Dieter Spaar

Auto, öffne dich!

Sicherheitslücken bei BMWs ConnectedDrive

Autos mit eingebautem Modem senden Daten an die Hersteller und der ADAC wollte wissen, was da genau übertragen wird. c't vermittelte einen Experten, der im Auftrag des ADAC die Übertragung am Beispiel von BMWs ConnectedDrive untersuchte. Er stieß dabei auf Sicherheitslücken, die sogar das unberechtigte Öffnen der Fahrzeuge ermöglichten.

Das Internet der Dinge macht auch vor dem großen Ding in der Garage nicht halt: In immer mehr Autos ist bereits ab Werk ein Mobilfunkmodem mit SIM-Karte eingebaut. Je nach Hersteller haben die Modems verschiedene Funktionen: Sie können den Fahrzeuginsassen Internet-Zugang gewähren, Telemetriedaten und Traffic-Infos zum Fahrzeughersteller übertragen sowie bei einem Unfall die Rettungskräfte verständigen. Bei einigen Marken lassen sich außerdem Fahrzeugfunktionen über eine Handy-App fernsteuern, etwa die Standheizung oder das Laden der Antriebs-Batterie von Elektro-Fahrzeugen. Selbst das Ver- und Entriegeln der Türen aus der Ferne ist so möglich.

Zu den auf diesem Gebiet führenden Herstellern gehört BMW; sein ConnectedDrive ist schon seit etlichen Jahren im Einsatz [1]. Ebenso wie c't interessiert sich auch der ADAC unter Aspekten des Verbraucher- und des Datenschutzes dafür, welche Daten dabei übertragen werden [2]. Er hat mich daher beauftragt, dies im Detail zu untersuchen. Mit überraschendem Ergebnis: Obwohl der Fokus gar nicht auf der Sicherheit lag, fanden sich erhebliche Lücken.

Der ADAC stellte für die Untersuchung einige BMW-Fahrzeuge mit ConnectedDrive zur Verfügung, darunter einen 320d Touring. Spezielle Informationen vom Hersteller gab es nicht – nur das, was man im Internet findet.

Um einen ersten Eindruck zu bekommen, untersuchte ich das für ConnectedDrive zuständige Steuergerät. Diese sogenannte Combox gibt es in verschiedenen Varianten. Sie ist unter anderem für Multimediafunktionen wie das Abspielen von Musikdateien von einem USB-Stick oder die Bluetooth-Kopplung eines Mobiltelefons mit der Freisprecheinrichtung zuständig. Sie wird seit 2010 in diversen BMW-Modellen verbaut.

Als Hauptprozessor nutzt die Combox einen SH-4A von Renesas, einen leistungsfähigen 32-Bit-RISC-Prozessor. Die Mobilfunkkommunikation erfolgt über ein GSM/GPRS/EDGE Modul von Cinterion (ehemals Siemens). Außerdem steckt noch ein V850ES-Mikrocontroller von Renesas drin. Er kommt vermutlich wegen seines geringen Stromverbrauchs zum Einsatz, damit das System auch bei abgestelltem Fahrzeug empfangsbereit bleiben kann. Der SH-4A und die daran angeschlossene Peripherie würden die Batterie zu schnell entleeren.

Aufgeschraubt

Für die ersten Experimente baute ich die Combox aus, schloss sie an ein Netzteil an und startete die Notruffunktion, die normalerweise über einen Taster im Fahrzeug ausgelöst wird. Die Belegung der Pins am Steckverbinder für die Stromversorgung und den Notruftaster konnte ich durch Analyse der Bauteile auf der Platine ermitteln. Man findet im Internet aber auch eine BMW-Diagnosesoftware für Werkstätten, in der die Anschlussbelegung der Steuergeräte dokumentiert ist. Um die Kommunikation der Combox mit dem Mobilfunknetz mitschneiden zu können, habe ich in einer Testumgebung mit OpenBSC (siehe c't-Link am Ende des Artikels) und einer davon unterstützten Basisstation ein Mobilfunknetz simuliert.

Beim Notruf versendet die Combox eine SMS und baut danach eine Sprachverbindung auf. Der Inhalt der SMS enthält keinen Klartext und hat keine erkennbare Struktur. Bei jedem Notruf sehen die Daten anders aus, was auf eine Verschlüsselung hinweist.

Um herauszufinden, wo die Daten verschlüsselt werden, habe ich die Kommunikation zwischen dem Mobilfunkmodem und dem V850ES Mikrocontroller mitgeschnitten. Sie erfolgt über eine serielle Schnittstelle. Die Anschlussbelegung des Mobilfunkmodems lässt sich anhand von Datenblättern ermitteln, die man im Internet findet. Da die Daten der Notruf-SMS im Mitschnitt nicht auftauchten, lag die Vermutung nahe, dass die Nachricht im Modem selbst erzeugt und verschlüsselt wird. Das war plausibel, da sich das verwende-

te Mobilfunkmodem um solche benutzerdefinierte Funktionen erweitern lässt.

Ausgelötet

Ich musste also an die Firmware des Modems gelangen. Auf dem Modem-Modul waren keine Standardtestpins (Joint Test Action Group, JTAG) zu finden, über die sich die Firmware eventuell hätte auslesen lassen. Daher musste ich den Flash Chip des Modems auslöten, auf eine Adapterplatine setzen und auslesen. Das ist nicht ganz einfach, da der Chip ein BGA-Gehäuse hat. Man muss daher nach dem Auslöten ein sogenanntes Reballing durchführen. Damit kann man aber auch einen Dienstleister beauftragen [3].

Zum Auslesen der Firmware wurde der Flash Chip auf der Adapterplatine an ein STM32-Evaluationboard mit ausreichend vielen I/O-Pins und dem passenden I/O-Spannungsbereich von 1,8 Volt angeschlossen. Mit einigen Zeilen C-Code ließ sich der Inhalt des Flashspeichers auslesen und über die serielle Schnittstelle des Evaluationboards zum PC übertragen. Zur Analyse der ausgelesenen Firmware nutzte ich das für Assemblercode übliche Tool „IDA Pro“ von Hex-Rays, das die ARM-CPU des Modems unterstützt.

Mit IDA Pro konnte ich sehr schnell verschiedene Verschlüsselungs- und Hash-Algorithmen in der Firmware identifizieren. Denn die gängigen Krypto-Algorithmen verwenden bestimmte Tabellen oder Konstanten, nach denen man automatisiert suchen kann. Mit diesen Informationen konnte ich weitere Code-Teile identifizieren, die diese Verschlüsselungs- und Hash-Algorithmen nutzen.

Schlüsselsuche

Woher stammten aber die Krypto-Schlüssel? Meine optimistische Anfangsvermutung war, dass fahrzeugindividuelle Schlüssel eventuell im V850ES Mikrocontroller gespeichert seien und von dort zum Mobilfunkmodem übertragen würden. Da die Suche danach zunächst zu aufwendig erschien, analysierte ich das beim Notruf verwendete Protokoll weiter. Zeichenketten in der Firmware zeigten schnell, dass offensichtlich NGTP (Next Generation Telematics Protocol) als Grundlage für die Kommunikation dient. Das verwundert nicht weiter, da BMW zu den Hauptinitiatoren von NGTP gehört.

NGTP verwendet die standardisierte Beschreibungssprache ASN.1 (Abstrakte Syntaxnotation Eins) für die Definition des Kommunikationsprotokolls. Man kann in der Firmware erkennen, dass die Beschreibung mit dem Open-Source-Compiler „asn1c“ übersetzt wurde. Anhand der Datenstrukturen in der Firmware und Kenntnissen, wie asn1c arbeitet, lässt sich die ASN.1-Beschreibung des verwendeten Protokolls recht genau rekonstruieren. Dieser Schritt ist nötig, da NGTP keine konkrete Implementierung vorgibt, sondern nur Vorschläge dazu macht.

Als Nächstes machte ich mich erneut auf die Suche nach den Krypto-Schlüsseln. Das NGTP-Protokoll enthält Funktionen zum Update der Schlüssel, was die Vermutung bestärkte, irgendwo seien Schlüssel gespeichert. Doch die Suche blieb lange erfolglos. Quasi als letzten Ausweg untersuchte ich einen auffällig zufällig aussehenden Datenblock in der Firmware. Ich versuchte Teile davon als Schlüssel zu nutzen, um die aufgezeichneten Notruf-SMS zu dekodieren – was nach einigem Experimentieren tatsächlich gelang.

Das war seltsam: Sollte tatsächlich für alle Fahrzeuge identisches Schlüsselmaterial verwendet werden? Andererseits hatte ich bislang nur die Notruf-SMS untersucht. Für diese Anwendung wären identische Schlüssel eher unkritisch.

Ich hatte also herausgefunden, dass zum Verschlüsseln DES (56-Bit-Schlüssel) oder AES128 (128-Bit-Schlüssel) verwendet wird. Für die Signatur von Daten sind drei Methoden implementiert: DES CBC-MAC, HMAC-SHA1 oder HMAC-SHA256. Der verwendete Algorithmus wird im Header der Nachricht angezeigt. Außerdem gibt es für Verschlüsselung und Signatur 16 Paare aus zwei jeweils 64 Bit langen Schlüsseln. Das verwendete Schlüsselpaar wird ebenfalls im Header der Nachricht vermerkt.

Unklar ist, warum BMW die DES-Verschlüsselung benutzt, denn dieser Algorithmus gilt seit Langem als gebrochen. Er hat zwar gegenüber den anderen Krypto-Verfahren eine kürzere Blocklänge, was zu kürzeren Nachrichten führen kann, aber 3DES (Triple-DES) bietet diesen Vorteil ebenfalls und gilt zumindest noch als halbwegs sicher.

Eingebaut

Nach dem erfolgreichen Entschlüsseln und Dekodieren der Notruf-SMS setzte ich die Untersuchung am Fahrzeug fort. Ich wollte herausfinden, ob die Kommunikation bei sicherheitsrelevanten Funktionen besser geschützt ist. Dazu schaute ich mir das ferngesteuerte Entriegeln der Fahrertür näher an.

Um diese Funktion zu nutzen, richtet man einen Account auf dem BMW-Portal ein und schaltet die sogenannten „Remote Services“ frei. Mit den Apps „My BMW Remote“ für iOS und Android lässt sich dann die Fahrertür entriegeln. Um zu verstehen, was dabei genau passiert, musste ich wieder die Kommunikation mitschneiden. Die konnte nur mit einer SMS an das Fahrzeug beginnen, da eine Datenverbindung zum abgestellten Fahrzeug nicht möglich wäre.

Der einfachste Weg, an diese SMS zu gelangen, war die Überwachung der seriellen Schnittstelle zwischen dem Mobilfunkmodem und dem V850ES-Mikrocontroller der Combox. Nachdem ich mit der App eine Entriegelung ausgelöst hatte, fand sich in den aufgezeichneten Daten tatsächlich

Bild: ADAC

Die geöffnete Combox: Dieses Steuergerät im BMW stellt unter anderem die Online-Verbindung für ConnectedDrive her. Das Modem dafür befindet sich rechts oben auf der Platine.

Bild: D. Spaar

Mit einer Basisstation wie der SysmoBTS (oben) oder der nanoBTS lässt sich ein Mobilfunknetz simulieren, um den Datenverkehr des eingebuchten Steuergeräts zu belauschen.

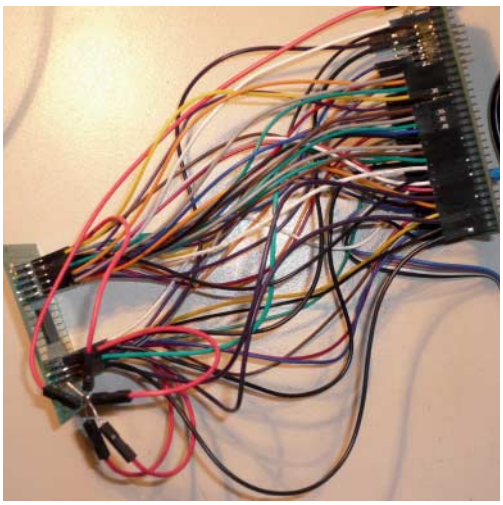

Bild: D. Spaar

Der Flashspeicher des Modems muss ausgelötet und auf eine Adapterplatine (links) gesetzt werden. Der Aufbau zum Auslesen mutet zwar abenteuerlich an, funktioniert aber.

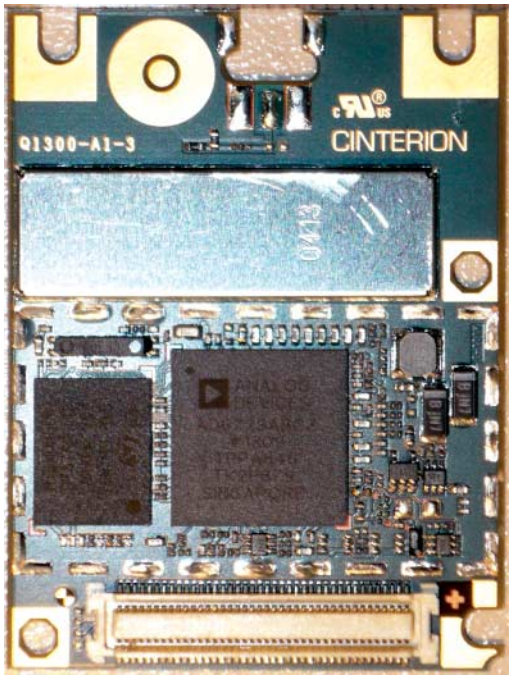

Bild: D. Spaar

Das Modem-Modul der Combox verschlüsselt Daten, die per SMS verschickt werden.

die vom Fahrzeug empfangene SMS. Es handelt sich offensichtlich um eine Art Debug-Nachricht, da die eigentliche Verarbeitung der SMS im Mobilfunkmodem erfolgt.

Die Nachricht ließ sich mit Kenntnis der Krypto-Algorithmen und Schlüssel-Tabelle problemlos dekodieren und analysieren. Dann habe ich im simulierten Mobilfunknetz eine Kopie der SMS erneut ans Fahrzeug geschickt (Replay-Angriff), um dessen Reaktion zu beobachten.

Nachdem das Fahrzeug die SMS empfangen hatte, dauerte es etwa eine Minute, bis das System um den Hauptprozessor hochgefahren war. Dann baute die Combox über das Mobilfunknetz eine Datenverbindung zum BMW-Backend und versuchte, von dort Daten abzurufen. Da ohne Öffnungsbefehl keine Daten vorlagen, brach die Kommunikation ab; weiter passierte nichts. Die SMS hatte also zum Öffnen nicht ausgereicht, sondern nur den Abruf weiterer Anweisungen vom Backend ausgelöst (siehe Infografik auf S. 89).

Das Unglaubliche daran: Die Kommunikation zwischen Fahrzeug und BMW-Backend ließ sich im simulierten Mobilfunknetze problemlos mitschneiden. Denn das Fahrzeug schickte einen einfachen HTTP-GET-Request an den Server. Es gab keine Transportverschlüsselung per SSL oder TLS.

Um herauszufinden, welche Daten das Fahrzeug vom BMW-Backend erwartet, musste ich vor dem Replay der SMS lediglich mit der App die Entriegelung auslösen. So lagen auf dem Server Daten für das Fahrzeug bereit, die es abrief. Kurz danach wurde die Tür entriegelt.

Auch diese Daten ließen sich mit den bisher gewonnenen Kenntnissen entschlüsseln und analysieren. Als Protokoll diente wiederum NGTP. Im Unterschied zur SMS wurde lediglich ein anderes Verschlüsselungs- beziehungsweise Signaturverfahren verwendet, AES128 anstelle DES und HMAC-SHA256 anstelle DES CBC-MAC. Die Schlüsseltabelle war dieselbe.

Einbruch

Damit waren alle Informationen vorhanden, um alle an der Türfernentriegelung beteiligten Komponenten zu simulieren: Ich konnte mit selbst erzeugten Daten das Fahrzeug öffnen. Dazu waren nur die Basisstation und ein Laptop notwendig, der die gefälschte SMS schickte und sich als Backend-Server von BMW ausgab.

Doch würden die bei der Kommunikation verwendeten Schlüssel tatsächlich auch bei anderen Fahrzeugen funktionieren? Tests mit mehreren BMWs bestätigten dies. Dabei kamen auch noch weitere Erkenntnisse hinzu. So können in Fahrzeugen mit ConnectedDrive durchaus die Remote Services deaktiviert sein, wodurch die Fernentriegelung nicht funktioniert. Die Aktivierung des Dienstes kann aber ebenfalls per simuliertem Mobilfunknetz erfolgen und läuft ähnlich ab, wie bereits bekannt.

Dabei erhält das Fahrzeug eine SMS, die es anweist, eine neue Konfiguration vom BMW-Backend zu laden. Dies tut es per einfachem HTTP-GET-Request; das Format der Daten ist unverschlüsseltes XML und ohne größere Probleme verständlich. Die Konfiguration ist nicht gegen Manipulation geschützt, was man etwa durch eine Signatur einfach erreichen könnte. Daher lassen sich im simulierten Mobilfunknetz problemlos zuerst die Remote Services im Fahrzeug aktivieren, um danach die Tür zu entriegeln.

Immerhin gibt es in den ans Fahrzeug adressierten Nachrichten ein Element, anhand dessen es prüft, ob korrekt adressiert ist: die Fahrgestellnummer oder neudeutsch VIN (Vehicle Identification Number). Stimmt die VIN nicht, führt das Fahrzeug die gewünschte Aktion nicht aus. Aber auch das stellte kein Hindernis dar, denn freundlicherweise erwies sich die Combox als sehr kooperativ: Wenn sie eine ansonsten gültige NGTP-SMS erhielt, in der lediglich die VIN falsch war, so antwortete sie mit einer Fehler-SMS, ebenfalls im NGTP-Format. Die enthielt als Absender die korrekte VIN des Fahrzeugs.

Bei der Untersuchung an weiteren Fahrzeugen waren auch sehr aktuelle Modelle dabei. Bei einigen ist die Combox durch andere Steuergeräte ersetzt: Die Multimedia- und Freisprechfunktionen sind in der sogenannten Headunit (Bordcomputer, Navigation und Infotainment) integriert, für die Mobilfunkkommunikation ist die TCB (Telematic Communication Box) zuständig. Sie beherrscht zusätzlich zu GSM/

Betroffene Fahrzeuge und was zu tun ist

Der ADAC hat BMW über die Erkenntnisse informiert und als Verbraucherschützer Abhilfe gefordert. Der Hersteller bestätigte die Sicherheitslücken. Demnach sind alle mit ConnectedDrive ausgestatteten Modelle der Marken BMW, Mini und Rolls Royce betroffen, die zwischen März 2010 und dem 8. Dezember 2014 produziert wurden. Das sind in Deutschland rund 423 000 Fahrzeuge, weltweit 2,2 Millionen. Der ADAC hat eine Aufstellung der über 50 betroffenen Modelle veröffentlicht (siehe c't-Link).

BMW wurde vor der Veröffentlichung nach Absprache ausreichend Zeit eingeräumt, um Maßnahmen zu treffen. Eine über Mobilfunk ausgelöste Konfigurationsänderung hat mittlerweile die Transportverschlüsselung der Daten bei den betroffenen ConnectedDrive-Diensten aktiviert. Dabei wird laut BMW auch das Zertifikat des Servers geprüft.

Die Besitzer können jedoch nicht selbst erkennen, ob ihr Fahrzeug die Änderung erhalten hat. Wer hierüber Gewissheit erlangen will, kann sich bei der BMW-Hotline unter 0 89/1 25 01 60 10 erkundigen. Dies wird besonders bei Fahrzeugen empfohlen, die in den vergangenen Monaten in Tiefgaragen oder an anderen Orten ohne Mobilfunkempfang gestanden haben oder bei denen die Starterbatterie zeitweise abgeklemmt war. Über die Funktion „Dienste aktualisieren“ im Fahrzeugmenü kann man die Änderung selbst auslösen.

GPRS/EDGE auch UMTS. Außerdem ignoriert die TCB Nachrichten mit falscher VIN, statt darauf zu antworten. Die korrekte Fahrgestellnummer lässt sich daher nicht so einfach ermitteln wie bei der Combox. Es werden aber weiterhin die bekannten, für alle Fahrzeuge identischen Schlüssel benutzt.

In der Praxis

Wie könnte nun ein Türöffnen per simuliertem Mobilfunknetz praktisch aussehen? Das nötige Equipment passt in einen Aktenkoffer oder Rucksack. Die Reichweite des simulierten Mobilfunknetzes kann auch in der Stadt hundert Meter und mehr betragen. Es wird so aufgesetzt, dass Telefone das stärkere Signal des simulierten Netzes erkennen und sich dort einbuchen (IMSI-Catcher). Der IMSI-Catcher muss nicht die Telefonnummer des Fahrzeugs kennen, um ihm eine SMS zustellen zu können. Er nutzt die TMSI (Temporary Subscriber Identity), die er beim Einbuchen vergibt. Sollen auch Fahrzeuge mit der TCB geöffnet werden, muss man ein vorhandenes UMTS-Signal mit einem sogenannten Jammer stören, um das Steuergerät zum Fallback auf GSM zu zwingen.

Da sich vermutlich nicht nur Fahrzeuge mit ConnectedDrive in das simulierte Netz einbuchen, ist eine Vorauswahl anhand der IMEI, also der Seriennummer von Telefonen und Mobilfunkmodems sinnvoll. Die ersten acht Ziffern der IMEI identifizieren das Gerät (Type Allocation Code, TAC). Hieran kann man auch zwischen Combox und TCB unterscheiden.

Bei einem Combox-Fahrzeug lässt sich die VIN wie beschrieben ermitteln, danach werden die Remote Services aktiviert und schließlich die Fahrertür entriegelt. Bei Fahrzeugen mit TCB muss man die VIN anders ermitteln. Je nach Auslieferungsland muss sie durch die Frontscheibe zu sehen sein oder sie steht auf einem Etikett im Türrahmen, das man zum Beispiel beim Aussteigen der Insassen fotografieren kann. Das Entriegeln hinterlässt keine Spuren und fällt auch in belebten Straßen nicht auf.

Zusammenfassung

Zum Zeitpunkt der Untersuchung hatte ConnectedDrive sechs Schwachpunkte, die seine Sicherheit kompromittierten:

- BMW verwendet in allen Fahrzeugen dieselben symmetrischen Schlüssel.
- Einige Dienste verzichten bei der Datenübertragung zum BMW-Backend auf eine Transportverschlüsselung.
- Die Integrität der ConnectedDrive-Konfiguration wird nicht geschützt.
- Die Combox verrät mit NGTP-Fehlermeldungen die VIN des Fahrzeugs.
- Per SMS versendete Daten im NGTP-Format werden mit dem unsicheren DES-Verfahren verschlüsselt.
- Die Combox hat keinen Schutz vor Replay-Angriffen.

Diese Probleme wären einfach vermeidbar gewesen. So sind Funktionen zur Transportverschlüsselung durchaus vorhanden, wurden aber nur für einige ConnectedDrive-Dienste genutzt. Außerdem individualisiert der Hersteller die betroffenen Steuergeräte, indem er beispielsweise die VIN einprogrammiert. Dabei sollte es möglich sein, auch fahrzeugindividuelle Schlüssel abzuspeichern.

Dr. Klaus Büttner von BMW Forschung und Technik hatte c't vor einem Jahr im Interview erklärt, die Sicherheit und der autorisierte Zugriff auf das Fahrzeug stünden im Vordergrund der Online-Dienste von BMW. Zum einen würden alle Dienste über ein BMW-eigenes, mit diversen Sicherheits-Features ausgestattetes Backend geroutet, zum anderen würden diese Dienste im Fahrzeug an ein Gateway geroutet, das nur autorisierte und vorher festgelegte Nachrichten und Daten weitergibt.

Im Prinzip traf das zu, doch der Fehler steckte im Detail. Nun hat BMW die Sicherheitslücken nach eigener Aussage durch Einschalten der Verschlüsselung geschlossen (siehe Kasten). Was können aber Fahrzeugbesitzer tun, die dennoch verunsichert sind? Leider gibt es keine Möglichkeit, die Mobilfunkkommunikation von ConnectedDrive bei Bedarf ein- und auszuschalten, ähnlich dem Flugzeugmodus bei Mobiltelefonen.

Man kann zwar ConnectedDrive permanent deaktivieren, das erfordert aber einen schriftlichen Antrag und einen Werkstattbesuch. Als Selbsthilfe könnte man den Antennenstecker an der Combox beziehungsweise an der TCB abziehen. Je nach Fahrzeugmodell ist das einfach möglich, da das Steuergerät unter der Kofferraumabdeckung eingebaut ist. Allerdings wird dadurch auch der automatische Notruf abgeschaltet.

Wer das nicht möchte, muss darauf hoffen, dass die Fahrzeughersteller ausreichende Sorgfalt auf die Details ihrer Online-Systeme verwenden. Der ADAC fordert jedenfalls, dass Computertechnik im Auto zeitgemäß gegen Manipulation und illegale Zugriffe geschützt wird. Dieser Schutz müsse nach Standards erfolgen, wie sie in anderen Branchen längst üblich sind. Außerdem müsse dieser Schutz von neutraler Stelle bestätigt werden, etwa per Common-Criteria-Zertifizierung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in Bonn. (ad@ct.de)

Literatur

[1] Axel Kossel, Internet-Mobil, BMW fährt mit ConnectedDrive, c't 8/09, S. 72

[2] Christiane Schulzki-Haddouti, Schädliche Daten-Emissionen, Wem Ihr Auto was über Sie verrät, c't 19/14, S. 62

[3] Benjamin Benz, Neue Bälle, bitte!, Reparaturtechniken für Chips und Platinen, c't 12/14, S. 84

c't Dokumentation und Software: ct.de/yapx

Angriff auf BMW ConnectedDrive

Wenn der Besitzer in der BMW Remote App die Türentriegelung veranlasst, erhält das Fahrzeug eine SMS vom BMW-Backend. Es holt daraufhin den Öffnungsbefehl von einem Server und führt ihn aus.