

Projekt im SoSe 2019 (6 SWS, 9 CPs)

CAZ: Cybersecurity im Auto der Zukunft!

Für TI, AI 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 von 2014 sogar die Bremsen deaktiviert werden.

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

Daher ist Security ein grundlegendes Ziel bei der Entwicklung von zukünftigen 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 Angriffe auf das Kommunikationsnetzwerk von Fahrzeugen erkennen und mit gezielten Gegenmaßnahmen reagieren.

Teilprojekte

- Sicheres Netzwerkarchitekturdesign
- Erprobung von Intrusion Detection Systems (IDS) zum Erkennen von Angriffen im Netzwerk
- Gegenmaßnahmen basierend auf Software Defined Networking (SDN)

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