Security in Safety-Critical Environments of Real-Time Automotive Domains

Motivation

Bereits heute haben Fahrerassistenzsysteme in vielen Fahrzeugen Einzug gefunden und MarketResearch.com prognostiziert, bis 2020 werden die meisten neuen Fahrzeuge zumindest mit Advanced Driver Assistance Systems (ADAS) ausgestattet sein. Die intelligente Mobilität wird weiter voranschreiten und bringt durch hochautomatisierte Fahrfunktionen bis zum autonomen Fahren einen regelrechten Paradigmenwechsel mit sich. So nimmt die Anforderung an die im Automobil zur Verfügung stehende Rechenleistung aufgrund der Vielzahl an zu verarbeitenden Sensordaten, rapide zu, was den Einsatz von High Performance Rechner im Fahrzeug zur Folge hat. Zudem erhöht sich die Komplexität eines Fahrzeugnetzes, aufgrund der ausgeweiteten Abhängigkeiten zwischen einzelnen Komponenten (auch zwischen unterschiedlichen Domänen), sowie der ausgedehnten Kommunikationsbeziehungen (zum zentralen Backend, anderen Verkehrsteilnehmern, der Verkehrsinfrastruktur, ...) weiter. Die Anforderungen an eine größere Bandbreite (beispielsweise durch die anfallenden Datenmengen von Kameras, RADAR, etc.) wird den Einsatz von Ethernet-basierten Vernetzungsstrukturen mit sich bringen. Neben den bestehenden Anforderungen an die Betriebssicherheit (Safety), sowie denen an die Echtzeit-fähigkeit zeitsynchronisierter Systeme, rücken zunehmend auch Anforderungen an die Manipulationssicherheit (Security) in den Vordergrund.

Die Vielzahl der verwendeten Daten und die Kritikalität der darauf basierenden Entscheidungen machen es unabdingbar, Vertrauenswürdigkeit der verwendeten Daten einerseits, jedoch auch die Vertrauenswürdigkeit der die Daten verarbeitenden Komponenten zweifelsfrei sicherzustellen. Als umfassendes Ziel setzt sich das Projekt SeSaRe daher, die informationstechnischen Grundlagen für ein vertrauenswürdiges autonomes Fahren zu identifizieren, diese weiterzuentwickeln, zu implementieren und in einem Versuchsträger zu erproben. Dabei sollen die zu entwickelnden Maßnahmen speziell auf die bestehenden Safety-Anforderungen und unter Berücksichtigung von zeitsynchronisierten Netzwerken abgestimmt und mit einer ressourcenschonenden Anomalieerkennungskomponente verknüpft werden. Somit soll eine Basis für eine Überwachung und speziell auch Visualisierung des Security und Safety-Zustandes eines Fahrzeuges geschaffen und erprobt werden.

Vorgehen

Das Vorhaben SeSaRe entwickelt Maßnahmen, die einerseits einen Manipulationsschutz fahrzeuginterner zeitsynchronisierter Kommunikation unter Berücksichtigung von Anforderungen an die Betriebssicherheit ermöglichen, andererseits eine spezielle Art ressourcenschonender Anomalieerkennung domänenübergreifend im Fahrzeug bereitstellen. Zudem wird ein Verfahren entwickelt, mit dem der aktuelle Zustand eines Fahrzeugs, im Sinne von Security und Safety, dem Fahrer in geeigneter komprimierter Form visualisiert, dem OEM als ausführlicher Bericht, zur Verfügung gestellt werden kann. Das Projekt betrachtet somit verstärkt den Aspekt Security.

Um dies zu garantieren werden folgende Teilziele definiert:

Manipulationssichere fahrzeuginterne Kommunikation Wichtige Grundlage für die Betriebssicherheit hochautomatisierter Fahrzeuge ist die Integrität und die Authentizität der fahrzeugintern kommunizierenden Sensordaten. Standardlösungen, beispielsweise für die Sicherheit auf OSI Layer 2 (wie MACsec) finden derzeit, u.a. aus wirtschaftlichen Gründen keinen Einzug in Fahrzeugkomponenten. Ein technisches Hemmnis vor deren Einführung ist die stark eingeschränkte Kompatibilität dieser Lösung mit zeitsynchronisierten (time aware) Systemen, wie Time-Sensitive-Networking (TSN). SeSaRe adressiert dieses Problem, indem eine speziell für Automobile abgestimmte Variante von Sicherheitsmechanismen für zeitsynchronisierte Systeme entwickelt wird.

Ressourcenschonende Anomalieerkennnung und Netzwerk-Überwachung durch selektive Paketanalyse Aufgrund der rapide ansteigenden Netzwerklast und komplexeren Kommunikationsabläufen ist es annähernd unmöglich jegliche Nachricht in ihrem Gesamtkontext hin zu untersuchen. Im Rahmen von SeSaRe sollen leichtgewichtige

Anomalieerkennungs- und Netzwerk-Monitoring-Funktionen entwickelt werden, welche an dezentralen Stellen im Fahrzeug-Netzwerk zur Überwachung eingesetzt werden. Eine selektive Paketauthentifizierung und dynamisch anpassbares Security Logging (Forensik) werden als Incident Reaction Maßnahmen etabliert.

Darstellung des Sicherheitszustands eines Fahrzeugs und anpassbare Incident Reaction Maßnahmen bei kritischen Vorfällen Die in SeSaRe entstehenden Sicherheitsmechanismen werden genutzt, um ein Incident Response Verfahren zu etablieren, welches eine automatisierte Unterstützung zum Aufbereiten und Darstellen des aktuellen Security- und Safety-Zustands des Fahrzeugs bietet. Ein Risk Dashboard übermittelt dabei dem Fahrer eine einfache Visualisierung des Fahrzeugzustands. Zudem kann der Fahrzeughersteller durch einen technisch detaillierten Bericht des Risk Zustands beispielsweise einen flottenübergreifenden Angriff erkennen und entsprechend reagieren.

Eckdaten

Kurztitel

SeSaRe

Forschungsschwerpunkt

Digital Technologies and their Applications

Laufzeit

01.01.2018 - 31.12.2019

Fördergeber

Bayerisches Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst

Projektleitung

Prof. Dr. Martin Schramm

Ziele

- Manipulationssichere fahrzeuginterne Kommunikation
- Netzwerk-Überwachung durch selektive Paketanalyse
- Darstellung des Sicherheitszustands eines Fahrzeugs
- Anpassbare Incident Reaction Maßnahmen bei kritischen Vorfällen