DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Automotive Security

Studienarbeit

für die Prüfung zum

Bachelor of Science

des Studienganges Informatik / Angewandte Informatik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

Jonas Kölblin

Abgabedatum 22. Mai 2023

Bearbeitungszeitraum	24 Wochen
Matrikelnummer	7150881
Kurs	TINF20B5
Ausbildungsfirma	SICK AG Waldkirch
Gutachter der Studienakademie	Ralf Brune

Erklärung

Ich versichere hiermit, dass ich meine Studienarbeit mit dem Thema: »Automotive Security« selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort Datum

Unterschrift

Abstract

abstract

Inhaltsverzeichnis

1 Einführung **1**
1.1 Motivation 1
1.2 Zielsetzung 2

2 Grundlagen **3**
2.1 Automotive Networking 3
2.1.1 Controller Area Network 4
2.1.2 Local Interconnect Network 5
2.1.3 Schnittstellen 6
2.2 Cyber Security 6
2.2.1 Security Lifecycle 6
2.2.2 ISMS 6

3 Angriffsflächen **7**
3.0.1 Bootvorgang 7

4 Schutzmaßnahmen **8**
4.0.1 SecureBoot 8

Literaturverzeichnis **9**

Abbildungsverzeichnis

2.1 Verschiedene Kommunikationsprotokolle in Automobil-Netzwerken 3
2.2 Beispiel des CAN-Netzwerks eines 2010 Ford Escape 4

Abkürzungsverzeichnis

ECU Electronic Control Unit 3
CAN Controller Area Network 4
DLC Data Link Connector 4
LIN Local Interconnect Network 5

Kapitel 1

Einführung

Autos stellen einen sehr großen Anteil der Infrastruktur heutzutage dar. In einer Umfrage im Jahr 2022 gaben über 70 Prozent der Befragten an, ein eigenes Auto zu besitzen [vgl. Statista 2022]. Unzählige Autos sind täglich auf den Straßen unterwegs. Im Zuge der Digitalisierung werden moderne Autos zunehmend mit neuen Features und Technologien ausgestattet, mit dem Ziel, die Bedienung des Fahrzeugs möglichst komfortabel zu gestalten. Das Auto nimmt der fahrenden Person immer mehr Aufgaben ab, wie zum Beispiel das Abblenden, Einparken oder im Fall von selbst-fahrenden Autos sogar das Steuern des Fahrzeugs an sich. Zudem steigt die Anzahl der Entertainmentfeatures, wie zum Beispiel das Verbinden eines Mobiltelefons mit dem Fahrzeug. Ein Effekt dieser Entwicklung ist, dass zum einen die einzelnen Fahrzeugteile intern zunehmend miteinander vernetzt werden. Zum anderen steigt aber auch die Relevanz der Kommunikation des Fahrzeugs mit externen Systemen. Insgesamt sind die elektronischen Systeme in heutigen Fahrzeugen deutlich komplexer und bieten mehr Schnittstellen als noch vor 20 Jahren. Diese zunehmende Komplexität schafft neue Angriffsflächen für Cyberangriffe. Experimente in der Vergangenheit wie zum Beispiel von Charlie Miller und Chris Valasek [vgl. Greenberg 2015] haben jedoch bereits gezeigt, dass die Sicherheitsmaßnahmen der Automobilhersteller oft nicht ausreichen, um die Fahrzeuge zuverlässig gegen solche Angriffe zu schützen.

1.1 Motivation

Eines der schockierendsten Ereignisse der letzten Jahre im Bereich der Automotive Cyber Security war die oben erwähnte Aktion von Miller und Valasek im Jahr 2015 [vgl. Greenberg 2015]. Den beiden Hackern gelang es, einen Jeep Cherokee über das Internet zu

kompromittieren. Dabei verschafften sie sich nicht nur Zugriff zur grundlegenden Board-Elektronik wie dem Radio oder den Scheibenwischern, sondern es gelang ihnen auch, die Bremsen und den Motor zu deaktivieren. Sie konnten das Fahrzeug fernsteuern und der eingeweihte Fahrer war ihnen hilflos ausgeliefert. Dieses Experiment fand natürlich nur zu Forschungs- und Demonstrationszwecken statt. Aktionen wie diese zeigen jedoch anschaulich, wozu eine Person mit böswilligen Absichten theoretisch in der Lage wäre. Sicherheitslücken wie diese können schlimmstenfalls zum Verlust von Menschenleben führen. Aus diesem Grund ist es wichtig, das dem Thema der Automotive Security noch mehr Aufmerksamkeit gewidmet wird. Hersteller müssen sich intensiver mit den durch die zunehmende Vernetzung der Autos entstandenen Angriffsmöglichkeiten beschäftigen und Sicherheitslücken bestenfalls präventiv, ansonsten so schnell wie möglich, schließen. Daher widmet sich diese Arbeit diesen besagten Angriffsmöglichkeiten.

1.2 Zielsetzung

Diese Arbeit soll einen Überblick über die Angriffsflächen eines Automobils sowie über einige Lösungsansätze für diese Schwachstellen schaffen. Hierzu erfolgt zunächst eine Erläuterung der notwendigen theoretischen Grundlagen wie dem Aufbau des internen Netzwerks eines Automobils sowie notwendigen Grundlagen der Cyber Security. Anschließend sollen die verschiedenen Angriffsmöglichkeiten eines Autos aufgezeigt werden. Darauf folgt die Sammlung und Evaluierung von Schutzmaßnahmen gegen diese Angriffsmöglichkeiten mit Blick auf die Frage, wo die Hersteller ansetzen können oder müssen, um ihre Autos sicherer zu gestalten.

Kapitel 2

Grundlagen

In diesem Kapitel sollen die für das weitere Verständnis notwendigen theoretischen Grundlagen erläutert werden. Dazu gehört zunächst der Aufbau des Netzwerks in einem Fahrzeug. Des Weiteren werden relevante Grundlagen der Cyber Security erklärt.

2.1 Automotive Networking

Im Inneren von Autos befinden sich heutzutage eine Vielzahl elektronischer Systeme, von denen jedes mit benachbarten Komponenten kommunizieren kann. Die einzelnen elektronischen Systeme werden als Electronic Control Units (ECUs) bezeichnet. Moderne Autos enthalten in der Regel über 50 verschiedene ECUs [vgl. Miller und Valasek 2013, S. 6]. Da diese Kontrolleinheiten zum Teil lebensentscheidende Aufgaben übernehmen, muss die Kommunikation zwischen den Einheiten möglichst in Echtzeit erfolgen.

Data-rates supported by the low-latency in-vehicle communication protocols.

In-vehicle Communication Protocol	Maximum Data-rate
Local Interconnect Network (LIN)	20 kbit/s
Controller Area Network (CAN)	1 Mbit/s
CAN-FD (Flexible Data)	5 Mbit/s (data), 1 Mbit/s (arbitration, ack)
CAN XL	10 Mbit/s (data)[a], 1 Mbit/s (arbitration, ack)
FlexRAY	10 Mbit/s
Ethernet with Time-Sensitive Networking	100 Mbit/s to 10 Gbit/s

Abbildung 2.1: Verschiedene Kommunikationsprotokolle in Automobil-Netzwerken
Quelle: [Mohammad Ashjaei u. a. 2021, S. 2]

Für die Venetzung der ECUs kommen verschiedene Technologien zum Einsatz (siehe Abbildung 2.1). Diese werden im Folgenden genauer erläutert. Die relevanteste davon ist im Automotive-Bereich der sogenannte CAN-Standard.

2.1.1 Controller Area Network

Die elektronischen Kontrolleinheiten eines Autos sind typischerweise über einen oder mehrere Busse, die auf dem Controller Area Network (CAN)-Standard basieren, miteinander verbunden. Hierbei kommunizieren die ECUs über CAN-Pakete. Diese werden an alle Komponenten gesendet, welche dann jeweils basierend auf dem Inhalt entscheiden, ob das Paket für sie bestimmt ist oder nicht. Eine Identifikation der Quelle oder Authentisierung gibt es in diesem Standard nicht. [vgl. Miller und Valasek 2013, S. 7]
In Abbildung 2.1.1 ist das CAN-Netzwerk eines 2010 Ford Escape dargestellt. Das abgebildete Netzwerk verfügt über zwei Busse, einen medium speed (MS) und einen high speed (HS) CAN-Bus. Beide Busse enden hier im Data Link Connector (DLC) (siehe Kapitel 2.1.3). In Automotive Netzwerken lassen sich zwei Arten von CAN-Paketen finden: normale CAN-Pakete und diagnostische CAN-Pakete.

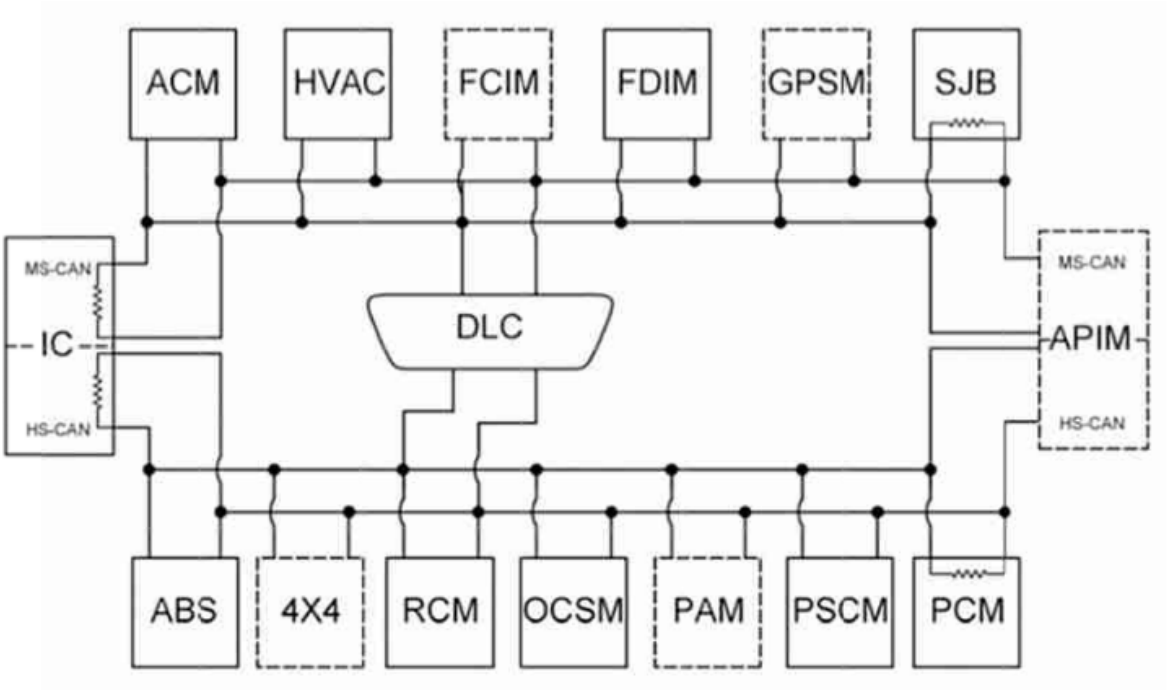

Abbildung 2.2: Beispiel des CAN-Netzwerks eines 2010 Ford Escape
Quelle: [Miller und Valasek 2013, S. 19]

Normale CAN-Pakete

Normale Pakete werden von ECUs gesendet und können entweder Informationen oder Befehle enthalten. Typischerweise werden sie alle Millisekunden gesendet. Auf Anwendungsebene enthalten die CAN-Pakete einen Identifier, die zu übertragenden Daten und manchmal noch eine Prüfsumme, um sicherzustellen, dass das Paket korrekt übertragen wurde. Der Identifier gibt sowohl an, für welche ECUs das Paket bestimmt ist, als auch, welche Priorität das Paket hat. [vgl. Miller und Valasek 2013, S. 9]

Diagnostische CAN-Pakete

Diagnostische Pakete tauchen während des normalen Betriebs des Autos im Normalfall nicht auf. Sie werden von Diagnose-Werkzeugen gesendet, die beispielsweise von Mechanikern genutzt werden um mit den ECUs im Auto zu kommunizieren. So können Mängel und Fehlfunktionen entdeckt oder andere Informationen gewonnen werden. Das Format von diagnostischen CAN-Paketen ähnelt dem von normalen Paketen, erfolgt jedoch meist nach strengeren Konventionen. Standards hierfür sind zum Beispiel ISO-TP, ISO 14229 und ISO 14230. [vgl. Miller und Valasek 2013, S. 10]

2.1.2 Local Interconnect Network

Ein weiteres relevantes Protokoll im Automotive Bereich ist das Local Interconnect Network (LIN) Protokoll. Es wurde 1998 in Zusammenarbeit von Audi, BMW, Daimler-Chrysler, Volvo, Volkswagen, VCT und Motorola entwickelt mit dem Ziel, ein möglichst kosteneffizientes Kommunikationsprotokoll zu schaffen [Fijalkowski 2011, S. 57]. Das LIN-Protokoll basiert auf dem Serial Connections Interface Datenformat und ist in einer Single Master/Multiple Slaves Architektur aufgebaut. Das bedeutet, dass eine elektronische Kontrolleinheit als Masterknoten fungiert und andere elektronische Slave-Einheiten miteinander verbindet.

Aufbau

Nachrichtenpakete bestehen im LIN-Standard aus einem Header und einem Data Frame. Der Header enthält einen Synchronisation Break, ein Synchronisation Byte und einen Message Identifier. Die ersten beiden Bestandteile sind für die Nachrichtensynchronisierung notwendig. Der Identifier wird benötigt, damit Knoten erkennen können, ob eine Nachricht für sie bestimmt ist. Der Data Frame ist nach dem 8N1-Schema aufgebaut.

Das bedeutet, dass jedes Paket ein Startbit, acht Datenbits, kein Paritätsbit und ein Stopbit besitzt. [Fijalkowski 2011, S. 58]
Im LIN-Standard sind drei Arten von Kommunikation erlaubt.

1. Master to Slave, beziehungsweise Master to Multiple Slaves
2. Slave to Master
3. Slave to Slave

Die Slaves können somit auch untereinander ohne Beiteiligung des Masters kommunizieren. [Fijalkowski 2011, S. 59]

Anwendung

LIN zeichnet sich wie oben erwähnt vor allem durch seine Kosteneffizienz aus. Allerdings bietet das Protokoll deutlich weniger Bandbreite als CAN. Somit wird es vor allem an Stellen im Fahrzeug eingesetzt, wo nicht viel Bandbreite notwendig ist. Beispielsweise wird LIN häufig für die Steuerung von Türen, Dach, Sitzen und dem Lenkrad verwendet. [Fijalkowski 2011, S. 59]
Für den Aufbau eines Netzwerks mit den zwei Protokollen gibt es zwei gängige Ansätze:

1. Mehrere ECUs werden über LIN mit einer zentralen ECU verbunden. Die Verbindung dieser zentralen ECUs erfolgt mit dem CAN-Standard.
2. Alle ECUs werden über LIN mit einer zentralen ECU verbunden.

Der zweite Ansatz ist skalierbarer, da ohne großen Aufwand neue Knoten hinzugefügt werden können. Der erste Ansatz ermöglicht jedoch eine deutlich höhere Bandbreite bei der Kommunikation zwischen den Einheiten. [Fijalkowski 2011, S. 58]

2.1.3 Schnittstellen

OBD-II Port

2.2 Cyber Security

2.2.1 Security Lifecycle

[Wurm 2022]

2.2.2 ISMS

Kapitel 3

Angriffsflächen

3.0.1 Bootvorgang

[Wurm 2022]

Kapitel 4

Schutzmaßnahmen

4.0.1 SecureBoot

[Wurm 2022][84]

Literatur

Fijalkowski, B. T. [2011]. »Local Interconnect Networking«. In: *Automotive Mechatronics: Operational and Practical Issues: Volume I*. Dordrecht: Springer Netherlands, S. 57–59. ISBN: 978-94-007-0409-1. DOI: 10.1007/978-94-007-0409-1{\textunderscore}5 [siehe S. 5, 6].

Greenberg, Andy [2015]. *Hackers Remotely Kill a Jeep on the Highway - With Me in It*. URL: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [besucht am 04. 01. 2023] [siehe S. 1].

Miller, Charlie und Chris Valasek [2013]. »Adventures in automotive networks and control units«. In: *Def Con* 21.260-264, S. 15–31 [siehe S. 3–5].

Mohammad Ashjaei u. a. [2021]. »Time-Sensitive Networking in automotive embedded systems: State of the art and research opportunities«. In: *Journal of Systems Architecture* 117, S. 102137. ISSN: 1383-7621. DOI: 10.1016/j.sysarc.2021.102137. URL: https://www.sciencedirect.com/science/article/pii/S1383762121001028 [siehe S. 3].

Statista [2022]. *Besitz eines Pkw in Deutschland im Jahr 2022*. URL: https://de.statista.com/prognosen/999770/deutschland-besitz-eines-pkw [besucht am 04. 01. 2023] [siehe S. 1].

Wurm, Manuel [2022]. *Automotive Cybersecurity*. Springer Berlin Heidelberg. ISBN: 978-3-662-64227-6 [siehe S. 6–8].