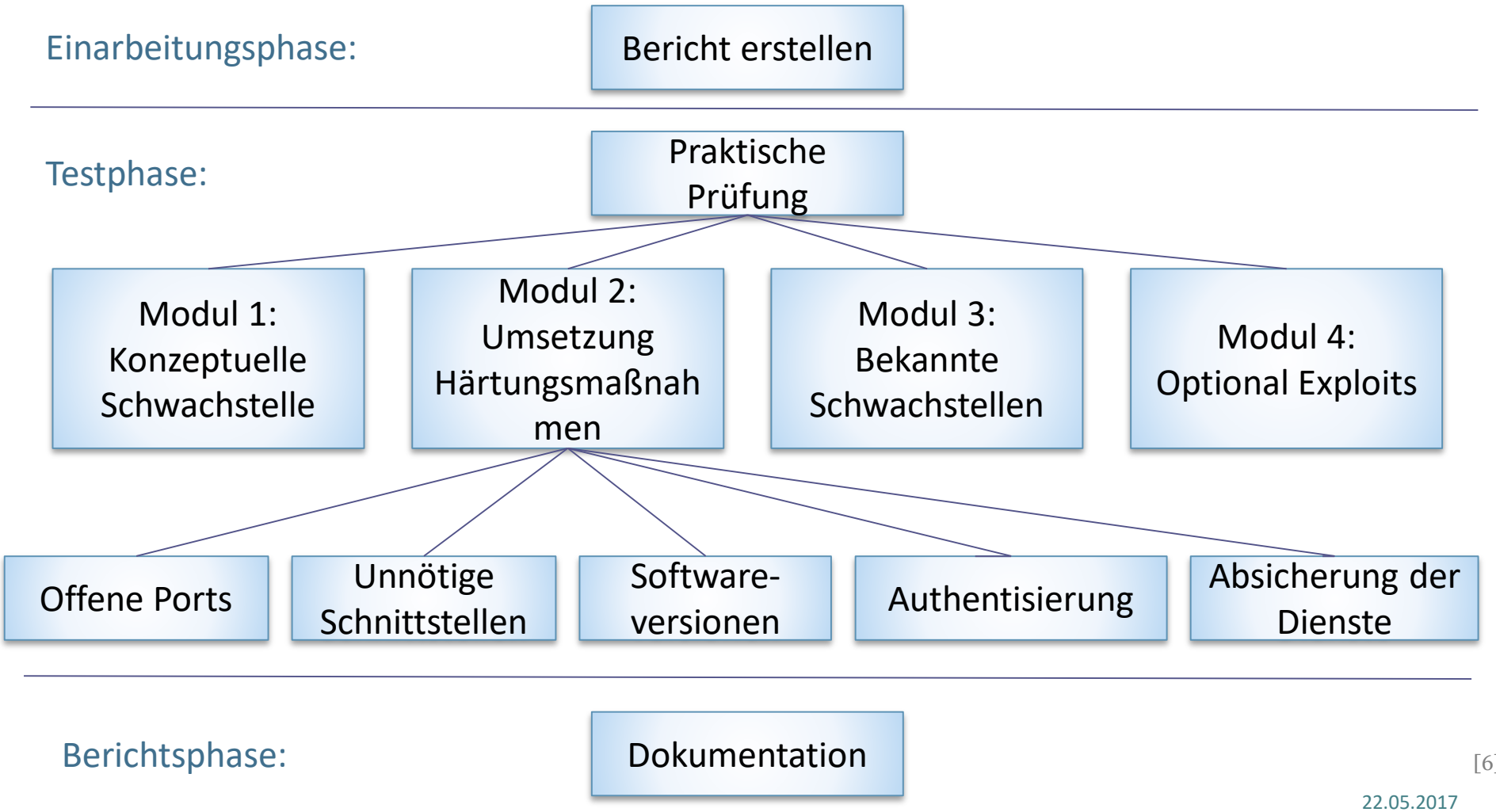
- escar - Automotive Cyber Security Conference
- VDI-Konferenz - IT-Sicherheit von Fahrzeugen
- Automotive – Safety & Security 2017

# 6. Ausblick

- Analyse von Netzwerken, Protokollen und Architekturen
- Analyse von Security Mechanismen
- Identifikation von Schwachstellen in vernetzten Fahrzeugen mittels Penetrationstest
- Empfehlungen um Lücken zu schließen

→Ein Praxisleitfaden für IS-Penetrationstest - BSI (Bundesamt für Sicherheit in der Informationstechnik, Version 1.2, Stand 2016) [6]

# Ablauf eines IS-Penetrationstest




[6]

# 7. Fazit

- Mangel an existierenden Security Mechanismen in aktuellen Automobil-Netzwerken ist ein ernstes Thema
- Schwachstellen in Modulen die solch wireless Protokolle durchführen, erlauben es Angreifern entfernten Zugang und die Integrität von eventuell jeder ECU des Netzwerkes zu gefährden
- 3 Hauptaspekte für die Durchführung von Security in Automobilen Netzwerken:
  - Verschlüsselung der Kommunikation,
  - Detektion von Anomalien und
  - Integrität der embedded Software

# 8. Quellen

[1] Survey on security threats and protection mechanisms in embedded automotive networks; Ivan Studnia, Vincent Nicomette, Eric Alata, Yves Deswarte, Mohamed Kaniche, Youssef Laarouchi (2015)

[2] http://produkte.bosch-mobility-solutions.de/de/de/_technik/component/PT_PC_PFI_Engine-Management_PT_PC_Port-Fuel-Injection_1484.html#

[3] Security Authentication System for In-Vehicle Network, Hiroshi UEDA, Ryo KURACHI, Hiroaki TAKADA, Tomohiro MIZUTANI, Masayuki INOUE and Satoshi HORIHATA (Oktober 2015)

[4] A Survey of Security and Privacy in Connected Vehicles; Lotfi ben Othmane, Harold Weffers, Mohd Murtadha Mohamad, and Marko Wolf (2015)

[5] http://www.itwissen.info/RSU-roadside-unit.html

[6] Ein Praxis-Leitfaden für IS-Penetrationstests, BSI (Version 1.2, November 2016)

[7] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[8] 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, and Tadayoshi Kohno

[9] evita-project.org

# Video Empfehlung

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

[7]

Vielen Dank
für die
Aufmerksamkeit!