

## Sicherheit in Kognitiven Automobilen

Martin Thoma | 23. Juli 2015



#### Inhalt



- 1 Einleitung
- 2 Standards und Verordnungen
- 3 Angriffe
- 4 Verteidigung

Verteidigung

End



- 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

# Standards und Verordnungen



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

Martin Thoma - Sicherheit in Kognitiven Automobilen

## Angriffsziele



- Beschleunigen und Bremsen
- Auto öffnen
- Lichter
- Radio, Klimaanlage

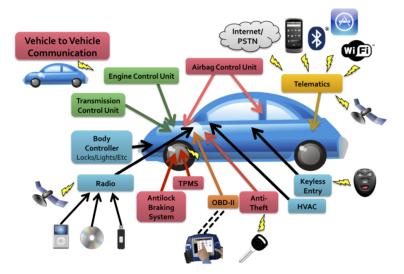
Martin Thoma - Sicherheit in Kognitiven Automobilen

23. Juli 2015

End

#### Angriffsvektoren







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

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



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

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



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



- Wenig Elektronik? Getrennte Bus-Systeme?
- Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
- Plausibilität von CAN-Nachrichten prüfen
- Authentifizierung vor Software-Updates
- Andere Sprachen (Java, Rust)
- Besserer CodeCode ReviewsStatic Code Analysis
- Speizielles (Stack Cookies, strncpy() anstatt strncpy())



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



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



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



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



23. Juli 2015

7/10

- Wenig Elektronik? Getrennte Bus-Systeme?
- Obfuscation: Debugging-Symbole entfernen um Reverse-Engineering zu erschweren
- Plausibilität von CAN-Nachrichten prüfen
- Authentifizierung vor Software-Updates
- Andere Sprachen (Java, Rust)
- Besserer Code
  - Code Reviews

Martin Thoma - Sicherheit in Kognitiven Automobilen

- Static Code Analysis
- Speizielles (Stack Cookies, strncpy() anstatt strncpy())

## Bildquellen



 Folie: Comprehensive Experimental Analyses of Automotive Attack Surfaces

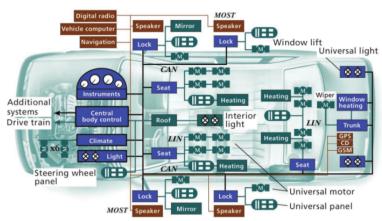
# **Paper**



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

#### Thanks for Your Attention!





CAN Controller area network GPS Global Positioning System

GSM Global System for Mobile Communications

LIN Local interconnect network

MOST Media-oriented systems transport