Universität Hamburg
Fachbereich Informatik

IT-Sicherheit und Schutz vor Malware im Automobil

am Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

Arne Beer, Stefan Grusche, Joshua Stock

8. Dezember 2015

Zusammenfassung

Für den eiligen Leser sollen auf etwa einer halben, maximal einer Seite die wichtigsten Inhalte, Erkenntnisse, Neuerungen bzw. Ergebnisse der Arbeit beschrieben werden.

Durch eine solche Zusammenfassung (im engl. auch Abstract genannt) am Anfang der Arbeit wird die Arbeit deutlich aufgewertet. Hier sollte vermittelt werden, warum der Leser die Arbeit lesen sollte.

Inhaltsverzeichnis

1 Einleitung

Sicherheit im Auto - ein Thema, dessen Relevanz kaum geleugnet werden kann. Hunderte Millionen Automobile verkehren auf den Straßen unseres Planeten, zwangsläufig ergeben sich hierbei gefährliche Situationen. Nicht zuletzt um Autos sicherer zu gestalten, wurden in der Vergangenheit bereits zahlreiche computergestützte Systeme entwickelt, die anfangs vor allem das Ziel hatten, den Fahrer in Notsituationen bei der Handhabung des Fahrzeuges unterstützen (wie beispielsweise das 'Elektronische Stabilitätsprogramm' ESP oder Mercedes' Intelligent Drive). Angetrieben von der Digitalisierung in vielen Bereichen unseres Alltags, folgten weitere Systeme, komplexe Infotainment-Systeme, im Auto integrierte Navigationsgeräte, oder gar Einpark- und Spurhalteassistenten, die dem Nutzer vor allem höheren Komfort bieten sollen. Doch auch hier ist oftmals eine sehr enge Kopplung an sicherheitskritische Komponenten (Bremsen, Lenkung, etc.) gegeben.

Betrachtet man die Kommunikation zwischen den digitalen Systemen und der physischen Hardware eines Autos, so fällt schnell auf, dass die meisten Botschaften unverschlüsselt über ein Bus-System ausgetauscht werden. Die Literatur zeigt, dass Zugriff auf den Bus häufig Zugriff auf die an den Bus angeschlossenen Komponenten bedeutet...

In der heutigen Zeit befindet sich in jedem modernen Automobil eine hohe Anzahl fortgeschrittener technischer Systeme. Viele dieser Systeme sollten die Sicherheit der Insassen verbessern oder dem Fahrer assistieren, können durch enge Kopplung an sicherheitskritische Komponenten (Bremsen, Servolenkung, etc.) jedoch missbraucht werden um das Fahrzeug zu manipulieren.

Ein hoher Grad an Vernetzung macht es immer leichter extern Zugriff auf das Auto zu erlangen. Daher rückt durch zunehmenenden Digitalisierung die Frage der Systemsicherheit immer mehr in den Vordergrund.

2 Hauptteil

2.1 CAN-Bus

2.1.1 Funktion und Aufbau

Alle im folgenden erörterten Probleme ergeben sich aus Schwachstellen in der Zentralen Kommunikationsschnittstelle eines Autos, dem sogenannten CAN-Bus.
Der Controller Area Network Bus ist ein klassisches Binary Unit System, welches die meisten Systeme eines PKW's miteinander verbindet. Hierbei ist anzumerken, dass in vielen Autos mehrere CAN-Busse verbaut sind, welche unabhängig voneinander agieren können.
Die angebundenen Systeme an einem CAN-Bus werden Electronic Control Units genannt, kurz ECUs.
Im Folgenden möchte ich die typische Funktionsweise eines CAN-Busses erörtern, wie zum Beispiel beim Toyota Prius.
ECU's kommunizieren untereindander über den Bus, wobei jedes gesendete Paket an jede andere ECU am selben Bus gesendet wird. Die ECU's selbst entscheiden anschließend anhand der Struktur des Paketes, ob die Information für sie bestimmt sind und verarbeiten diese, falls dies zutrifft.
Ein Paket auf einem CAN-Bus hat Beispielsweise diese Form in hexadezimaler Schreibweise:

00 B4 08 00 00 00 00 3C 18 C0 FF

Dieses Paket kann wie folgt interpretiert werden: Die ersten 2 byte, in obiger Schreibweise durch 00 *B*4 repräsentiert, definieren die ID des ECU's, für welches das Paket bestimmt ist.

Die nachfolgenden 4 Bit definieren die Länge der nachfolgenden Payload, also der relevanten Daten oder dem Befehl. In diesem Falle sind es 8 Bytes, also die Sequenz (00 00 00 00 3C 18 C0 FF).

Obiger Befehl hätte sich Beispielsweise auch in folgender Schreibweise darstellen lassen können, auch wenn hierbei durch die fehlenden Bytes ein potentieller Informationsverlust auftritt:

00 B4 04 3C 18 C0 FF

In diesem Paket wird lediglich eine Payloadlänge von 4 definiert. Um eine korrekte Nachricht zu garantieren, wird häufig eine Checksum erstellt, um das Risiko auf einen fehlerhaften Befehl zu minimieren. Die Checksum ist üblicherweise das letzte Byte der Payload und setzt sich aus einem vom jeweiligen Hersteller definierten Algorithmus zusammen. Im folgenden beispielhaft ein Befehl an das Geschwindigkeitstacho eines Ford Escape: Die Addresse ist wie vorher 00 *B*4 mit einer Payloadlänge von 08. Die Payload eines solchen Befehls hat die Struktur:

AA BB 00 00 CC DD 00 00

AABB definiert die RPM, während *CCDD* die Geschwindigkeit angibt. Die Werte werden nach folgenden Formeln berechnet:

$$\text{Speed}(mph) = 0.0065 * (CCDD) - 67$$

$$RPM = .25 * (AABB) - 24$$

Dementsprechend würde ein Befehl mit ca. 100km/h und 2000RPM folgendermaßen aussehen.

1F 40 00 4E BC 00 00

Der komplette Befehl hätte die Form:

00 B4 08 1F 40 00 4E BC 00 00

Nehmen wir an, dass noch eine Checksum hinzugenommen wird, nach der Formel:

$$\text{Checksum} = (IDH + IDL + Len + Sum(\text{Data}[0]\text{˘Data}[Len-2]))\&0xFF$$

Dementsprechend ist der letzte Byte *CC*:

00 B4 08 1F 40 00 4E BC 00 CC

Nach diesem Beispiel sollte ersichtlich sein, dass es relativ einfach ist ein CAN-Bus Paket zu erstellen. Da alle Geräte am selben Bus sitzen und jedes Gerät an alle ECU's sendet, ergibt sich daraus eine relativ drastische Problematik. Für den Fall, dass es einem Angreifer gelingt Zugang zu einem der ECU's am Bus zu bekommen, ist er in der Lage Befehle an alle Geräte am Bus zu senden, eingeschlossen kritische Systeme, wie Bremsen, Motor oder Fahrhilfe.

Im folgenden Abschnitt wird auf die Schwachstellen und die Unsicherheit des CAN-Busses eingegangen.

2.1.2 (Un-)Sicherheit

Wie bereits im vorherigen Abschnitt erläutert, stellt die Kommunikation am CAN-Bus das größte Sicherheitsproblem dar. Bei den meisten Autos ist die Kommunikation auf dem Bus vollkommen unverschlüsselt.
ECU's kommunizieren ohne jegliche Authentifizierung. Dieser Umstand ermöglichte es ohne Hindernisse schadhafte Pakete an ECU's zu senden. Das Fehlen einer Kontrollinstanz bei einer derartig wichtigen Komponente eines Autos lässt sich durchaus als grob fahrlässig bezeichnen. Alle am Bus hängenden Geräte werden als vollkommen glaubwürdig anerkannt.

Durch die unverschlüsselte Kommunikation, tritt ein weiteres, wenn nicht sogar drastischeres Problem auf.
Die Protokolle, mit denen die ECU's kommunizieren sind nicht öffentlich einsehbar und nur dem Hersteller bekannt. Ohne die Dokumentation der API der jewelige ECUs ist es um ein vielfaches schwerer Pakete zu designen, welche von den ECUs als valid angesehen werden. Da Pakete auf einem CAN-Bus jedoch an alle verbundenen Geräte gesendet werden, kann ein Angreifer diese ohne Probleme für eine spätere Analyse mitschneiden. Selbstverständlich braucht man hierfür Zugriff auf den Bus, aber dies kann z.B. an einem baugleichen Modell geschehen, welches der Angreifer besitzt oder mietet. Da der Traffic auf dem Bus unverschlüsselt ist, kann der Mittschnit nun benutzt werden benutzt werden um die API der ECUs zu rekonstruieren. Hierfür muss lediglich nach Mustern im Paketstrom gesucht werden, welche in Abhängigkeit zu dem Zustand des Auto stehen. Durch dieses Verfahren wurde z.B. die vorher gezeigte API des Geschwindigkeitstachos rekonstruiert.

Durch das Senden und Empfangen Aller an Alle entsteht ein weiteres Problem. Mit jedem Gerät, welches an dem Bus hängt, wird ein neuer Angriffsvektor bereitgestellt. Im schlechtesten Fall benötigt ein Angreifer physikalischen Zugriff um einen Empfänger am Bus zu befestigen oder die Firmware der ECU's zu manipulieren. Durch die zunehmende Vernetzung oder technische beabsichtigte Bequemlichkeiten wie Firmware-Updates per CD/USB oder gar Funk/Internet, steigt die Kompromitierbarkeit von an dem CAN-Bus befindlichen Geräten zunehmend. In einem späteren Abschnitt wird näher auf mögliche Angriffsvektoren eingegangen.

Dies sind alles Probleme, welche mit einer Verschlüsselung und einem gut implementieren Authorisierungssystem hätten vermieden werden können.

2.2 Geräte am CAN-Bus

scasasdfasfasfa

2.2.1 Eingebaute TCU

2.2.2 Bluetooth

Eine Bluetooth-Schnittstelle zählt mittlerweile zu den Standards eines modernen Autos. Ihre Hauptfunktion ist meist die Verbindung eines Mobiltelefons zum Media-System des Autos, um beispielsweise Anrufe über eine integrierte Freisprecheinrichtung entgegenzunehmen, aber auch, um Anrufe aus dem Auto über das Mobiltelefon zu starten oder Musik vom Mobiltelefon direkt über das Mediasystem des Autos wiederzugeben. In dem PKW, der in **Quelle: cars-usenixsec2011** betrachtet wird, befindet sich das Bluetooth Modul in der Telematik-Einheit. Die Autoren des Papers (oder Artikel?) konnten durch Reverse-Engineering das Unix-ähnliche Betriebssystem analysieren, inklusive der Bluetooth-Stack-Implementation. Mittels eines via Bluetooth gekoppelten Gerätes gelang es den Forschern wegen Sicherheitslücken der Bluetooth-Stack-Implemenatation, einen Kommandozeileninterpreter ('Shell') auf der Telematik-Einheit zu öffnen.

Sie unterscheiden zwischen zwei Angriffsmöglichkeiten: Zum einen werden *Indirekte* drahtlose Kurzstrecken-Attacken aufgeführt, bei denen ein bereits über Bluetooth mit der Telematik-Einheit gekoppeltes, beliebiges Android- oder iOS-Smartphone benötigt wird, zum anderen beschreiben sie *direkte* drahtlose Kurzstrecken-Attacken. Für letztere muss die MAC-Adresse des Bluetooth-Moduls im Auto bekannt sein, diese kann allerdings mit wenig Aufwand durch verschiedene 'Sniffing'-Software herausgefunden werden. Um nun eine Bluetooth-Kopplung zwischen Automobil und Angreifer zu erzwingen, muss lediglich eine PIN, die sich erst nach Neustart des PKWs ändert, herausgefunden werden. Auch diese stellte kein großes Hindernis dar, mittels Brute-Force-Methode gelang es den Forschern teilweise innheralb 15 Minuten, sich ohne jede Benutzerinteraktion mit der Telematik-Einheit des Autos zu verbinden und die Bluetooth-Sicherheitslücken auszunutzen.

Die Autoren des Papers (oder Artikels?etc) **Quelle: remote attack surfaces**, die sich mit dem 2010 Ford Escape beschäftigten, konnten zwar keine Möglichkeit finden, ein Gerät ohne Benutzer-Interaktion mit dem Auto zu koppeln, sehen den Bluetooth Stack jedoch trotzdem

durch seine Größe als 'eine der größten und machbarsten Angriffsflächen eines modernen Automobils'.

2.2.3 Media Player

2.2.4 Mobilfunk

2.2.5 Nachrüstbare TCUs

Zusätzlich zu den unterschiedlichen Medien- und Diagnosesystemen, die bereits in die Fahrzeuge durch den Hersteller integriert sind, gibt es verschiedenste nachrüstbare Gerätschaften, die dazu dienen können, den Funktionsumfang eines Automobils zu erweitern (komplexere Mediennutzung etc.) oder dem Fahrzeughalter detaillierte Informationen über den Zustand des Autos zu geben. Besonders interessant ist hierbei die Sparte der TCUs, *Telematic Control Units*, die verschiedenste Funktionen und Anwendungszwecke besitzen können.
Die meisten dieser TCUs verfügen dabei über einen GPS-Sensor, oft unterschiedliche Beschleunigungssensoren und eine Mobilfunk und/oder Internetanbindung, um entweder mit den externen Systemen beim Hersteller kommunizieren zu können, sei es um z.B. aufgezeichnete Daten zu Auswertungszwecken zu übertragen oder die eigene Soft- oder Firmware zu aktualisieren, oder um sich mit Endgeräten der Fahrzeuginsassen bzw. des Fahrzeughalters zu verbinden.
Ein prominentes Einsatzfeld nachgerüsteter TCUs ist die Aufzeichnung des Fahrverhaltens durch Versicherungen, die basierend auf den aufgezeichneten Daten ihre Beiträge berechnen (Bspw. Progressives *Snapshot*). Andere TCUs zielen direkt darauf ab, das Fahrverhalten zu verbessern, indem sie über Smartphones der Fahrzeughalter in Echtzeit z.B. Hinweise für eine motor- und benzinschonenderes Beschleunigungs- und Bremsverhalten geben (Bspw. Automatic Labs *Automatic*. Häufig finden TCUs auch im Flottenmanagement Anwendung, wo sie zur Lokalisierung und Überwachung der Geschäftfahrzeuge dienen. Delphis *Connect* ist eine besonders funktionsreiche TCU, die neben bereits erwähnten Anwendungen wie der Lokalisierung auch detaillierte Informationen über die Gesundheit des Fahrzeugs ausgibt, für Eltern die Möglichkeit bietet, ihren jugendlichen Kindern einen Bereich zur Nutzung des Fahrzeugs festzulegen, als Schlüsselersatz zum Öffnen, Schließen und Starten des Autos dient und über 4G-Mobilfunk einen Internet-Hotspot für die Fahrzeuginsassen bereitstellen kann.
TCUs von Fremdherstellern werden üblicherweise direkt an den OBD-Port des Fahrzeugs angeschlossen und werden auf diese Weise direkt in das interne Netzwerk integriert, können im Allgemeinen Nachrichten vom CAN-Bus mitlesen und beinhalten oft auch selbst die Funktionalität Nachrichten auf den CAN-Bus zu schreiben. Dies ist dabei die größte Gefahr einer nachgerüsteten TCU: eine oft umfangreiche Internet- oder Mobilfunkfähigkeit und dabei theoretisch uneingeschränkter Zugriff auf sicherheitskritische Systeme bietet Angreifern eine optimale Angriffsfläche, die bei einem erfolgreichen Eindringen von außen u.U. eine volle Kontrolle über das Fahrzeug bedeutet.
In <hier richtigen Verweis einfügen> haben Foster et al. anhand einer TCU zur Fahrstilanalyse für Versicherungszwecke aufgezeigt, wie ein unsicherer Entwurf des Update-Protokolls letztendlich zur Übernahme des Geräts und damit zum Zugriff auf das Fahrzeug führen konnte. Im beschriebenen Fall waren sie in der Lage, nach Herausfinden der Telefonnummer der TCU, die sie für Mobilfunkdienste besaß, selbst mit einer simplen SMS einen Update-Vorgang an einem beliebigen Server anzustoßen. Aufgrund einer nicht vorhandenen Authentifizierung des Servers und Signatur der Updates konnten einfach beliebige eigene Dateien auf die TCU

heruntergeladen werden und mit entsprechenden Befehlen ausgeführt werden. Im Endeffekt erlangten die Angreifer so die Möglichkeit, sich mit Root-Zugriff in die TCU einzuwählen und erhielten somit freie Verfügung über das komplette System. Die Verbindung zum CAN-Bus bot dann an, selbst Nachrichten zu verschicken. In einer Proof-of-Concept-Attacke zeigten Foster et al. abschließend, dass sie u.a. in der Lage waren, die Scheibenwischer und einzelne Bremsen betätigen zu können.
Ähnliche Fehler bei dem Entwurf derart sicherheitsrelevanter Systeme stellen also eine große Gefahr für den Fahrzeughalter dar. Dies wird noch dadurch verstärkt, dass der Fahrzeughersteller selbst nicht in der Lage ist, diese Fehler zu beheben, da es sich um ein fremdes System handelt, hier muss der jeweilige Hersteller selbst aktiv werden und dafür sorgen, dass alle sich im Umlauf befindenen TCUs eventuelle Updates erhalten.

2.2.6 weiteres Gerät

2.3 Geräte

2.4 Vorgehen

2.5 Beispiele

2.5.1 Jeep Cherokee

Im Folgenden stellen wir anhand der Forschungsergebnisse von Miller und Valasek (<hier Verweis einfügen>) dar, wie ohne direkten Zugang verschiedene Funktionen auf diversen Systemen eines konkreten Fahrzeugs, in diesem Fall eines 2014er Jeep Cherokees, ausgeführt werden können und so eine direkte Gefahr für den Straßenverkehr geschaffen werden kann.

Der Jeep Cherokee besitzt einige Systeme, die für einen Angreifer von großem Interesse sein können. So ist u.a. ein adaptiver Tempomat, der von sich aus Fahrzeugbremsen auslöst, ein Kollisionswarnungssystem, welches das Fahrzeug ebenfalls zu einem kompletten Halt bringen kann, ein Spurassistent, der, wenn auch minimal, in die Lenkung eingreifen kann, und einen Einparkassistenten, welcher wiederum komplette Kontrolle über das Lenkrad erhält, integriert. Des weiteren ist ein Multimediasystem mit Wlan- und Mobilfunkverbindung eingebaut, welches gleichzeitig an beide CAN-Netzwerke im Auto angeschlossen ist. Aus genau diesem Grund ist dieses System das Hauptaugenmerk von Miller und Valaseks Arbeit, da über ein Kompromittieren der Medieneinrichtung potentiell die größte Kontrolle über das Auto erlangt werden kann.

Miller und Valasek konzentrieren sich zuerst auf Schwächen der eingebauten Hotspots-Funktionalität. Sofern der Fahrzeughalter ein Abonnements beim Hersteller abschließt, bietet das Fahrzeug an, einen Wlan-Hostpot für die Fahrzeuginsassen bereitzustellen. In dieses Netzwerk einzudringen benötige im Allgemeinen ein übliches Vorgehen beim Einbrechen in Wlan-Netze, Miller und Valasek konnten aber Schwächen bei der zufälligen Generierung der Netzpasswörter entdecken; das Passwort wird stets als Funktion eines Zeitpunkts berechnet, dieser kann zusätzlich stark eingeschränkt werden, da sich das System, so lange keine Uhrzeit über GPS oder Mobilfunk

empfangen wurde, auf eine Standarduhrzeit einstellt, und dies immer eine gewisse Zeit nach Systemstart benötigt, um sich zu aktualisieren.

Mit Verbindung zum Wlan-Netzwerk konnten Miller und Valasek mithilfe üblicher Netzwerkanalysetools diverse offene Ports identifizieren, die sich zum Angreifen anbieten. Insbesondere der Port 6667 erwies sich als interessant, da hier nicht, wie von der Port-Nummer zu erwarten, ein IRC-Server lief, sondern eine Variante von D-Bus über IP. D-Bus ist ein Framework, welches der Interprozesskommunikation dient.

2.6 Sicherheitsmaßnahmen

Interfaces der ECUs sind meist viel ausführlicher und offener als notwendig. Z.B. ist es unnötig, Bluetooth-Kopplungen ohne Interaktion, oder unbemerkte Datenverbindungen zum Auto zuzulassen. PassThru (Werkstätten-) Geräte sollten über verschlüsselte Verbindungen arbeiten, um das Interface intransparenter zu machen.

Außerdem wurden viele Attacken erst möglich, da auf den ECUs telnetd, ftp und vi vorinstalliert waren, ohne dass sie im gewöhnlichen Betrieb notwendig wären.

Außerdem müsse es mehr Sicherheitsupdates für Autos geben.

3 Schluss/Fazit