Cybersecurity

Sichere Automotive Cyber Systems mit Distributed-Ledger-Technologie

28.06.19 | Autor / Redakteur: Markus Soppa* / Maximiliane Reichhardt

Digitale Prozesse sind immer stärker in den Alltag des Menschen eingebunden.(Bild: Andrew Ostrovsky/Bosch)

Beim autonomen Fahren kommuniziert das Auto mit anderen Fahrzeugen. Damit wird die Sicherheit innerhalb des Automotive Cyber Systems immer wichtiger. Bei der Authentifizierung stoßen Public-Key-Infrastrukturen an ihre Grenzen. Es gibt jedoch neue Ansätze.

Der Begriff „Autonomes Fahren“ beschreibt die Vision eines intelligenten und vernetzten Fahrzeugs. Das Auto passt sich dabei nicht nur dynamisch an neue Aufgaben an, sondern kommuniziert auch mit anderen Fahrzeugen. Neben der Fähigkeit, Fahroperationen zunehmend selbstständig ausführen zu können, interagieren intelligente Fahrzeuge mit der straßenseitigen Infrastruktur (z. B. mit Lichtsignalanlagen) sowie mit Backends der Automobilhersteller, Straßenbetreiber und anderer Mobilitätsdienste-Anbieter.

Durch diese Vernetzung entsteht ein Automotive Cyber System (ACS), auch „Internet of Things der Car IT“ genannt. In Folge des steigenden Vernetzungsgrades rückt das Thema IT-Sicherheit in ACS jetzt verstärkt in den Fokus. Ähnlich wie bei Industrie-4.0-Systemen prognostiziert, muss auch bei ACS von einer zunehmenden Bedrohung der IT-Infrastruktur ausgegangen werden, da Fahrzeuge verschiedener Hersteller, Infrastruktureinrichtungen und Mobilitätsdienste verschiedener Anbieter zu einem heterogenen System werden.

IT-Sicherheit
Hacker-Angriffe auf Autos: Wie die Branche reagiert
09.01.19 - Neue Fahrzeuge sind praktisch immer und zunehmend vernetzt – und bieten damit potenzielle Möglichkeiten für Hacker. Automobilhersteller und -zulieferer

müssen geeignete Gegenmaßnahmen entwickeln, die auch nach Jahren noch wirken. lesen

Kooperative Sicherheitskonzepte

Für den Schutz der Nutzer und für die gesamte Fahrzeug-Infrastruktur sind sicher vernetzte ACS und der sichere Zugang zu den relevanten Systemkomponenten unerlässlich. Auch, weil davon ausgegangen werden muss, dass Stakeholder oder Fahrzeuge zunehmend selbst auf Komponenten, integrierte Software, Daten und Funktionen im gesamten Life Cycle zugreifen, um Aktionen vornehmen zu können (z. B. für Predictive Maintenance, Software Updates, automatisiertes Platooning, etc.). In der Konsequenz werden immer mehr Akteure Zugriff auf ein Fahrzeug, seine Infrastruktur, seine Funktionen oder seine Daten haben. Künftige Automotive Cyber Systeme brauchen deshalb herstellerspezifische Sicherheitslösungen. Dafür sind kooperative Sicherheitskonzepte ein mögliche Ansatz. Sie bieten Nutzern und Technik gleichermaßen einen umfassenden Schutz innerhalb eines hochgradig vernetzten ACS.

In der aktuellen Entwicklungsphase vermissen viele Experten einen ganzheitlich betrachteten IT-Sicherheitsansatz. Vielmehr werden aktuelle Schutzmaßnahmen oft erst nachträglich oder als partielle Lösung realisiert, was nicht selten durch das immer noch weit verbreitete „Silo-Denken“ vieler Akteure begründet ist. Ein herstellerübergreifender und damit sicherer Ansatz fehlt, was in der Konsequenz das Vertrauen in die Technologie schmälert und zu Unsicherheiten beim Anwender führt.

Keine übergreifende Public-Key-Infrastruktur
Ziel aller technischen Entwicklungen muss es vor diesem Hintergrund sein, die Gefahr für Insassen und die Behinderung von Verkehrsteilnehmern zu minimieren (Safety) und bestenfalls gänzlich zu eliminieren. Fahrfunktionen müssen so abgesichert sein, dass sie nicht durch Cyber-Angriffe beeinträchtigt werden (Security). Aktuell existieren nur anwendungsfallbezogene, herstellerspezifische, automobile Authentifizierungs- und Autorisierungskonzepte, die die Mechanismen einer Public-Key-Infrastruktur (PKI) nutzen. Ein ganzheitlicher, übergreifender Ansatz über die gesamte Wertschöpfungskette und alle Stakeholder existiert nicht.

Bereits in der Entwicklungs- und Produktionsphase sollte aber der Fokus auch auf Sicherheitskonzepten liegen, mit denen sich ausschließen lässt, dass Komponenten bereits während der Wertschöpfung kompromittiert werden. Nur so lassen sich koordinierte Angriffe zu einem späteren Zeitpunkt von vornherein sicher vermeiden. Ist ein Fahrzeug in Betrieb, braucht es Sicherheitskonzepte, die vermeiden helfen, dass unbekannte Akteure, wie etwa nicht lizenzierte Werkstattmitarbeiter, auf kritische Systemkomponenten zugreifen. Nur so lassen sich unberechtigte oder nicht nachvollziehbare Handlungen auf Fahrzeug- bzw. Fahrzeugkomponenten-Ebene vermeiden.

Produktion
Neue Norm: Datenschutz und Security von Beginn an
15.03.19 - Forscher, unter anderem vom Fraunhofer Institut für sichere IT, erarbeiten in Projekten Konzepte für Safety, Security und Datenschutz. Für den Bereich der Security soll bald eine neue Norm die Standards setzen. lesen

Digitale Identität nachweisen
Erreichbar ist das nur durch Systeme, die eine menschliche und maschinenbasierte digitale Identität technisch nachweis- und erfassbar machen und zudem manipulationssicher sind. Auf dieser Basis entfällt der Zwang, unterschiedlichen Stakeholdern eine zentrale, intransparente und aufwendig zu verwaltende Vertrauensinstanz für ein global verteiltes System aufbauen zu müssen. Das Automotive Cyber System von Accessec soll künftig zum Einsatz kommen, wenn klassische Public-Key-Infrastrukturen im Kontext digitaler und zertifikatsbasierter Authentifizierungs- und Autorisierungsanwendungen an ihre Grenzen stoßen.

Das passiert vor allem dann, wenn massenhaft Zertifikatsanfragen an zentralisierte Certificate Authorities als wesentlicher Teil einer Public-Key-Infrastruktur (PKI) gestellt werden, um digitale Identitäten mittels Zertifikaten für Systemkomponenten zu erneuern.

Damit wird verhindert, dass Unternehmen den Blick für ihr Kerngeschäft verlieren und sich kontinuierlich mit Problemen und Gefahren mit PKI und Zertifikaten auseinandersetzen müssen. Das Accessec-Team hat einen Prototyp entwickelt (auch bekannt unter „accessec Carwallet“ und „Point of Sale Lösung“), der auf der Distributed Ledger Technologie basiert und eine Authentifizierung für ACS ermöglicht. Die Idee dahinter: Jedes künftige ACS bekommt einen sicheren digitalen Zwilling, der wiederum als autonom handelnder Akteur in seiner Umgebung agieren kann und Handlungen auf seinem System auf dessen Berechtigung prüft – ganz ohne die sehr teuren und verwaltungsaufwändigen Public-Key-Infrastrukturen.

Automobilzulieferer ZF gründet Technologiezentrum für KI und Cybersecurity
12.03.19 - ZF eröffnet in Saarbrücken ein eigenes Technologiezentrum für künstliche Intelligenz und Cybersecurity. Im Rahmen dessen geht der Automobilzulieferer Partnerschaften mit dem Forschungsinstitut DFKI und dem Helmholtz-Zentrum CISPA ein. lesen

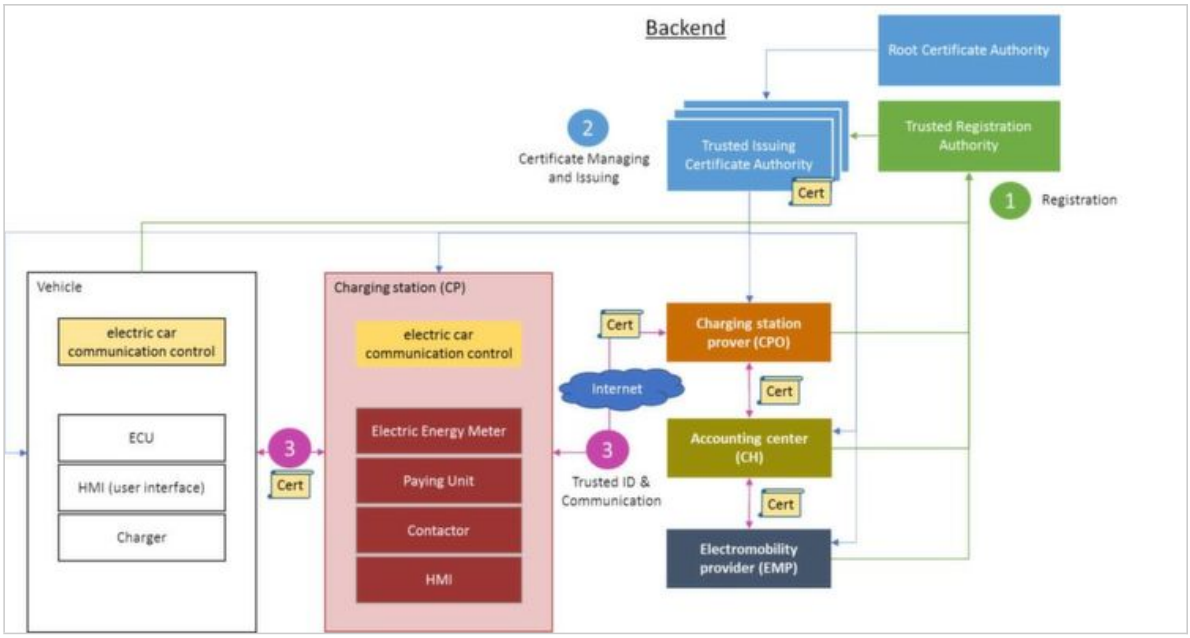
Vorangetrieben wird das Projekt durch die Zusammenarbeit mit Professor Hans-Joachim Hof an der Technischen Hochschule Ingolstadt. Das Ziel: eine föderierte, sichere und skalierbare dezentrale ACS-Anwendung umzusetzen, die erstmalig sämtliche Anforderungen der Stakeholder und die des automobilen Lebenszyklus vollständig abbildet. Gleichzeitig ermöglicht sie die entscheidende Verwaltung des Zugang zum Automotive Cyber System: In jedem Lebenszyklus-Abschnitt liegen die Zugriffsrechte beim „Owner“. Die Forschungsgruppe von Professor Hof ist an der Technischen Hochschule Ingolstadt im Automotive Testcenter „Carissma“ angesiedelt und liefert somit gute Voraussetzungen, eine solche Lösung zu erforschen und diese ausgiebig zu testen.

**Markus Soppa ist Geschäftsführer der Accessec GmbH*

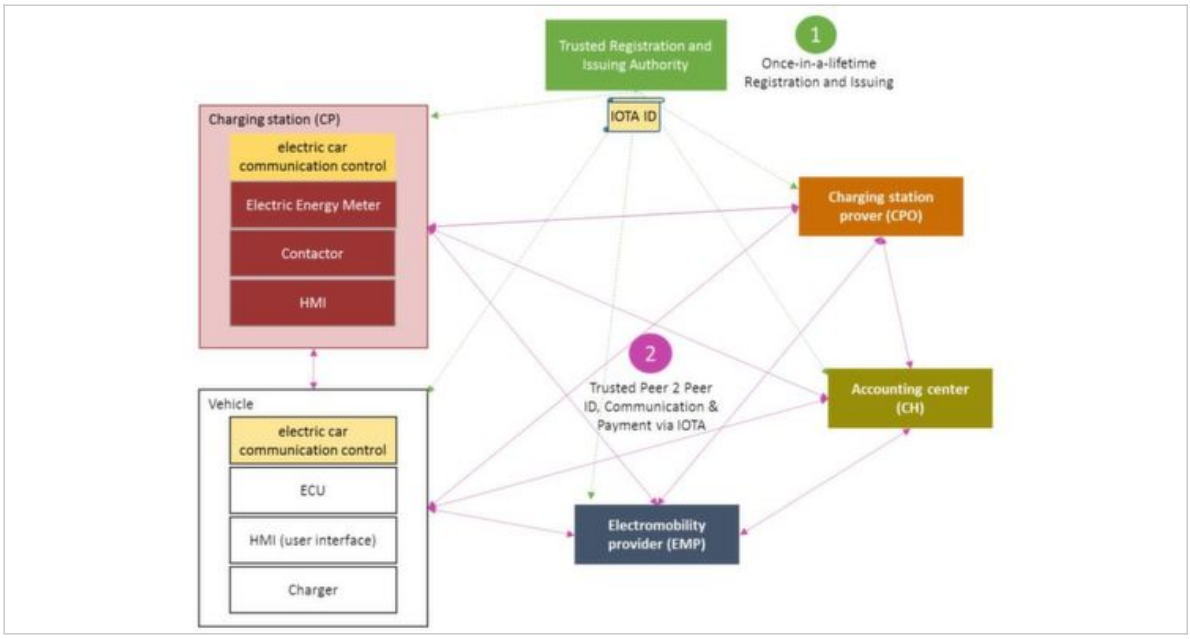
Copyright © 2019 - Vogel Communications Group

Dieser Beitrag ist urheberrechtlich geschützt.
Sie wollen ihn für Ihre Zwecke verwenden?
Infos finden Sie unter www.mycontentfactory.de.

Dieses PDF wurde Ihnen bereitgestellt von http://www.automobil-industrie.vogel.de



(Accessec)



(Accessec)

Digitale Prozesse sind immer stärker in den Alltag des Menschen eingebunden. (Andrew Ostrovsky/Bosch)

Digitale Prozesse sind immer stärker in den Alltag des Menschen eingebunden. (Andrew Ostrovsky/Bosch)