IT-Sicherheit und Schutz vor Malware im Automobil

Arne Beer, Stefan Grusche, Joshua Stock

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Gliederung

1. Can Bus

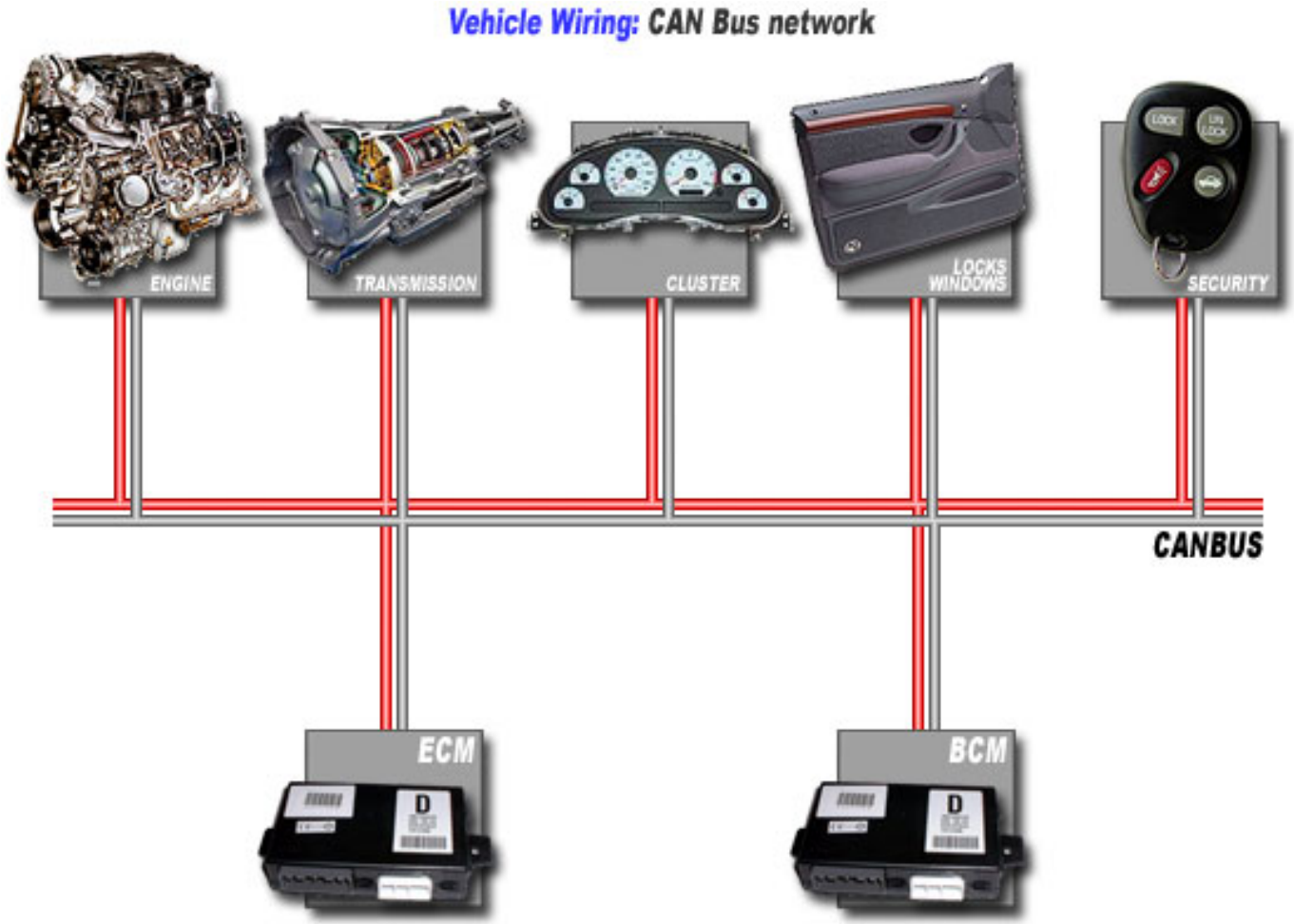
2. Ausgewählte Angriffsvektoren
   - Mobilfunk
   - WLAN
   - Bluetooth

CAN-Bus: Was ist der CAN-Bus?

- Electron control Units (ECU's)
- Zentrale Kommunikationsschnittstelle
- Controller Area Network (CAN)

CAN-Bus: Kommunikation am Can Bus

- Alle Geräte kommunizieren gleichzeitig.
- Jedes Gerät sendet an jeden.



CAN-Bus: Unsicherheiten

- Kompletter Verkehr ist unverschlüsselt
- Keine Verschlüsselung

$\Rightarrow$ Sniffing

CAN-Bus: Messages

Ein CAN-Bus Paket:

```
00 B4 08 00 00 00 00 3C 18 C0 FF
```

22 Hexadezimalstellen = 88 bit or 11 Byte

CAN-Bus: Messages

Ein CAN-Bus Paket:

00 B4 08 00 00 00 00 3C 18 C0 FF

Byte 1-2 Address

CAN-Bus: Messages

Ein CAN-Bus Paket:

```
00 B4 08 00 00 00 00 3C 18 C0 FF
```

Byte 1-2 Address
Byte 3 Payload length

CAN-Bus: Messages

Ein CAN-Bus Paket:

`00 B4 08` **`00 00 00 00 3C 18 C0`** `FF`

Byte 1-2 Address
Byte 3 Payload length
byte 4-10 Payload

CAN-Bus: Messages

Ein CAN-Bus Paket:

`00 B4 08` **00 00 00 00 3C 18 C0** `FF`

Byte 1-2 Address
Byte 3 Payload length
Byte 4-10 Payload
Byte 11 Checksum
E.g.: $(IDH + IDL + Len + Sum(\text{Data}[0] - \text{Data}[Len - 2]))\&0xFF$

CAN-Bus: Messages

Ein CAN-Bus Paket:

`00 B4 08` **`00 00 00 00 3C 18 C0`** `FF`

Byte 1-2 Address
Byte 3 Payload length
byte 4-10 Payload

CAN-Bus: Building own packets

Wäre es nicht praktisch konstatt 100 km/h zu fahren?

```
AA BB 00 00 CC DD 00 00
```

CAN-Bus: Building own packets

Wäre es nicht praktisch konstatt 100 km/h zu fahren?

```
XX YY LL AA BB 00 00 CC DD 00 SS
```

CAN-Bus: Building own packets

Wäre es nicht praktisch konstatt 100 km/h zu fahren?

$$\text{Speed}(mph) = 0.0065 \cdot (CCDD) - 67$$

$$RPM = 0.25 \cdot (AABB) - 24$$

Angriffsvektoren: verwundbare Komponenten am CAN-Bus

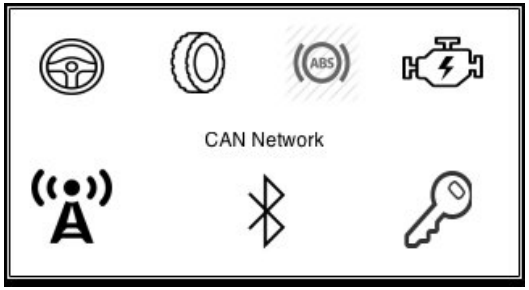


Abbildung: Sedan Infiniti (2010) und Komponenten im CAN-Netzwerk

[?]

- (zu) offene Schnittstellen
- Redundanzen in der Implementierung
- Telematik-Modul bündelt ausgehende Verbindungen

Mobilfunk I

Abbildung: Mobilfunk-Einheit im Jeep Cherokee

[?]

- Funktionen:
  - Internetverbindung (3G)
  - Mobilfunk

Mobilfunk II

- Unbemerkte Anrufe an Telematik-Einheit sind möglich
  - Modem übersetzt akustische Töne in Bits
  - Verwundbarkeiten: Pufferüberlauf und Authentifizierung
- Beispiel für Angriff:
  - Automatisiertes Anrufen bis Authentifizierung erfolgt
  - Aufhebung der maximal erlaubten Anruflänge
  - Download von zusätzlichem Code über 3G-Modem

WLAN

- Bla

Bluetooth

Hack des 2014er Jeep Cherokees

Abbildung: Ziel des Angriffs: 2014 Jeep Cherokee

- veröffentlicht im Juli 2015
- durchgeführt von Charlie Miller und Chris Valasek

Jeep Cherokee: CAN-Netzwerk

Abbildung: Übersicht über CAN-Netze

- zwei CAN-Netzwerke
- Radio als Verbindungsstück

Fahrassistenzsysteme des Jeeps

Abbildung:

- adaptiver Tempomat
- Kollisionswarnsystem
- Spurhalteassistent
- Parkassistent

Angriffsvektoren des Jeeps

- Bluetooth
  - herkömmliche Angriffe möglich
- Radio
  - vermutlich keine Code-Ausführung zu erreichen
- WLAN
  - Auto fungiert als WLAN-Hotspot
- Mobilfunk / Mobiles Internet
  - Freisprechanlage, diverse Apps etc.

$\Rightarrow$ UConnect-Mediensystem verbindet sämtliche Faktoren