ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 32:

Sichere Fahrzeugkommunikation

Stand: Juli 2016

Herausgeber:
Mike Weber
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut FOKUS
Kaiserin-Augusta-Allee 31, D-10589 Berlin
Telefon: +49 30 3463 - 7173
Telefax: + 49 30 3463 - 99 - 7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

Autorinnen und Autoren der Gesamtausgabe:
Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Nicole Opiela, Florian Friederici, Jan Gottschick, Jens Fromm

Autorinnen und Autoren einzelner Trendthemen:
Michael Rothe, Oliver Schmidt

ISBN: 978-3-9816025-2-4

Juli 2016

Autorinnen/Autoren:
Florian Friederici et al.

Bibliographische Angabe:
Florian Friederici et al. 2019, Sichere Fahrzeugkommunikation, In: Jens Fromm und Mike Weber, Hg., 2016: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT, http://www.oeffentliche-it.de/-/sichere-fahrzeugkommunikation

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 3.0 Deutschland Lizenz (CC BY 3.0 DE) http://creativecommons.org/licenses/by/3.0 de/legalcode. Bedingung für die Nutzung des Werkes ist die Angabe der Namen der Autoren und Herausgeber.

Sichere Fahrzeugkommunikation

Allgegenwärtige Vernetzung und Kommunikation unterwegs ist für viele Menschen zur Normalität geworden. Doch nicht nur Menschen kommunizieren fortwährend, ihre Autos tun es auch. Eine immer umfassendere Sensorik dient zur Sammlung von immer mehr Daten, die andere Verkehrsteilnehmer nutzen können. Dies schafft neue Möglichkeiten – und wirft eine Reihe von alten und neuen Sicherheitsfragen auf: werden unsere Autos zu rollenden Botnetzen?

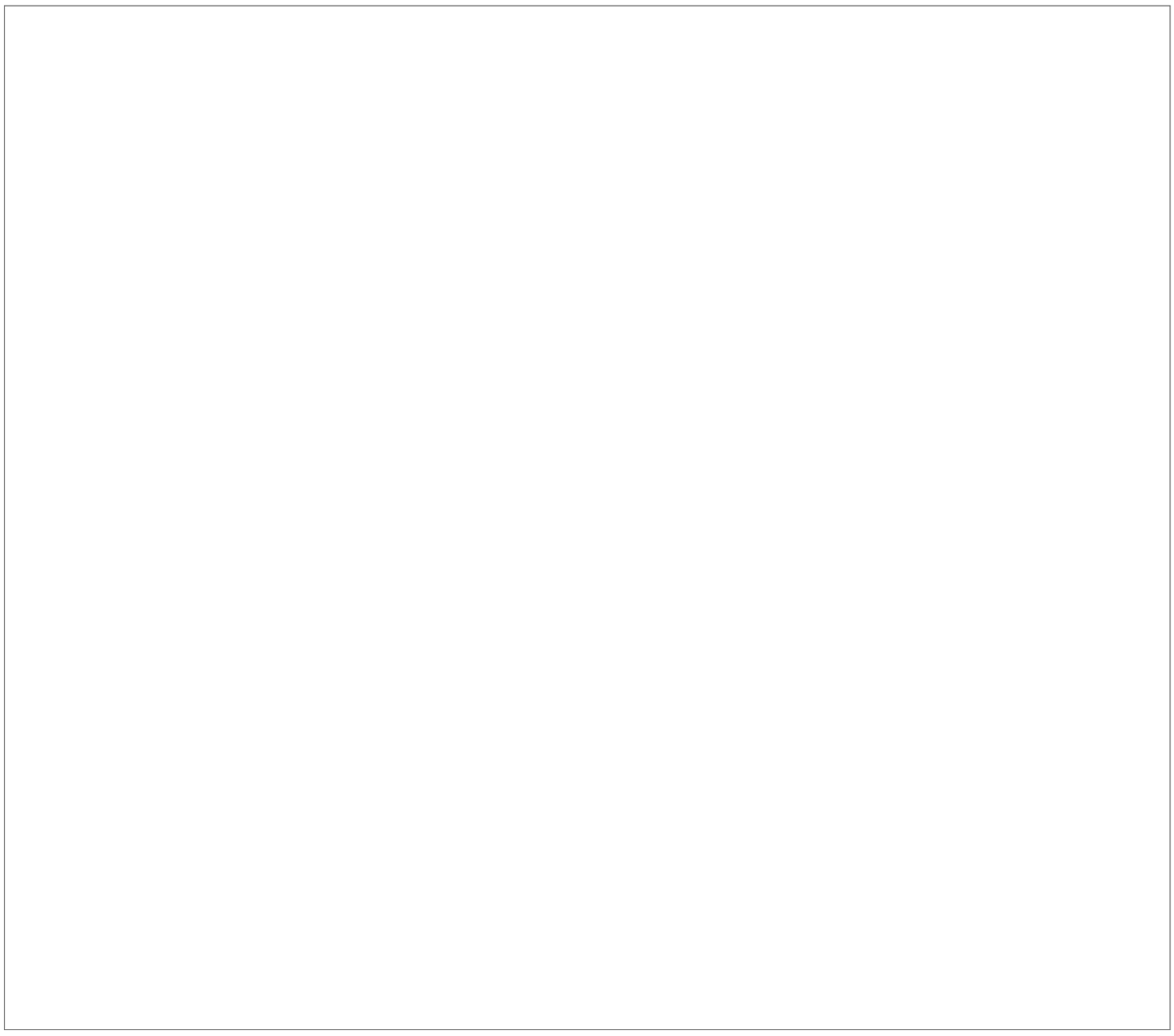
Fahrzeugkommunikation für Fahrsicherheit und effiziente Infrastrukturnutzung

In naher Zukunft werden zwischen Fahrzeugen sowohl regelmäßige als auch ereignisbezogene Nachrichten ausgetauscht. Regelmäßig wird die aktuelle Position, Richtung und Geschwindigkeit je nach Situation etwa ein- bis zehnmal pro Sekunde ausgesandt. Die Empfänger können damit eine Nachbarschaftstabelle aufbauen und so ein aktuelles Bild der Umgebung erhalten. Ereignisbezogene Nachrichten dienen beispielsweise der Warnung vor Gefahrensituationen wie Glätte, Stauende, Falschfahrern oder plötzlichem Bremsen.
Für die Kommunikation zwischen Fahrzeugen und der Verkehrsinfrastruktur kommen weitere Nachrichten hinzu, welche zum Beispiel Ampelphasen oder eine Kreuzungsgeometrie übermitteln. Dies erlaubt die Anpassung von Route und Fahrweise. Beispiele dafür sind individualisierte Routenführung oder Geschwindigkeitsempfehlungen, um eine grüne Welle zu nutzen. Zugleich können sogenannte Floating-Car-Data (FCD) von der Verkehrsinfrastruktur genutzt werden, um die Verkehrslage hochaktuell und präzise zu erfassen. Die Fahrzeugkommunikation kann somit sowohl zur Fahrsicherheit als auch zur effizienten Infrastrukturnutzung beitragen.

Vertrauen durch digitale Signaturen

Die entscheidende Frage wird dabei sein, wie Vertrauen zwischen den diversen digitalen Teilnehmern der kritischen Infrastruktur Verkehr hergestellt werden kann. Denn die umfassende Vernetzung von Fahrzeugen mit der Verkehrsinfrastruktur, den Fahrzeugherstellern, Anwendungen von Drittanbietern, dem Internet und Notfallsystemen eröffnet auch ein großes Angriffspotenzial. Sicherheitslücken können ohne Kenntnis der Fahrer entdeckt und ausgenutzt werden. Angriffe richten sich dabei gegen die Anwendungen der Fahrzeugkommunikation oder gegen ihre Nutzer und deren Privatsphäre. Ein typischer Angriff besteht darin, durch Aussenden inhaltlich falscher Nachrichten die benachbarten Fahrzeuge zu falschen Warnungen an ihre Fahrer zu provozieren. Ein Angreifer könnte zum Beispiel versuchen, eine Fahrspur für sich allein zu beanspruchen. Dazu sendet er gefälschte Nachrichten aus, die sein Auto als Einsatzfahrzeug mit eingeschaltetem Blaulicht deklarieren.
Fahrzeuge im Umkreis werten diese Nachrichten aus und die sogenannte Einsatzfahrzeugwarnung informiert den Fahrer, die Spur zu räumen, um das Einsatzfahrzeug passieren zu lassen. Ein Ansatz in der digitalen Welt Vertrauen herzustellen ist der Einsatz sogenannter Signaturen, das heißt das digitale Unterschreiben einer Nachricht. Empfangende Fahrzeuge können durch Verifikation der Signatur die Vertrauenswürdigkeit des Absenders überprüfen. Auf diese Weise können falsche Warnungen an den Fahrer vermieden werden. Dies erfordert jedoch den Aufbau einer komplexen Vertrauensinfrastruktur (PKI = Public Key Infrastructure), die es überhaupt erst ermöglicht, solche digitalen Signaturen auf Echtheit zu prüfen. Wer eine solche PKI aufbauen und betreiben kann und soll, muss sich angesichts der Vielzahl privatwirtschaftlicher und behördlicher Akteure im öffentlichen Raum des Straßenverkehrs erst noch herausbilden.

Begriffliche Verortung

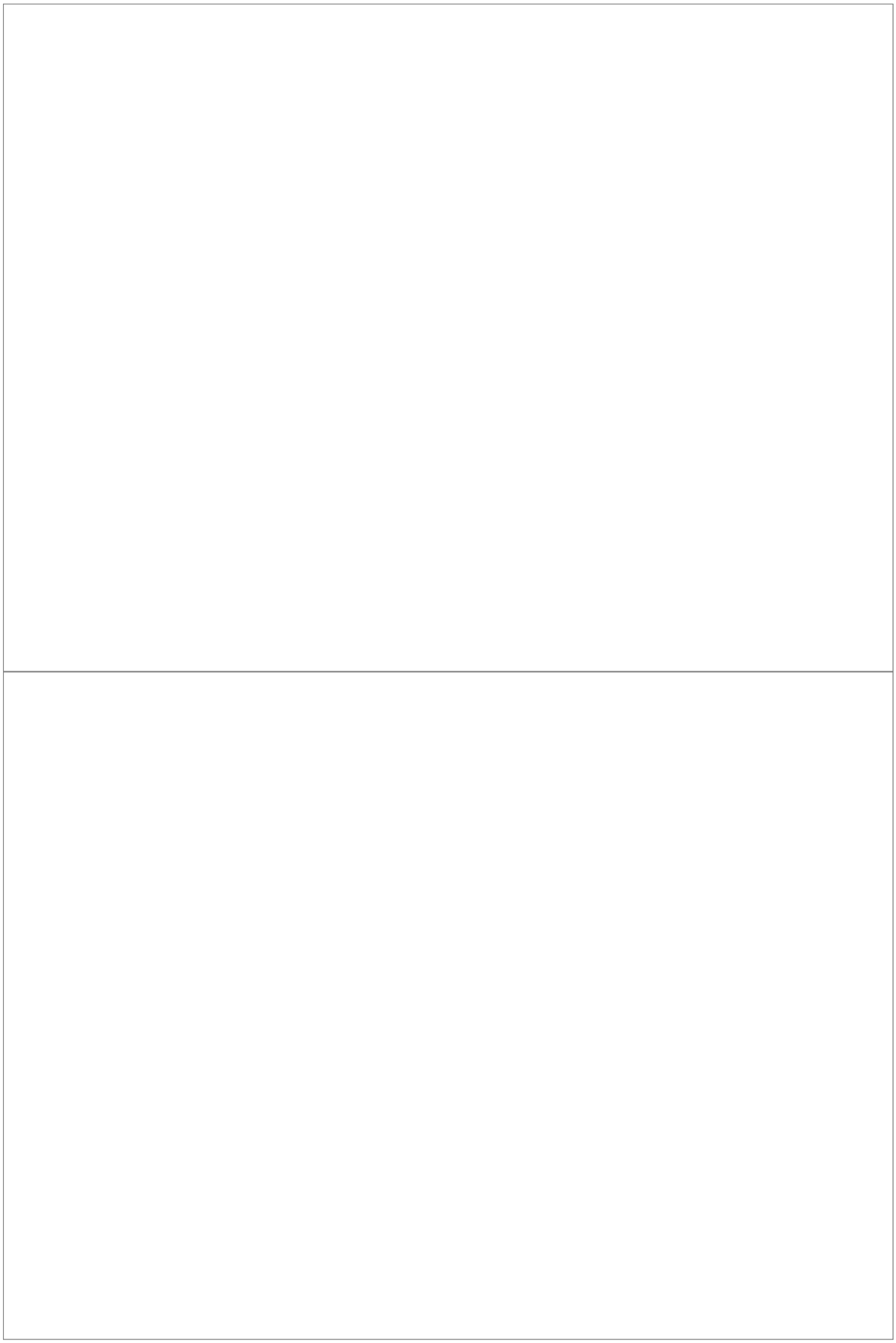


Vertrauenswürdigkeit der Empfänger

Angriffe gegen die Privatsphäre der Nutzer zielen darauf ab, Kenntnis über persönliche Daten wie Fahrtrouten oder Fahrprofile zu erhalten. Viele neue Anwendungen der Fahrzeugkommunikation werden erst dadurch möglich, dass Positionsdaten mitgeteilt werden. Diese Nachrichten werden derzeit unverschlüsselt auf dem dedizierten Funkkanal übertragen, damit benachbarte Fahrzeuge und die Verkehrsinfrastruktur diese Nachrichten empfangen und verwerten können. Dies ermöglicht allerdings auch den Missbrauch dieser Daten. Hier stellt sich also auch die Frage nach der Vertrauenswürdigkeit von Informationen und dem designierten Empfängerkreis. Die hier beschriebene Fahrzeugkommunikation steht kurz vor der Einführung in die Serienproduktion von Fahrzeugen. Systeme, die ausschließlich Mobilfunkkommunikation nutzen, sind bereits heute in Neufahrzeugen verfügbar. Es ist zu erwarten, dass die verschiedenen Teilbereiche der Fahrzeugkommunikation in Zukunft zusammenwachsen, wobei die Nutzung unterschiedlicher Kommunikationsnetze für die Fahrer verborgen bleibt.
Die Vielfalt der Hersteller setzt voraus, dass Standards festgelegt werden, damit die Fahrzeuge und Infrastrukturkomponenten korrekt miteinander kommunizieren können und nach gleichen Maßstäben funktionieren. Existierende Standards definieren ausschließlich das Senderverhalten, nicht jedoch das Empfängerverhalten. Eine Standardisierung in diesem Bereich ist jedoch sowohl für die wirtschaftliche Verwertbarkeit, als auch die Erhöhung der Verkehrssicherheit notwendig. Aber was passiert, wenn sich doch ein Fehler oder eine Schadsoftware in das komplexe Netz immer autonomer agierender Fahrzeugassistenz- und Verkehrssicherheitssysteme einschleicht, auf die sich die Fahrer mehr und mehr

verlassen? IT-Sicherheit (Safety und Security) hängt hier unmittelbar mit rechtlichen Haftungs- und gemeinwohlrelevanten Infrastrukturfragen zusammen.

Themenkonjunkturen



Folgenabschätzung

Möglichkeiten

- Verbesserte Verkehrssicherheit
- Geringerer Flottenverbrauch
- Optimierte Routenführung
- Erschließung neuer Anwendungsgebiete (etwa Autonomes Fahren)
- Genauere und schnellere Verkehrserfassung und –steuerung für Dienste mit Livedaten sowie langfristig zur politischen Planung (siehe Verwaltung x.0)

Wagnisse

- Wahrung der Privatsphäre der Nutzer (siehe Digitale Unversehrtheit)
- Nutzungsrechte der erhobenen Daten
- Offenheit des Kommunikationssystems und seine Absicherung
- Unterschiedliche Innovationsgeschwindigkeit zwischen Automobil- und Kommunikationsindustrie
- Gestaltung der Anwendungen im Fahrzeug (Ablenkung statt Unterstützung)
- Sach- und Personenschäden durch erfolgreiche Angriffe (siehe Security by Design)
- Sicherheitsparadoxie: Nachlässigkeiten durch falsches Sicherheitsgefühl
- Weitere Verkehrsteilnehmer (Fußgänger, Radfahrer) sind nicht Teil des vernetzten Verkehrssystems

Handlungsräume

Standardisierung begleiten

In der Standardisierung durch ETSI und CEN wurde das Profil für den Start intelligenter Transportsysteme festgelegt (sogenannt Day 1). Darauf aufbauend werden weitere Ausbaustufen mit neuen Anwendungsfällen in weiteren Profilen standardisiert.

Rechtsrahmen

Die Abbildung der technischen Möglichkeiten wirft Rechtsfragen jenseits der Straßenverkehrsordnung auf: Sind etwa in den Bereichen der Produkthaftung und des Datenschutzes weitergehende Regelungen erforderlich?

Aufbau einer Vertrauensinfrastruktur

Für den Aufbau einer vertrauenswürdigen Verkehrsinfrastruktur ist eine hierarchische Public-Key-Infrastruktur notwendig. Organisation und Betrieb der dafür notwendigen Zertifizierungsstellen gilt es zu regeln – europaweit und international.