

# Sicherheit in Kognitiven Automobilen

Martin Thoma | 23. Juli 2015



# Chrysler Uconnect-Hack

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



- Kognition: Wahrnehmung der Umwelt
  - Sensoren: Reifenrotation und -druck, Unfall-Detektion, ...
  - Aktoren: Motor, Bremsen, Licht
- VIEL Elektronik: 30 und mehr ECUs in modernen Autos

- Kognition: Wahrnehmung der Umwelt
  - Sensoren: Reifenrotation und -druck, Unfall-Detektion, ...
  - Aktoren: Motor, Bremsen, Licht
- VIEL Elektronik: 30 und mehr ECUs in modernen Autos

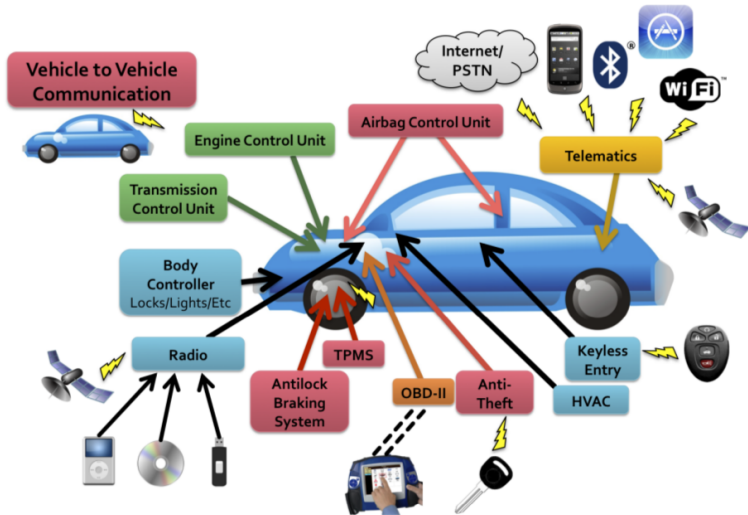
- Kognition: Wahrnehmung der Umwelt
  - Sensoren: Reifenrotation und -druck, Unfall-Detektion, ...
  - Aktoren: Motor, Bremsen, Licht
- VIEL Elektronik: 30 und mehr ECUs in modernen Autos

- Kognition: Wahrnehmung der Umwelt
  - Sensoren: Reifenrotation und -druck, Unfall-Detektion, ...
  - Aktoren: Motor, Bremsen, Licht
- VIEL Elektronik: 30 und mehr ECUs in modernen Autos

- CAN-Bus
- OBD (On-Board-Diagnostics)
- TPMS (Tire pressure measurement system)
- eCall (Elektronischer Notruf)

- *Mord / Körperverletzung*: Beschleunigen, Bremsen, Lenken
- *Diebstahl*: Auto öffnen, Position des Autos, Metadaten
- *Ablenkung*: Lichter, Radio
- *Trollen*: Klimaanlage, Dashboard





## ■ Auto-Spezifisch

- Weniger Elektronik? Getrennte Bus-Systeme?
- Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
- Plausibilität von CAN-Nachrichten prüfen

## ■ Allgemein

- Authentifizierung vor Software-Updates
- Andere Sprachen (Java, Rust)
- Besserer Code
  - Code Reviews
  - Static Code Analysis
- Spezielles (Stack Cookies, strncpy() anstatt strcpy())

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, strncpy() anstatt strcpy())

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, strncpy() anstatt strcpy())

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, strncpy() anstatt strcpy())

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)



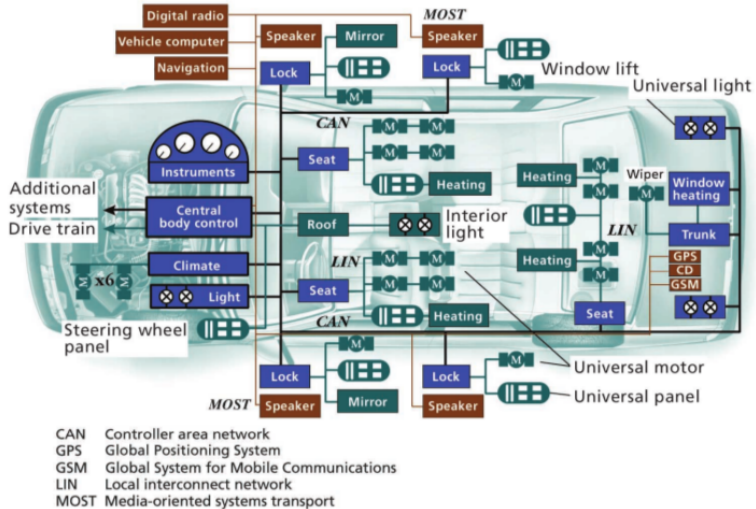
- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)

- Auto-Spezifisch
  - Weniger Elektronik? Getrennte Bus-Systeme?
  - Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
  - Plausibilität von CAN-Nachrichten prüfen
- Allgemein
  - Authentifizierung vor Software-Updates
  - Andere Sprachen (Java, Rust)
  - Besserer Code
    - Code Reviews
    - Static Code Analysis
  - Spezielles (Stack Cookies, `strncpy()` anstatt `strcpy()`)

# Thanks for Your Attention!



## Wichtigste Paper

- Checkoway et al.: Comprehensive Experimental Analyses of Automotive Attack Surfaces
- Koscher et al: Experimental Security Analysis of a Modern Automobile

## Bildquellen:

- Folie „Angriffsvektoren“: Paper „Comprehensive Experimental Analyses of Automotive Attack Surfaces“
- Folie „Chrysler Uconnect-Hack“:  
[wired.com/2015/07/hackers-remotely-kill-jeep-highway](http://wired.com/2015/07/hackers-remotely-kill-jeep-highway)

- A. Davis: Black Hat 2015 - Broadcasting Your Attack: Security Testing DAB Radio in Cars, 2015.
- C. Miller, C. Valasek: Black Hat 2015 - Remote Exploitation of an Unaltered Passenger Vehicle, 2015.
- C. Miller, C. Valasek: [Hackers Remotely Kill a Jeep on the Highway—With Me in It](#), 2015. 5:05 Minuten.
- C. Miller, C. Valasek: [Black Hat 2014 - Embedded: A Survey of Remote Automotive Attack Surfaces](#), 2014. 57:36 Minuten.
- C. Miller, C. Valasek: [Defcon 22 - A Survey of Remote Automotive Attack Surfaces](#), 2014. 50:24 Minuten.
- C. Miller, C. Valasek: [Defcon 21 - Adventures in Automotive Networks and Control Units](#), 2013. 48:10 Minuten.