IT-Sicherheit im Automobil

F. Hartung, M. Hillgärtner, G. Schmitz, M. Schuba, F. Adolphs, J. Hoffend, J. Theis
ISiA Research Group
FH Aachen, University of Applied Sciences, Eupener Str. 70, 52066 Aachen

Kurzfassung

Die zunehmende Vernetzung elektronischer Steuergeräte, Sensoren und Aktoren in Fahrzeugen gibt Anlass zur Sorge, dass die Elektronik von außen angreifbarer wird. Im Forschungsprojekt IT-Sicherheit im Automobil werden Bord-Netze, Multimedia-Systeme und Kontroll-Einheiten sowie Schnittstellen und Protokolle im Automobil analysiert. Diese Untersuchungen werden durchgeführt, um die Gefährdung der Insassen im Falle einer gewollten Manipulation beispielsweise durch Hacking-Angriffe zu vermeiden und somit die Sicherheit zu gewährleisten bzw. zu verbessern.

1 Einleitung

Mit den ständig wachsenden Anforderungen an Komfort, Konnektivität und Transparenz der Systeme im Automobil (wie z.B. der Anbindung von Smartphones und der Nutzung von Apps) kommen zusätzliche Schnittstellen zum Einsatz. Diese Zugangspunkte sind im Bereich von Infotainment/Multimedia (WLAN, Bluetooth, Mobilfunknetze) sowie auch bei der Diagnose-Schnittstelle (OBD2) zu finden. Sie stellen ein immer größeres Potential für den kriminellen Zugriff (Cracking) für das Fahrzeug dar.

Ist es dem Angreifer erst einmal gelungen in das Bord-Netz des Fahrzeuges einzudringen, besteht die Gefahr, dass dieser die Kontrolle über Infotainment-Systeme, Motorsteuerung, Getriebe und im schlimmsten Fall sogar die Bremsen oder die Lenkung übernehmen kann, was die Sicherheit der Insassen gefährdet und im Extremfall zu einer tödlichen Gefahr werden kann [1].

Die Forschergruppe, die im Jahr 2013 gegründet worden ist, hat im ersten Schritt eine Analyse der Elektrik/Elektronik (E/E) Architektur und der IT-Infrastruktur eines modernen Automobils in Bezug auf Sicherheit sowie die Identifizierung von möglichen Einfallstoren durchgeführt. Neben dem Multimedia- und Infotainment-System mit Anbindung eines Smartphones im Fahrzeug ist die Diagnoseschnittstelle mit der Verbindung zum zentralen Gateway-Modul ein weiterer Schwerpunkt der Untersuchungen.

2 IT-Struktur im Fahrzeug

Die IT-Struktur in Fahrzeugen unterliegt einem ständigen Wandel. Anfang der 80er Jahre wurde in den Volumenmodellen noch vergleichsweise wenig Elektronik eingesetzt und die Basisfunktionalität beschränkte sich auf die Antriebseinheit (Motor mit Zusatzaggregaten wie Anlasser oder auch Scheibenwischer etc.). Die Anforderungen des Marktes und des Gesetzgebers nach immer leistungsfähigen und wirtschaftlichen Fahrzeugen bei erheblich reduzierten Abgasemissionen erforderten nicht nur eine Optimierung der mechanischen und thermodynamischen Eigenschaften des Antriebstrangs, sondern auch im Bereich des Fahrkomfort und Sicherheit. Das führte dazu, immer mehr Elektronik und Softwarefunktionen einzusetzen. Daraus entstanden viele Innovationen, die dazu beigetragen haben, dass heute die elektronische Ausstattung den Fahrer und das Fahrzeug in verschiedenen Gebieten wie Motorsteuerung, Komfort und Sicherheit unterstützt. ABS, ESP und auch die elektrische Lenkkraftunterstützung (EPS) ermöglichen eine immer bessere Unterstützung des Fahrers. Der Bereich Multimedia und Navigation spielt heutzutage eine immer größere Rolle. Hier zu nennen ist die Telefonie, Radio/ CD' s, Media Interfaces (z.B. Bluetooth, USB und Speicherkarten) sowie TV/ Entertainment Systeme. Zusätzlich erhöhen sich die Anforderungen an die Kommunikation, beispielsweise Notrufe über das Mobilfunknetz absetzen zu können oder auch die Möglichkeit, das Smartphone über WLAN oder Bluetooth mit dem Infotainment System zu verbinden und integrieren.

Auf dem Gebiet der E/E- Architektur haben Komponenten wie elektronische Steuergeräte (ECU‘s), Sensoren, Aktoren und standardisierte Bussysteme (z. B. CAN, MOST, Flexray und Ethernet) Einzug gehalten.

2.1 Analyse der Infrastruktur

Die Kommunikation im Fahrzeug kann in eine interne Kommunikation und externe Kommunikation aufgeteilt werden. Der Datenaustausch zwischen dem Motorsteuergerät und dem Dashboard ist ein Beispiel für die interne Kommunikation und das Auslesen des Fehlerspeichers des Fahrzeugs über die OBD Schnittstelle mit dem Abgastester während der Abgasuntersuchung oder die Integration des Mobiltelefons an das Infotainment- System sind beispielhalft für die externe Kommunikation zu nennen.

Aufgrund der funktionalen Komplexität in den Fahrzeugen besteht die Notwendigkeit, dass diverse Netzwerke eingesetzt werden. Wie in Abbildung 1 gezeigt, werden unterschiedliche Bussysteme im Fahrzeug betrieben. Neben dem CAN Powertrain (Aktoren und Sensoren für Motorsteuerung) wird beispielsweise ein weiterer CAN-Comfort Bus für Komfortfunktionen (z.B. Ansteuerung Fensterheber, Türschloss, Klimakontrolle) eingesetzt.

Zudem wird im Bereich der Multimediaeinheit und deren Komponenten LIN, MOST und CAN Bussysteme genutzt. Es besteht oft die Notwendigkeit, dass Daten nicht nur direkt zwischen zwei Steuergeräten ausgetauscht werden, sondern indirekt jedem Busteilnehmer zur Verfügung stehen. Die Verbindung der einzelnen Netzwerke wird über ein zentrales Gateway Modul realisiert.

Mit Hilfe des Gateways können Nachrichten gefiltert werden, d.h. die Informationen sind zum Teil nicht sichtbar, werden jedoch auf Anfrage (Request) versendet. Hier ist als Anwendungsbeispiel die Diagnoseschnittstelle OBD zu nennen, wo mit Hilfe eines Motortesters relevante Abgasdaten und der Zustand des Fehlerspeichers abgefragt werden können.

Ebenfalls sind in dem System drahtlose Netzwerke zu finden. Im Bereich Infotainment wird hier Bluetooth verwendet, um eine Kommunikation zwischen dem Mobiltelefon und dem Infotainment System herzustellen. Dadurch wird das Mobiltelefon integraler Bestandteil im Fahrzeug und kann auch über das Lenkrad (z. B. Freisprecheinrichtung Telefon) bedient werden. Eine weitere Vernetzung in Form eines WLAN Hotspots im Fahrzeug ist in Zukunft möglich. Weiter zu erwähnende Anwendungen, die in Zukunft eine große Rolle spielen werden sind CAR to CAR (C2C) und CAR to Infrastructure (C2I). Mit der Nutzung von Bluetooth und WLAN Adaptern an der OBD Schnittstelle, werden teils auch drahtlose Netzwerke für die Kommunikation über die Diagnoseschnittstelle (OBD) eingesetzt. Diese Schnittstellen ergeben, ähnlich wiebei einem PC Netzwerk, eine Menge Potential, um bösartige Angriffe auszuüben und Funktionen der Komponenten im Fahrzeugnetz zu manipulieren [1].

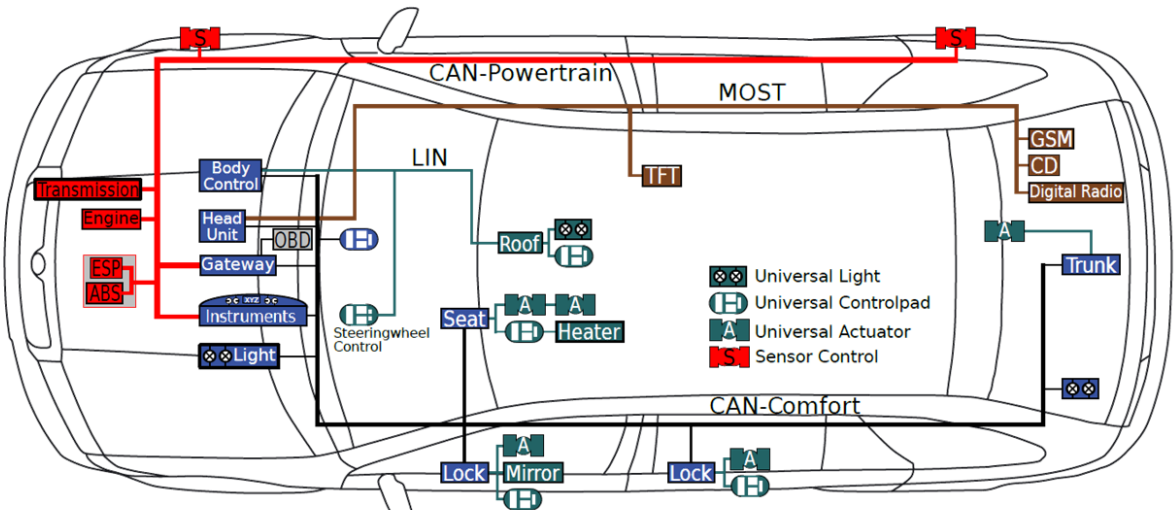

Abbildung 1: Übersicht Netzwerke im Automobil

In weiteren Bericht liegt der Fokus der Untersuchungen auf dem Infotainment System und der OBD Schnittstelle mit der Vernetzung im Fahrzeug.

2.2 Beschreibung möglicher Einfallstore

Wie schon in Abbildung 1 gezeigt, sind die verschiedenen Bussysteme über ein zentrales Gateway Modul verbunden. Ebenfalls ist die gesetzlich vorgeschriebene OBD (On Board Diagnose) Schnittstelle zwischen dem Gateway und der Außenwelt in jedem Fahrzeug vorhanden. Mit einem Laptop und entsprechender Software kann nun eine Verbindung mit den Steuergeräten hergestellt werden. Eine typische Anwendung ist hier die Abfrage abgasrelevante Daten und der Zustand des Fehlerspeichers während der Hauptuntersuchung mit Prüfung des Abgasverhaltens, die an jedem Fahrzeug regelmäßig durchgeführt werden muss. Interessant ist hier, dass die Abfrage dieser Daten ohne eine Authentifizierung mit den Steuergeräten erfolgt. Physikalisch ist der CAN Bus (Diagnose CAN) und zum Teil auch schon Ethernet in der OBD Buchse integriert. Mit Hilfe von Adaptern, die mit dem Diagnose Interface verbunden werden können, werden die OBD Betriebsdaten, die in der SAE 1979 Norm beschrieben werden, von außen abgefragt und dargestellt. Die Beschaffung dieser Adapter und der Software ist sehr einfach, da hier viele Anbieter zur Verfügung stehen. Zudem sind das Protokoll und der Nachrichtenaufbau für OBD2 in der Norm beschrieben und daher zwingend für jedes Fahrzeug, welches in Europa betrieben wird.

Es besteht aber auch die Möglichkeit, neben der Abfrage von Daten auch Nachrichten in das Fahrzeug zu senden und damit gezielt ungewollte Funktionen auszulösen. Der Inhalt der Nachrichten ist nicht wie bei OBD2 standardisiert oder in einer gesetzlichen Norm beschrieben, jedoch werden auch hier Protokolle beschrieben und angewendet. KWP 2000 Protokoll findet hier Anwendung, welches in Zukunft mehr und mehr von dem UDS (Unified Diagnostic Services) Protokoll abgelöst wird. Auf Basis dieser Kommunikationsprotokolle werden Updates und die Kodierung von Steuergeräten durchgeführt, wobei ein Authentifizierungsvorgang nötig ist. Die OBD Diagnose Buchse wird als Einfallstor betrachtet und ist mit verschiedenen Methoden im Hinblick auf die IT-Sicherheit untersucht worden.

Ein großes Potential der Angreifbarkeit des Automobils stellt ebenso das Infotainment dar, da es heutzutage direkt mit dem Fahrzeug-Bord-Netz verbunden ist.

Daten wie sie für den Board-Computer benötigt werden, können über solche Multimedia-Systeme abgerufen werden. In moderneren Fahrzeugen können zudem personalisierte Einstellungen exportiert und eingespielt werden wie beispielsweise Fahrereinstellungen wie Sitz- und Lenkradeinstellungen. Auch können persönliche Kontakte und Mitteilungen auf dem System gespeichert werden, die nicht für Jedermann zugänglich sein sollten.

Ein manipulierter Updatevorgang eines solchen Systems, der beispielsweise über die USB-Schnittstelle oder einer CD-ROM eingespielt werden kann, könnte während der Fahrt die genannten Einstellungen ändern und dadurch Ablenkung oder Schaden anrichten.

3 Praktische Untersuchungen

Untersuchungen sind im Bereich der OBD Schnittstelle und im Infotainment System durchgeführt worden.

3.1 Untersuchungen im Bereich OBD Schnittstelle

Die aufgeführten Untersuchungen wurden an verschiedenen Fahrzeugen durchgeführt, um Unterschiede und auch Gemeinsamkeiten in den Nachrichten (Botschaften) zu erkennen, die über die OBD Schnittstelle ausgetauscht werden. Die Fahrzeuge waren vom Baujahr 2008 und jünger und die Kommunikation für die OBD Daten erfolgte über die CAN Bus Schnittstelle.

Im ersten Schritt wurde an der OBD Schnittstelle ein Adapter mit passender Software eingesetzt, um OBD Daten aus dem Fahrzeug auszulesen. Die Verbindung zwischen dem OBD Adapter und dem PC wurde über USB hergestellt. Die OBD Daten und auch der relevante Fehlerspeicher konnten ausgelesen werden. Ein aufgetretener Fehler wie z. B. ein nicht ordnungsgemäßer abgeschlossener Regenerationsprozeß für den Rußpartikel Filter konnte hier zurückgesetzt bzw.

gelöscht werden. Für die Anfrage der OBD Daten aus dem Fahrzeug sowie das Rücksetzen der Fehlerspeicher wird keine Authentifizierung für die Verbindung zwischen dem PC und dem Fahrzeug benötigt.

Im zweiten Schritt wurden die CAN Nachrichten untersucht, die während einer OBD Session übermittelt werden. Hierzu wurde mit einem CAN Analysetool Datenlogfiles erzeugt und ausgewertet. Es konnte ermittelt werden, welche Daten aus dem Software Tool an das Fahrzeug gesendet (Request an das Fahrzeug) und welche darauf hin empfangen (Response aus dem Fahrzeug) wurden.

In Schritt drei wurde nur ein CAN Analyse Tool direkt an den OBD Port angeschlossen und wiederholt CAN Nachrichten analysiert, die permanent auf dem Diagnose CAN Netzwerk zur Verfügung stehen, ohne das Anfragen (Request) gestellt werden. Zudem wurden schrittweise verschiedene Bedienfunktionen im Fahrzeug wie beispielsweise Zündung ein, Radio ein, Blinker-Betätigung oder Licht einschalten, durchgeführt. Hier wurde in den Ergebnissen Unterschiede zwischen den Fahrzeugen festgestellt. Bei zwei Fahrzeugen fiel eine Veränderung der CAN Botschaften in Abhängigkeit der Bedienung auf. Im Gegensatz dazu war in einem Fahrzeug nur eine einzige CAN Botschaft zu sehen, sobald die Zündung eingeschaltet wurde. Durch die Auswertung der CAN Botschaften konnten Funktionen und Bedeutung mit Hilfe von Reverse Engineering ermittelt werden, die dann anschließend in das Fahrzeugnetzwerk gesendet wurden. Bei einem Fahrzeug konnten beispielsweise Dashboardanzeigen angesteuert werden.

In Schritt 4 wurde an einem Fahrzeug mit einer spezifischen Diagnose- und Parametrier-Software in Kombination mit dem CAN Analysetool Tests durchgeführt, indem elementare Funktionen im Fahrzeug über diese Software aktiviert und parametriert wurden. Im Anschluß erfolgte eine Auswertung der CAN Botschaften, die dann wiederum über den OBD Diagnose Anschluß in das Fahrzeug gesendet wurden. Man war in der Lage, Funktionen zu aktivieren, die in verschiedenen Steuergeräten im Fahrzeug überwacht und ausgeführt werden. Man konnte z. B. das Radio einschalten und die Lautstärke regeln oder auch das Abblendlicht, das Fernlicht und die Rücklampen einzeln ansteuern. Die Steuerung der Klimaanlage sowie eine Manipulation im Dashboard konnten durchgeführt werden, in dem beispielsweise eine Drehzahl und die Geschwindigkeit im Dashboard angezeigt wurde, obwohl das Fahrzeug stand bzw. der Motor nicht lief. Es machte kein Unterschied, ob das Fahrzeug gefahren wurde oder sich im Stillstand befand. Eine spezielle Authentifizierung zwischen dem Sender (z. B. Laptop) und dem Fahrzeug findet dabei nicht statt.

3.2 Untersuchungen im Bereich Infotainment System

Die Motivation der Untersuchungen im Bereich des Infotainments steht im Zusammenhang mit der steigenden Anzahl der eingebetteten Systeme im Automobil, die in der Abbildung 2 dargestellt wird. Es wird prognostiziert, dass die Anzahl der weltweit aufgelieferten vernetzten Infotainment Systeme in den kommenden fünf Jahren auf einen sechsfachen Wert ansteigt [2].

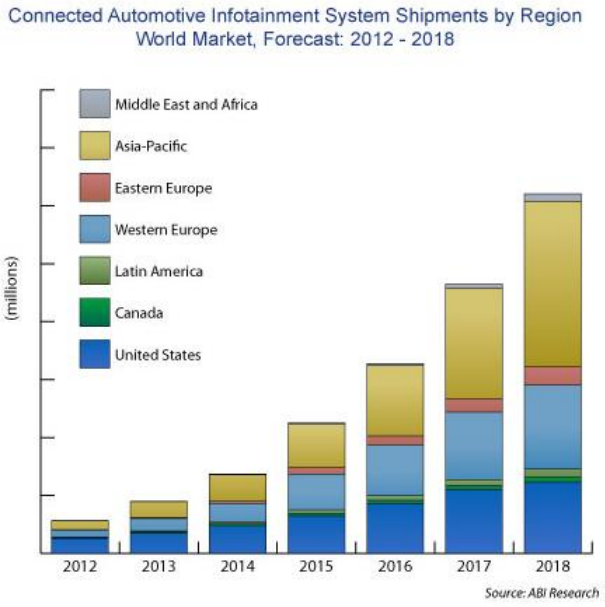

Abbildung 2: Prognose der weltweit verkauften, vernetzten Infotainment Systeme

Ein starker Trend zeigt auch [3], dass der Einsatz modernen Infotainment Systeme durch Unix und Linux-ähnliche Betriebssysteme ermöglicht wird, die Schnittstellen wie standardmäßige Computer bereitstellen. Abbildung 3 zeigt eine Prognose der Betriebssysteme in Infotainment Systemen. Zusätzlich zu USB, Bluetooth, WLAN und Ethernet finden auch Peripherieschnittstellen zu

Abbildung 3: Prognose der Betriebssysteme in Auto Motiven Infotainment Systemen

Steuergeräten und dem Mobilfunknetz eine Anwendung.

Grundlegend basieren moderne Infotainment Systeme auf den Strukturen und Ansätzen bestehender Informationssysteme. Die Problematik wie etwa der langen Lebenszyklus und wenig Wartungsaufwand stellt eine große Hürde dar, da bekanntwerdende Sicherheitslücken nur mit einem sehr hohen und kostspieligen Aufwand behoben werden können.

Weitere Gefahren kommen hinzu, wenn kompromittierte mobile Geräte (wie beispielsweise Smartphones) mit solchen Infotainment Systemen verbunden werden.

In ersten Untersuchungen wurden Schnittstellen betrachtet, die für den Fahrzeugbesitzer durch einfachen Zugriff erreichbar sind. Dabei konnten bei den untersuchten Systemen festgestellt werden, dass Sicherheitsmaßnahmen beim Verbinden von mobilen Geräten durch Authentifizierungsprozesse vorgenommen werden (beispielsweise bei der Bluetooth-Verbindungen).

Weiterhin werden Vorgänge der Firmware-Aktualisierung untersucht, die meist per USB- oder die Diagnoseschnittstelle eingespielt werden können. Für den Austausch der Daten wird kein einheitliches Konzept angewendet. Es werden teils Roh-Daten auf einem USB-Datenspeicher bereitgestellt, die von der Einheit im Automobil erkannt und entgegengenommen werden. Weitere Infotainment Systeme akzeptieren wiederum nur Dateien, die durch Prüfsummen und asymmetrische Schlüssel zertifiziert sind.

Ein Umgehen eines solchen Algorithmus könnte zur Folgen haben, dass das Einspielen von Schadsoftware möglich wird. Eine Kommunikation zwischen Infotainment System und Steuergeräte über das Bordnetz (CAN- oder MOST-Bus) könnte zur Übernahme des Fahrzeuges führen. Ein Beispiel eines solchen Zugriffes auf das Bordnetz und deren verheerende Folgen wurde bereits auf der DefCon-Konferenz 2013 in Las Vegas gezeigt [4].

4 Zusammenfassung

Die beschriebenen Untersuchungen und die Ergebnisse im Bereich der OBD Schnittstelle zeigten, dass eine Gefahr der Manipulation und daraus entstehenden Sicherheitsrisiken in Abhängigkeit der Anwendungssoftware durchaus existiert. Es ist jedoch zu berücksichtigen, dass die vorliegenden Ergebnisse fahrzeugspezifisch

und daher nicht als allgemein gültig anzusehen sind.

Im Bereich Infotainment System soll die Angreifbarkeit dieser Systeme weiter erprobt werden, um eventuell auftretende Schwachstellen frühzeitig zu erkennen. Das Ziel weiterer Untersuchungen ist eine Bewertung des Zustands des gesamten Systems in Hinsicht auf die IT-Sicherheit im Automobil.

Im Endeffekt zielt das Projekt grundsätzlich auf die Verbesserung der Sicherheit aller möglichen Einfallstore für Manipulationen an der Fahrzeugelektronik.

5 Literatur

[1] Center for Automotive Embedded System Security (CAESS), Experimental Security Analysis of a Modern Automobile, http://www.autosec.org/pubs/cars-oakland2010.pdf, Datum des Zugriffs: 13. Dezember 2013

[2] ABIresearch, „Connected Automotive Infotainment System Shipments to Exceed 62 Million by 2018 as Feature Set Explodes“, https://www.abiresearch.com/analyst-insider/archive/9/, Datum des Zugriffs: 11. Dezember 2013.

[3] IHS, „Linux to Take the Lead in Automotive Infotainment Operating System Market“, http://press.ihs.com/press-release/design-supply-chain-media/linux-take-lead-automotive-infotainment-operating-system-mar, Datum des Zugriffs: 11. Dezember 2013.

[4] CNET, „Car hacking code released at DefCon“, http://news.cnet.com/8301-1009_3-57596847-83/car-hacking-code-released-at-defcon/, Datum des Zugriffs: 10. Dezember 2013.