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 festlegbaren 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. Über ihn kommunizieren elektronische Steuergeräte, sog. *ECUs* (engl. *electronic control units*).

II. Standards und Verordnungen

Für den Automobilbereich existieren viele Standards und Verordnungen. In diesem Abschnitt wird eine relevante Auswahl vorgestellt. Diese Auswahl betrifft Fahrzeuge der Klassen M_1 und N_1, d.h. Fahrzeuge zur Personenbeförderung „mit mindestens vier Rädern und höchstens acht Sitzplätzen außer dem Fahrersitz“ sowie „für die Güterbeförderung ausgelegte und gebaute Kraftfahrzeuge mit einer zulässigen Gesamtmasse von 3,5 Tonnen.“ [Euro70]

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 (engl. *tire pressure monitoring system*, kurz *TPMS*) 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 wie Beschaffung von persönlichen Informationen, Diebstahl, Zerstörung und Mord, vorstellbar, die einen Angriff auf ein Auto erfordern. Je nach Motivation sind verschiedene Ziele im Auto für den Angreifer von Interesse:

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

Im Folgenden wird beschrieben, wie diese Daten abgegriffen werden können.

B. Angriffsvektoren

Jeder Empfänger stellt als Schnittstelle zum Auto einen möglichen Angriffsvektor dar. Allerdings sind in Bezug auf die

Privatsphäre auch Sender mögliche Angriffswege. Dabei ist insbesondere die OBD-Schnittstelle, TPMS und eCall zu nennen.

C. Reverse-Engineering

Reverse-Engineering bezeichnet den Vorgang ein System nachzuentwickeln. Im Bezug auf Computersicherheit wird dies von Angreifern gemacht um die genaue Funktionsweise des Originals nachvollziehen und mögliche Fehler in der Entwicklung oder sogar im Design zu entdecken. Reverse-Engineering kann nicht verhindert, aber erschwert werden.

Die Sicherheit keines Computersystems sollte ausschließlich auf der Geheimhaltung der Implementierung beruhen [ScJT08], sie kann aber eine weitere Sicherungsschicht sein. Diese kann es dem Angreifer erschweren, den eigentlichen Angriff durchzuführen oder Fehler in der Implementierung verdecken.

Aus diesem Grund sollte das Reverse-Engineering schwer sein. Insbesondere sollten sog. Debugging-Symbole, also Informationen welche im der Binärdatei hinterlegt werden um Fehler aufzuspüren, nicht in verkauften Autos sein. Des Weiteren sollten Fehlernachricht aus dem Produktivcode entfernt werden. Beides wurde in [CMKA+11] in einem untersuchtem Auto im Code von ECUs gefunden gefunden.

D. Angriffszenarien

IV. Verteidigungsmassnahmen

Wie in den vorherigen Abschnitten beschrieben wurde, ist der CAN-Bus eine große Schwachstelle der IT-Sicherheit in Autos. Über ihn müssen viele ECUs kommunizieren und einige, wie das Autoradio, werden nicht als Sicherheitskritsch wahrgenommen.

Daher ist es wichtig die Nachrichten, welche über den CAN-Bus empfangen werden, zu filtern. Die Informationen müssen auf Plausibilität geprüft werden.

Literatur

[CMKA+11] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner und Tadayoshi Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, Berkeley, CA, USA, 2011. USENIX Association, S. 6–6.

[Euro70] Europäischer Rat. Richtlinie des Rates 70/156/EWG, Februar 1970.

[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.

[ScJT08] Karen Scarfone, Wayne Jansen und Miles Tracy. *Guide to general server security*. U.S. Dept. of Commerce, National Institute of Standards and Technology. 2008.