Studienarbeit Automotive Security

—

Grobkonzeption

Jonas Kölblin
Kurs: TINF20B5
Betreuer: Ralf Brune
Studiengang: Allgemeine Informatik
Duale Hochschule Baden-Württemberg Karlsruhe

October 31, 2022

1 Einführung

1.1 Hinführung

Einstieg in das Thema

1.2 Motivation

Relevanz: fortschreitende Vernetzung, mangelhafte Sicherung, Konsequenzen einer Schwachstelle

1.3 Zielsetzung

Netzwerkaufbau erläutern, Angriffsflächen aufzeigen, Schutzmöglichkeiten erläutern und bewerten

2 Grundlagen

2.1 Automotive

Aufbau des Netzwerks in Fahrzeugen

2.2 Cybersecurity

Cybersecurity Grundlagen (Kryptographie etc.)

3 Ausarbeitung

3.1 Überblick Angriffsflächen

Welche Angriffsflächen gibt es?

3.2 Schutzmaßnahmen

Sammlung und Erklärung von Schutzmaßnahmen gegen die Angriffsmöglichkeiten mit Blick auf Effektivität und Wirtschaftlichkeit, Kann man sich überhaupt gegen alle Angriffsmöglichkeiten schützen?

4 Fazit

4.1 Schlussfolgerung

Zusammenfassung und Bewertung der Ergebnisse

4.2 Ausblick

Ausblick auf weitere Entwicklung der Thematik

5 Bisherige Literatur

Manuel Wurm: Automotive Cybersecurity (2022)
Tobias Brennich & Martin Moser: Putting Automotive Security to the Test (2020)
Charlie Miller: Lessons learned from hacking a car (2019)
Stephen Checkoway et al: Comprehensive Experimental Analyses of Automotive Attack Surfaces (2011)
Ishtiaq Rouf et al: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study (2010)
Guillermo A. Francia Automotive Vehicle Security Metrics (2021) Andreea-Ina Radu & Flavio Garcia: LeiA: A Lightweight Authentication Protocol for CAN (2016)
Van Huynh Le et al: Security and privacy for innovative automotive applications: A survey (2018)
...