Connect und gehackt

Vernetzte Fahrzeuge und ihre Schwachstellen

Wie sieht die Vernetzung im Fahrzeug heute und morgen aus?

Mit der zunehmenden Anzahl an Fahrerassistenzsystemen, Energierückgewinnungssystemen und ausgefeiltem Infotainment steigt die Anzahl an Steuergeräten in den Fahrzeugen seit dem letzten Jahrzehnt exponentiell.

Dabei stellen die Steuergeräte – je nach Funktion und Sicherheitsrelevanz – unterschiedliche Anforderungen an die Qualität und Geschwindigkeit der Übertragung. Es muss jedoch auch berücksichtigt werden, dass unterschiedliche Übertragungsformen via Kupferkabel oder Glasfaserkabel verschiedene Eigenschaften hinsichtlich Robustheit, Datenübertragungsgeschwindigkeit, Materialkosten, Platzbedarf und Gewicht aufweisen. Während der letzten Jahre entwickelten sich so diverse Bussysteme (LIN, CAN, FlexRay, MOST, Ethernet etc.), weshalb sich in den heutigen Fahrzeugen meist ein Mix an Bussystemen wiederfindet *(Abbildung 1)*.

Die Komplexität der Signalübertragung steigt stetig und bisherige Bussysteme können oft die notwendigen Daten nicht in der richtigen Geschwindigkeit übertragen, sind überlastet oder der

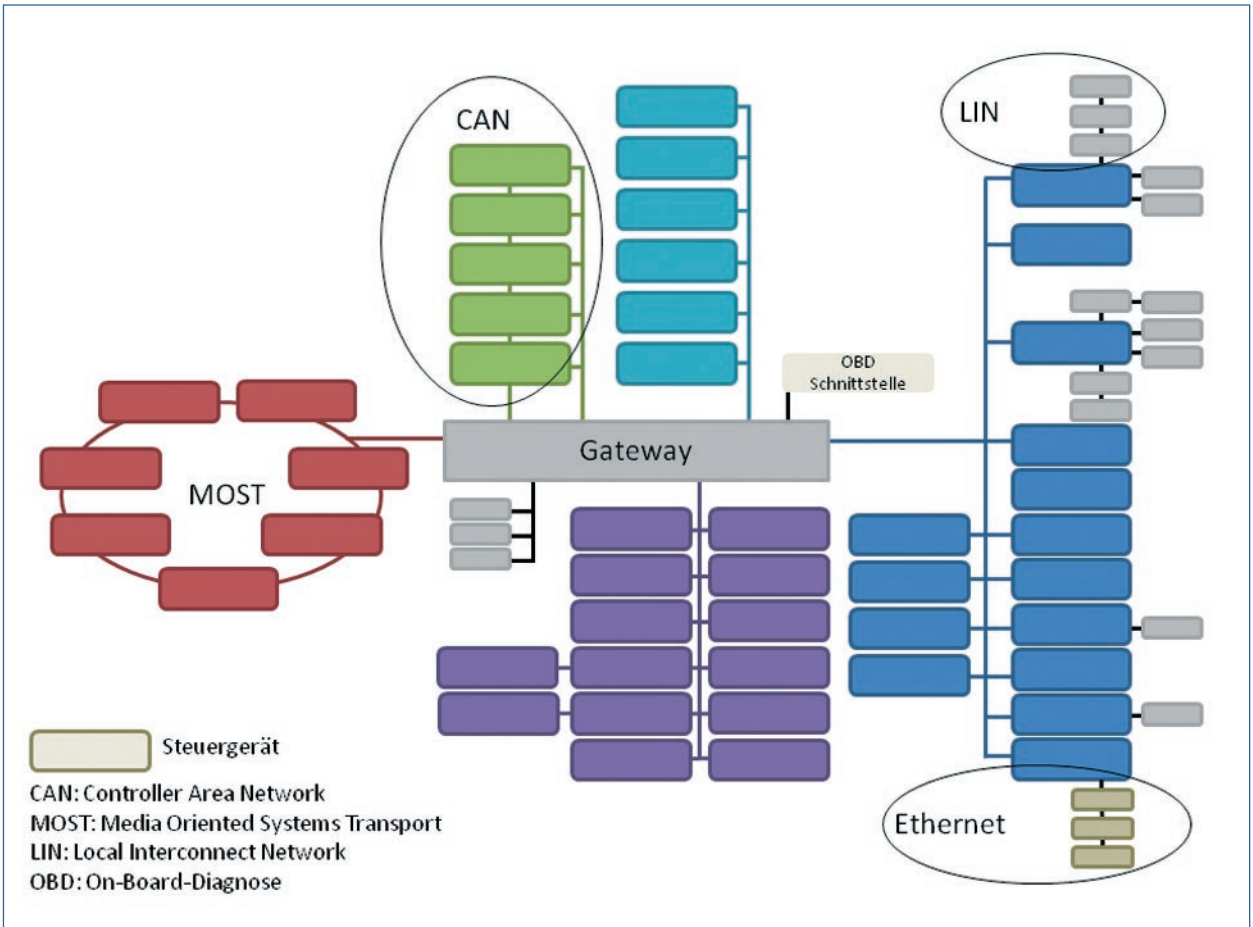

Abb. 1: Schematische Darstellung einer Kombination von diversen Bussystemen im Fahrzeug ■

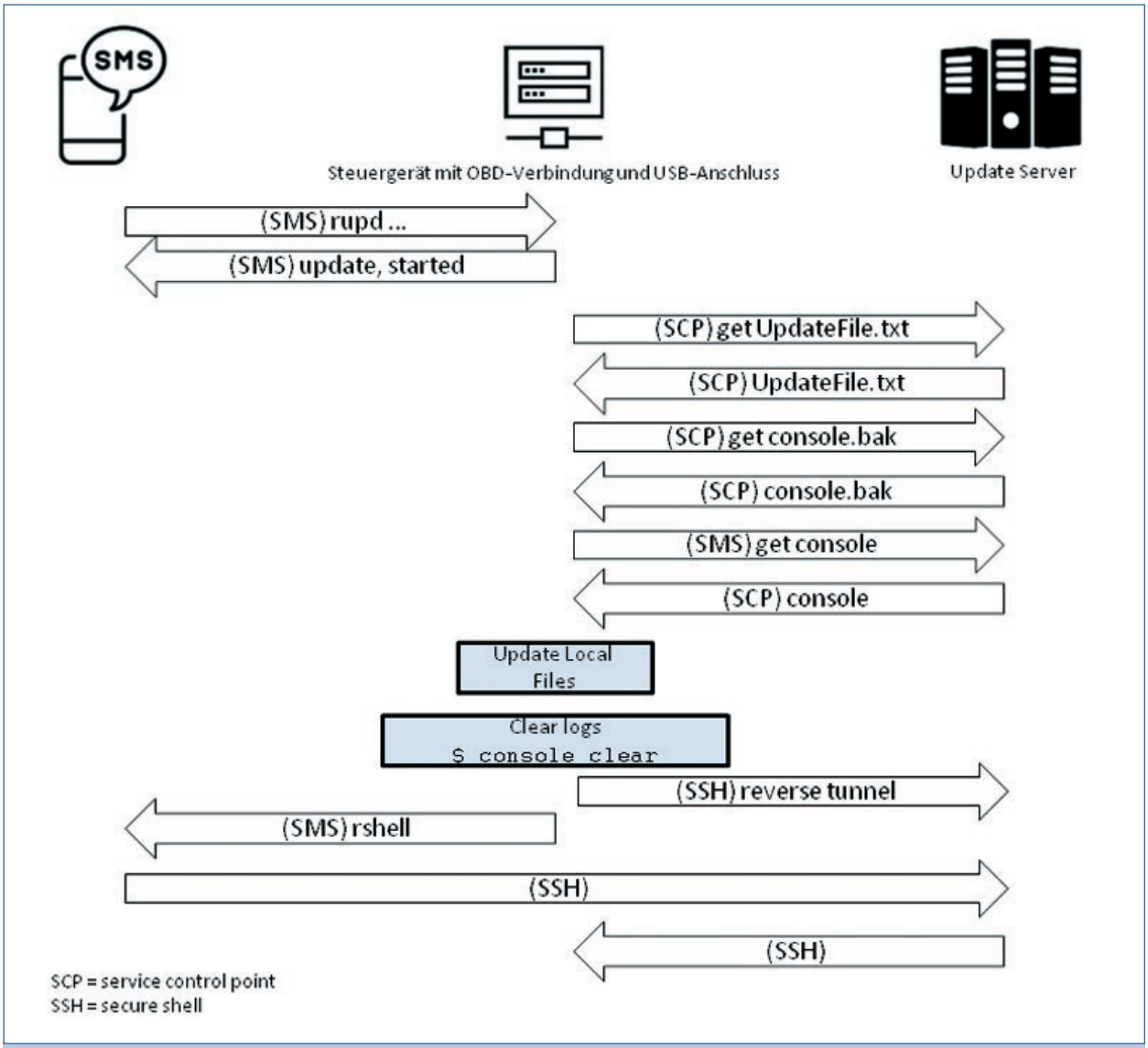

Abb. 2: Fernzugriff über „bösartigen" Update-Server (siehe Foster et al. 2015, S. 6) ■

Bauraum ist begrenzt bzw. eine Gewichtsreduzierung nötig. Aktuelle Trends verweisen hier stark auf den zukünftig verstärkten Einsatz von Ethernet und FlexRay, jedoch begegnet man derzeit nach wie vor den oben beschriebenen Systemen in Kombination mit dem zentralen Gateway, vor allem bei den europäischen OEMs. Auch wenn hier die Absicherung durch den Automobilhersteller gewährleistet wird, muss angesichts des komplexen Systems von einer gewissen Verletzlichkeit und einem Hacker-Risiko ausgegangen werden. Was geschieht jedoch, wenn das Fahrzeug nach der Auslieferung mit zusätzlichen Geräten (z.B. Steuergerät oder Smartphone) verbunden wird? ■

Welche Möglichkeiten gibt es um sich in ein Fahrzeug zu hacken und wie können diese reduziert werden?

Eine Studie (Foster et al., 2015) beschäftigte sich z.B. mit den Möglichkeiten, via eines nachträglich verbauten Telematik-Steuergeräts die Kontrolle über das Fahrzeug zu übernehmen. Der Fokus lag dabei auf Geräten, die der Fahrzeugbesitzer nicht vom OEM, sondern von einem Drittanbieter erwerben konnte (z.B. zum Flottenmanagement).
Diese Steuergeräte werden über die OBD-Schnittstelle mit dem Fahrzeug verbunden. Die OBD-Schnittstelle ermöglicht üblicherweise auch Zugang zu den oben beschriebenen Bussystemen. In der Regel sind zusätzliche Steuergeräte dazu konzipiert nur Informationen „mitzulesen" und zu verarbeiten, jedoch kann aufgrund der Gestaltung z.B. des CAN-Busses jedes Gerät dort auch Botschaften senden.
Und genau hier besteht die eigentliche Schwachstelle.
Bisherige Bussysteme wurden unter der Prämisse entwickelt, gewissermaßen als abgeschlossene Systeme zu dienen. Die heutige Vernetzung jedoch ermöglicht es auf diese Systeme zuzugreifen und sogar sicherheitsrelevante Funktionen (Gaspedal, Bremse etc.) aktiv zu beeinflussen.
In der besagten Studie konnte das angeschlossene Steuergerät über eine dort enthaltene USB-

Schnittstelle (ursprünglich zum Programmieren vorgesehen) mit einem strombetriebenen Gerät verbunden werden. Damit war eine USB-Netzwerkschnittstelle eingerichtet. Mit der vorhandenen Dokumentation auf dem Steuergerät stand die IP-Adresse zur Verfügung. Das Steuergerät antwortete sowohl auf standardisierte Dienste wie Telefonnetz, Web als auch SSH. Fahrzeugdaten standen dabei nicht nur zur Verfügung, sondern bei dem Durchsuchen des NAND Flash Containers konnte der private Key des Root Users identifiziert werden. Diese SSH Keys schienen für diverse Steuergeräte identisch zu sein und somit erschloss sich ein noch größeres Feld für den Fernzugriff auf das identische Steuergerät, welches in diversen Fahrzeugen verbaut wurde. Aber auch Zugriffe via Internet oder SMS waren relativ leicht durchzuführen *(Abbildung 2)*.

Lösungsvorschläge zur Absicherung in diesen Fällen beinhalteten u.a. die Authentifizierung von Updates via Code Signing, verstärkte Authentifizierung von SMS und ein verbessertes Management des Keys (kein Verbleib auf dem Steuergerät). Aber auch ein verbessertes Passwortmanagement, die Inaktivierung der WAN Administration, die Authentifizierung jedes einzelnen Steuergeräts oder auch das Management des Update-Servers wurden als Optimierungspotenzial aufgezeigt. ■

Was bedeutet die Vernetzung von Fahrzeugen für den Automobilhersteller?

Neben der Vernetzung der Fahrzeuge durch nachträglich verbaute Steuergeräte nimmt auch das Angebot der Online-Dienste von OEMs zu. Hier kommuniziert das Fahrzeug (ausgestattet mit einer SIM-Karte) mit dem bereitgestellten Backend. Das Fahrzeug ist damit kein abgeschlossenes System sondern quasi mit dem gesamten Netz verbunden. Aktuell wird versucht die Vulnerabilität mittels Firewalls abzuwehren, jedoch stellt sich die Frage, ob nicht auch andere ganzheitliche Konzepte zur Fahrzeugabsicherung entwickelt werden sollten.

Betrachtet man zudem die Integration des Smartphones wie z.B. durch AndroidAuto, CarPlay oder Baidu, so kommt mit der Verbindung des Smartphones (via USB-Schnittstelle oder WLAN) eine weitere Schnittstelle mit dem Fahrzeug hinzu. Verbindet sich das Smartphone mit dem Internet, ist also auch das Fahrzeug verbunden und auch diese Schnittstelle will abgesichert sein. Die Integration des Smartphones bringt aber nicht nur einen Zusatznutzen für den Fahrer in das Fahrzeug, sondern steht in Konkurrenz zu den vom Automobilhersteller angebotenen Diensten (z.B. Parkplatzsuche, Wetter und weitere Funktionen des Infotainments). Interaktionen zwischen Nutzer und Fahrzeug gleichen sich entsprechend immer mehr den Interaktionen im Umgang mit Tablet und Smartphone an und herstellerspezifische Menüs und Bedienkonzepte geraten ins Hintertreffen. Unternehmen wie Google und Apple erhöhen dabei nicht nur ihre Präsenz, sondern erhalten auch Zugang zu fahrzeugspezifischen Daten.

Dieser Ausblick soll deutlich machen, wie dringend neue Absicherungskonzepte für die Automobilindustrie in Zusammenarbeit mit Technologieunternehmen wie Google und Apple entwickelt werden müssen.

In den vergangenen Jahren konnte Whiteblue sowohl im Kooperations- und Gremienmanagement als auch im Umfeld der Infotainment-Entwicklung und der Absicherung einen breiten und fundierten Erfahrungsschatz sammeln und ist damit genau in dieser Schnittstelle als kompetenter und vernetzter Partner aktiv.

Quelle

I. Foster, A. Prudhomme, K. Koscher, and S. Savage, “Fast and Vulnerable: A Story of Telematic Failures”, Proceedings of Workshop On Offensive Technologies (WOOT), Washington, D.C, (2015). ■

Herzlicher Dank ergeht auch an die Kollegen Steve Gonzalez, Carsten Braess, David Harnos, Marcel Meyer, Rolf Dieter Zschau und Radha Arnds für die Unterstützung und intensiven Gespräche im Vorfeld dieses Artikels. ■

Autor:

Andrea Hanebuth

Whiteblue Consulting GmbH

Emmy-Noether-Straße 4
80992 München
Mobil: +49 151 1135 5080
Tel.: +49 89 622 338-0
Fax: +49 89 622 338-50
andrea.hanebuth@whiteblue.com
www.whiteblue.com