Von Car2X- bis In-Vehicle-Security

Einführung und Überblick

Daniel Zelle

daniel.zelle@sit.fraunhofer.de

Fraunhofer SIT

Inhalt

- Motivation
- Drahtlose Verbindung zum Auto
- Physikalische Verbindungen
- Fazit & Ausblick

Motivation

- Mehr als 80 Steuergeräten
  - Kontrolle aller Fahrzeugfunktionen
    - Bremsen
    - Beschleunigen
    - Öffnen
    - Automatisches Einparken
    - usw.
  - Kommunikation untereinander
  - Kommunikation mit der Außenwelt
    - Car-2-Infrastruktur
    - Car-2-Car
    - Herstellerverwendung

Nachrichtenüberblick

golem.de
IT-NEWS FÜR PROFIS

HOME TICKER VIDEO ABO

TOP-THEMEN: Build 2015 Windows 10 Linux Apple Watch Netzpolitik Test mehr

AUTO

Programmierte Scheinwerfer leuchten nur Wichtiges aus

Der Scheinwerfer der Zukunft leuchtet Rehe am Fahrbahnrand an,

Adaptives Kurvenlicht in einem BMW (Bild

Datum: 28.4.2015, 08:26

Autor: Andreas Donath

Themen: Auto

heise AUTOS Fahrberichte

heise Autos > News > Kurzmeldungen

30.09.2014

Telefónica bringt auch ältere Autos ins Netz

Telefónica stellt auf dem carIT-Kongress im Rahmen der IAA-Nutzfahrzeuge am Dienstag in Hannover das Produkt "O2 Car Connection" vor, mit dem sich Fahrzeuge mit einem OBD2-Diagnoseport in ein Connected Car verwandeln lassen. Das Paket beinhaltet ein Hardwaremodul mit Netzanbindung sowie eine App und kostet 149 Euro inklusive einem Jahr Car Connection, danach kostet jeder weit

Das Modul wird ei
OBD2-Diagnosepo
„Das Smartphone
verbunden und ma
mobil im Griff", erl
Director Digital, Pe
Telefónica eignet s
die das Unternehn

heise AUTOS Fahrberichte T

heise Autos > News > Kurzmeldungen

16.04.2015

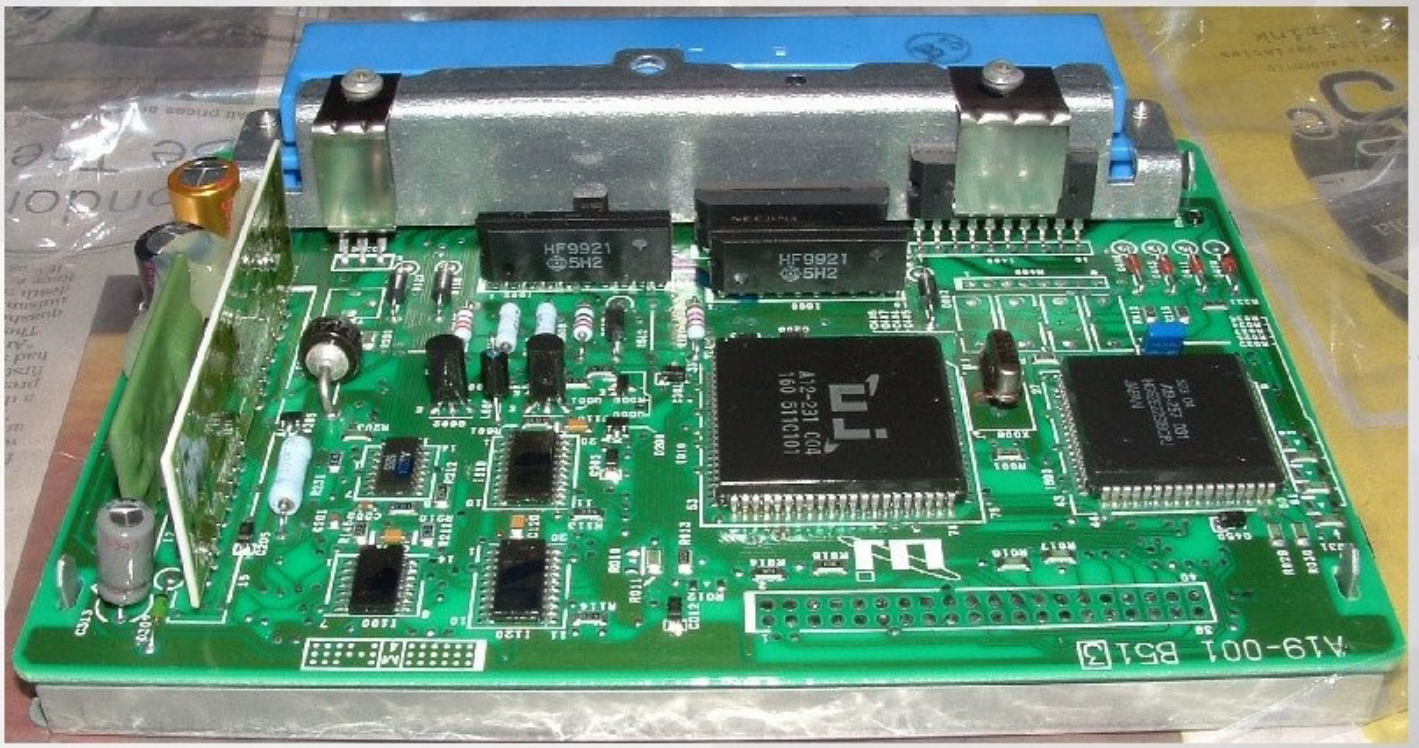
Audi: "Autonomer" A8 kommt 2017

Audi will die Technik zum pilotierten Autofahren in zwei Jahren in einem ersten Serienfahrzeug anbieten. Der 2017 erscheinende A8 soll laut *auto motor und sport* erstmals damit ausgestattet werden. Ziel ist es, dass der A8 bis Tempo 140 auf der Autobahn autonom fahren kann. Das Auto soll mit Sensoren, Ultraschall, Lasern, Kameras und der Vernetzung mit Karten- und Staudaten in der Lage sein, selbstständig die Spur und den Abstand zum Vordermann zu halten. Der A8 soll aber sogar selbstständig überholen können, versprechen die Ingenieure. Dazu orientiert sich der Autopilot dann an allen um das Auto herum fahrenden Fahrzeugen sowie den Informationen über den Verlauf der Strecke.

1) http://www.golem.de/news/auto-programmierte-scheinwerfer-leuchten-nur-wichtiges-aus-1504-113758.html
2) http://www.heise.de/autos/artikel/Audi-Autonomer-A8-kommt-2017-2608780.html
3) http://www.heise.de/autos/artikel/Telefonica-bringt-aeltere-Autos-ins-Netz-2405460.html

Electronic Control Unit (ECU)

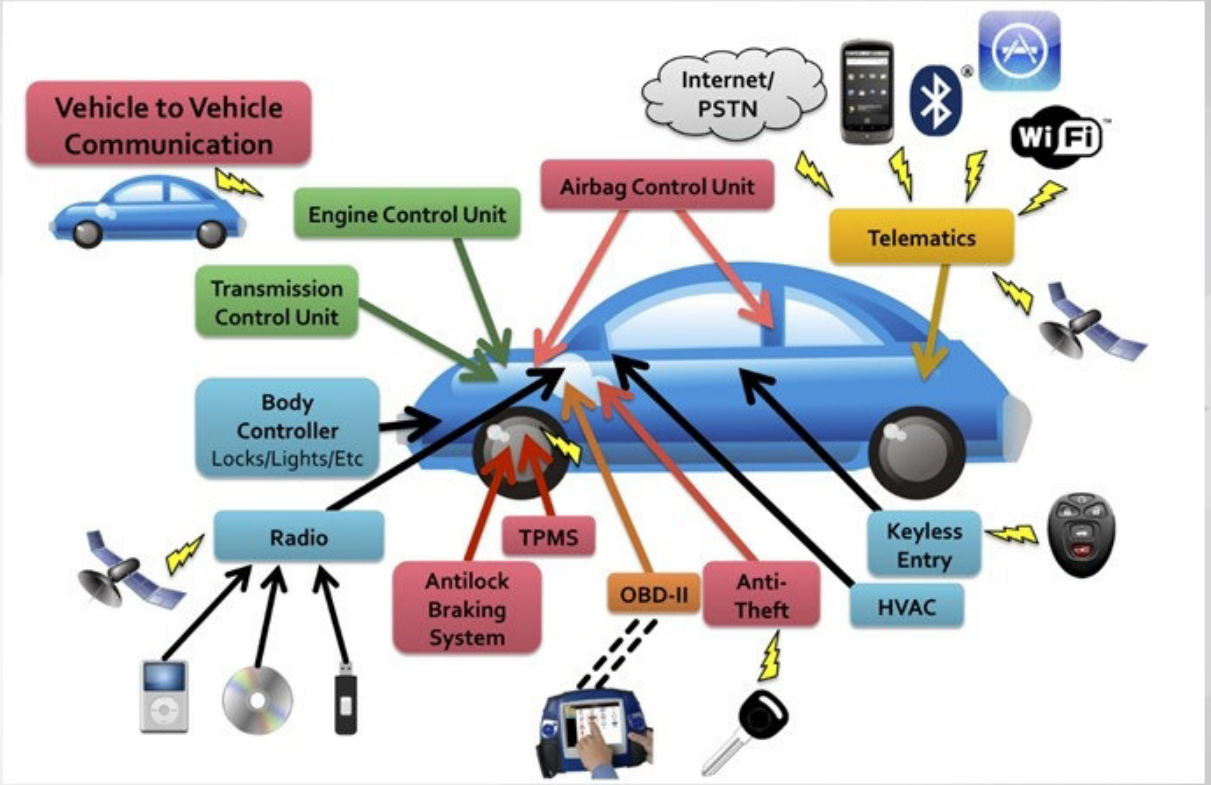
- Steuergeräte
  - Kleine Computer
  - Steuerung von:
    - Motor
    - Bremsen
    - Verriegelung
    - Heizung
    - Airbag
    - usw.



Quelle: https://commons.wikimedia.org/wiki/File:JECS_GA16DE_ECU.jpg

Verbindung zur Außenwelt

- Angriffsvektoren
  - Lokale drahtlose Kommunikation
    - WLAN
    - Bluetooth
    - Car2X
    - Remote Keyless Entry
  - Mobilfunk
    - GSM / UMTS / LTE
  - Physikalischer Zugang
    - OBD2
    - CD / USB
    - usw.



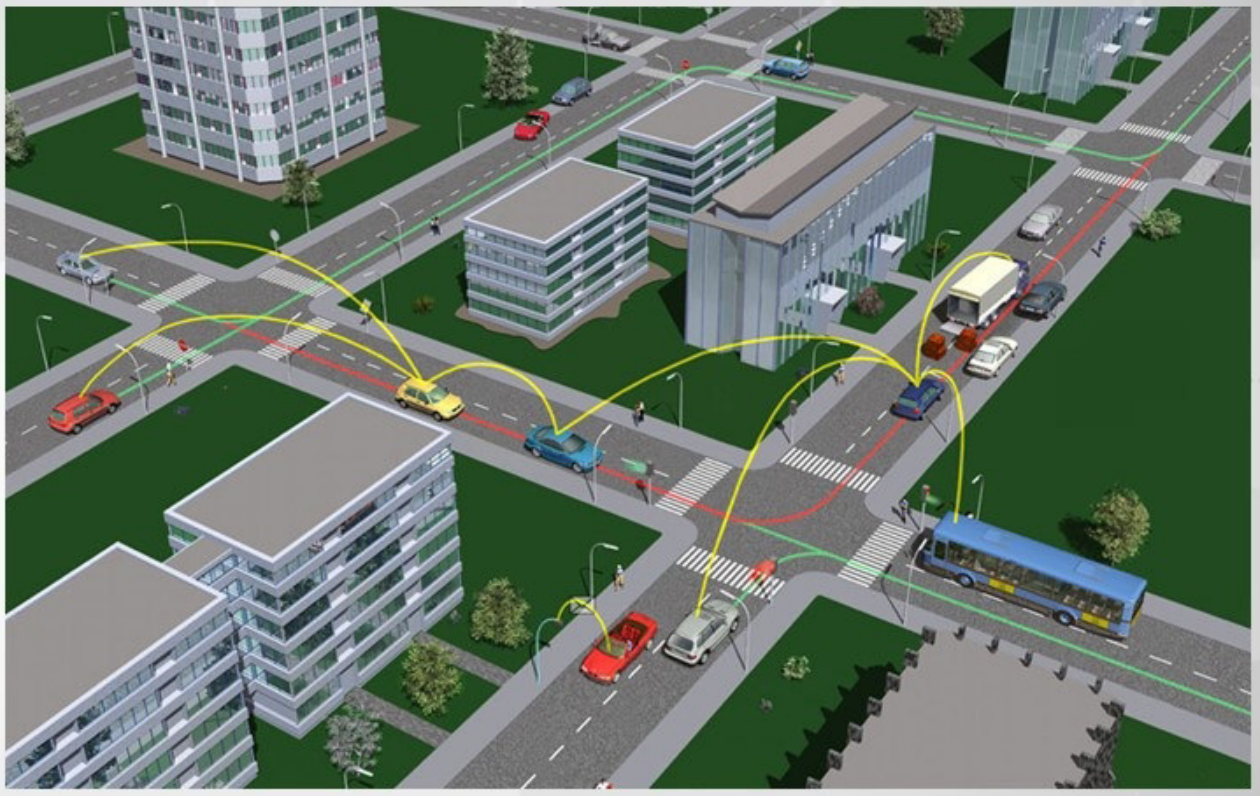
Quelle: Checkoway et al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces USENIX Security Symposium, 2011

Inhalt

- Motivation
- Drahtlose Verbindung zum Auto
- Physikalische Verbindungen
- Fazit & Ausblick

Car2X

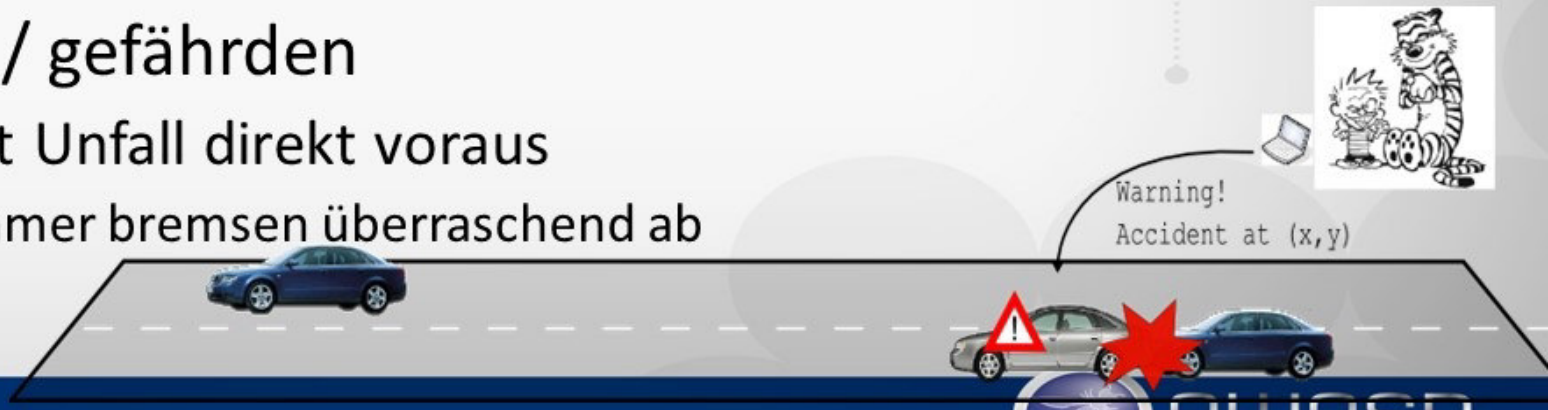
- Vorteile
  - Sicherheit
    - Warnung: Gefahren, Unfall,…
  - Verkehr
    - Stauprävention
  - Usw.



Quelle: CAR 2 CAR Communication Consortium
https://www.car-2-car.org/index.php?id=5

Car2X -Potenzielle Angriffe

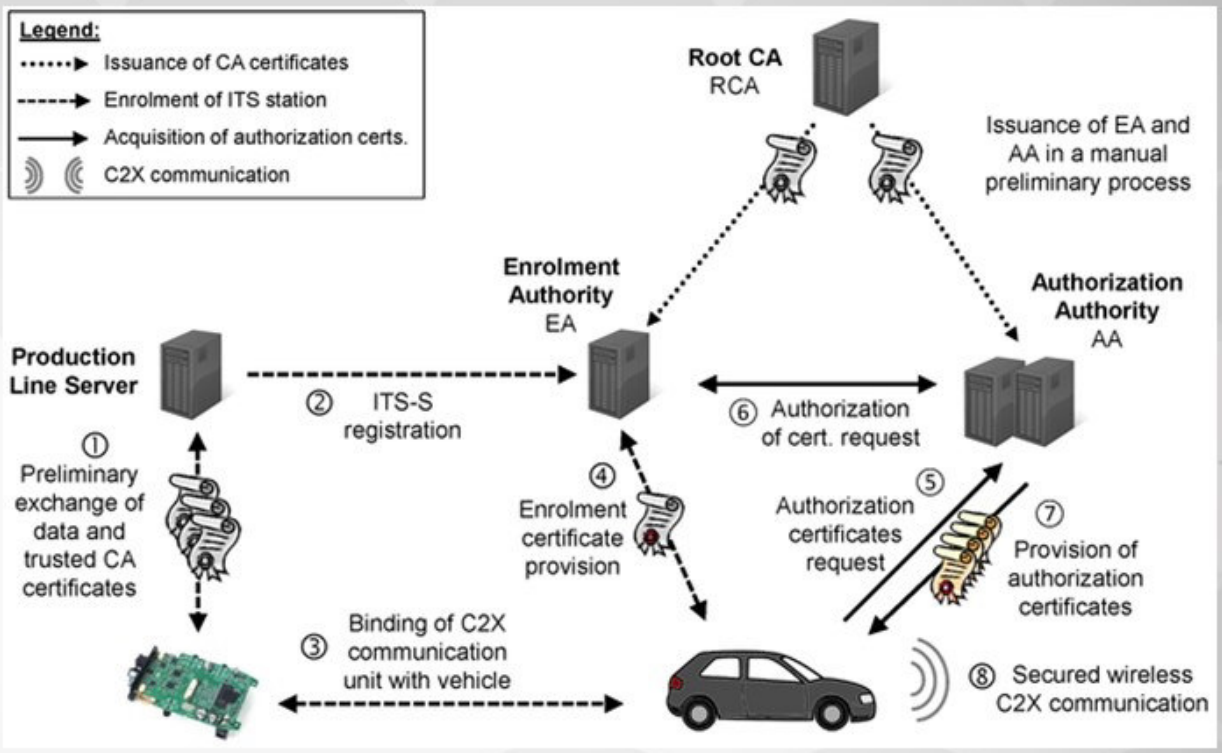
- Verkehr umlenken
  - Angreifer meldet Stau in den Straßen um seine Wohnung
    - Weniger Verkehr
- Verkehr verlangsamen
  - Angreifer meldet Glatteis
- Fahrer ablenken / gefährden
  - Angreifer meldet Unfall direkt voraus
    - Verkehrsteilnehmer bremsen überraschend ab



Car2X Infrastruktur

- Car-2-X PKI
  - Root CA (RCA)
    - Zertifiziert EA und AA
  - Enrolment Authority (EA)
    - Erstellt Langzeitzertifikat
  - Authorization Authority (AA)
    - Pseudonym Zertifikate

➢ Authentizität & Datenschutz

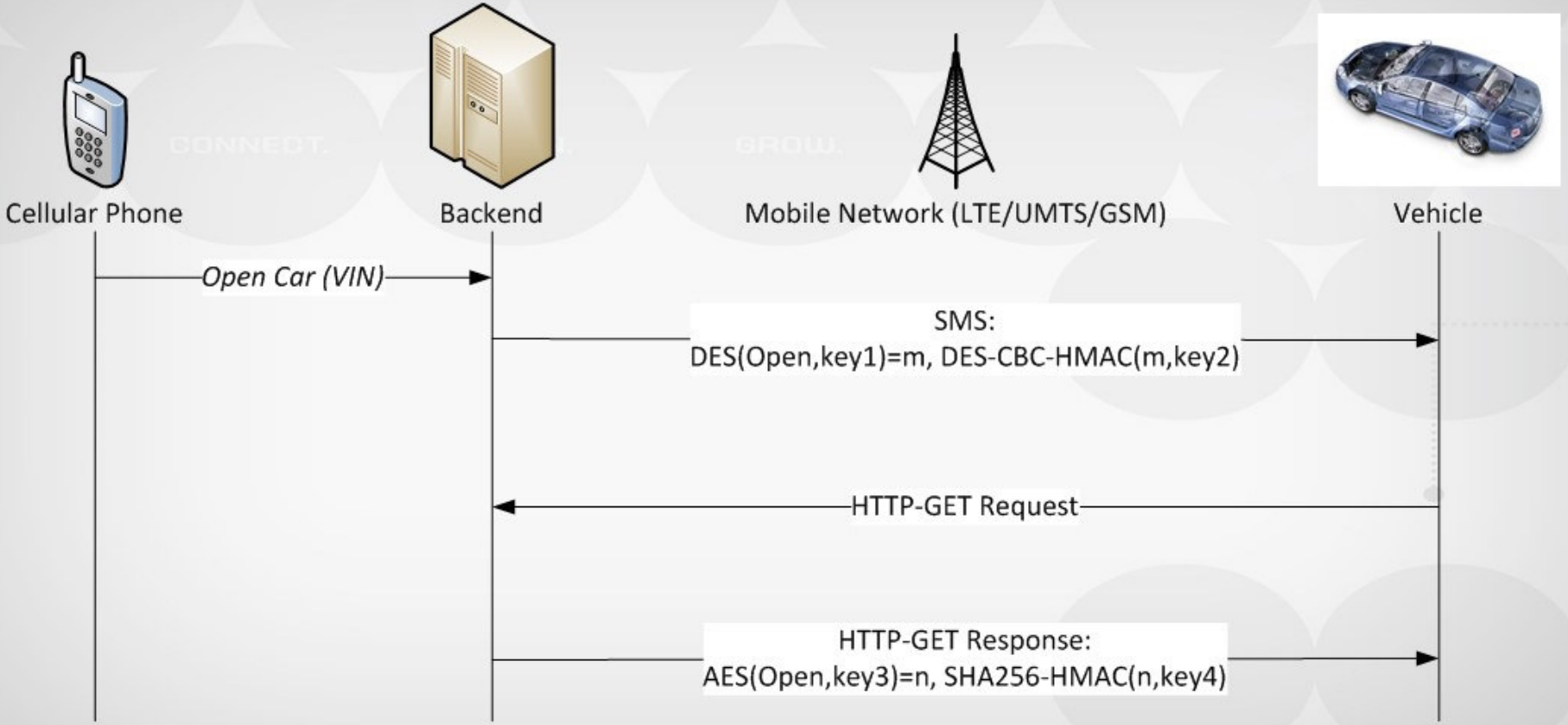


Quelle: Fraunhofer SIT, Secure Integration of a C2X Public Key Infrastructure
https://www.sit.fraunhofer.de/fileadmin/dokumente/info-material/englisch/Fraunhofer_SIT_Offer_-_C2X_PKI_Integration.pdf

Telematikdienst

- **Remote Services**
  - unberechtigtes Ausführen von Fern-Funktionen, z. B. Türöffnen
- **Last State Call**
  - Auskundschaften von Fahrzeugstandort und Verriegelungszustand
- **Real Time Traffic Informations (RTTI)**
  - Mitlesen aktueller Fahrzeugstandorte und z. B. gefahrene Geschwindigkeiten, Tracking von Fahrzeugen
- **Intelligenter Notruf**
  - im Steuergerät hinterlegte Rufnummern, z. B. für Notrufe, können verändert werden
- **Fahrzeughersteller Online**
  - private E-Mails

Telematikdienst Protokoll



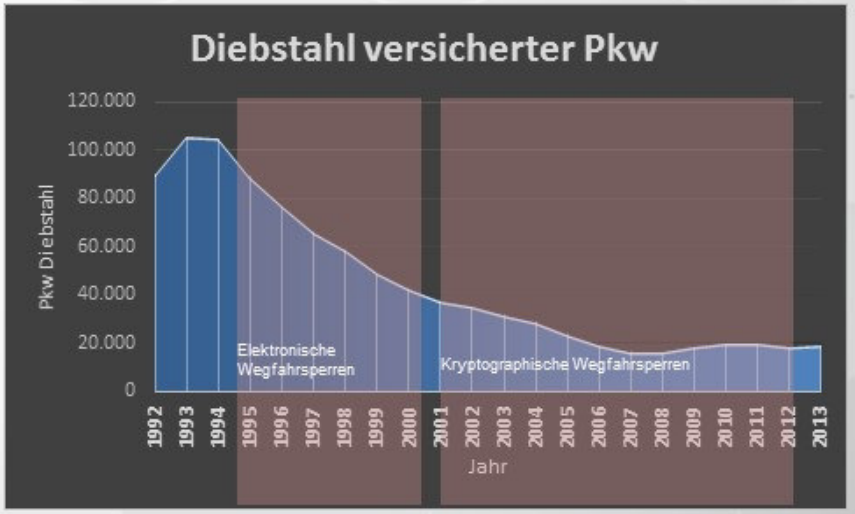
Telematikdienst

- Symmetrische Schlüssel
  - für alle Fahrzeuge identisch
- Keine Transportverschlüsselung (TLS/SSL)
- Kein Integritätsschutz
- Kein Replay-Schutz

Fahrzeugzugang und Wegfahrsperre

- Öffnen aus der Entfernung
- Schutz gegen Fahrzeugdiebstahl durch Verifikation der Authentizität des Fahrzeugschlüssels
- Herausforderungen
  - Energie, Kosten, Geschwindigkeit etc.

➢ Viele proprietäre Systeme mit kurzen Schlüssellängen
  - Alle proprietären Systeme wurden gebrochen *
  - Gebrochene Systeme oft noch im Einsatz



Quelle: GDV die deutschen Versicherer - Autodiebstahl 2013 – Alle Zahlen auf einen Blick http://www.gdv.de/2014/09/autodiebstahl-2013-alle-zahlen/

* Eisenbarth, Thomas, et al. *On the power of power analysis in the real world: A complete break of the KeeLoq code hopping scheme*. Advances in Cryptology CRYPTO 2008.
Verdult, Roel, Flavio D. Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with Hitag2. 21st USENIX 2012.

Inhalt

- Motivation
- Drahtlose Verbindung zum Auto
- Physikalische Verbindungen
- Fazit & Ausblick

Infotainment

- Navigationssystem
- Mediaplayer
- Rückfahrkamera
- Tacho
- **Browser**

Quelle: Steve Jurvetson,
https://en.wikipedia.org/wiki/Tesla_Model_S#/media/File:Tesla_Model_S_digital_panels.jpg

Angriffe über indirekten physikalischen Zugang

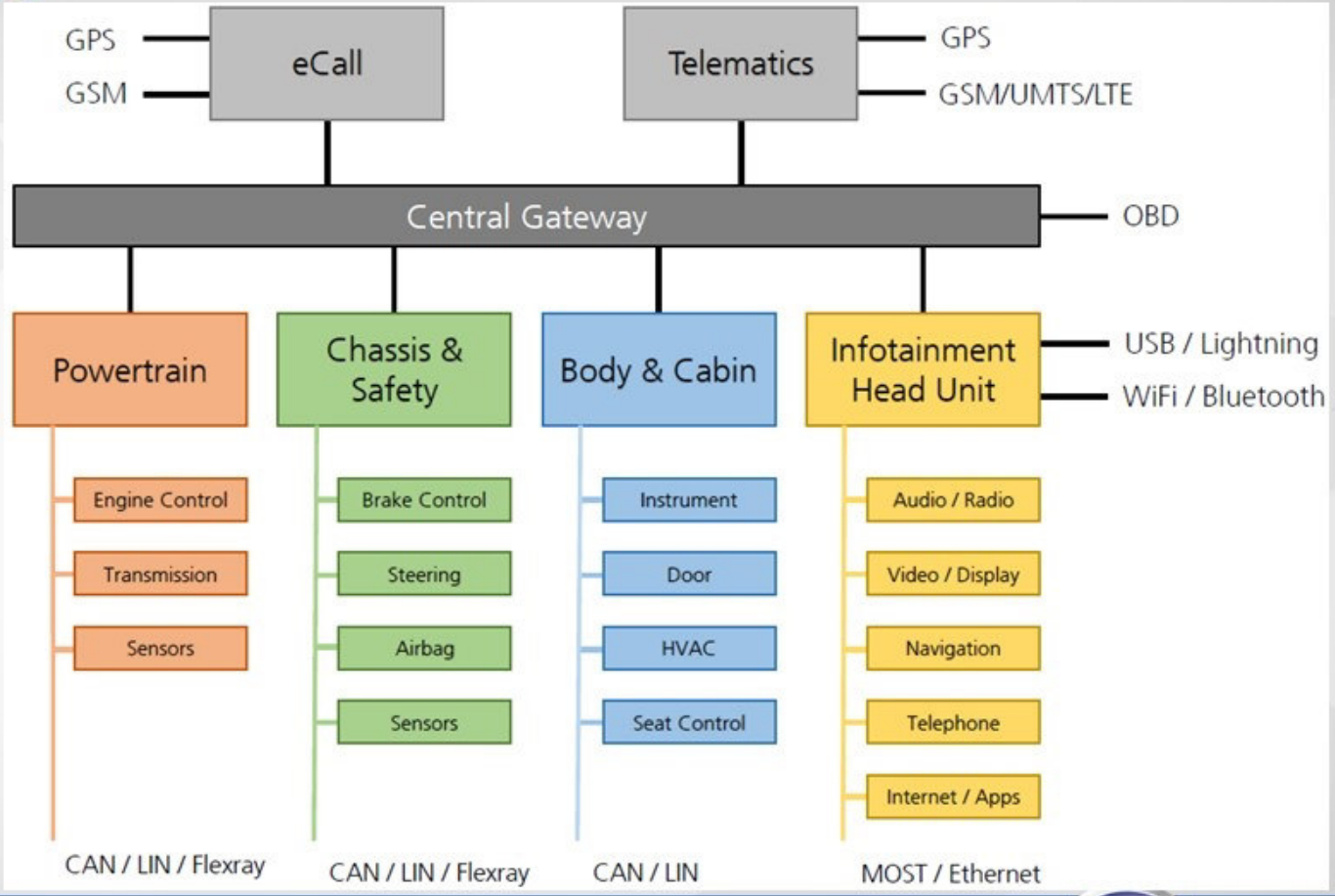
- Angriff auf Infotainment System (Checkoway et al.)
  - Media-Player spielt WMA und MP3 Dateien von CDs
  - Steuergerät für UI und Audio-Parsing kann mit CAN-Bus kommunizieren
  - Zwei schwerwiegende Schwachstellen
    - Updatefunktion ermöglicht bösartige Firmware zu installieren
    - Buffer Overflow ermöglicht Ausführung beliebigen Codes
      - Manipulierte WMA Datei kann CAN-Nachrichten senden

Checkoway et al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces USENIX Security Symposium, 2011

Quelle: https://en.wikipedia.org/wiki/Compact_disc#/media/File:Compact_disc.svg

BUS-Systeme

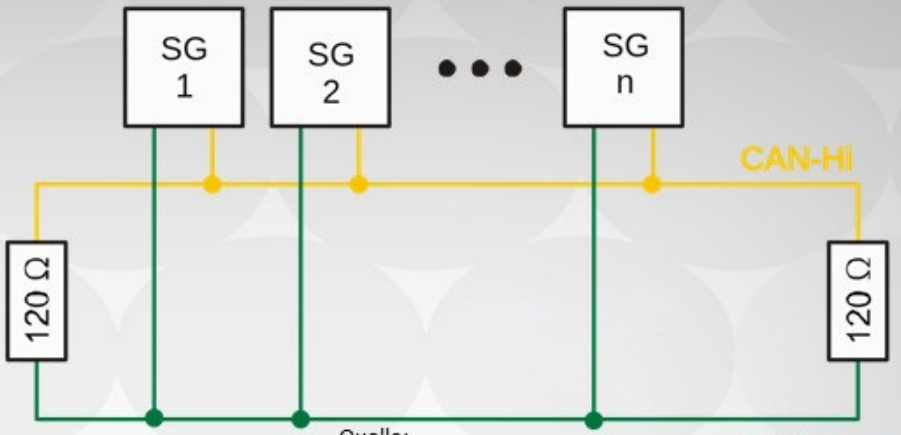
- CAN
- FlexRay
- LIN
- MOST
- Ethernet



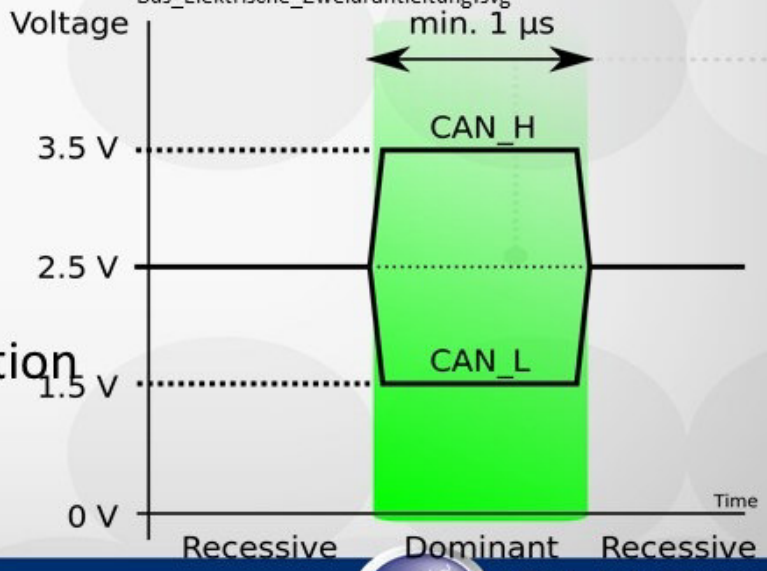
CAN-Bus

- Verbreitetes System im Auto
- Hohe Zuverlässigkeit

- Zwei Leitungen
  - CAN-High
  - CAN-Low
- Versenden entgegengesetzter Signale
- Pioritäts Bussystem
  - **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **R**esolution
  - Nachricht mit höchster Priorität bleibt erhalten



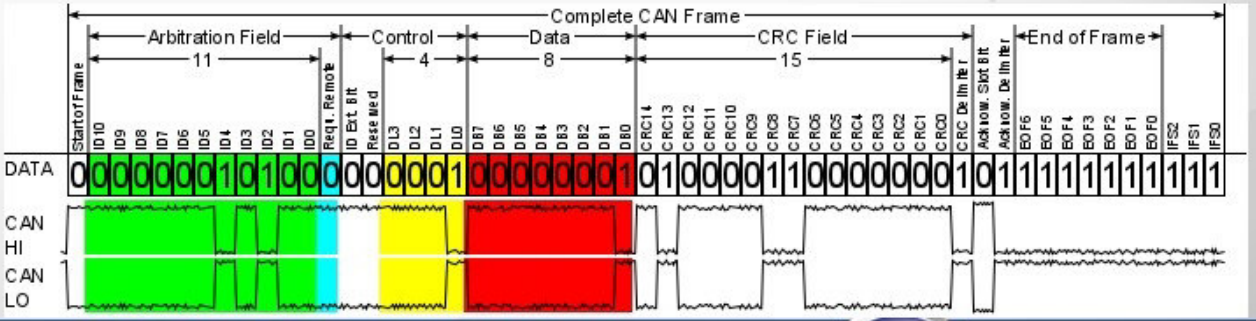
Quelle: https://de.wikipedia.org/wiki/Controller_Area_Network#/media/File:CAN-Bus_Elektrische_Zweidrahtleitung.svg



Quelle: https://de.wikipedia.org/wiki/Controller_Area_Network#/media/File:canbus_levels.svg

CAN Security

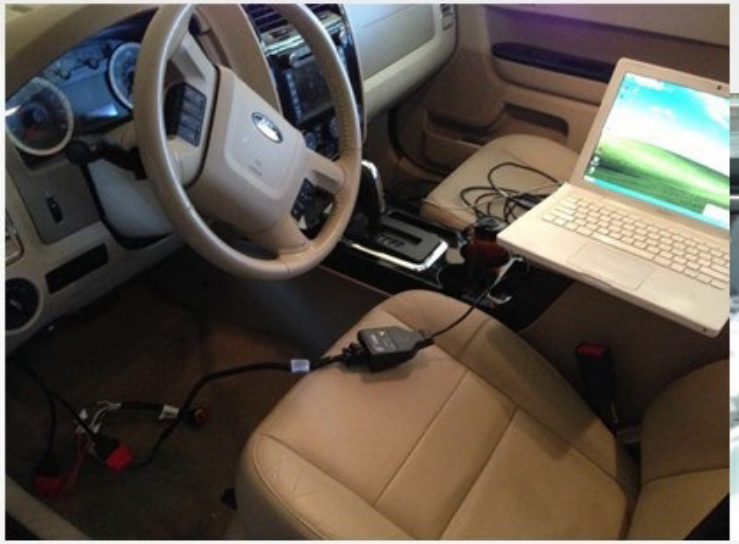
- **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **R**esolution
  - Nachrichten werden gleichzeitig versendet
  - ECUs mit niedrigerer Priorität erkennen Kollisionen
  - Nur die Nachricht mit der höchsten Priorität wird vorgesetzt
- Integritätsprüfung
  - CRC …
- Authentizitätsprüfung
  - -



Quelle: https://de.wikipedia.org/wiki/Controller_Area_Network#/media/File:CAN-Bus-frame_in_base_format_without_stuffbits.svg

CAN-Bus Kontrolle

- Charlie Miller & Chris Valasek verbinden PC mit CAN-Bus
  - Kontrolle über
    - Lenkrad
    - Gas
    - Bremse
    - Öffnen
    - Schließen
    - Licht
    - Auto starten
    - usw.



Quelle: Miller, Charlie, and Chris Valasek. "Adventures in automotive networks and control units." *DEF CON 21 Hacking Conference. Las Vegas, NV: DEF CON*. 2013

Diagnosezugang

- Standardisierte Diagnoseschnittstelle: On-Board Diagnostic (OBD)
- OBD ermöglicht direkten Zugriff auf das Bordnetz
- Da keine Sicherheitsmechanismen
  - Abhören, (Wieder-)Einspielen von Nachrichten
  - Zugriff auf Steuergeräte - Auslösen von Funktionen
    - Bsp.: Bremsen Motor, Radio, Instrument Cluster (Koscher et al.)
- Zugriff für weitere Angriffe wie Chiptuning
- OBD-Adapter oft von Versicherungen für Pay-as-you-drive Modelle genutzt

Quelle: M. Minderhoud, https://de.wikipedia.org/wiki/On-Board-Diagnose#/media/File:OBD_002.jpg

Quelle: http://www.app-drive.de/

Quelle: Miller, Charlie, and Chris Valasek. "Adventures in automotive networks and control units." *DEF CON 21 Hacking Conference. Las Vegas, NV: DEF CON*. 2013

Inhalt

- Motivation
- Drahtlose Verbindung zum Auto
- Physikalische Verbindungen
- Fazit & Ausblick

Fazit

- Technologien im Auto entwickeln sich immer schneller
- Das vernetzte Auto wird Realität
- Wenige bis gar keine Sicherheitsstandards
  - **ISO 26262** („*Road vehicles – Functional safety*“)
  - Ausschließlich funktionale Sicherheit
- Autos sind ein sehr attraktives Angriffsziel
  - Wert des Autos
  - Gefahr für Leib und Leben des Fahrers
  - Vermeidlich leichtes Ziel (keine Sicherheitsstandards)