Fernüberwachung

OBD2-Dongles im Security-Check

Dongles im Auto sollen Fahr- und Motordaten sammeln, sie aber nur an Befugte weitergeben. Auch andere interessieren sich dafür, fand c't heraus.

Von Ronald Eikenberg

Naturgemäß hantieren OBD2-Dongles und die dazugehörigen Apps mit allerhand interessanten Daten: Koordinaten, umfassenden Fahrzeuginformationen, Zugangsdaten und mehr. In vielen Fällen wird alles in eine Cloud geschickt.

Um herauszufinden, ob und welche Unterschiede es in puncto Datenaufkommen und Sicherheit gibt, haben wir die Dongles aus dem Test auf Seite 108 einer umfangreichen Traffic-Analyse unterzogen. Im Einzelnen waren das die Dongles Bosch Drivelog, TomTom Curfer, Pace Link One, Nonda ZUS Smart Vehicle Health Monitor sowie Thinxnet Ryd (vormals Tanktaler) und Telekom CarConnect. Zusätzlich untersuchten wir auch den Datenverkehr bei Verwendung eines einfachen OBD2-Dongle und der verbreiteten Diagnose-App Torque.

Unser Hauptaugenmerk galt dabei der Online-Verbindung der Dongles. Die meisten Dongles sprechen nicht direkt mit dem Internet, sondern kommunizieren über Bluetooth mit einer Smartphone-App, welche die erfassten Daten auswertet und häufig an externe Server weitergibt. Zwei Testkandidaten, Telekom CarConnect und ThinxNet Ryd, kommunizieren über Mobilfunk direkt mit der Hersteller-Cloud.

Kommunikation belauschen

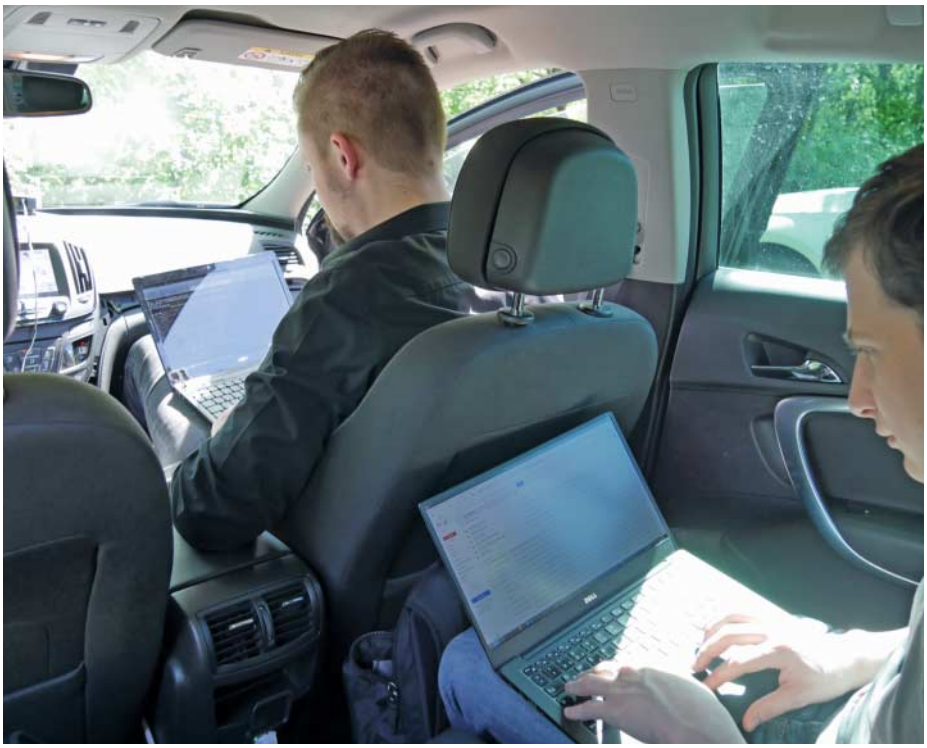
Für die Analyse der App-Kommunikation setzten wir einen Rechner als Man-in-the-Middle-Proxy ein, über den wir die zumeist verschlüsselten Verbindungen im Klartext mitlesen konnten (siehe Grafik). Die Apps installierten wir auf zwei Smartphones, auf denen die alternativen Android-Distributionen Cyanogenmod (Android 6) und LineageOS (Android 7.1) liefen. Als Analyse-Werkzeuge kamen unter anderem die SSL-Proxies sslsplit und Burp zum Einsatz. Damit hatten wir in den meisten Fällen Erfolg.

Jedoch stießen wir auch auf zwei harte Nüsse, die so nicht zu knacken waren: die beiden OBD2-Dongles von Pace und Drivelog. Den ersten Fall konnten wir mit einigem Aufwand lösen, nachdem wir das Authentifizierungsverfahren auseinandergenommen hatten: Die Pace-App nutzt ein Client-Zertifikat, um sich gegenüber dem Hersteller-Server zu authentifizieren. Dieses ist verschlüsselt in der App versteckt, lässt sich jedoch mit einigen Handgriffen extrahieren und in den Analyse-Proxy Burp einfügen. An Drivelog bissen wir uns hingegen die Zähne aus – der Hersteller hat mehrere Anti-Analyse-Verfahren wie Certificate Pinning und eine komplexe Form der Verschleierung (Obfuscation) implementiert, die wir nicht mit angemessenem Zeitaufwand umgehen konnten. Ärgerlich für uns – gut für den Kunden.

Der Datenverkehr der GSM-Dongles wurde in einem funktechnisch abgeschotteten Raum mit einer GSM-Basisstation erfasst, die von einem Software Defined Radio (SDR) aufgespannt wurde.

Schweiger und Quassler

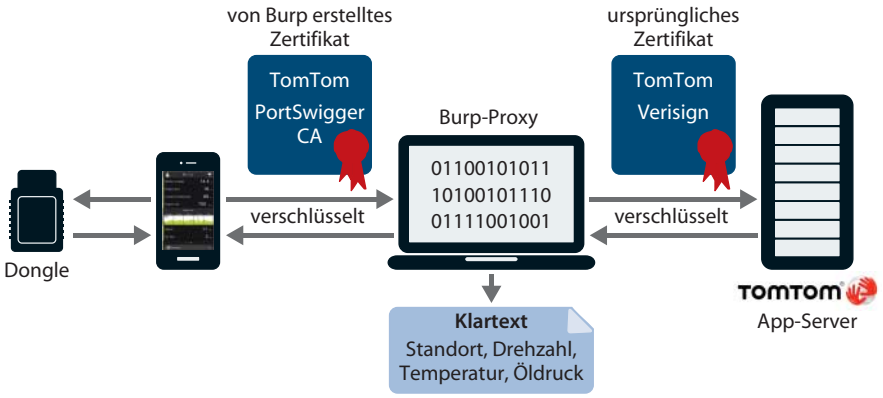
Bei der Auswertung zeigte sich, dass alle Apps das Thema Verschlüsselung ernst nehmen und sensible Daten nach Stand der Technik TLS/SSL-verschlüsselt ins Internet übertragen. Beim Umfang der ausgetauschten Daten gibt es jedoch erhebliche Unterschiede: Während etwa **TomTom Curfer** lediglich mit der Hersteller-Cloud kommuniziert, ist **Nonda ZUS** das andere Extrem und telefoniert nicht nur nach Hause, sondern unter anderem auch mit dem Facebook-SDK, mit dem Tracking-Dienst Amazon Pinpoint, dem Debugging-Dienst Crashlytics, dem Analysedienst Amplitude und dem Backend-Hoster Back4aApp. Der Umfang der übertragenen Daten ist vergleichsweise groß und bezieht sich teilweise auf Produkte



Während umfangreicher Testfahrten schnitten die Tester den Datenverkehr zwischen Dongle und externen Servern mit.

Daten als „Man in the Middle“ abgreifen

Bei verschlüsselten Übertragungen gaukelt der Proxy der Gegenstelle ein vertrauenswürdiges SSL-Zertifikat vor, um Informationen im Klartext lesbar zu machen.



wie die Smart Backup Camera, die hierzulande nicht einmal erhältlich sind. Über Amplitude werden offenbar Daten über die Nutzung der App erfasst.

Zwischen diesen Extremen liegt der **Pace Link One**, der mit dem Hersteller und Facebook kommuniziert.

Drivelog Connect wehrte sich – wie oben geschildert – gegen unsere Traffic-Analyse, wir konnten jedoch mithilfe der SSL-Zertifikate zumindest feststellen, dass die App nicht nur mit ihrem Hersteller, sondern auch mit dem Google-Maps-API sowie mit Analysediensten wie Google Analytics kommuniziert.

Die App von **Telekom CarConnect** spricht unter anderem mit der Hersteller-API, dem Statistikdienst Segment und dem Debugging-Dienst Crashlytics. Der zugehörige Dongle verschickt über das Mobilfunknetz der Telekom offenbar Daten wie seine IMEI unverschlüsselt an die eigene Cloud.

Die zu **Thinxnet Ryd** gehörige App kommuniziert umfassend mit dem Hersteller-API, dem Kartendienst Mapbox und dem IoT-Dienst PupNub. Der Ryd-Dongle bucht sich ins Vodafone-Netz ein und verschickt darüber unter anderem die Fahrzeugidentifikationsnummer (VIN) im Klartext.

Die Kombination aus günstigem Dongle und **Torque**-App überträgt kaum Daten ins Internet. Die App kommuniziert lediglich mit einem Server des Herstellers, um zu überprüfen, ob eine neue Software-Version vorliegt. Zudem überträgt die App Standortanfragen mit Koordinaten an einen Server, der offenbar zu Googles Standortdiensten (Maps) gehört. Zu bemängeln ist, dass die von uns beobachteten Anfragen im Klartext (HTTP) erfolgten.

Eine detaillierte Auswertung der übertragenen Daten würde Bücher füllen; die ausführliche Erläuterung unserer Analyseverfahren sprengt den Umfang dieser Veröffentlichung und ist Gegenstand eines späteren Artikels.

Festzuhalten ist: Wer einen ODB2-Dongle mit Cloud-Anbindung einsetzt, sollte sich darüber im Klaren sein, dass diese Geräte schon prinzipbedingt den Zweck erfüllen sollen, Daten über das Fahrzeug zu erfassen und zu übertragen – und das tun sie auch. Von der Batteriespannung über die aktuelle Umdrehungszahl bis hin zur Kühlmitteltemperatur haben wir alles gefunden. Der Hersteller des Dongles erfährt in den meisten Fällen sehr viel über Fahrzeug, Fahrverhalten und Aufenthaltsort des Fahrzeugs.

Immerhin stießen wir auf keine Übertragungen von Daten, deren Zweck wir uns nicht erklären konnten. Die allgegenwärtige Anbindung an Analysedienste ist kein Phänomen der OBD2-Apps, sondern bei Apps äußerst verbreitet – ganz gleich, ob kostenlos oder kostenpflichtig. Wer großen Wert auf Datensparsamkeit legt und dafür Abstriche beim Komfort in Kauf nimmt, greift zu Torque und einem günstigen OBD2-Dongle. Komfortabler und ebenfalls recht schweigsam ist TomTom Curfer, das zumindest nur mit der Hersteller-Cloud kommuniziert. *(mil@ct.de)* c't