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 Studienarbeitmit 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

Abbildungsverzeichnis

Abkürzungsverzeichnis

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 um 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 mehr Aufmerksamkeit gewidmet wird. Hersteller müssen sich intensiver mit den durch die zunehmende Vernetzung der Autos entstandenen Angriffsflächen beschäftigen und solche Lücken bestenfalls präventiv, ansonsten so schnell wie möglich, schließen.

Literatur

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].

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].