Sicherheit der Verbraucher in vernetzten Fahrzeugen

Kerstin Lemke-Rust

DOI 10.15501/978-3-86336-912-5_4

Abstract

Dieser Beitrag betrachtet den Stand der Entwicklung bei der Vernetzung von Fahrzeugen aus Sicht der IT-Sicherheit. Etablierte Kommunikationssysteme und Verkehrstelematikanwendungen im Automobil werden ebenso vorgestellt und diskutiert wie auch zukünftige Kommunikationstechnologien Car-2-Car und Car-2-X. IT-Sicherheit im Automobil ist ein schwieriges Feld, da es hier um eine Integration von neuen innovativen Anwendungen in eine hochkomplexe bestehende Fahrzeugarchitektur geht, die zu keinen neuen Gefährdungen für die Fahrzeuginsassen führen darf. Zudem bleibt die Funktionsweise dieser Anwendungen mit ihren Auswirkungen auf das informationelle Selbstbestimmungsrecht oft intransparent. Die abschließende Diskussion gibt Handlungsempfehlungen aus Sicht der Verbraucher.

1 Einleitung

Das moderne Automobil ist bereits heutzutage ein hoch komplexes IT-System, das mit vielfältigen externen Kommunikationsschnittstellen für Verkehrstelematikanwendungen ausgestattet ist (vgl. Abbildung 1). Diese Kommunikationsschnittstellen dienen dazu, extern verfügbare Informationen in dem Fahrzeug zu erhalten oder Informationen, die im Fahrzeug generiert werden, über eine vorhandene Funktechnologie mit einer festen Infrastruktur auszutauschen.

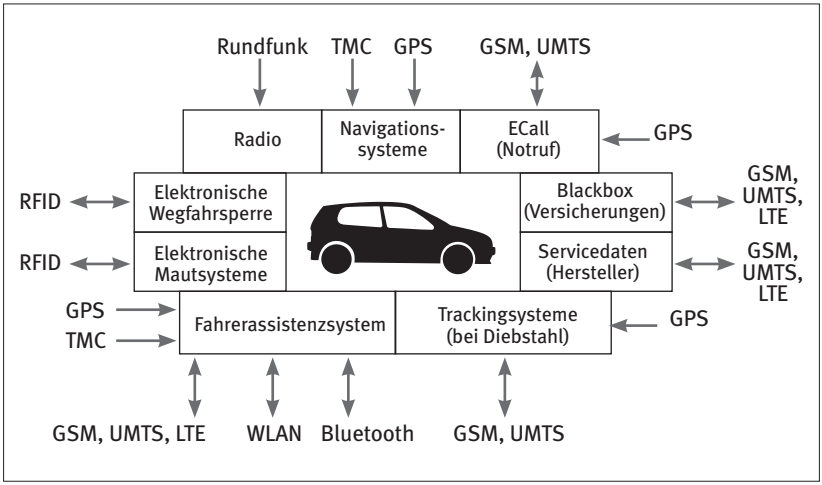

Abbildung 1: Funk basierte Kommunikationsschnittstellen eines modernen Automobils. Eigene Darstellung.

Altbewährt ist der Rundfunkempfang im Auto. Radios ermöglichen den Fahrzeuginsassen so den Empfang von Verkehrsnachrichten und Unterhaltungsprogrammen.

Seit Mitte der 1990er-Jahre sind elektronische Wegfahrsperren eingeführt worden, um die Fahrzeuge stärker gegen Diebstahl zu schützen. Bei der Wegfahrsperre startet der Motor erst, wenn das Motorsteuerungsgerät die Echtheit des Zündschlüssels im Zündschloss durch ein kryptografisches Protokoll ve-

rifiziert hat. Die verwendete Funktechnologie ist eine RFID (Radio Frequency Identification) Technik, die auf induktiver Kopplung im Abstand von einigen Zentimetern zwischen Zündschloss und Zündschlüssel basiert.

Mit RFID-Technik basierend auf elektromagnetischer Rückstrahlkopplung können Kommunikationsreichweiten bis zu 100 Metern erzielt werden. Hiermit funktionieren elektronische Mautsysteme, die zwischen einer Bordeinheit im Automobil und fest installierten Barken an Straßen oder mobilen Kontrollfahrzeugen Nachrichten zur Bezahlung der Maut austauschen.

Für den Fahrzeugführer brachten die Navigationssysteme einen Durchbruch bei der individuellen Routenführung mit sich. Die Navigationssysteme empfangen Nachrichten des globalen satellitengestützten Positionsbestimmungsdiensts GPS (Global Positioning System) und des Funknachrichtendiensts TMC (Traffic Message Channel). Während der Fahrt ist kein Informationsfluss aus dem Auto an Hintergrundsysteme möglich. Es gibt jedoch einen Rückkanal zum Hersteller des Navigationsgeräts, sobald das Navigationsgerät an das Internet angeschlossen ist, beispielsweise wegen einer Aktualisierung der Software oder des Kartenmaterials. Hierbei können im Navigationsgerät gespeicherte Fahrtrouten und auch gefahrene Geschwindigkeiten an den Hersteller übertragen werden (Fahn 2013). Navigationssoftware auf einem Smartphone ist aus Datenschutzsicht wesentlich kritischer, da hierdurch direkt eine Verknüpfung mit persönlichen Daten möglich ist und eine Kommunikationsverbindung zum Anbieter der Navigationssoftware bei Verfügbarkeit einer Internetanbindung geöffnet werden kann (Fahn 2013).

Fahrerassistenzsysteme verfügen neben GPS und TMC über Mobilfunkschnittstellen GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System) oder LTE (Long Term Evolution). Ferner nutzen Fahrerassistenzsysteme die Funktechnologien Wireless LAN (WLAN) und Bluetooth mit einer Kommunikationsreichweite von zehn bis 100 Metern. Teilweise sind auch weitere Technologien verbaut wie Ultraschall und Kameras, die dem Fahrer beispielsweise als Einparkhilfe dienen können. Diese Fahrerassistenzsysteme unterstützen den Fahrer bei der Fahrzeugführung, beispielsweise durch eine Warnung vor kritischen Situationen. Ferner bieten sie Komfortfunktionen wie eine Freisprecheinrichtung und die Einbindung von persönlicher Informationstechnik (Smartphones etc.) in das Automobil an.

Weitere Anwendungen benötigen einen Kommunikationskanal, auf dem Fahrzeugdaten direkt an Hintergrundsysteme verschickt werden können und das Fahrzeug auch von Hintergrundsystemen kontaktiert werden kann. Hierfür wird typischerweise Mobilfunk genutzt. Trackingsysteme dienen dazu, ein gestohlenes Fahrzeug mittels GPS auf Anfrage zu lokalisieren. Servicedatensysteme dienen zum bi-direktionalen Austausch von Kommunikationsdaten mit dem Fahrzeughersteller. Über diese Schnittstelle kann der Hersteller auch neue Software oder neue Konfigurationsdaten beispielsweise für personalisierte Fahrwerkseinstellungen in das Fahrzeug einspielen. Sogenannte Blackboxes werden von der Versicherungswirtschaft zunehmend in Fahrzeuge eingebaut, um das Fahrerverhalten analysieren zu können, sofern ein Versicherungsnehmer hierzu seine Einwilligung gegeben hat. Am 28. April 2015 hat das EU-Parlament beschlossen, dass das vom Nutzer nicht deaktivierbare eCall Notrufsystem ab April 2018 werksseitig in alle neuen Fahrzeuge eingebaut werden muss, um bei einem Unfall automatisiert einen Notruf über den Mobilfunk durch das Fahrzeug auszulösen (European Commission 2015). Zusätzliche Dienste, die das fahrzeugseitig eingebaute System von eCall nutzen, sind optional vorgesehen (Das Europäische Parlament und der Rat der Europäischen Union 2015).

Daneben gibt es weitere Anwendungen, zum Beispiel in der Verkehrsflussanalyse, die sich die Verfügbarkeit von Bluetooth und vermutlich zukünftig auch von WLAN in den Fahrzeugen zunutze machen. Durch an den Straßen positionierte Bluetooth Scanner werden ausgesendete individuelle MAC (Media Access Control) Adressen der in den Fahrzeugen vorhandenen Bluetooth-Geräte empfangen. Durch die Zeitdifferenz des Empfangs von derselben MAC Adresse an zwei räumlich entfernten Scannern kann die Durchschnittsgeschwindigkeit berechnet werden.

1.1 Autohersteller vs. Internetfirmen

Anwendungen der Fahrerassistenz und Mehrwertdienste im Automobil wecken auch die Begehrlichkeiten von großen Internetfirmen wie Google und Apple nach Integration ihrer Smartphone-Technologie in das Automobil. Die Automobilhersteller streben dagegen an, ihre Kunden durch neue digitale Angebote an sich zu binden (Schwan 2015). Aufmerksamkeit erregte kürzlich die Mel-

dung, dass Porsche nur die iPhone-Integration mit Apples CarPlay unterstützt, nicht aber Android Auto (Becker 2015). Grund hierfür sei Googles Forderung nach umfangreichen Fahrzeugdaten. Die Automobilhersteller Audi, BMW und Porsche erwägen aktuell, Sensordaten aus ihren Fahrzeugen für den dazugekauften Kartendienst „Here“ von Nokia zu öffnen (siehe dpa und axk, 2015), Kartendaten werden als eine Schlüsseltechnologie bei der zukünftigen Entwicklung von vernetzten und selbstfahrenden Autos eingeschätzt.

2 IT-Sicherheit im Automobil

2.1 Safety vs. Security

Sicherheit hat in der deutschen Sprache zwei Bedeutungen: funktionale Sicherheit (Safety) und Angriffssicherheit (Security). Funktionale Sicherheit gewährleistet, dass ein System unter allen normalen Betriebsbedingungen funktioniert und keine unzulässigen Zustände annimmt (Eckert 2014). Funktionale Sicherheit schützt damit vor zufälligen Fehlerzuständen, die in dem normalen Betrieb auftreten können. Angriffssicherheit schützt Systeme vor intelligenten Angreifern, die Sicherheitsfunktionen überwinden oder umgehen können, und damit das System und die zu schützenden Ressourcen angreifbar machen. Der Grad der Angriffssicherheit ist proportional zu den Aufwänden, die ein Angreifer investieren muss, um Sicherheitsmaßnahmen außer Kraft zu setzen.

Beide Bedeutungen der Sicherheit sind fundamental bei der Entwicklung von Automobilen. Primäres Ziel ist der Schutz der Unversehrtheit von Fahrzeuginsassen im Falle von Unfällen oder zufälligen Störungen der IT-Systeme im Automobil. Als Beispiel für ein funktionales Sicherheitssystem sei der Airbag genannt, der im Falle eines Zusammenstoßes automatisch auslöst, um den Aufprall der Fahrzeuginsassen abzubremsen. Die elektronische Wegfahrsperre als Beispiel für ein IT-Sicherheitssystem verhindert ein einfaches Kurzschließen am Zündschloss durch eine kryptografische Authentifikation zwischen Zündschlüssel und Motorsteuerung.

Funktionale Sicherheitsfunktionen können durch funktionale Tests unter realistischen Einsatzbedingungen geprüft werden. Schwieriger ist die Prüfung des Grads der Angriffssicherheit, hierzu bedarf es einer Schwachstellenanalyse.

2.2 Kommunikationssicherheit im Automobil

In vernetzten Automobilen findet Kommunikation statt –

- zwischen einem Fahrzeug und einem Hintergrundsystem (1:1),
- zwischen einer stationären straßenseitigen Systemeinheit (ggf. verbunden mit einem Hintergrundsystem) und mehreren Fahrzeugen (1:n) sowie
- zukünftig auch untereinander zwischen mehreren Fahrzeugen (m:n), die sich zufällig innerhalb der Kommunikationsreichweite befinden und sogenannte Ad-Hoc Netze bilden. (Siehe Abschnitt 3.)

Informationen, die über Netzwerke gesendet werden, sind diversen Bedrohungen ausgesetzt. Dies ist in Abbildung 2 illustriert.

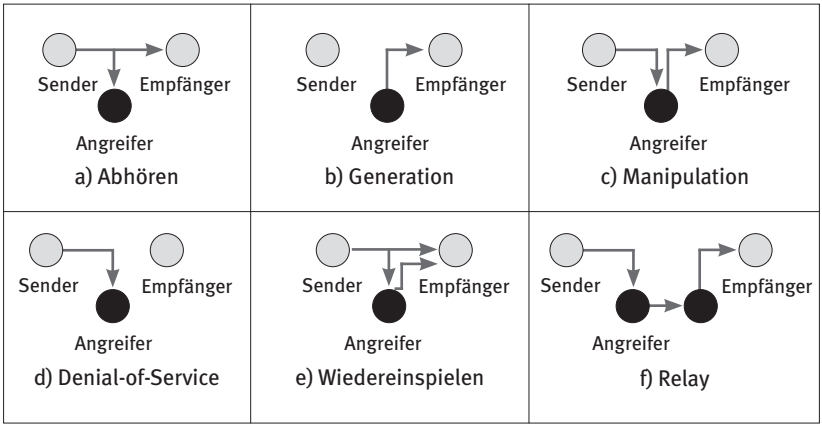

Abbildung 2: Angriffe auf Kommunikationssysteme. Eigene Darstellung.

Es handelt sich hierbei um
a) das Abhören von Informationen,
b) die Generierung neuer Informationen durch den Angreifer,
c) die Manipulation der Informationen auf der Kommunikationsstrecke,
d) das Unterdrücken der Weiterleitung von Informationen (Denial-of-Service),
e) das Wiedereinspielen aufgezeichneter Informationen durch den Angreifer zu einer späteren Zeit (Replay) und
f) das Weiterleiten der Informationen an einen entfernten Ort (Relay). Diese Bedrohung ist spezifisch für Funknetze mit begrenzter Reichweite, bei denen implizit angenommen wird, dass die Kommunikationspartner sich innerhalb der Kommunikationsreichweite eines Funknetzes befinden.

In der Netzwerksicherheit existieren kryptografische Sicherungsmaßnahmen zu den oben genannten Angriffen a) auf die Vertraulichkeit, b) auf die Authentizität und c) auf die Integrität.

Durch Verschlüsselung kann das Abhören der Informationen auf der Netzwerkschnittstelle unterbunden werden und Vertraulichkeit von Informationen erreicht werden. Zur Verschlüsselung können symmetrische oder asymmetrische Verfahren eingesetzt werden. Bei symmetrischen Verfahren müssen die Kommunikationspartner über einen gemeinsamen geheim zuhaltenden Schlüssel verfügen. Bei asymmetrischen Verfahren besteht jeder Schlüssel aus einem öffentlichen und privaten Teil, wovon nur der öffentliche an die Kommunikationspartner herausgegeben wird. Symmetrische Verfahren sind wesentlich performanter als asymmetrische Verfahren, diese Tatsache muss bei dem Design von zeitkritischen Anwendungen berücksichtigt werden.

Das Generieren von Informationen durch unautorisierte Angreifer sowie die Manipulation von gesendeten Informationen kann durch kryptografische Authentifikationsverfahren wie den Message Authentication Code (MAC) oder mittels einer digitalen Signatur detektiert werden. Während der MAC auf der symmetrischen Kryptografie beruht und die Verteilung von geheimen symmetrischen Schlüsseln erfordert, ist die digitale Signatur ein asymmetrisches Verfahren, bei der der Signaturersteller über den privaten Schlüssel verfügt und alle Empfänger den dazugehörigen öffentlichen Schlüssel brauchen.

Diese kryptografischen Verfahren sind sowohl vom Sender als auch vom Empfänger anzuwenden. Insbesondere bedeutet dies, dass die Kommunikationspartner über das erforderliche Schlüsselmaterial verfügen müssen. Der Einsatz von universellen symmetrischen Schlüsseln, die an alle Fahrzeuge ausgegeben werden, ist im automobilen Kontext nicht empfehlenswert, da ein Angreifer diesen Schlüssel nur aus einer Komponente eines Fahrzeugs extrahieren muss, um danach das gesamte System kompromittieren zu können. Bei 1:1 oder 1:n Kommunikationen kann der gemeinsame symmetrische Schlüssel vom Hintergrundsystem aus einem Masterschlüssel unter Verwendung einer Identität des Fahrzeugs abgeleitet werden, die Fahrzeuge erhalten damit einen individuellen Schlüssel. In automobilen Ad-Hoc Netzen ist ein solches Verfahren der Schlüsselableitung nicht möglich, es bleibt damit die asymmetrische Verschlüsselung und die digitale Signatur. Beides erfordert einen Austausch von Zertifikaten einer vertrauenswürdigen Zertifikatsstelle, um Man-in-the-Middle-Angriffe, bei denen sich der Angreifer aktiv in die Kommunikation einbindet, möglichst zu unterbinden. Bei Verwendung der asymmetrischen Verschlüsselung muss der Austausch von Zertifikaten vor der Verschlüsselung von Informationen verfolgen.

Die Angriffe d), e) und f) sind generell schwierig abzuwehren. Denial-of-Service Angriffen, beispielsweise durch Störsender, und damit dem Verlust der Verfügbarkeit kann entgegengewirkt werden, wenn Kommunikationssysteme redundant ausgelegt werden bzw. mehrere Kommunikationswege für eine Nachricht in einem Ad-Hoc Netzwerk vorgesehen sind. Das Wiedereinspielen von Nachrichten kann durch kryptografische Protokolle mit frischen Zufallszahlen, die von beiden Protokollteilnehmern erzeugt werden, erkannt werden. Diese Protokolle sind bei zeitkritischen Rundfunk-Nachrichten an viele Empfänger jedoch nicht geeignet. Alternativ kann angestrebt werden, die Uhrzeit aller Kommunikationsparteien zu synchronisieren und die Uhrzeit des Senders kryptografisch als Teil der Informationen zu sichern. Gegenmaßnahmen gegen Relay-Angriffe bedürfen einer möglichst genauen Ortsbestimmung des Senders und des Empfängers, die als Teil der gesendeten Information kryptografisch zu sichern und vom Empfänger zu prüfen ist.

2.3 Eingebettete Sicherheit im Automobil

2.3.1 Fahrzeug-internes Netzwerk

In einem Automobil der Luxusklasse gibt es heutzutage zwischen 70 und 120 Steuergeräte mit zusammen über 100 Millionen Zeilen Software Code (von Stokar 2015). Diese Steuergeräte sind in dem Fahrzeug über ein Controller Area Network (CAN) Bussystem vernetzt. Die Kommunikation zwischen Steuergeräten auf dem Fahrzeug-internen Bus ist im Regelfall nicht mit kryptografischen Maßnahmen geschützt. Wenn ein Angreifer Zugriff auf diesen Fahrzeug-internen Bus erlangt, so kann er praktisch alle Steuergeräte kontrollieren. In die Fahrzeuge ist werksseitig eine On-Board-Debugschnittstelle OBD2 eingebaut, mit der Hersteller und Werkstätten die Funktionsfähigkeit der einzelnen Steuergeräte prüfen und neue Software aufspielen können. Diese Schnittstelle OBD2 öffnet aber auch für Angreifer mit physischem Zugang zum OBD2 mannigfaltige Wege, sich in das Fahrzeug-interne Netzwerk einzuklinken und Steuergeräte neu zu konfigurieren oder zu programmieren.

Eine noch größere Bedrohung ergibt sich, wenn Angreifer ohne direkten Zugang auf das Fahrzeug in der Lage sind, sich Zugriff auf den Fahrzeug-internen Bus zu verschaffen und Nachrichten in das Fahrzeug schicken zu können. Die Machbarkeit solcher externen Angriffe ist bereits in Checkoway et al. (2011) demonstriert worden: Die Autoren entdeckten Schwachstellen in der Implementierung von Kommunikationssystemen, die durch Nutzung von CD-Spieler, Bluetooth-Schnittstellen und Mobilfunkschnittstellen ausgenutzt werden konnten. Die Autoren stellen fest, dass jede dieser entdeckten Schwachstelle es Ihnen erlaubte, volle Kontrolle über den Fahrzeug-internen Bus zu erlangen. Hohe Aufmerksamkeit in der Öffentlichkeit erregte die Meldung vom Sommer 2015, dass es Hackern in den USA gelungen ist, einen Jeep Cherokee über das Internet fernzusteuern (Eikenberg 2015; Miller und Valesek 2015). Hierfür verwendeten sie das Uconnect System, über das Fahrzeuge per Mobilfunk aus dem Internet erreichbar sind. Die Hacker konnten demonstrieren, dass eine Fernsteuerung von sicherheitsrelevanten Fahrzeugteilen wie Bremsen, Beschleunigung und teilweise auch von der Lenkung möglich ist.

2.3.2 Sicherheitsrelevante Komponenten

Durch den zunehmenden Einbau von Sicherheitsmechanismen in Hardware- und Softwarekomponenten in das Automobil wird die Resistenz dieser Steuergeräte gegen Implementierungsangriffe durch Angreifer mit physischem Zugriff wichtig. Hier lässt sich sagen, dass im Automobil überwiegend Standard-Mikrocontroller verbaut werden, die keine speziellen intrinsichen Hardware-Sicherheitsfunktionen mitbringen. Ein solcher spezieller Schutz wird wichtig, sobald kryptografische Schlüssel oder andere sensitive Konfigurationsdaten gespeichert werden. Implementierungsangriffe und Sicherheitsmaßnahmen zur Härtung von Komponenten und zum Schutz der kryptografischen Schlüssel und sensitiven Daten werden in Lemke et al. (2006) vorgestellt.

3 Zukünftige Technologien der Car-2-Car Kommunikation

Die nächste Generation von Kommunikationssystemen im Fahrzeug hat das Ziel, Nachrichten zwischen Fahrzeugen auszutauschen. Dies ist ein Teilbereich der intelligenten Transportsysteme (ITS). Bei den Kommunikationsnetzen handelt es sich um Ad-Hoc-Netze, die durch Fahrzeuge, die sich zufällig innerhalb der Kommunikationsreichweite des Senders befinden, gebildet werden. Die beteiligten Kommunikationspartner wechseln. Man unterscheidet

- Car-to-Infrastructure bzw. Infrastructure-to-Car (C2X) und
- Car-to-Car (C2C) Kommunikation

Bei der C2X Kommunikation kommuniziert das vorbeifahrende Fahrzeug mit einer festen Infrastruktur, deren Funkstationen stationär an einer Straße installiert sind. Bei C2C kommunizieren zwei oder mehrere Fahrzeuge während der Fahrt.

Beteiligte Entitäten an der C2C/C2X Kommunikation sind die entsprechend mit ITS-Systemen ausgerüsteten Fahrzeuge, stationäre ITS-Funkstationen an

der Straße und ITS-Hintergrundsysteme, die Nachrichten mit den stationären ITS-Funkstationen typischerweise über eine Mobilfunkverbindung austauschen (vgl. Abbildung 2). Die ITS-Funkstationen kommunizieren über eine WLAN-Funkverbindung mit den Fahrzeugen. Jedes Fahrzeug agiert auch als ein Router und kann Nachrichten so zu weiter entfernten Fahrzeugen übertragen, (vgl. CAR 2 CAR o. D.).

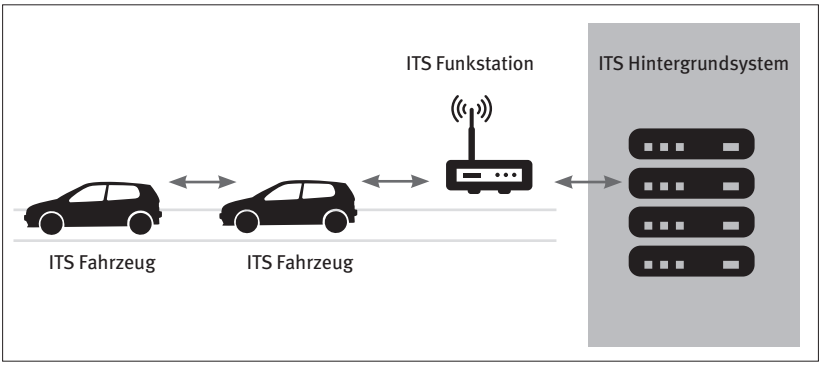

Abbildung 3: C2C/C2X System. Eigene Darstellung.

Die Ziele bei der Einführung von C2C/C2X sind die Erhöhung der Verkehrssicherheit, die Verbesserung des Verkehrsflusses und die Bereitstellung weiterer Mehrwertdienste. In den letzten Jahren gab es zu intelligenten Transportsystemen bereits Standardisierungsarbeiten durch ETSI und große Forschungsprojekte, die an der Realisierung gearbeitet haben. Dieser Artikel stützt sich überwiegend auf die öffentlich verfügbaren Informationen aus den kürzlich beendeten Projekten PRESERVE (www.preserve-project.eu) und simTD (www.simtd.de) ab.

Das Projekt PRESERVE benennt sicherheitssensitive Anwendungsfälle von hoher Relevanz: die Einsatzfahrzeugwarnung, das elektronische Bremslicht, Warnungen bei einem liegen gebliebenen Fahrzeug, Stauwarnungen, Gefahrenwarnungen, Kreuzungswarnungen, Verkehrsinformationen und Routenempfehlung, lokale Verkehrsflussdaten, Baustellenwarnungen, Ampelphasenassistenz, Verkehrszeichenwarnungen und Kollisionswarnungen (PRESERVE Konsortium 2014, 19 f.).

3.1 Sicherheits- und Datenschutzanforderungen

Aufgrund der Diversität von Anwendungsfällen ergeben sich je nach Anwendungsfall spezielle Bedrohungen und daraus resultierende Sicherheits- und Datenschutzanforderungen. Potenzielle Angreifer auf ein C2C/C2X Kommunikationssystem sind autorisierte Nutzer, die sich einen Vorteil in dem System verschaffen möchten, oder auch externe Angreifer, die das System sabotieren und dadurch autorisierte Nutzer auch gefährden können. Angreifer können die Kommunikationsnachrichten mitschneiden, generieren, manipulieren, einspielen oder weiterleiten und für das Senden von eigenen Nachrichten eine manipulierte oder gestohlene Identität verwenden.

3.1.1 Beispiel: Sicherheitsanforderungen für die Einsatzfahrzeugwarnung

Ein relevanter Anwendungsfall ist die Einsatzfahrzeugwarnung, die ein Einsatzfahrzeug zusätzlich zu Blaulicht und Martinshorn per Funk an andere Verkehrsteilnehmer sendet. Die gesendeten Informationen der Einsatzfahrzeugwarnung sind an alle Verkehrsteilnehmer adressiert, Vertraulichkeit der gesendeten Daten ist nicht erforderlich. Die wesentliche Bedrohung liegt darin, dass unberechtigte Fahrzeuge diese Einsatzfahrzeugwarnung generieren könnten, um sich eine freie Fahrt auf Kosten der anderen Verkehrsteilnehmer zu verschaffen. Dieser Bedrohung kann durch Verwendung und Prüfung eines Authentizitätsnachweises in der Nachricht entgegengewirkt werden. Damit ergibt sich die Sicherheitsanforderung, dass das Einsatzfahrzeug seine Nachricht der Einsatzfahrzeugwarnung signiert, und die anderen Verkehrsteilnehmer diese Signatur der Nachricht prüfen müssen, bevor sie auf diese Nachricht reagieren. Insbesondere muss unzweifelhaft aus der digitalen Signatur hervorgehen, dass es sich um ein autorisiertes Einsatzfahrzeug handelt. Eine weitere ähnlich gelagerte Bedrohung liegt darin, dass Angreifer eine von ihnen mitgeschnittene Einsatzfahrzeugwarnung selbst erneut senden (Replay). Da es sich um ein Wiedereinspielen einer echten Nachricht handelt, muss dieser Bedrohung durch Einbeziehung von Zeit- und Ortsdaten in die Signatur einer Einsatzfahrzeugmeldung entgegengewirkt werden. Hieraus ergibt sich die Sicherheitsanforderung, dass das Einsatzfahrzeug seine geografische Position und die aktuelle Zeit zum Zeitpunkt der Generierung der Nachricht als

Teil der Nachricht signieren muss und dass die anderen Verkehrsteilnehmer auch diese geografische Position und Uhrzeit mit der eigenen Position und Uhrzeit vergleichen müssen. Da eine Synchronisation der Uhren und Positionsdaten in verschiedenen Fahrzeugen schwer umsetzbar ist und damit gewisse Toleranzen in C2C/C2X Anwendungen vorgesehen werden müssen, ist davon auszugehen, dass in einem zeit- und ortsnahen Kontext von einem Angreifer wieder eingespielte authentische Nachrichten („Echos“) zumindest teilweise nicht erkannt werden können.

3.1.2 Datenschutzanforderungen vs. Zurechenbarkeit

Da C2C/C2X ein komplexes System darstellt, ist es aus Systemsicht wichtig, vermeintliche Angriffe analysieren zu können und Verursacher ausfindig zu machen. Dies erfordert fahrzeugseitig eine Speicherung von Ereignissen und einen Mitschnitt der gesendeten und empfangenen Nachrichten, die regelmäßig oder bei Bedarf an Hintergrundsysteme übertragen werden können.

Sicherheitsanforderungen nach Speicherung von Nachrichten stehen Datenschutzanforderungen an das Selbstbestimmungsrecht der Fahrer gegenüber. Die zentrale Bedrohung des Datenschutzes ist die Erstellung von Bewegungsprofilen des Fahrers durch das Hintergrundsystem oder durch Dritte. Eine weitere Bedrohung entsteht, wenn der Aufenthaltsort des Fahrzeugführers in Echtzeit abfragbar ist („Hotlisting“). Daraus ergibt sich als primäre Anforderung des Datenschutzes, die Identität des Fahrers eines Fahrzeugs gegenüber anderen Verkehrsteilnehmern und Dritten anonym zu halten und eine Verkettung von gesendeten Nachrichten des Fahrzeugs zu dem Fahrer zu verhindern. Ein abgeschwächtes Sicherheitsziel der Anonymität ist die Pseudonymität, bei der die Identität eines Einzelnen nur von einer hierfür autorisierten Stelle im Gesamtsystem offengelegt werden kann.

Es gilt einen Kompromiss zwischen den Anforderungen des Datenschutzes nach Schutz des Einzelnen gegenüber dem Systembetreiber oder Dritten und der IT-Sicherheit nach Schutz des Systems gegenüber Einzelnen oder externen Angreifern zu finden. Eine Lösung ist die kurzzeitige Verwendung von Pseudonymen, deren Konzeption im Folgenden erläutert wird.

3.1.3 Ausgabe von Pseudonymen durch eine PKI

Das Vertrauen zwischen Sender und Empfänger kann durch eine Public-Key-Infrastruktur (PKI) aufgebaut werden (vgl. PRESERVE Konsortium 2014, 83f. und Ullmann 2015). Hierzu bedarf es einer Wurzel-Zertifizierungsstelle (Root CA), die als Vertrauensanker dient. Unter der Root CA ist eine Long-Term CA (LTCA) und eine Pseudonym CA (PCA) vorgesehen. Von der LTCA erhält jedes Fahrzeug ein Langzeit-Zertifikat, mit dem es sich in kurzen Zeitabständen wiederholt von der PCA Zertifikate mit einem Pseudonym ausstellen lassen kann. Durch Pseudonym-Zertifikate wird der Fahrzeugführer geschützt vor einer lang andauernden Aufzeichnung seiner Bewegungsdaten durch Dritte. Die Erstellung von Bewegungsprofilen wird dadurch auf die Zeit limitiert, in der ein Fahrzeug dasselbe Pseudonymzertifikat nutzt. Von dem Betreiber der PKI kann allerdings die Identität des Fahrzeugführers, der ein bestimmtes Pseudonym nutzte, aufgedeckt werden. In PRESERVE Konsortium (2014, 83 f.) ist vorgesehen, dass in diesem Prozess die LTCA integriert sein muss, so dass die PCA nicht die Langzeit-Identität des Fahrzeugs kennt und die LTCA nicht die ausgegebenen Pseudonyme. Andere Verfahren, bei denen ein direkter Datenaustausch zwischen ausgegebenem Pseudonym und Langzeit-Identität in der PKI umgesetzt wird, werden auch in PRESERVE Konsortium (2014, 86) diskutiert.

3.2 Machbarkeit von sicherer Car-2-Car Kommunikation

In vielen Anwendungsfällen der C2C/C2X Kommunikation gibt es die Vorgabe von kritischen zeitlichen Restriktionen. Beispielsweise nennt das PRESERVE Projekt eine Latenzzeit von weniger als 100 ms für die Einsatzfahrzeugwarnung (PRESERVE Konsortium 2014, 23).

In dem Projekt simTD (www.simtd.de) unter dem Konsortialführer Daimler AG wurde ein Feldversuch zur C2C/C2X Technologie mit 120 Fahrzeugen und mehr als 100 fest installierten Funkstationen durchgeführt. Jedoch fand dieser Versuch aus Performancegründen ohne kryptografische Sicherheitsmaßnahmen statt, da sich herausgestellt hat, dass die simTDHardware nicht in der Lage war, die geforderte Anzahl eingehender Nachrichten kryptografisch zu bearbeiten (SIMTD Konsortium 2013, 130). Dies hat zur Folge, dass sämtliche Sicherheitsanforderungen, die kryptografische Verfahren erfordern, in diesem Feldtest

außer Acht gelassen wurden. Ein Feldtest für C2C/C2X Technologie ohne Einsatz von kryptografischen Verfahren wird als sehr fragwürdig bewertet.

Das EU-Projekt PRESERVE (www.preserve-project.eu) unter der Konsortialführerschaft der Universität Twente, Niederlande, hat sich zum Ziel gesetzt, ein sicheres und skalierbares C2C/C2X Subsystem für realistische Szenarien zu entwickeln. Unter anderem wurde das Ziel verfolgt, ein performantes Hardware Sicherheitsmodul zu entwickeln. Das PRESERVE Projekt arbeitet mit Elliptischer Kurvenkryptographie (ECC), AES und SHA-2. Nach Moser (2015) konnte die Machbarkeit der Performanzanforderungen von 1.000 ECC-Verifikationen in dem PRESERVE Projekt nachgewiesen werden. Der speziell entwickelte PRESERVE ASIC benötigt 3,4 ms für eine ECC-Signaturverifikation bei einer Taktrate von 160 MHz, auf dem PRESERVE ASIC stehen 6 Kerne parallel zur ECC-Verifikation zur Verfügung, so dass pro Sekunde 1760 ECC Verifikationen durchführbar sind. Ein Feldtest mit diesem Hardware Sicherheitsmodul hat in dem Projekt PRESERVE nicht stattgefunden.

Ein länderübergreifender ITS-Feldversuch befindet sich aktuell in Vorbereitung (http://www.c-its-korridor.de). In einem Dreiländerprojekt mit den Niederlanden, Deutschland und Österreich sollen auf den Autobahnen von Rotterdam über Frankfurt nach Wien (a) die Warnung vor Tagesbaustellen und (b) ein verbessertes Verkehrsmanagement der Fahrzeugdaten mit erprobt werden.

3.3 Schwierigkeiten und offene Probleme

3.3.1 Mensch-Maschine Schnittstelle zum Fahrzeugführer

Aus den bisherigen Forschungsarbeiten ist noch nicht offensichtlich, wie Fahrzeugführer über eingehende Nachrichten informiert werden und ob ein Fahrzeugführer über eine Benutzerschnittstelle in die Lage versetzt werden soll, Warnungen an andere Fahrzeuge zu generieren. Dies ist für jede C2C/C2X Anwendung festzulegen. Der Empfang von ITS-Warnungen darf nicht zu einer automatisch eingeleiteten Reaktion des Fahrzeugs an Bremsen oder Lenkung führen. Letztendlich bleibt der Fahrzeugführer in der Verantwortung, auf ITS Warnungen angemessen zu reagieren.

3.3.2 Langwierige Einführung

Bei der Einführung von C2C/C2X Kommunikation ist in den Anfangsjahren nur ein Bruchteil aller Fahrzeuge mit der entsprechenden Technik werksseitig ausgestattet. Die volle Funktionalität von C2C/C2X kann erst nach vielen Jahren erreicht werden.

3.3.3 Verwaltung der Zertifikate und Komponenten

Es gibt neuartige funktionale Anforderungen an die vorgesehene PKI. Die PCAs müssen mehrmals täglich neue Pseudonym-Zertifikate an alle Fahrzeuge mit C2C/C2X Technologie ausgeben, damit die Pseudonyme wirksam sind gegen eine Erstellung von Bewegungsprofilen. Es sind organisatorische Maßnahmen für den Zertifikatsrückruf vorzusehen, zum Beispiel wenn ein Fahrzeug infolge eines Unfalls verschrottet wird, und es sind Maßnahmen empfehlenswert, die den Lebenszyklus von bordseitig eingebauten C2C/C2X Einheiten von der Inbetriebnahme bis zu ihrer Zerstörung nachvollziehen.

3.3.4 Länderübergreifende PKI

Es ist zu erwarten, dass PKIs zur C2C/C2X Kommunikation in jedem Land aufgebaut werden müssen. Erfahrungsgemäß ist eine Harmonisierung von länderübergreifenden PKIs schwierig. Dies ist aber erforderlich, damit auch Verkehrsteilnehmer aus anderen Ländern, die die technischen Voraussetzungen für die C2C/C2X Kommunikation mitbringen, aktiv an dem Ad-Hoc Netz der Fahrzeuge teilnehmen können.

3.3.5 Angriffssicherheit der ITS Funkstationen

Sobald ITS-Funkstationen an der Straße Masterschlüssel oder private Signaturschlüssel von ITS-Anwendungen enthalten, können sie zu einem Angriffsziel von kriminellen Organisationen werden. Es sind entsprechende Schutzmaßnahmen gegen Kompromittierung des Schlüsselmaterials und gegen Manipulationen und Sabotage zu entwickeln und umzusetzen (Ullmann et al. 2015).

4 Handlungsempfehlungen

Es ist festzustellen, dass es sich bei dem Thema dieses Beitrags um ein hoch-komplexes Feld handelt. Die folgenden Handlungsempfehlungen decken aus Sicht der Autorin wichtige Teilaspekte ab, sie erheben aber keinen Anspruch auf Vollständigkeit.

4.1 Verfügbarkeit des Fahrzeugs

Sicherstellung der Primärfunktionen: Priorität für die Verbraucher hat die Aufrechterhaltung der Fahrtüchtigkeit des Fahrzeugs. Diese Primärfunktionen wie Motorsteuerung, Lenkung und Bremsanlage dürfen nicht durch Störungen oder Angriffe von bordseitigen Verkehrstelematikeinrichtungen beeinflusst werden können. Eine bereits bekannte Maßnahme, die hierzu weiterverfolgt werden sollte, ist die spezielle Abschirmung von Steuergeräten, die für Primärfunktionen zuständig sind, von dem übrigen Fahrzeug-Bussystem (Szerwinski 2014).

Jahrzehntelanger Betrieb von Fahrzeugen: Gegenüber klassischer IT-Technik, in der Hardware- und Softwarekomponenten nur wenige Jahre zum Einsatz kommen und danach durch Nachfolger ausgetauscht werden, haben wir es in der Automobilindustrie mit jahrelangen Vorlaufzeiten bis zur Produktionsreife und zusätzlich mit einer jahrzehntelangen Nutzung der Fahrzeuge im Feld zu tun. Ein großes Problem, was mit der Langlebigkeit von Komponenten einhergeht, ist die Wartung der Software- und auch der Hardwarekomponenten. Aus Verbrauchersicht ist es wünschenswert, Hardwarekomponenten über viele Jahre wartbar und Original-Ersatzteile verfügbar zu halten. Zudem sind Softwarestände für vielfältige Modelle aktualisierbar zu halten. Es ist wünschenswert, wenn ein Austausch von Hardwarekomponenten im Fahrzeug infolge von neueren Entwicklungen in den Spezifikationen möglichst vermieden werden kann.

Werkstätten: Aus Kostensicht ist es wünschenswert, dass auch freie Werkstätten weiterhin Reparaturen am Fahrzeug und an bordseitigen Telematikeinrich-

tungen durchführen können. Dies erfordert, dass freie Werkstätten auch die erforderlichen Handbücher und Tools zur Fehlerdiagnose und Zugang zu Originalersatzteilen und Software-Updates erhalten. Es ist aber auch festzuhalten, dass Werkstätten durch den OBD2-Zugang sehr einfach Manipulationen an Steuergeräten zum Schaden der Verbraucher durchführen können. Es ist damit wichtig, die Vertrauenswürdigkeit von Werkstätten und ihren Mitarbeitern durch unangemeldete und unabhängige Expertentests zu überprüfen.

Schutz vor Plagiaten: Gefälschte Ersatzteile haben üblicherweise keine vergleichbaren Prüfverfahren durchlaufen wie originale Ersatzteile. Der Einbau dieser Plagiate in die Fahrzeuge kann damit zu einer Bedrohung für die Fahrzeuginsassen werden, wenn funktionale Sicherheitsanforderungen nicht erfüllt sind. Plagiate können zudem zum Aushebeln von Sicherheitsmechanismen in Fahrzeugen eingesetzt werden. Hier sind organisatorische und technische Verfahren zu entwickeln und durchzusetzen, die die Detektion von Plagiaten seitens des Herstellers, in der Lieferkette, in den Werkstätten oder auch durch den Verbraucher ermöglichen.

Schadsoftware im Automobil: Für die Zukunft ist zu erwarten, dass Schadsoftware auch in das Auto Einzug hält, sobald Anwendungen großflächig ausgerollt werden, in denen kriminelle Organisationen einen Gewinn durch softwareseitige Manipulationen der Fahrzeug-internen Komponenten auf Kosten der Verbraucher erzielen können. Entfernung von persistenter Schadsoftware ohne komplette Neuinstallation des Betriebssystems ist bereits bei PCs ein sehr schwieriges Problem, das entsprechende Expertise erfordert. Auf einer komplexen Fahrzeug-IT mit Dutzenden von eingebetteten Steuergeräten gestaltet sich das Problem noch um Größenordnungen schwieriger, sodass zur Entfernung von persistenter Schadsoftware eine komplette Neuinstallation der Software zu empfehlen ist.

Kosten-Nutzen-Analyse bei jeder C2C/C2X Anwendung: Aus Verbrauchersicht ist es wichtig, dass vor einer Pilotierung einer C2C/C2X Anwendung eine positive Kosten-Nutzen-Betrachtung von unabhängigen Experten erfolgt ist. Aufgrund der Vielzahl von möglichen Anwendungen und den damit verbundenen zusätzlichen Kosten für den Fahrzeugeigner sollte eine Fokussierung auf wenige Anwendungen mit nachgewiesenem Nutzen für die Sicherheit der Verkehrsteilnehmer stattfinden.

4.2 Datenschutz

Kontrolle der Verbraucher über personenbezogene Fahrzeugdaten: Es wird dringend empfohlen, der unkontrollierbaren direkten Übertragung von personenbezogenen Informationen aus bordseitigen Komponenten, wie es aktuell zum Beispiel bei den Blackboxes der Versicherungen der Fall ist, Einhalt zu gebieten. Denkbar ist ein Ansatz, bei dem die bordseitige Komponente die Fahrzeugdaten lokal akkumuliert und die detaillierten im Fahrzeug erhobenen Daten – wie zum Beispiel erfasste Fahrtstrecken, Geschwindigkeiten, Beschleunigungen und Bremsvorgänge – löscht. Ein Datenübertrag sollte dann auf die Sendung eines Ergebnisberichts über einen längeren Zeitraum beschränkt werden. Der Fahrzeugführer ist darüber zu informieren, welche Daten an die Versicherung übersandt werden. Der Fahrzeugführer sollte berechtigt werden, den Datentransfer zu stoppen. Auch Anwendungen wie eCall und Trackingsysteme, die typischerweise vom Fahrzeugführer nicht deaktivierbar sind, haben die technische Möglichkeit, jederzeit bei Verfügbarkeit eines Mobilfunknetzes den aktuellen Aufenthaltsort des Fahrzeugs abzufragen (Hotlisting). Dies stellt praktisch eine Verwanzung des Fahrzeugs dar, die als eine starke Einschränkung des informationellen Rechts auf Selbstbestimmung zu werten ist. Bezüglich dieser Art von Anwendungen sollte eine Deaktivierbarkeit seitens des Fahrzeugführers zukünftig vorgesehen werden, so wie es auch bei Smartphones der Fall ist. Die Erstellung von Bewegungsprofilen eines Fahrzeugs ist möglich, sobald aus diesem Fahrzeug ein Gerät mit einer eindeutigen Identität sendet. Dies ist aktuell bei den Verkehrsflussanalysen mit Bluetooth den meisten Verbrauchern vermutlich nicht bewusst. Bei C2C/C2X ist es aus Datenschutzsicht empfehlenswert, an das Fahrzeug direkt einen Satz von mehreren Pseudonymen-Zertifikaten herauszugeben, aus denen das Fahrzeug sich für einen gewissen Zeitraum zufällig bedienen kann.

Definition von Datenschutzanforderungen: Der Gesetzgeber, die Wirtschaft und die Verbraucher sind gefordert, Datenschutzanforderungen für die vorhandenen und neuen Verkehrstelematikanwendungen zu definieren. Die korrekte Umsetzung in Fahrzeugkomponenten, straßenseitigen Funkstationen und Hintergrundsystemen ist mit Hilfe von unabhängigen Gutachtern zu prüfen, bevor eine Zulassung erteilt wird.

4.3 Offene Spezifikationen und Benutzerdokumente

Bereitstellung umfangreicher Informationen für den Verbraucher: Zu jeder Verkehrstelematikanwendung sollten umfangreiche Informationen an die Verbraucher herausgegeben werden. Diese Informationen können unterschiedliche Zielgruppen adressieren und damit im Detailgrad variieren. Die Verbraucher sollten letztendlich selbst entscheiden, bis zu welchem Detailgrad sie sich mit den vorgesehenen Verfahren auseinandersetzen möchten. Die bereitgestellten Informationen sollten es einem Verbraucher mit technischer Expertise ermöglichen, die Details der Protokolle und Schnittstellen der Verkehrstelematikanwendung zu analysieren.

4.4 IT-Sicherheit

Etablierte kryptografische Algorithmen: In der Vergangenheit sind in Fahrzeugen oft proprietäre, geheim gehaltene kryptografische Verfahren genutzt worden, die in den letzten Jahren durch teilweise aufwendiges Reverse-Engineering von Forschern in Erfahrung gebracht wurden und danach direkt aufgrund vorhandener Schwachstellen in den Kryptoverfahren, der Schlüsselgenerierung oder der Implementierung teilweise katastrophal gebrochen werden konnten. Beispielsweise sei hier die Veröffentlichung (Verdult et al. 2015) genannt, in der die Wegfahrsperre Megamos analysiert worden ist. Diese Wegfahrsperre wurde in vielen Fahrzeugmodellen unterschiedlicher Fahrzeughersteller in den Jahren 2000 bis 2011 verbaut und galt bisher als sicher, im Gegensatz zu den bereits gebrochenen Konkurrenzsystemen DST40, Keeloq und Hitag2 (Gleich 2015). Volkswagen hatte diese Veröffentlichung im Jahr 2013 auf dem USENIX Symposium 2013 gerichtlich verhindern lassen, die Veröffentlichung geschah damit erst zwei Jahre später (Gleich 2015). Es ist damit dringend anzuraten, dass die Verkehrstelematikanwendungen zukunftsfähige etablierte kryptografische Verfahren nach dem Stand der Technik nutzen. Dies bezieht auch den Wechsel auf vertrauenswürdigere elliptische Kurvenparameter wie beispielsweise die Brainpool-Kurven bei C2C/C2X Anwendungen ein (Ullmann et al. 2015). Es ist dringend zu empfehlen, Klartextnachrichten wie etwa SMS (Short Message Service) aus den Verkehrstelematikanwendungen komplett zu eliminieren und eine Ende-zu-Ende Verschlüsselung durchgängig einzuführen.

IT-Sicherheitsnachweise seitens der Hersteller: Da technische Schwachstellen von den Herstellern bisher oft geheimgehalten werden konnten, sind sie auch den Strafverfolgungsbehörden und den Gerichten vermutlich unbekannt. Der Verbraucher kann damit zum Beispiel beim Autodiebstahl schnell zu Unrecht in den Verdacht geraten, mit kriminellen Organisationen kooperiert zu haben. Das Vertrauen in die Verkehrstelematikanwendungen ist für die Verbraucher und die Gesellschaft insgesamt entscheidend. Durch die Offenlegung von Schnittstellen und durch Schwachstellenanalysen der Software- und Hardwarekomponenten durch unabhängige IT-Sicherheitsexperten können potentielle Angriffswege erkannt und anschließend unterbunden werden. So kann insgesamt ein höheres Sicherheitsniveau erreicht werden.

Definition von IT-Sicherheitsanforderungen: Der Gesetzgeber, die Wirtschaft und die Verbraucher sind gefordert, geeignete Sicherheitsanforderungen und technische Richtlinien für die vorhandenen und neuen Verkehrstelematikanwendungen zu definieren. Die Sicherheitsanforderungen sollten – je nach der Bedrohungslage der konkreten Anwendung durch kriminelle Organisationen – ein mittleres bis hohes Sicherheitsniveau anstreben. Die korrekte Umsetzung in Fahrzeugkomponenten, straßenseitigen Funkstationen und Hintergrundsystemen sollte mit Hilfe von unabhängigen IT-Sicherheitsexperten im Rahmen einer Zertifizierung geprüft werden, bevor eine Zulassung erteilt wird.

Literatur

Becker, Leo. 2015. Bericht: Porsche setzt auf CarPlay statt Android Auto wegen Datenschutzbedenken. *Mac & i* (6. Oktober). http://www.heise.de-2839133 (Zugriff: 1. März 2016).

Bißmeyer, Norbert, Sebastian Mauthofer, Jonathan Petit, Mirko Lange, Martin Moser, Daniel Estor, Michel Sall, Michael Feiri, Rim Moalla, Marcello Lagana und Frank Kargl. 2014. *V2x security architecture v2,* hg. von Norbert Bißmeyer. Version 1.0. Preserve 31. Januar 2014. https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.3-V2X_Security_Architecture_V2.pdf.

CAR 2 CAR (CAR 2 CAR Communication Consortium). o. D. https://www.car-2-car.org/ (Zugriff: 1. März 2016).

Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner und Tadayoshi Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. *USENIX Security* (10.–12. August).
(10.–12. August). http://www.autosec.org/pubs/cars-usenixsec2011.pdf

Eckert, Claudia. 2014. *IT-Sicherheit*. 9. Auflage. Berlin: De Gruyter Oldenbourg.

Eikenberg, Ronald. 2015. Hacker steuern Jeep Cherokee fern. *heise Security* (22. Juli).http://www.heise.de/-2756331 (Zugriff: 1. März 2016).

Das Europäische Parlament und der Rat der Europäischen Union. 2015. *Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigungen zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG*. Amtsblatt der Europäischen Union. http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R0758&from=EN (Zugriff: 1. März 2016).

European Commission. 2015. *eCall: Time saved = lives saved*. http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved (Zugriff: 1. März 2016).

Fahn, Christian. 2013. Ich weiß, wo du gestern vor einem Jahr warst. *Donaukurier* (6. August). http://www.donaukurier.de/nachrichten/digital/datenschutz/datenschutztipps/Datenschutz-Digital-Ich-weiss-wo-du-gestern-vor-einem-Jahr-warst;art267994,2801060 (Zugriff: 1. März 2016).

Gleich, Clemens. 2015. VW-Wegfahrsperren: Volkswagen-Hack endlich veröffentlicht. *heise online* (13. August). http://www.heise.de-2778632 (Zugriff: 2. März 2016).

Kannenberg, Axel. 2015. Autobauer prüfen Daten-Freigabe aus vernetzten Fahrzeugen für ihren Kartendienst Here. *heise online* (7. Dezember). http://www.heise.de/-3033589 (Zugriff: 1. März 2016).

Lemke, Kerstin, Christof Paar und Marko Wolf. 2006. *Embedded Security in Cars*. Heidelberg: Springer VS.

Miller, Charlie und Chris Valesek. 2015. *Remote exploitation of an unaltered passenger vehicle.* http://illmatics.com/Remote%20Car%20Hacking.pdf

Moser, Martin. E-Mail Nachricht an Autorin, 30. Oktober 2015.

Schwan, Ben. 2015. Gegen Apple und Co.: Autobauer wollen „direkte Schnittstelle“ zum Kunden behalten. *Mac & i* (9. November). http://heise.de/-2911839 (Zugriff: 2. März 2016).

Stokar, Rudolf von. 2015. Warum die Autoindustrie neue Software Updates braucht. Herausforderung beim Update von ECUs. *Elektroniknet.de*. http://www.elektroniknet.de/automotive/tools/artikel/117489/1/ (Zugriff: 2. März 2016).

Stotz, Jan Peter, Norbert Bißmeyer, Frank Kargl, Stefan Dietzel, Panos Papadimitratos und Christian Schleiffer, Hg. 2011. *Security requirements of VSA*. Version 1.1. Preserve Juni 2011. https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.1-Security%20Requirements%20of%20Vehicle%20Security%20Architecture.pdf.

Szerwinski, Robert. 2014. *Security in the automotive domain*. CAST Workshop Mobile and Embedded Security. (22. Mai).

Ullmann, Markus, Christian Wieschebrink und Dennis Kügler. 2015. Public key infrastructure and crypto agility concept for intelligent transportation systems. Proceedings VEHICULAR, in: *IARIA* 2015, 14–19.

Wenzel, Andreas, Hrsg. 2013. *Sichere intelligente Mobilität. Testfeld Deutschland: Deliverable D5.5, TP5-Abschlussbericht – Teil B-3 – Technische Bewertung* Version 1.0. SIMTD Konsortium. (9. Dezember). http://www.simtd.de/index.dhtml/object.media/deDE/8118/CS/-/backup_publications/Projektergebnisse/simTD-TP5-Abschlussbericht_Teil_B-3_Technische_Bewertung_V10.pdf.

Verdult, Roel, Flavio D. Garcia und Baris Ege. 2015. *Dismantling megamos crypto: wirelessly lockpicking a vehicle immobilizer*. Supplement to the Proceedings of the 22nd USENIX Security Symposium 2013.