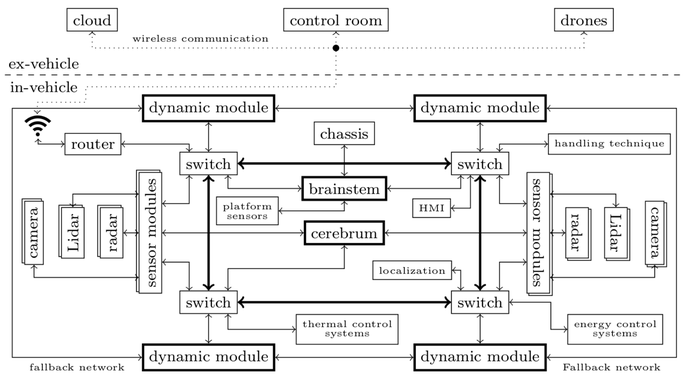
IT-Sicherheit
Schutz vor digitalen Angreifern

Dominik Püllen
Universität Passau
dominik.puellen@uni-passau.de

Prof. Dr. Stefan Katzenbeisser
Universität Passau
stefan.katzenbeisser@uni-passau.de

„No Safety Without Security"

Risikoanalyse nach ISA-62443



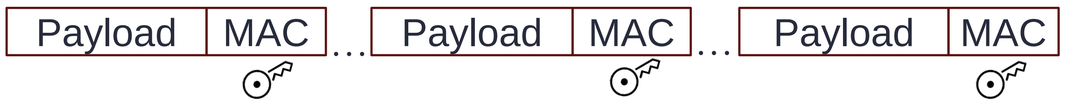
Bedrohungen Schwachstellen Angreifer

Risikoanalyse nach ISA-62443

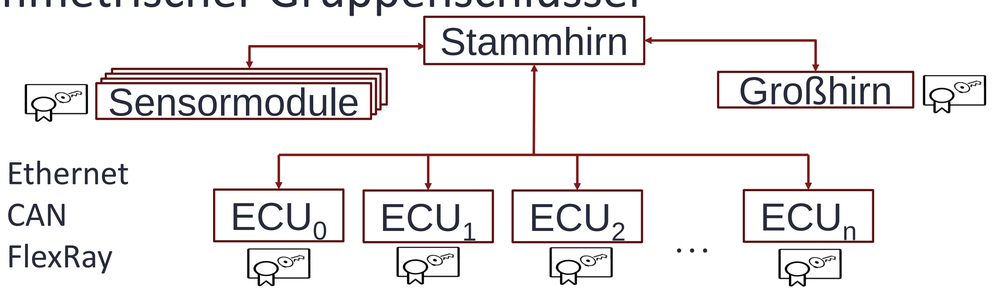
- Authentifizierung der Steuerbefehle
- Integrität der Steuergeräte im Fahrzeug
- Verhaltensbeobachtung
- Trennung safety-kritischer Daten von Nutzerdaten

Authentifizierung von Steuerbefehlen

- Angreifer können durch Manipulation des Netzwerkverkehrs Einfluss auf das Fahrverhalten nehmen.
- Lösungsansatz: Authentifizierung safety-kritischer Datenströme



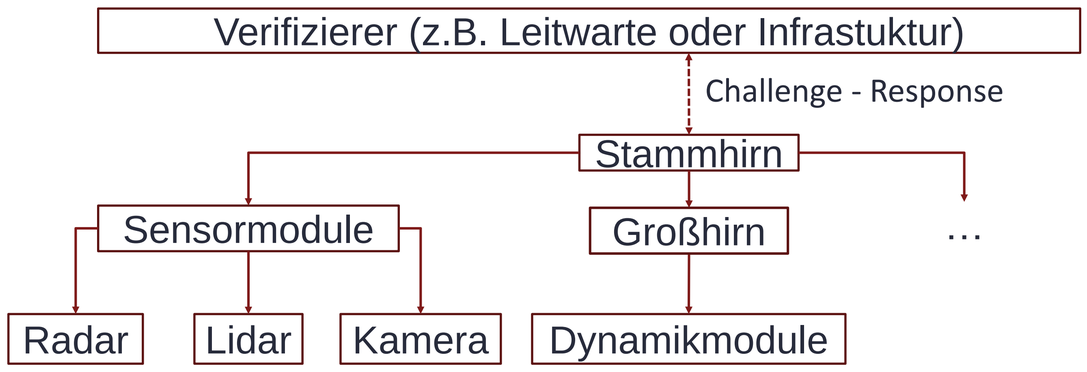
- Protokoll zur effizienten Erstellung und Verteilung symmetrischer Gruppenschlüssel



1. **Authentifizierungsphase:** Identifizierung legitimer Steuergeräte anhand physikalischer Eigenschaften
2. **Zeritifizierungsphase:** Ausstellung impliziter Zertifikate für geprüfte Steuergerät
3. **Schlüsselberechnungsphase:** Berechnung von Gruppenschlüsseln (z.B. pro ASOA-Dienst)

Integrität der Steuergeräte

- Angreifer können durch Manipulation von Steuergeräten Einfluss auf das Fahrverhalten nehmen.
- Lösungsansatz: Hierarchische Attestierung der Steuergeräte vor dem Fahrzeugstart mithilfe eines "Challenge-Response" - Verfahrens



- Remote Attestierung:
  - Geräte haben unterschiedliche Voraussetzungen hinsichtlich Hardware-Unterstützung
  - Unterscheidung zwischen "simple", "medium" und "advanced" Geräten
- Verifizierer veröffentlicht Schlüsseltoken nach erfolgreichem Attestierungsvorgang, das für die fahrzeuginterne Kommunikation notwendig ist.

Weitere Maßnahmen

- Bewertung von Sicherheitsvorfällen nach Safety-Kriterien und Einleitung entsprechender Maßnahmen
  - z.B. reduzierte Geschwindigkeit, sicherer Halt, Meldung an Passagiere
- Regelbasierte Zugangsüberwachung zwischen fahrzeuginterner und -externer Umgebung
- sichere Firmware-Updates der fahrzeuginternen Steuereinheiten

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung