Benjamin Weigl
Prof. Dr. Andreas Aßmuth

Bedrohungslage fahrzeuginterner Kommunikations-netzwerke und Bus-Systeme

Zusammenfassung

Die Konnektivität aktueller Fahrzeugreihen jeder Marke steigt so kontinuierlich, wie die Meldungen verschiedenster Sicherheitsforscher über neue Schwachstellen und Sicherheitslücken im Fahrzeugbau. In diesem Aufsatz wird das Kommunikationsnetzwerk eines modernen Fahrzeugs dargestellt und auf die unterschiedlichen Schwachstellen eingegangen. Die Ergebnisse münden in einem Bedrohungsmodell, das als Basis dient, um neue und zukunftsgerichtete Sicherheitsmechanismen für die Fahrzeugindustrie zu evaluieren. Zusammen mit den fundamentalen Wissensbereichen der Fahrzeugkommunikation kann anschließend der Einsatz unterschiedlicher kryptografischer bzw. allgemeiner sicherheitsrelevanter Algorithmen und Methoden zur Verbesserung der Sicherheit informationsverarbeitender eingebetteter Systeme im Fahrzeugbau diskutiert werden.

Abstract

The increasing number of connected cars interacting with each other and the environment has revealed a variety of vulnerabilities. These vulnerabilities made it possible to hack car internal communication networks and protocols. This paper gives an overview of common car communication and provides certain attack scenarios of automotive systems related IT security incidents. These findings are gathered in a level zero threat model. This model covers the attack surface of a modern car and serves as a base to evaluate new and futureoriented security features. Combined with basic car network and protocol knowledge, this paper tries to address the demand of lightweight cryptographic primitives and common IT security mechanisms to improve the protection of automotive related embedded communication against external threats.

Einleitung

We basically had complete control of the car except the steering. [1]

In einem modernen Fahrzeug sind unzählige Sensoren, Aktoren, Assistenzsysteme und Mikrocontroller im Einsatz, um ein bestmögliches Fahrerlebnis zu erzielen. So unterstützen Abstandssensoren den Fahrer bei der Abschätzung von Distanzen, Stabilisierungsassistenten überwachen die unterschiedlichen physikalischen Kräfte, die auf das Fahrzeug einwirken und Scheibenwischer, gekoppelt mit einem Regensensor, ermöglichen freie Sicht bei nahezu jeder Wetterlage. Nach „Industrie 4.0“ hat auch das moderne Fahrzeug einen Zugang zum Internet erhalten. Da möglichst viele Komponenten vom „Internet of Things“-Trend profitieren sollen, müssen die einzelnen Steuergeräte und Informationsquellen effizient und ausfallsicher kommunizieren können. Häufig wird dabei auf bewährte Technologien wie den CAN (Controler Area Network)-Bus, FlexRay oder MOST (Media Oriented Systems Transport) gesetzt. Während diese Kommunikationsnetzwerke und -protokolle auf höchstem Niveau gegen einen Ausfall durch technische oder umweltbedingte Störfaktoren abgesichert sind, berücksichtigte bei deren Entwicklung und Standardisierung der zum Teil aus den 1980er-Jahren stammenden Technologie, niemand den Schutz gegen eine vorsätzliche Manipulation durch den Menschen.

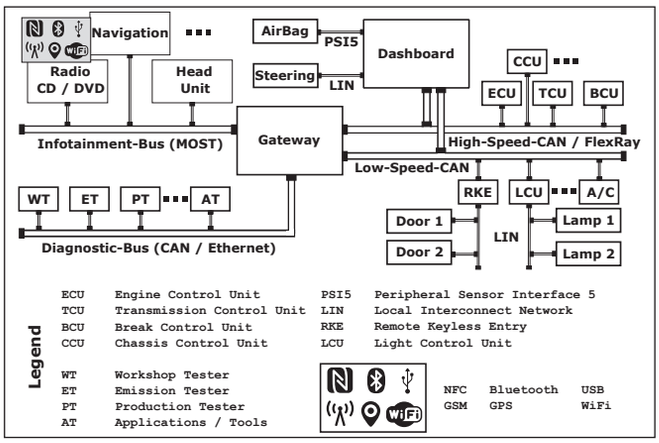

Abbildung 1: Kommunikationsnetzwerke in einem Fahrzeug nach [2]

Das Resultat dieser Entwicklung vom informationstechnisch autarken Fahrzeug hin zum „Connected Car“, bei dem Fahrzeuge ihre durch Sensoren gewonnene Einschätzung der Verkehrs- und Umweltlage teilen, kann heute in den aktuellen Trends der Forschungsvorhaben aller Fahrzeughersteller beobachtet werden. Neben all den Meldungen über neue Funktionalitäten häufen sich auch Verlautbarungen diverser Hacker und Sicherheitsforscher über die unterschiedlichsten Sicherheitslücken dieser Evolution. Bereits 2010 konnte ein Team aus Sicherheitsforschern um den Hacker Karl Koscher der University of California, San Diego und der University of Washington erfolgreich in das CAN-Bus-System eines General Motors 2009 Chevy Impala eindringen. General Motors konnte die Schwachstelle erst nach fünf Jahren schließen. Grund genug, gängige fahrzeuginterne Kommunikationsmittel zu analysieren und gleichzeitig die aktuelle Bedrohungslage für moderne Fahrzeuge aufzuzeigen. In dieser Arbeit wird, nach Aufbau des Grundwissens in die technologischen Hilfsmittel innerhalb des Fahrzeugbaus, auf bereits entdeckte Schwachstellen hingewiesen und abschließend die Gesamtsituation bewertet. Auch erste Ansätze für Gegenmaßnahmen sind Teil dieses Artikels. [1]

Fahrzeuginterne Kommunikation

Um ein vollumfängliches Verständnis der aktuellen Sicherheitslage fahrzeuginterner Kommunikationsnetze (siehe Abbildung 1) zu erhalten, ist ein grundsätzliches Know-how der verbreitetsten Technologien notwendig. Dieser Abschnitt soll dieses Wissen vermitteln und gleichzeitig bekannte Schwachstellen benennen und mit aktuellen Hacks deren aktive Ausnutzung beweisen.

Der Powertrain

Die Kommunikation aller Komponenten des Triebstrangs (engl. Powertrain, siehe Abbildung 2) wird in nahezu allen Fahrzeugen über ein Controller Area Network abgewickelt. Dieser Bereich des Informationsaustausches aller Steuergeräte, die den Fahrzeugtriebstrang bedienen, gilt als besonders schützenswert, da hier für die funktionale Sicherheit des Fahrbetriebes wichtige Nachrichten versendet werden. Auf diesem Bus-System können Mitteilungen über den allgemeinen Zustand des Triebstrangs, wie Messwerte verschiedenster Motorüberwachungssensorik oder spezielle Anweisungen an sicherheitskritische Komponenten, wie die Bremsanlage, an alle Teilnehmer des Busses verschickt werden. Neben Signalen, die der Benutzer auslöst, z. B. das Einleiten eines Beschleunigungsvorganges, setzen in diesem Informationsnetzwerk auch „Advanced Driver Assistent Systems“ (ADAS) die jeweiligen Kommandos ab. So kann jeder Steuerungsversuch einer automatischen Einparkhilfe in diesem Bus-System mitgelesen werden. [2]

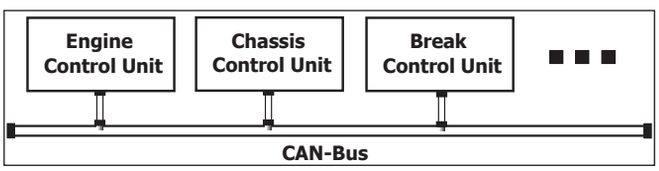

Abbildung 2: Triebstrangnetzwerk alias Powertrain

Ein Eindringen in diesen durch einen Gateway (siehe Abbildung 1) geschützten Bereich ist im Allgemeinen vergleichbar mit dem Erlangen von administrativen Rechten eines herkömmlichen Computersystems. Nahezu jedes Ausnutzen von Schwachstellen eines modernen Fahrzeugs dient langfristig dazu, in das Kommunikationsnetz einzugreifen, mindestens jedoch mitzulesen. Der Aufbau dieses Bus-Systems und die Vielzahl der Eigenschaften, die diesen Bus besonders anfällig gegenüber nicht authentifiziertem Nachrichtenverkehr machen, wird im nächsten Abschnitt genauer betrachtet. [3]

Das Controller Area Network

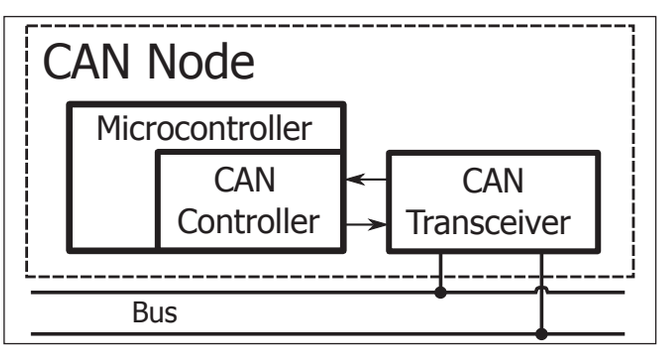

Abbildung 3: CAN-Knoten im Bus-System nach [4]

Das Controller Area Network bildet in nahezu jedem Kraftfahrzeug (z. B. im Auto, LKW, Motorrad, Flugzeug, u. v. m.) und in vielen industriellen Anlagen (z. B. in der Robotik oder als Sensor-Aktor-Bus) die grundlegende Kommunikationstechnologie. Der simple und dadurch günstige Aufbau eines, CAN-Node genannten, Bus-Teilnehmers (siehe Abbildung 3), die Echtzeitfähigkeit sowie die hohe Ausfallsicherheit begründen die heute starke Verbreitung des bereits in der zweiten Hälfte der 1980er-Jahre entwickelten Bus-Systems. [2]

Das CAN-System ist ein Bitstrom-orientierter Linien-Bus. Bei einer maximalen Bitrate von 1 MBit/s verwendet CAN ein CSMA/CR-Buszugriffsverfahren (Carrier Sense Multiple Access/Collision Resolution) sowie eine Fehlererkennung, die die Reaktion aller Steuergeräte innerhalb einer Bitzeit erfordert. Gerade in der Fahrzeugtechnik sind die beiden Variationen Low-Speed-CAN sowie High-Speed-CAN oft vertreten. Durch kurze Bus-Leitungen kann im High-Speed-CAN eine deutlich höhere Bitrate (üblicherweise 250 kbit/s bis 500 kbit/s) erreicht werden. Vor allem im Powertrain wird durchgehend auf den High-Speed-CAN-Bus gesetzt, da hier hohe Bus-Raten einen enormen Vorteil für die Steuerung der zeitkritischen Triebstrangkomponenten bieten. Der Low-Speed-CAN-Bus hingegen wird in der Karosserieelektronik verwendet, da durch niedrigere Bus-Raten eine höhere Distanz zwischen den Bus-Teilnehmern überbrückt werden kann. An dieser Stelle sei die erste triviale Schwachstelle des CAN-Bus-Systems zu erwähnen: Durch den einfachen Bus-Aufbau (siehe Abbildung 3) ist es einem Angreifer mit physischem Zugriff ein Leichtes, mit einem Abzweigverbinder (auch Kabel- bzw. Stromdieb genannt) einen neuen CAN-Node in das Bus-System einzuschleusen. Besonders der Aufbau des CAN Data Link Layers begünstigt vielfältigste Angriffsszenarien. [2]

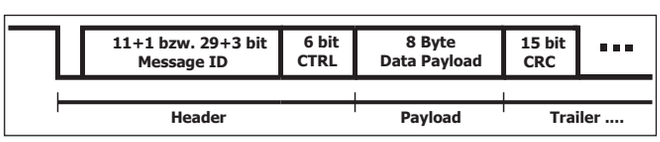

Abbildung 4: Aufbau einer CAN-Botschaft (stark vereinfacht, ohne Stuffing-Bits) nach [2]

Der Aufbau einer CAN-Botschaft, wie er im Data Link Layer von Bosch und Intel festgelegt wurde, ermöglicht eine Reihe einfacher Angriffe auf die Kommunikation. Die schwerwiegendste Schwachstelle entsteht allein durch den Aufbau des Protokolls. Weder beim Verbindungsaufbau (bzw. beim Anmelden eines neuen Teilnehmers) noch bei der Datenübertragung noch beim Verbindungsabbau wird die Identität des Bus-Teilnehmers verifiziert. Betrachtet man die Struktur einer CAN-Botschaft (siehe Abbildung 4), fällt auf, dass kein Datenfeld für eine Authentifizierung der Quelle vorgesehen ist. Zusätzlich ist CAN ein Broadcast-Bus-System. Das bedeutet, dass alle auf dem Kanal anliegenden Nachrichten von jedem Teilnehmer gelesen werden können. Für einen Angreifer, der z. B. mit einem Abzweigverbinder bzw. auf einem anderen Weg, Zugriff auf den Bus erhält, ist es keine große Hürde, selbst erzeugte Nachrichten in die Kommunikation der Teilnehmer einzuschleusen. [2]

Sicherheitsforscher haben kürzlich entdeckt, dass es Hersteller gibt, die Schlüsselinformationen, die auf dem Bus ausgetauscht werden, auf die Breite des Datenfeldes reduzieren, um die Buslast zu reduzieren. Es kommt vor, dass kryptografische Schlüssel eine Länge von 8 Byte (64 bit) aufweisen. Nach aktuellem Stand (2016) werden Schlüssellängen von mindestens 128 bit empfohlen. Dieser Umstand stellt eine enorme Schwachstelle dar, die zwar durch die Hersteller behoben werden kann und nicht zwingend auf das CAN-Protokoll zurückzuführen ist, in der Praxis aber immer noch viel zu häufig auftritt. [3][5]

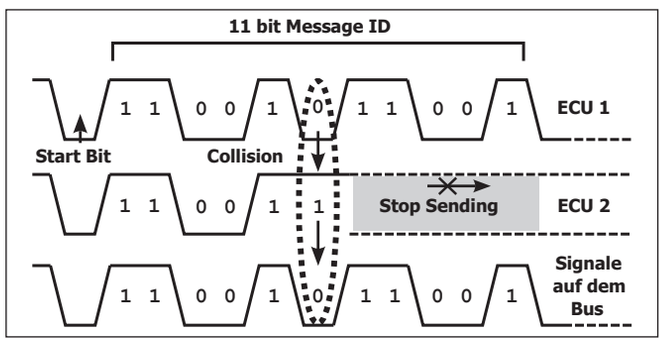

Abbildung 5: Arbitrierung bei einer Kollision nach [2]

Eine weitere Schwachstelle verbirgt sich im Verfahren zur Nachrichtenpriorisierung einzelner Teilnehmer im CAN-Standard. Das Identifikationsfeld mit der Identifikationsnummer (ID) eines Senders bildet zugleich das Prioritätensystem des CAN-Protokolls ab. Dabei gilt, je niedriger die ID, desto höher die Priorisierung. Die ID 0 hat die höchste Priorität. Die vorrangige Bearbeitung hochpriorer Nachrichten geschieht hier nicht auf Softwareebene, sondern wird vom CAN Transceiver in Hardware gelöst. Im CAN-Protokoll ist die physikalische Darstellung des Wertes 0_2 dominant gegenüber der rezessiven 1_2. Dies bedeutet, dass jeder Bus-Teilnehmer jede auf dem Bus anliegende 1_2 mit einer dominanten 0_2 überschreiben kann. Ein Sender liest dabei nach jedem Schreibvorgang den aktuellen Buspegel und überprüft so, ob der gesendete Wert auch auf dem Bus anliegt. Erkennt ein Teilnehmer, dass sein Sendevorgang mit dem einer höher priorisierten Nachricht kollidiert, unterbricht der Sender den Schreibvorgang und wartet, bis der Bus frei ist (siehe Abbildung 5). Hieraus resultiert für jeden CAN-Node die Möglichkeit, Nachrichten aller anderen Teilnehmer zu überschreiben, bis der Bus maximal ausgelastet ist – ein klassischer „Denial of Service“ (DOS). [6]

The less the driver is involved, the more potential for failure when bad people are tampering with it. [7]

Nicht nur eine DOS-Attacke ist im CAN-Bus sehr einfach umzusetzen. Der CAN-Standard ist nicht wie Ethernet verbindungs-, sondern nachrichtenorientiert. In einem nachrichtenorientierten Kommunikationsmodell entscheiden Sender und Empfänger selbst, welche Nachrichtenarten, die alle Teilnehmer gleichermaßen senden bzw. empfangen können, für sie von Bedeutung sind. Verbindungsorientierte Systeme zeichnen sich dadurch aus, dass vor einer Datenübertragung zuerst ein Verbindungsaufbau zwischen den Kommunikationspartnern stattfindet. Dabei sind diese Verbindungen gültig, bis ein Teilnehmer sie abbaut. Der CAN-Standard bietet somit eine große Angriffsfläche gegenüber Nachrichten, die ein Angreifer

erzeugt und in das Bus-System einschleust. Berechtigte Teilnehmer der Kommunikation können nicht unterscheiden, ob eine Nachricht mit einer bestimmten ID (und Priorität) auch von einem berechtigten Sender stammt. [2][8]

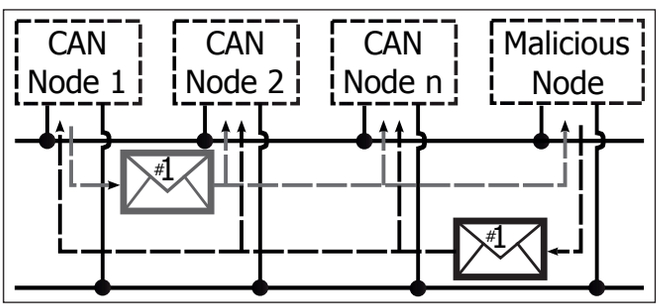

Abbildung 6: Aktiver Angriff auf den Nachrichtenaustausch

Da alle Nachrichten an jeden Teilnehmer gesendet werden (siehe Abbildung 6) und häufig nicht verschlüsselt sind, kann ein Angreifer, der physischen Zugriff auf das Medium hat, alle Nachrichten mitlesen und auswerten. Dass diese Daten einen hohen Informationsgehalt haben, zeigt eine wissenschaftliche Arbeit von Forschern der University of Washington und University of California, San Diego. In der Arbeit „Automobile Driver Fingerprinting“ untersuchen die Autoren, ob mit den Sensor- und Aktuatordaten des Powertrains bzw. des Low-Speed-CANs ein Fahrzeugführer eindeutig identifiziert werden kann. Dazu schickten sie mehrere Fahrer desselben Fahrzeugs auf eine bestimmte Teststrecke und speicherten bei dieser Testfahrt alle Nachrichten, die auf den Bus-Netzwerken entstanden. Die gesammelten Daten wurden aggregiert und mit Mustererkennungsalgorithmen analysiert. [9]

Sensor(s)	Parking Lot	Drive Part1	Drive Part2	All Data
Brake Pedal	50.00	87.33	100	100
Steer Angle	31.33	64.67	83.33	86.67
Accel. Pedal	15.33	18.00	30.00	31.33
Max Torque	75.33	60.67	100	91.33
Lat. Accel.	25.33	62.00	91.3	72.67
Top 3 Sensors	80.06	92.67	100	100
Top 5 Sensors	84.67	99.33	100	100
All Sensors	91.33	100	100	100

Abbildung 7: Identifizierungswahrscheinlichkeit (in %) verschiedener Sensor- und Fahrkombinationen nach [5]

Eine Auflistung (siehe Abbildung 7) mit den entscheidensten Sensoren zeigt, wie viele Fahrten nötig sind, um einen Fahrer anhand seines einzigartigen Fahrverhaltens zu identifizieren. Bemerkenswert, dass Sensordaten der Bremspedalinteraktionen des Benutzers reichen, um nach der zweiten Fahrt den Fahrer mit einer Wahrscheinlichkeit von 87,33 Prozent zu identifizieren bzw. zu unterscheiden. Teilweise kann bereits im noch stehenden Fahrzeug, z. B. am Parkplatz, eine hohe Unterscheidbarkeit erreicht werden. Jeder weitere Sensor erhöht die Differenzierbarkeit deutlich. Die Arbeit zeigt, dass die Verkehrsdaten des Powertrains bzw. anderer Busse von größtem Interesse sein können. Um diese Daten abzugreifen, ist ein physischer Zugriff auf das Bus-System oft gar nicht nötig. Infotainment-Systeme und der Diagnostik-Bus nehmen einem Angreifer diesen Aufwand ab. [9]

Das Infotainment-System

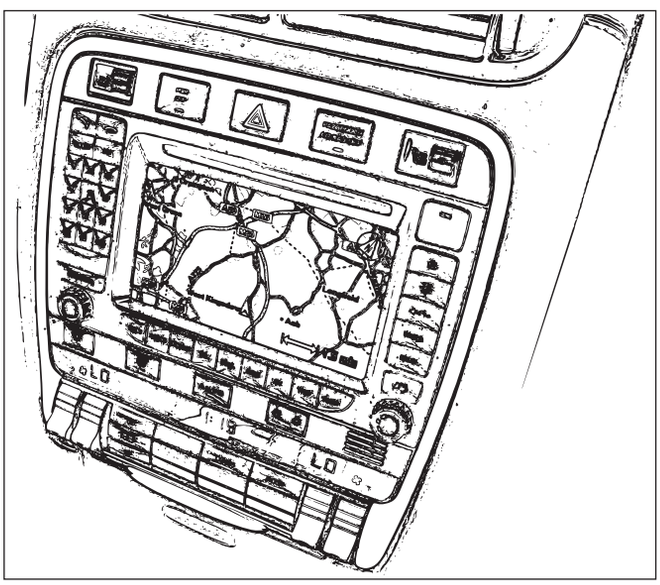

Abbildung 8: Infotainment-System eines 200 Porsche Cayenne 4.5 Turbo S (vgl. [10])

Jedes moderne Fahrzeug hat im Zentrum der Fahrgastzelle ein sog. Infotainment-System verbaut (siehe Abbildung 8). Diesem System sind eine Vielzahl Aufgaben zugedacht. Es steuert alle für den Fahrkomfort notwendigen elektromechanischen Module wie die Klimaanlage, Sitzbelüftung oder Lautstärkeregelung. Daneben gibt das Display Auskunft über jeden erdenklichen Sensor, Aktuator oder Assistenten, der im Fahrzeug verbaut ist. Nicht nur Fahrgeschwindigkeit oder Füllstände der Betriebsmittel sind für den Fahrer interessant, sondern auch die eigene Position in Relation zur vorgeschlagenen Fahrstrecke des Navigationssystems. Der Wetterbericht und aktuelle Staumeldungen runden das Informationspaket ab.

Zur Unterhaltung kann das als In-Vehicle Infotainment (IVI) bekannte System das UKW-Radio aktivieren oder einen Live-Stream aus dem Internet abspielen. Dank Bluetooth-Verbindung zum Handy können auch Anrufe und Kurznachrichten über das Onscreen-Display angenommen bzw. gelesen werden. Sollte das eigens für die Aktualität der Daten verbaute Mobilfunk-Modul keine Long-Term Evolution(LTE)-Verbindung zu einem Carrier aufbauen können, so kann sich das WiFi-Modul in vorhandene Hotspots einwählen. Das rechenstarke Infotainment-System kann parallel zum Abspielen eines Filmes auf dem Hauptbildschirm alle Daten des Powertrains mitlesen, speichern, aggregieren, versenden oder im besten Fall dem Fahrer anzeigen. Die weite Verbreitung und hohe Bandbreite aktueller Mobilfunkstandards ermöglicht es einem Fahrzeug, jederzeit online zu sein, Informationen

abzurufen oder zu senden, Befehle von einer Handy-App oder vom Hersteller zu erhalten oder andere Fahrzeuge über die eigene Umweltwahrnehmung (z. B. Verkehrsunfall) zu unterrichten. [11]

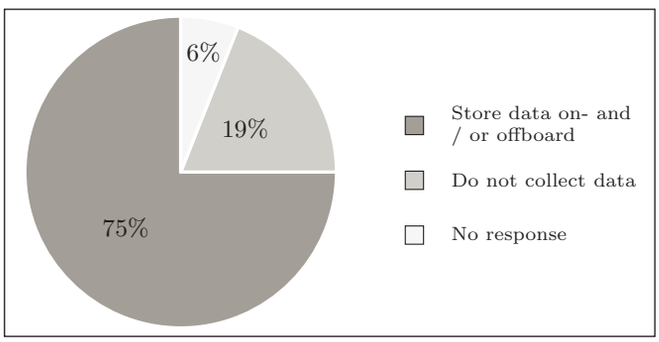

Abbildung 9: Umfrageergebnisse zur Datenspeicherung/-verwertung nach [12]

Im Februar 2015 veröffentlichten die Mitarbeiter des US Senators Ed Markey eine Studie mit dem Titel „Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk“. In dieser Arbeit werden die anonymisierten Antworten auf einen offenen Brief an 19 der weltweit führenden Fahrzeughersteller publiziert. Darunter war die Frage, ob Daten erhoben, gespeichert und evtl. an den Hersteller oder Dritte versendet werden. Über 75 Prozent der Befragten gaben an, Daten on- bzw. offboard zu speichern. Das bedeutet, dass drei Viertel der Fahrzeughersteller mindestens Daten im Fahrzeug speichern, wovon ein Großteil (ca. 50 Prozent) die Daten sammelt oder an Dritte weiterreicht (siehe Abbildung 9). Diese Daten, die natürlich der Steigerung des Fahrerlebnisses dienen, sind auch für einen Angreifer interessant. [12]

Aufgrund der verschiedenen Aufgaben, die ein IVI bewältigen muss, ist die Entwicklungskomplexität der Betriebssoftware enorm. Die hohe Anzahl unterschiedlicher Kommunikationshardware, wie Mobilfunk-, WiFi-, Bluetooth-Module oder CAN-Transceiver und MOST-Verbindungen, machen das Softwarepaket anfällig für Design- und Programmierfehler. So gelang es den Forschern Valasek und Miller 2015 einen unveränderten 2014 Jeep Cherokee über das Infotainment-System zu hacken. Die Hacker erhielten dabei Zugriff auf den Powertrain und konnten im Anschluss das Fahrzeug im Notlauf steuern (Bremsmechanik und Lenkimpulse). Bereits im August 2016 konnten diese beiden Forscher den Hack ausweiten und das Fahrzeug ebenso ohne Notlauf beeinflussen. Das Absetzen der notwendigen Befehle erfolgte über die Mobilfunkverbindung des IVIs. Zwar musste die Firmware des Gateways (siehe Abbildung 1) verändert werden, dies war nach Reverse Engineering des ECU-Update-Prozesses jedoch kein Problem. [11][13]

Hinzuzufügen ist an dieser Stelle, dass ein Angreifer ausschließlich an den Daten des Infotainment-Systems interessiert sein kann. In diesem Fall ist der Zugriff auf das IVI ausreichend. Die Hürde, das IVI zu infiltrieren, ist bei Weitem niedriger als zusätzlich den CAN-Bus zu übernehmen. Ende Juli 2015 teilte der Hacker Samy Kamkar über seinen Twitter- und Youtube-Account mit, dass eine als geschlossen markierte Lücke im OnStar RemoteLink, Teil des IVIs von General Motors, wie zuvor genutzt werden kann, um in das Infotainment-System einzudringen. Kamkars Forschungen zeigen, dass wie in der Home-Automation eine Kopplung des Smartphones an das Fahrzeug eine weitere Quelle für zahlreiche Schwachstellen sein kann. [14]

Die oftmals direkte Anbindung des IVIs an die unterschiedlichen internen Bus-Systeme des Fahrzeugs und die voranschreitende Aufgabenzentrierung führen zu einem unübersichtlichen Funktionsumfang und zu einer schwachen Kohäsion der einzelnen Baugruppen. Hieraus können unzählige Angriffsvektoren durch bereits übliche Technologien geerbt (z. B. Angriffe auf den Bluetooth-Stack) oder neue Angriffsvektoren durch ungünstige Anwendung von Technologien und Standards erzeugt werden. Eine solche Kombination nutzten Miller und Valasek im obigen Beispiel aus, um über eine manipulierte Medien-Datei Zugriff auf das Infotainment-System zu erhalten. Diese Schwachstelle verwendeten die beiden Sicherheitsforscher, um Nachrichten auf dem CAN-Bus abzusetzen. Das mangelnde Design eines vorsätzlichen Single-Point-of-Failure lässt diesen kausalen Hack zu. [13][15]

Abbildung 10: Typisches OBD USB KKL Diagnoseinterface [16]

Der Diagnostik-Bus

Um die Emissionswerte neuer Fahrzeuggenerationen einfacher und regelmäßiger kontrollieren zu können, schreiben die USA und Europa seit den späten 1980er-Jahren die Präsenz eines OBD(On-Board-Diagnose)-Ports vor. Es sollte damit sichergestellt werden, dass Emissionswerte nicht nur zum Zeitpunkt der Zulassung, sondern

über den gesamten Lebenszyklus des Fahrzeuges hinweg innerhalb des Toleranzbereichs bleiben. [2]

Aus Sicht eines Angreifers bietet der OBD-II-Port eine mächtige Schnittstelle, um Daten in das fahrzeuginterne Kommunikationsnetz zu senden oder verschiedenste Informationen aus den einzelnen Steuergeräten zu erhalten. Diese Schnittstelle stellt für das Sicherheitskonzept eines jeden Fahrzeugs eine große Bedrohung dar, da ein direkter Zugang aus der nicht vertrauenswürdigen Fahrgastzelle in den sensiblen High-Speed- bzw. Low-Speed-CAN-Bus ermöglicht wird. Oftmals ist der OBD-II-Port leicht zu erreichen. Er befindet sich häufig in der Nähe der Fahrzeugsteuerung bzw. unter einer Abdeckung im Armaturenbrett. Es ist für einen Angreifer ein Leichtes, an diesem Port mit der entsprechender Konnektivität (siehe Abbildung 10) schadhafte Soft- oder Hardware in das Fahrzeug einzuschleusen. [17]

Description	Domain
Engine Load	$0 \ldots 100\,\%$
Engine Coolant Temperature	$-40 \ldots 215\,^{\circ}\mathrm{C}$
Suction Pipe Pressure	$0 \ldots 255\,\mathrm{kPa}$
Speed	$0 \ldots 255\,\mathrm{km/h}$
Accelerator Pedal Position	$0 \ldots 100\,\%$
Operating Time	$0 \ldots 65535\,\mathrm{min}$
⋮	⋮

Abbildung 11: Auswahl verschiedener OBD-Messwerte nach [2]

Im November 2015 gelang es einer Gruppe von Hackern, eine unveränderte 2013 Corvette mithilfe eines OBD-II-Dongles zu infiltrieren und die Kontrolle über nahezu jede Funktion des Fahrzeugs zu erhalten. Dazu reichte der OBD-II-Dongle sowie eine von den Sicherheitsforschern versendete SMS, um die mangelhaften Schutzmechanismen zu überwinden. Der ab Baujahr 2000 in fast jedem Fahrzeug verbaute OBD-II-Port führt zu einer neuen Bedrohung durch präparierte Hardware. Gerade im Güter- oder Personentransport werden für das Flottenmanagement sog. TCUs (Telematic Control Units) eingesetzt. Das sind kleine konnektive Geräte, die meist über Mobilfunktechnologien eine Brücke zwischen der fahrzeuginternen Diagnose (z. B. dem OBD-II-Port) und dem Management-System des Fahrzeugeigners herstellen. Somit ist es für den Eigentümer möglich, Daten (siehe Abbildung 11) wie Position, Geschwindigkeit, Route und vieles mehr live aus dem Fahrzeug zu erhalten, um damit z. B. eine höhere Auslastung oder niedrigere Versicherungsbeiträge der Transportflotte zu erzielen. [18]

Um effizient das World Wide Web nach internetfähigen Geräten abzusuchen, existieren Suchmaschinen wie „Shodan“. Dieser Crawler sucht das Internet nach aktiven Geräten ab und kartografiert deren erreichbare Dienste. Es lässt sich z. B. für einen Web-Server auflisten, welche Ports geöffnet sind und mit welchem „Welcome-Text“ der Server auf Anfragen reagiert. Da jeder Dienst einen individuellen Header zur Begrüßung neuer Clients versendet, kann der Crawler zwischen der unterschiedlichen Software, die den Dienst zur Verfügung stellt, differenzieren. Diesen für Sicherheitsforscher extrem nützlichen Dienst nutzte der Programmierer Jose Carlos Norte, um eine Liste ganz bestimmter TCUs des Herstellers C4Max zu erhalten. Dabei suchte er gezielt nach der Header-Response, die das Gerät bei einem Einwahlversuch auf dem am Port 23 lauschenden Telnet-Servers ausliefert. Norte stellte dabei in einer ersten Suche fest, dass er über 733 dieser Einheiten direkt aufdecken konnte. Natürlich liegt das unter anderem an der Natur eines Nutzfahrzeugs, nicht zu jeder Zeit verwendet zu werden, und dementsprechend sind TCUs nur während der Betriebszeiten im Internet erreichbar. Das Problem mit diesen Gateways ist, dass sie ab Werk kein Passwort verwenden, um administrativen Zugriff auf den Dongle zu erhalten. Nun kann jeder, der eines dieser Systeme entdeckt, ohne Passwort eine Reihe Informationen abgreifen oder einschleusen. Es ist möglich, neben der Position des Fahrzeugs auch CAN-Bus-Nachrichten über den Dongle in den Powertrain zu senden. Wie im ersten Abschnitt beschrieben, ist diese Rechteeskalation mit einem administrativen Vollzugriff auf ein reguläres Computersystem vergleichbar. [19][20]

Auch das FBI (Federal Bureau of Investigation) hat bereits, zusammen mit dem Department of Transportation und der National Highway Traffic Safety Administration, auf die Gefahr sog. Car Gadgets reagiert. In einem Public Service Announcement warnen die Behörden ausdrücklich davor, ungeprüfte Car Gadgets in das eigene Fahrzeug einzubringen bzw. ganze Fahrzeugflotten mit diesen Dongles auszurüsten. Weitere Schutzmechanismen werden im nächsten Abschnitt vorgestellt. [21]

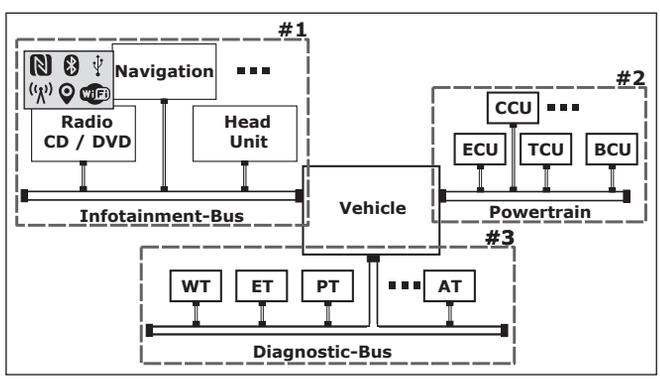

Abbildung 12: Level 0 Threat-Model

Schutzmechanismen – IT Security und Kryptografie

Aus den vorangegangenen Abschnitten kann ein sog. Bedrohungsmodell (engl. threat model, siehe Abbildung 12) aufgestellt werden. Um die Übersicht zu erhöhen und um die Komplexität zu reduzieren, beschränkt sich das Bedrohungsmodell auf die in den letzten Abschnitten angesprochenen Netzwerke und Komponenten. Die drei informationsverarbeitenden Systeme Diagnostik, Power-

train und Infotainment sind in der Abbildung 12 nummeriert dargestellt. Im Folgenden soll auf die drei Teilsysteme eingegangen und bereits existierende bzw. notwendige Strategien zur Verbesserung der IT-Security vorgestellt bzw. vorgeschlagen werden.

Infotainment-System (# 1)

Die hohe Konzentration verschiedenster Zuständigkeiten erhöht die Komplexität der Betriebssoftware eines Infotainment-Systems enorm. Mit jedem weiteren Feature steigt die innere Komplexität, jede Funktion zu beherrschen. Softwareentwickler müssen bei der Umsetzung all dieser Anforderungen darauf achten, bei jeder Schicht des Systems kein Fehlverhalten zuzulassen bzw. Fehlerzustände kontrolliert abzuhandeln. Abbildung 13 zeigt einen grundlegenden Application Stack (ohne Anspruch auf Vollständigkeit). Es ist leicht zu erkennen, dass viele unterschiedliche Softwarepakete kombiniert werden müssen, um das gesamte Funktionsspektrum abzudecken. Verständlicherweise steigt mit jedem zusätzlichen Feature der Aufwand, die unterschiedlichen Abhängigkeiten und Versionen zu verbinden und zu verwalten.

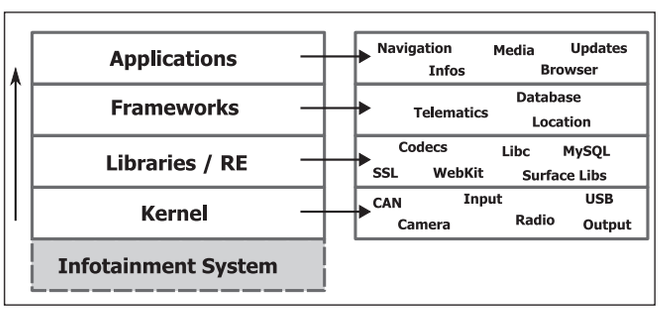

Abbildung 13: Vereinfachter Application Stack

Um die Angriffsfläche zu verringern, muss das Infotainment-System aus Sicht eines Angreifers betrachtet werden. Ein durchschnittliches IVI bietet unzählige Eingabemöglichkeiten, die im Application Stack unterschiedlich verarbeitet werden. Der Angreifer hat eine sehr große Auswahl an Eingabemöglichkeiten, die jede für sich Fehleingaben oder gezieltes Ausnutzen bekannter Schwachstellen ermöglicht. Mit jedem neuen Feature gewinnt ein Angreifer so eine neue Möglichkeit hinzu, in das System einzudringen. Durch die enge Verzahnung des Infotainment-Systems mit den kritischen Infrastrukturen wie dem High- bzw. Low-Speed-CAN ist es nach Eindringen in das IVI nur eine Frage der Zeit und des Aufwandes, bis ein Angreifer erfolgreich auf den Triebstrang oder andere sensible Systeme und Assistenten einwirken kann. Nur eine strickte Trennung der Zuständigkeiten (hohe Kohäsion) und eine lose Kopplung der einzelnen Komponenten kann hier für mehr Sicherheit sorgen. Es soll nicht möglich bzw. sehr schwierig sein, dass ein Angreifer eine Schwachstelle, z. B. im Media Framework, ausnutzt und zugleich Zugriff auf sicherheitskritische Netzwerkkomponenten erhält. Es darf nicht nur an einem gemeinschaftlich einheitliches Betriebssystem inklusive Applikation-Stack (wie z. B. AUTOSAR) entwickelt werden, sondern es muss zeitgleich die Netzwerk- und Komponentenstruktur überdacht werden. Klassische und bewährte Sicherheitskonzepte aus der Netzwerktechnik, wie z. B. eine DMZ (Demilitarized Zone), könnten einfach umgesetzt werden. Bereits diese grundlegenden Schutzmechanismen würden das Fahrzeug deutlich besser gegen das Ausnutzen etwaiger Rechteeskalationen auf dem Infotainment-System schützen.

Powertrain(# 2)

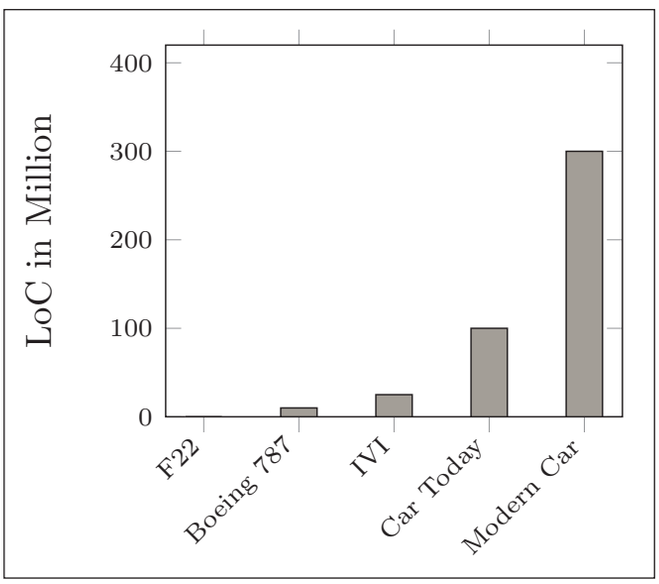

Abbildung 14: Codezeilen (engl. Lines of Code, LoC) in Fahrzeug-ECUs nach [22]

Ist ein Angreifer in diesen Bereich der internen Fahrzeugkommunikation eingedrungen, ist es wegen der im Abschnitt „Der Powertrain“ beschriebenen Schwachstellen, schwierig, weitere Angriffe auf das Fahrzeug zu verhindern. Damit ein Dritter nicht einfach Nachrichten mit einer bestimmten Identität absetzen kann, müssen kryptografische Primitive den Informationsaustausch absichern. Dies kann durch Verschlüsselung der Nachrichten geschehen. Die Verschlüsselung einer Nachricht bedeutet einen zusätzlichen mitunter beträchtlichen Berechnungs- und Verwaltungsaufwand für die einzelnen ECUs und andere Komponenten, deren Softwarekomplexität stetig ansteigt. In einem BMW der 7er-Serie können z. B. über 90 Steuergeräte (Maximalausstattung, Baujahr 2009) verbaut sein, die zum Betrieb über 100 Mio. Zeilen Code abarbeiten müssen, was sogar den Codeumfang einer Boeing 787 übersteigt (siehe Abbildung 14). Je nach Fahrzeug unterscheiden sich diese Steuergeräte in der technischen Spezifikation sowie genereller Aufgabe. Hinzu kommen unzählige Sensoren und Aktuatoren, die die Zahl der Kombinationsfehler, die potenziell auftreten können, noch weiter steigern. Kryptografische Primitive, die im Design schlank genug sind, um möglichst viele dieser unterschiedlichen Hardware-Spezifikationen zu unterstützen, könnten die Vertraulichkeit und Authentizität des gesamten Systems merklich verbessern. Authenti-

fizierte Nachrichten schützen durch Nachrichtensignaturen die Kommunikation vor selbst erzeugten Botschaften durch einen Angreifer. Viele der bereits vorgestellten Angriffszenarios könnten so verhindert, mindestens erschwert werden. [23]

Gerade eingebettete Steuerungen, die meist auf eine Aufgabe reduziert und hardwaretechnisch stark eingeschränkt sind, können den Mehraufwand an Rechenzeit, um kryptografische Berechnungen oder Security-Mechanismen auszuführen, nicht leisten. Sind leistungsstarke ECUs hinreichend abgesichert, kann ein Angreifer den Umweg über eine schwächere Steuerung eines Sensors oder Aktuators wählen. Es ist wirtschaftlich nicht sinnvoll, alle Steuergeräte im Fahrzeug auf ein Leistungsniveau umzurüsten, das die Mindestanforderungen kryptografischer Primitive erfüllt. Der Abschnitt „Der Powertrain“ zeigt, welche grundlegenden Schwachstellen in vielen Angriffen die Basis für den Erfolg des Angreifers bilden.

- Keine Authentizität / Vertraulichkeit – CAN-Botschaften enthalten keinerlei Information über den Sender noch sind Schutzmechanismen vorhanden, die eine Rechtmäßigkeit der Nachricht bezeugen. Jeder Teilnehmer kann jede Botschaft erzeugen.

- Abstreitbare Botschaften – Fehlende Identifikatoren, z. B. durch eine Signatur, geben keine Information über die Quelle einer Nachricht. Es ist für einen Bus-Teilnehmer schwer bis unmöglich, festzustellen, welcher anderer Teilnehmer falsche bzw. schadhafte Nachrichten sendet.

Eine durch Forscher der University of Michigan vorgeschlagene Alternative, das sog. CIDS (Clock-based Instruction Detection System), überwacht die Kommunikation aller Bus-Teilnehmer und analysieren die Metadaten jeder CAN-Botschaft. Dabei werden bei periodisch versendeten Nachrichten (die die Masse der Botschaften ausmachen) zeitspezifische Eigenschaften des Senders protokolliert, sog. Zeitvarianzen. Diese entstehen z. B. durch nicht synchronisierte Hardware-Uhren der einzelnen Steuergeräte. Da eine Synchronisation der Uhren eine zu große Auslastung auf dem Bus erzeugen würde, wird meist darauf verzichtet. So können aus jeder Botschaft, senderspezifisch, Zeitcharakteristiken extrahiert werden. Diese Charakteristiken dienen als Fingerabdruck, der jeder Nachricht anhaftet und den Sender eindeutig identifizieren kann. Nach der Anlernphase des CIDS sucht das System nach Nachrichten, die von den vorher analysierten Zeitvarianzen abweichen. Erkennt das Gerät eine solche Botschaft, können verschiedenste Gegenmaßnahmen getroffen werden. Der Motor könnte in den Notlauf versetzt oder der Fahrer über die Unstimmigkeit informiert werden. Einzig aperiodische Nachrichten, die in einer ereignisgesteuerten Kommunikation auftreten, können durch das System nur schwer bis unmöglich detektiert werden. Viele Kommunikationsmodelle verzichten jedoch auf aperiodische Nachrichten, da ein Ausfall einer Steuereinheit durch periodisch auftretende Botschaften besser erkannt werden kann – bleibt eine Nachricht aus, so wird davon ausgegangen, dass sich die verantwortliche ECU in einem Fehlerzustand befindet. [24]

Diagnostik-Bus und OBD-II (# 3)

Der Diagnostik-Bus ist unter Verwendung des OBD-II-Protokolls nicht nur ein beliebtes Angriffsziel für Sicherheitsforscher. Bereits gewöhnliche Autodiebe verwenden Technologien, um über die Diagnoseschnittstelle die Alarmanlage und die Wegfahrsperre moderner Fahrzeuge abzuschalten. Das Wall Street Journal berichtete im Juli 2016, dass Autodiebe mithilfe eines Notebooks einen 2010 Jeep Wrangler stahlen. Die naheliegendsten Erklärungen gehen davon aus, dass die Diebe über die Diagnoseschnittstelle neues Schlüsselmaterial in das Fahrzeug einbrachten, um die Diebstahlsicherungen zu umgehen. [25]

Ein einfacher Weg, unerlaubten Zugriff auf den Diagnose-Port zu verhindern, wäre der Einsatz eines Hardware-Schalters im Innenraum des Fahrzeuges, der die Diagnoseschnittstelle bei Bedarf physikalisch von der Fahrzeugkommunikation trennt. Da in Zukunft nur noch schlüssel- bzw. kontaktlose Entriegelungen des Fahrzeugs im Einsatz sein werden, muss für einen solchen Schalter ein geeigneter Ort im Fahrzeug gefunden werden, für den ein echter Schlüssel unnötig ist. Ist der Port physikalisch deaktiviert, ist es für einen Angreifer nicht mehr so trivial, Hardware an dem Diagnostik-Bus zu betreiben. Auch schadhafte Dongles, die in ein unbeaufsichtigtes, offen stehendes Fahrzeug eingebracht werden könnten, können nicht direkt auf den Bus einwirken. Ein Angreifer muss einen deutlich größeren Aufwand betreiben, was die Angriffsfläche des Diagnostik-Busses folglich verkleinert. [6]

Abbildung 15: Kleiner Daten-Logger mit einer USB-Schnittstelle [26]

Auch Miller und Valasek haben einen OBD-Dongle vorgeschlagen, der im OBD-II-Port des Fahrzeugs angeschlossen wird (siehe Abbildung 15). Als eher klassisches

IDS (Intrusion Detection System) erzeugt der Dongle ein Profil der Botschaften auf dem Bus-System. Viele Diagnose-Nachrichten sind, z. B. während der Fahrt, äußerst untypisch, werden aber von Angreifern sehr oft verwendet, um auf den Powertrain einzuwirken. Erkennt der Dongle eine dieser Nachrichten, so kann der Fahrer informiert oder das Fahrzeug kontrolliert angehalten werden. Ist ein Angreifer über den Einsatz eines IDS informiert, kann er Nachrichten dennoch so absetzen, dass ein IDS unberechtigte Botschaften nicht erkennen kann. Ähnlich wie Virenscanner würde ein solches System ein falsches Sicherheitsgefühl erzeugen. Es kann jedoch eine ausgezeichnete Ergänzung und weitere Hürde in einem schlüssigen Sicherheitskonzept sein. [6]

Zusammenfassung

In dieser Arbeit wurde aufgezeigt, dass aktuelle Fahrzeugreihen mehr denn je von Angriffen auf die Kommunikation und Datenverarbeitung betroffen sind. Außerdem wurden erste grundlegende Vorschläge benannt, um Maßnahmen zur Steigerung der IT-Sicherheit im Auto zu ergreifen. Jedoch betrachten viele Hersteller das moderne Fahrzeug als ein Fortbewegungsmittel, das durch aktuelle Technologie verbessert werden soll. Geht es um funktionale Sicherheit, sind diese Fahrzeuge auf allerhöchstem Niveau. Dies zeigt die Auswertung des Statistischen Bundesamtes aller Verkehrsunfälle in Deutschland 2014. So sind in diesem Jahr in nur 3624 Fällen technische Mängel Ursache für einen Unfall. Das sind nicht mehr als 0,15 Prozent der 2.406.685 polizeilich erfassten Verkehrsunfälle. Die kontinuierliche Verbesserung aller Systeme, die für die funktionale Sicherheit zuständig sind, führt jährlich zu einem Rückgang der Unfälle mit Personenschaden. In der Realität ähneln Kraftfahrzeuge eher einem fahrbaren Computer. Im Gegensatz zur Unfallstatistik steigen die Zahlen der Cyber-Angriffe auf Fahrzeuge. Aus diesem Grund ist es für die zukünftige Sicherheit auf den Straßen notwendig, dass die IT-Sicherheit in den fahrenden Computern Gegenstand aktueller Forschung bleibt und stärker ausgebaut wird. Vor allem kryptografische Primitive und Protokolle haben sich in der herkömmlichen IT bewährt und sollten auf ihre Tauglichkeit für Fahrzeugkommunikation hin untersucht werden. Auch hochmoderne leichtgewichtige kryptografische Verfahren versprechen effizient die Kommunikation absichern zu können. Hierzu müssen weitere Untersuchungen durchgeführt und Testumgebungen geschaffen werden. Ob diese oder andere Verfahren alle oder wenigstens einige der sicherheitstechnischen Probleme in der Fahrzeugkommunikation lösen können, wird die Zukunft zeigen. [27]

Referenzen:

[1] Andy Greenberg. Gm took 5 years to fix a full-takeover hack in millions of onstar cars. https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/. Abgerufen: 08.08.2016.

[2] Werner Zimmermann und Ralf Schmidgall. Bussysteme in der Fahrzeugtechnik, 5., aktualisierte und erweiterte Auflage. Springer Vieweg, 2014.

[3] Craig Smith and Eric Evenchick. Car hacking tools. http://livestream.com/internetsociety2/hopeconf/videos/130605456. Abgerufen: 16.08.2016.

[4] EE JRW. Can bus node. https://upload.wikimedia.org/wikipedia-/commons/c/c0/CAN Node.png. Abgerufen: 31.08.2016 Lizenz: CC BY-SA 4.0 Modifiziert durch: b.weigl@oth-aw.de.

[5] Nigel Smart. ECRYPT II Yearly Report on Algorithms and Keysizes. European Network of Excellence in Cryptology II, 2011.

[6] Charlie Miller and Chris Valasek. Adventures in Automotive Networks and Control Units. www.ioactive.com, 2013.

[7] Andy Greenberg. Hackers reveal nasty new car attacks – with me behind the wheel. http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video. Abgerufen: 03.08.2016.

[8] Marcus Börger. Gegenüberstellung bestehender Echtzeit-Netzwerk-Konzepte. Marcus Börger, 1998.

[9] Miro Enev, Alex Takakuwa, Karl Koscher, and Tadayoshi Kohno. Automobile Driver Fingerprinting. Proceedings on Privacy Enhancing Technologies, 2016.

[10] The Car Spy. 2006 porsche cayenne 4.5 turbo s. http://flickr.com/photos/25632349@N04/4722323724, 2010. Abgerufen: 23.08.2016 Lizenz: CC BY-2.0 Modifiziert durch: b.weigl@oth-aw.de.

[11] Charlie Miller and Chris Valasek. Remote Exploitation of an Unaltered Passenger Vehicle. www.illmatics.com, 2015.

[12] Staff of Senator Edward J. Markey. Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk. Ed Markey – United States Senator of Massachusetts, 2015.

[13] Andy Greenberg. The jeep hackers are back to prove car hacking can get much worse. https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. Abgerufen: 23.08.2016.

[14] Samy Kamkar. Ownstar – hacking cars with onstar to locate, unlockand remote start vehicles. https://www.youtube.com/watch?v=3olXUbS-prU&feature=youtu.be. Abgerufen: 23.08.2016.

[15] Tommi Mäkilä, Jukka Taimisto, and Miia Vuontisjärvi. Fuzzing Bluetooth Crash-testing bluetooth-enabled devices. Frontline Test Equipment www.fte.com, 2011.

[16] Florian Schäffer. Typisches obd usb kkl diagnoseinterface. https://upload.wikimedia.org/wikipedia/commons/7/79/Obd usb-kkl interface.jpg, 2012. Abgerufen: 25.08.2016 Lizenz: CC BY-SA 3.0 Modifiziert durch: b.weigl@oth-aw.de.

[17] Craig Smith. The Car Hacker's Handbook – A Guide for the Penetration Tester. No Starch Press, 2016.

[18] Andy Greenberg. Hackers cut a corvette's brakes via a common car gadget. https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/. Abgerufen: 30.08.2016.

[19] Shodan. https://www.shodan.io/. Abgerufen: 31.08.2016.

[20] Jose Carlos Norte. Hacking industrial vehicles from the internet. http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html. Abgerufen: 31.08.2016.

[21] Federal Bureau of Investigation (FBI), Department of Transportation, and National Highway Traffic Safety Administration. Motor vehicles increasingly vulnerable to remote exploits. https://www.ic3.gov/media/2016/160317.aspx. Abgerufen: 23.08.2016.

[22] Andrew Patterson. Automotive infotainment systems: Open source drives innovation. http://embedded-computing.com/articles/automotive-source-drives-innovation/. Abgerufen: 06.09.2016.

[23] Harald Richter. Elektronik und Datenkommunikation im Automobil. Institut für Informatik, Technische Universität Clausthal, 2009.

[24] Kyong-Tak Cho and Kang G. Shin. Fingerprinting electronic control units for vehicle intrusion detection. In 25th USENIX Security Symposium (USENIX Security 16), pages 911–927, Austin, TX, August 2016. USENIX Association.

[25] Jeff Bennett. Thieves go high-tech to steal cars. http://www.wsj.com/articles/thieves-go-high-tech-to-steal-cars-1467744606. Abgerufen: 07.09.2016.

[26] Florian Schäffer. Texa obd log. small data logger with a usb interface for transferring logs. https://upload.wikimedia.org/wikipedia/commons/a/aa/Texa obd-log.png. Abgerufen: 07.09.2016 Lizenz: CC BY-SA 3.0 Modifiziert durch: b.weigl@oth-aw.de.

[27] Statistisches Bundesamt. Verkehr – Verkehrsunfälle – 2014. Statistisches Bundesamt, 2014.

Fördergeber:

Die Autoren danken der Bayerischen Forschungsstiftung (BayFor) und demForschungsverbund FORMUS³IC „Multi-Core safe and software-intensiveSystems Improvement Community“ für die finanzielle Unterstützung.
Förderkennziffer AZ-1165-15.

Bayerische
Forschungsstiftung

Kontakt:

Benjamin Weigl

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Laboratory for Safe and Secure Systems (LaS³)
Kaiser-Wilhelm-Ring 23
92224 Amberg

b.weigl@oth-aw.de

Prof. Dr. Andreas Aßmuth

Ostbayerische Technische
Hochschule (OTH) Amberg-Weiden
Fakultät Elektrotechnik, Medien
und Informatik
Laboratory for Safe and Secure Systems (LaS³)
Kaiser-Wilhelm-Ring 23
92224 Amberg

a.assmuth@oth-aw.de