Projekt im WS 2020 (6 SWS, 9 CPs)
PAZ: Penetration Tests im Auto der Zukunft!

Für TI, ITS, AI, WI und IE

In modernen Fahrzeugen arbeitet eine Vielzahl von Sensoren, Aktoren und Steuergeräten (ECUs). Ihre Funktionen verbessern die Leistungsfähigkeit, den Komfort und die Sicherheit. Dies ermöglicht unter anderem fortgeschrittene Fahrerassistenzsysteme und soll in Zukunft das autonome Fahren erlauben.

Die Kommunikation mit externen Quellen wird das Auto der Zukunft ausmachen. Beispiele dafür sind der Informationsaustausch zwischen Fahrzeug und Umgebung (Car-to-X) und die Anbindung an Internet- und Cloud-Dienste.

Dadurch sind kritische Teile der Fahrzeuginfrastruktur angreifbar, die sogar die Sicherheit der Personen im Fahrzeug gefährden. Beispielsweise konnten beim Jeep Cherokee '14 die Bremsen manipuliert werden.

➔ https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Daher ist Security ein zentrales Thema für zukünftige Kommunikationstechnologien im Fahrzeug. Es ist wichtig, dass die Kommunikation zwischen den ECUs geschützt ist und nicht durch Angriffe von außen manipuliert werden kann.

Ziel des POs

Wir werden anhand von Angriffen – Penetration Tests – den Prototyp eines zukünftigen Fahrzeugnetzwerks analysieren und dessen Sicherungsmaßnahmen evaluieren.

Teilprojekte

- Penetration Tests für Ethernet basierte Fahrzeugnetzwerke
- Fahrzeugspezifische Penetration Tests
- Schwachstellenanalyse für zukünftige Fahrzeugkommunikationsarchitekturen

AG INET:
Prof. Thomas C. Schmidt
t.schmidt@haw-hamburg.de
Timo Häckel
timo.haeckel@haw-hamburg.de

AG CoRE:
Prof. Franz Korf
franz.korf@haw-hamburg.de
Philipp Meyer
philipp.meyer@haw-hamburg.de