Angriff aufs Auto

Wenn der Hacker auf dem CAN-Bus sitzt

29.03.16 | Autor / Redakteur: Bernd Schöne / Stephan Augsten

Moderne Fahrzeuge erfordern, dass die Autobauer die traditionellen Bus-Systeme überdenken und zusätzlich absichern. (Bild: BMW Group)

Die Auto-IT hat ein Problem: Forscher der Allianz-Versicherungsgruppe haben unzulängliche Wegfahrsperren und Netzwerke ohne ausreichenden Schutz aufgespürt. Viele Fehler kommen Sicherheitsexperten bekannt vor – aus der Büro-IT vor 20 Jahren. Die Folgen können dramatisch sein. Der Fahrer verliert die Kontrolle über sein Gefährt.

Dass Rechnernetze angreifbar sind, hat sich weitläufig herumgesprochen. Eines der wichtigsten Wirtschaftsgüter scheint noch weitgehend ungeschützt zu sein: Das (intelligente) Auto. Fahrzeuge aller Hersteller sind mittlerweile eine Ansammlung an computergesteuerten Komponenten, die über diverse Bussystem miteinander in Kontakt stehen.

Auch in diesem Bereich ist nicht neu, dass solche Systeme angreifbar sind, doch über konkrete Angriffsvektoren wurde bislang von unabhängiger Seite wenig berichtet. Der Computers-Sicherheitsspezialist Stephan Gerhager von der Allianz Versicherungsgruppe gab auf der Sicherheitskonferenz IT-Defense der Cirosec GmbH erstmals einer breiten Fachöffentlichkeit detailiert Einblick in Forschungen beim Münchner Autoversicherer Allianz.

ERGÄNZENDES ZUM THEMA

Über das Allianz Zentrum für Technik
Über das Allianz Zentrum für Technik

Die Allianz Versicherungsgruppe versichert nicht nur viele Autos in Deutschland, sondern auch zahlreiche Zulieferer und OEMs. Das Interesse der Allianz an bekannten und unbekannten Risiken bei Automobilen ist daher verständlich und auch keineswegs neu. Das Allianz Zentrum für Technik in Ismaning bei München forscht seit 1971 auf den Gebieten Reparaturforschung und Schadensverhütung „rund ums Blech“. Hier wurden Crashteststandards entwickelt und zudem dafür gesorgt, dass nicht jeder Stoßstangerempler ein Versicherungsschaden wird.

Dort hatten die Vorfälle rund um die Hacker-Angriffe auf Autos der Marke Jeep in den USA für Aufregung gesorgt. Charlie Miller und Chris Valasek demonstrierten im US-Fernsehen, wie sie aus einem Kilometer Entfernung über Funkbefehl die Kontrolle über ein Auto vom Typ Jeep Cherokee übernahmen, und das Vehikel und seine Insassen in den Straßengraben bugsierten.
Als Folge der Versuche musste der italienisch-amerikanische Autobauer Fiat Chrysler Automobiles (FCA) in den USA 1,4 Millionen Autos zurückrufen. Betroffen waren Modelle der Marken Dodge, Ram und Jeep. Als Einfallstor diente den Hackern ein Mobilfunkmodul im Infotainment-Bereich des Autos, das es so in Europa nicht gibt. Doch viele Komponenten sind gleich oder ähnlich. Schlummern unterm Blech ungeahnte Risiken? Diese Frage stellte sich der IT-Experte Stephan Gerhager.

Studium am offenen Herzen

Als Leiter der Abteilung Informationssicherheit der Allianz beauftragte er einen mit der Materie bereits seit der Ausbildung vertrauten Werksstudenten, sich im Rahmen einer achtwöchigen Bachelor-Arbeit mit den Netzwerken moderner Autos näher zu befassen.

„Wir wollten wissen, ob so etwas auch bei anderen Typen und Marken möglich ist. Das Resultat hat uns etwas beunruhigt“, so Stephan Gerhager.
Reale Autos und Steuersysteme dienten als „Versuchskaninchen“. Mit handelsübliche Analysewerkzeuge schaute das Mini-Team ins Innere der Autosteuerung. Das Ziel: Zunächst die Kommandos der Steuergeräte im Auto verstehen, später Schwachstellen finden um anschließend zu versuchen, das Auto von außen zu kontrollieren. Die aus der Standard-IT bekannten Angriffsvektoren funktionieren auch beim Auto, so das Ergebnis, und sie ließen sich zudem innerhalb kurzer Zeit finden. Im Schnitt reichten ein bis zwei Tage pro Schwachstelle.

Die Krux der Digitalisierung

Moderne Autos können viel, manchmal vielleicht zu viel. Wer hätte sich etwa 1970 träumen lassen, dass ein Auto selbständig per Parkassistent zentimetergenau in eine Parklücke fährt. Inzwischen gibt es bereits Exemplare, die man per App sogar steuern kann. Zum Beispiel in Garagen, die so schmal sind, dass selbst Twiggy nur über das Schiebedach aussteigen könnte.
Möglich sind diese Servicefunktionen durch die seit den 90er Jahren massiv vorangeschrittene Digitalisierung des Autos. In jedem Mittelklasse-Auto fährt mehr IT durch die Landschaft, als in Form des Büro-PCs auf dem Schreibtisch steht. Mehr als einhundert ECUs (Electronic Control Units) sind verbaut.
Die Rechner arbeiten mit spezieller, nur für einen Aufgabenbereich optimierter Software, und sind untereinander über Bussysteme verbunden, die ebenfalls für diesen Aufgabenbereich spezialisiert sind. Enorm schnell, um etwa das Crash-Signale vom Beschleunigungssensor schnell genug an den Airbag weitergeben zu können.
Der Bus verbindet Sensoren, Aktoren und Scheinwerfer. Alle ließen sich beim Jeep manipulieren, zeigten Charlie Miller und Chris Valasek. Sogar das Lenkrad folgte den Funkbefehlen, denn auch hier sitzt ein Motor, damit der Einparkassistent ohne Hilfe des Fahrzeugführers lenken kann. Das diese Busse angreifbar sind, und welche Befehle benötigt werden, darüber hatte zuvor Eric Evenchick auf der Konferenz Black Hat Asia 2015 berichtet.

Einblick in das Bus-System moderner Fahrzeuge

Das Team analysierte zunächst das Rückgrat jedes modernen Fahrzeugs, das Bussystem. Dies verbindet die Sensoren und Aktoren wie das LAN im Büro den PC mit Drucker, Scanner und Internet. Am Bus hängen unter anderem die elektrisch verstellbaren Außenspiegel, das ABS, die Telemetrie und das Infotainment-System. In praktisch jedem modernen Fahrzeug gibt es mehrere dieser Netzwerke, optimiert und

abgestimmt auf die Anforderungen der jeweiligen Aggregate und eingekauft nach strikten Kostenvorgaben, bei denen Zehntelcent den Ausschlag geben.

ERGÄNZENDES ZUM THEMA

Die wichtigsten Bussysteme im Auto

Die wichtigsten Bussysteme im Auto

CAN-Bus (Controller Area Network, verfügbar seit 1986): Der CAN-Bus ist der bis heute der wichtigste Bus im Auto. Er ist echtzeitfähig und dient zusammen mit Flex Ray dazu, die wichtigsten Fahrzeugkomponenten zu steuern, also etwa Bremse, ABS und Motor.
Flex Ray (seit 2000): Dieses serielle, deterministische und fehlertolerante Feldbussystem unterstützt wie erwähnt den CAN-Bus.
LIN-Bus (Local Interconnect Network, seit 2001): Wird vor allem als preiswerte Alternative zur Vernetzung von Türen und motorisch verstellbaren Sitzen verwendet.
MOST-Bus (Media Oriented Systems Transport, seit 2007): Dient vor allem der schnellen Übermittlung von Multimedia-Daten wie Audio- Video- und Sprachsignalen.

Seit 1980 versuchen Automobilfirmen, Geld zu sparen, indem sie zunehmend die parallele Verkabelung von Sensoren und Aktoren durch serielle Feldbusse zu ersetzen. Vor allem der weit verbreitete CAN-Bus ist hoch sensibel, denn er ist der älteste der Bussysteme und verbindet die wichtigsten Teile des Autos. Die Entwickler legten seinerzeit aber keinen Wert auf Authentifizierung oder Schutz vor Falschinformationen durch gehackte Sensoren.
Jeder der mit dem Netz verbunden ist, darf hören und sprechen und kann sich zum “root” machen, wie die Allianz-Forscher herausfanden. Schon ein einfacher, kommerziell verfügbarer CAN-Bus Snifffer ermöglichte es ihnen, den Bus lahmzulegen, indem sie einfach nur die vorher aufgefangenen Signale mit höchster Priorität wiederholten. Ein klassischer DoS-Angriff, wie ihn erstmals Eric Evenchick auf der Black Hat Asia 2015 dokumentierte.

Erstes Kennenlernen per Monitoring

Wer den Bus mit handelsüblichen Analysewerkzeugen beobachtet, lernt zudem schnell, welche Befehle dazu führen, dass sich der Scheibenwischer in Bewegung setzt oder der Außenspiegel verstellt. Schon nach einem Tag Arbeit konnten die Forscher mit dieser

Methode die Scheinwerfer an- und ausschalten sowie die Türen ver- und entriegeln. Alles per direktem Computerbefehl über den CAN-Bus, ganz so, wie Charlie Miller und Chris Valasek bei ihrem Jeep.
Das klingt spektakulär, ist aber kaum ein großes Risiko, denn stets wurde ein direkter Zugriff zum Fahrzeug benötigt. Der Angreifer saß also quasi hinterm Lenkrad und hätte alle Kommandos auch über das Armaturenbrett eingeben können. Natürlich ist es nicht sinnvoll, das Auto, in dem man selbst fährt, mit einem DoS-Angriff auf den Bus selbst lahmzulegen. Allerdings lernte die Techniker so die inneren Abläufe und die Struktur der Befehle kennen.
Gefährlich wird es dann, wenn die Befehle drahtlos auf den Bus gesendet werden können. Immer mehr Fahrzeuge besitzen einen eigenen Mobilfunkzugang, mit dem sich das Gefährt eigenständig mit dem Hersteller verbinden kann, etwa um Serviceberichte zu senden. Die Werkstatt kann dann lange vor einem möglichen Schaden den Halter kontaktieren.
Das ist bequem, aber eben nicht ganz risikolos. Da Mobilfunkeinheit und CAN-Bus miteinander verbunden sind, ist ein Angriff hier zumindest theoretisch möglich. Exakt so lief der Hack des Jeeps in den USA ab. Die beiden Hacker arbeiteten sich vom Mobilfunkteil über den CAN Bus bis hin zu den Steuergeräten vor.

Bessere Abschirmung bei deutschen Fahrzeugen

Ganz so einfach wie in den USA ist es allerdings nicht, wie die Forschungen des Allianz-Teams ergaben. In deutschen Fahrzeugen sind die einzelnen Gerätegruppen durch Segmentierung besser voneinander abgeschirmt, sodass der Angreifer hier zusätzliche Hürden überwinden muss. Außerdem sind alle Serien, auch die ein und desselben Herstellers, stark heterogen aufgebaut.
Das bedeutet: Wer die A-Klasse hacken kann, weiß über die B-Klasse nichts. Ein 3er BMW besteht aus anderen elektronischen Komponenten als ein 5er. Der Hacker muss bei jedem Modell wieder von vorne anfangen. Natürlich sind diese Hürden überwindbar, aber es erhöht den Aufwand beträchtlich.

ERGÄNZENDES ZUM THEMA

Aktuelle Herausforderungen
Aktuelle Herausforderungen

Mit Sorge beobachten Sicherheitsexperten nicht nur die zunehmende Vernetzung durch

Funkmodule, sondern auch einen expandierenden Graumarkt für Manipulationsgeräte. Diese werden verwendet, um bei Gebrauchtfahrzeugen die Kilometerangaben herunterzusetzen, oder das von vielen als störend empfundene Warnsignale bei nicht angelegtem Sicherheitsgurt auszuschalten.
Techniker, die hier einmal Blut geleckt haben, könnten schnell auf den Gedanken kommen, auch mit anderen Befehlen zu experimentieren. Ebenfalls bereits kommerziell erhältlich sind Tools, die Motorleistung per Softwareupdate zu erhöhen. Diese Update-Funktion könnte theoretisch für eine ganze Reihe von Angriffsvektoren genutzt werden, etwa für Sabotage und damit einhergehend Erpressung, denn wer die Motorleistung erhöht, kann sie auch vermindern, und so ganze Fahrzeugflotten lahmlegen.

Generell gilt: je mehr Features der Hersteller eingebaut hat, was insbesondere bei teureren Modellen der Fall ist, desto mehr Angriffsmöglichkeiten bieten sich dem Hacker. Ein Auto ohne Park-Assistenz-Funktion hat auch kein Stellglied an der Lenksäule, dessen Herrschaft der Hacker übernehmen kann.
Um die Segmentierung aufzuheben, müssten wichtige Netzwerkkomponenten eine neue Firmware erhalten, die den Hackern über einen Proxy Zugang verschafft. Diese Hürde scheint überwindbar, etwa durch die Schnittstelle zur On-Bord-Diagnose (OBD 2). Eigentlich als Diagnosesystem gedacht, das während des Betriebs des Autos die Steuergeräte des Autos überwacht und an das Servicepersonal weiterleitet, akzeptiert sie auch Befehle. So ist es möglich, Zugriff auf den Bus und damit auf das Fahrzeug zu erhalten.

Sicherheitsforscher befürworten neue Bus-Systeme

Reale Angriffe wurden während des Vortrages in Mainz nicht demonstriert. Anders als beim Hack des Jeeps in den USA von Charlie Miller und Chris Valasek gelang es dem Mini-Team binnen der selbst gesetzten Achtwochenfrist nicht, sich von der Mobilfunkschnittstelle bis hin zu den Aktoren an der Lenksäule vorzuarbeiten, um das Auto fernzusteuern.
Die Befehle, mit denen die Steuergeräte über den CAN-Bus angesprochen werden, hatten sie aber weitgehend verstanden und gelernt. Mit etwas mehr Zeit und genauerem Studium von Schulungs- und Werkstattunterlagen, hätte das Ergebnis anders ausschauen können.
Ganz generell kritisiert Stephan Gerhager den etwas laxen Umgang mit dem Thema IT-Sicherheit bei den Autobauern. Fahrzeuge lassen sich heute mit gut bekannten

Methoden angreifen und sind so verwundbar wie ein Büro-PC, allerdings mit dramatisch schlimmeren Folgen für die Insassen und die Automobilindustrie.
Jeder Patch-Day bedeutet den Rückruf von Millionen Fahrzeugen in die Werkstatt. Da OEMs und Zulieferer versichert sind, könnte das für alle Beteiligten extrem teuer werden. Es sollte sich also etwas tun.
Stephan Gerhager setzt auf neue Busse. Der wichtige CAN-Bus stammt aus dem Jahr 1986 und sollte dringend überarbeitet werden. Die Erfahrungen aus dem Bereich der Standard -IT sollten zügig Einzug in die Netzwerke der Automobile Einzug halten, etwa durch gegenseitige Authentifizierung auf dem Bus und Schutz der Signale durch starke Kryptographie. Automobilbauer reden viel von Security, meinen aber Safety. Das Wissen um IT-Security Probleme schlummert in der IT Abteilung und findet nur schwer seinen Weg zu den Konstrukteuren.
Die Automobilindustrie denkt allerdings schon weiter, alles soll zur App werden. Ab 2017 will Volvo ganz auf den Zündschlüssel verzichten, Tür öffnen und Auto starten funktioniert dann nur noch über eine App und ein Smartphone, das über Bluetooth mit dem Auto kommuniziert. Hacker dürften sich darüber freuen.

Über den Autor
Bernd Schöne