# Sicherheit im Automobilbereich

Martin Thoma Karlsruhe Institute of Technology
Email: info@martin-thoma.de

***Zusammenfassung*—Moderne Automobile verfügen über eine Vielzahl von Assistenz- und Fahrsicherheitssystemen. Diese Systeme haben Schnittstellen, welche das Ziel von Angriffen sein können. In dieser Seminararbeit wird der aktuelle Stand der IT-Sicherheit kognitiver Automobilie untersucht. Dabei wird auf mögliche Angriffsvektoren und Ziele sowie Möglichkeiten zum Schutz eingegangen.**

**Keywords: Sicherheit**

## I. Einleitung

Kognitive Automobile sind, im Gegensatz zu klassichen Automobilen, in der Lage ihre Umwelt und sich selbst wahrzunehmen und dem Fahrer zu assistieren. So benötigt ein Auto mit Antiblockiersystem beispielsweise die Drehzahl an jedem Reifen; für Einparkhilfen werden Sensoren benötigt, welche die Distanz zu Hindernissen wahrnehmen sowie Aktoren, die das Auto lenken und beschleunigen könne. Weitere dieser System sind Spurhalteassistenz, Spurwechselassistenz und Fernlichtassistenz. Um die Funktionalität dieser Assistenzsysteme bereitstellen zu können, muss das Auto die Umwelt wahrnehmen und – in festgelegten Grenzen – autonom agieren können.

Als immer mehr elektronische Systeme in Autos verbaut wurden, die teilweise redundante Aufgaben erledigt haben, wurde der CAN-Bus entwickelt [KiDL86]. Dieser wurde in ISO 11898 international standardisiert.

## II. Standards und Verordnungen

In der EU wurde mit [Euro98] die OBD Schnittstelle verpflichtend für Fahrzeuge der Klasse $M_1$ und $N_1$ mit Fremdzündungsmotor ab 1. Januar 2004. Die EU-Direktive führt weiter die in der ISO DIS 15031-6 Norm aufgeführten Fehlercodes als Minimalstandard ein. Diese müssen „für genormte Diagnosegeräte [...] uneingeschränkt zugänglich sein“. Außerdem muss die Schnittstelle im Auto so verbaut werden, dass sie „für das Servicepersonal leicht zugänglich, zugleich aber vor unbefugten Eingriffen durch nichtqualifizierte Personen geschützt ist“.

Um die Daten bereitzustellen, werden verschiedene elektronische Komponenten über den CAN-Bus vernetzt. Dieser ist in ISO 11898 genormt.

Weiterhin wurde in der EU mit [Euro09] beschlossen, dass ab 1. November 2012 alle PKWs für Neuzulassungen ein System zur Reifendrucküberwachung besitzen müssen. Ab 1. November 2014 müssen alle Neuwagen ein solches System besitzen.

Mit [Euro15] wird für Fahrzeuge, die ab dem 31. März 2018 gebaut werden das eCall-System verpflichtend.

## III. Angriffsarten und -ziele

In der IT-Sicherheit unterscheidet man zwischen Angriffsvektor und *Angriffsziel*. Als *Angriffsvektor* wird der Weg sowie die Art und Weise bezeichent, wie ein Angriff durchgeführt wird [SaSc12], [Kenn12]. Außerdem unterscheidet man Sicherheitslücken und Exploits. Eine Sicherheitslücke stellt eine Schwachstelle in einem System dar. Wenn diese Lücke genutzt werden kann um Schaden zuzufügen, dann spricht man von einem *Exploit*.

### A. Angriffsziele

Im Automobilbereich sind verschiedene Motive vorstellbar, die einen Angriff auf ein Auto erfordern

- Beschaffung von Persönlichen Informationen
- Diebstahl
- Zerstörung
- Mord

Je nach Motivation sind verschiedene Ziele im Auto vorstellbar:

- Positionsinformationen
- Meta-Informationen wie Modell, gefahrene Kilometer
- Öffnen der Türen
- Beschleunigen, Bremsen

### B. Angriffsvektoren

Jede Schnittstelle zum Auto stellt einen möglichen Angriffsvektor dar. Allerdings stellen nicht nur Empfänger mögliche Angriffsvektoren dar, sondern in bezug auf die Privatsphäre auch Sender.

- OBD-Schnittstelle
- TPMS
- eCall

### C. Reverse-Engineering

- CAN-Bus
- OBD-Diagnosegerät
- TPMS
- eCall?

## IV. Verteidigungsmassnahmen

- Sanitizing User input
- „Encryption“ der Pakete
- „Obfuscation“ (Debugging-Symbole entfernen)

## Literatur

[Euro98] European Parliament, Council of the European Union. Richtlinie 98/69/EC des Europäischen Parlaments und des Rates, Oktober 1998. http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31998L0069.

[Euro09] European Parliament, Council of the European Union. Verordnung (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates, Juli 2009.

[Euro15] European Parliament, Council of the European Union. Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates, April 2015.

[Kenn12] David Kennedy. *Metasploit*. mitp Professional. 2012.

[KiDL86] Uwe Kiencke, Siegfried Dais und Martin Litschel. Automotive Serial Controller Area Network. Technischer Bericht, Robert Bosch GmbH, Februar 1986.

[SaSc12] J. Sambleben und S. Schumacher. *Informationstechnologie und Sicherheitspolitik: Wird der dritte Weltkrieg im Internet ausgetragen?* Books on Demand. 2012.