Sichere Fahrzeugkommunikation mit Open-Source Software:

Verbunden – und trotzdem abgeschirmt

(Bild: Minerva Studio – Shutterstock)

Über Netzwerkverbindungen werden Fahrzeuge mit Software Updates versorgt oder senden Diagnosedaten an einen Server. Um die Kommunikation sowie die im Fahrzeug gespeicherten Daten abzusichern, hält Linux viele erprobte Mechanismen parat. Emlix setzt sie in mehreren Projekten ein.

Lange Zeit war Linux im Bereich Automotive auf den Einsatz in der Entertainment Unit reduziert. Das ändert sich zur Zeit rasant. Das Open-Source-Betriebssystem findet sich zukünftig in ECUs, der „Smart Antenna“ oder anderen Modulen mit Gateway-Funktionalität – übrigens ein Trend, der bei Nutzfahrzeugen deutlich früher eingesetzt hat. In Projekten, in denen einerseits Betriebs- und Diagnosedaten des Fahrzeugs nach außen verfügbar gemacht, andererseits Konfigurations- und Software Updates von außen an die jeweiligen Steuermodule im Fahrzeug weitergegeben werden sollen, ist das Linux-System in aller Regel die Kommunikationszentrale zwischen dem AUTOSAR-System und der Außenwelt. Damit ist es auch Gatekeeper und erste Sicherheitsinstanz gegen unautorisierten Zugriff, Schad-Software und sonstige Manipulationsversuche.

Die primäre Gegenstelle wird typischerweise über einen Back End Server realisiert, der durch den Kfz-Hersteller bereitgestellt wird. Hinzu kommen davon völlig unabhängige Dienste, wenn über die Smart Antenna auch Multimediainhalte oder Apps (ausführbare Programme) ins Fahrzeug geleitet werden sollen oder zukünftig eine Car-to-Car-Kommunikationsinfrastruktur verfügbar ist.

Datenschutz und Manipulationsschutz

Embedded Linux kann in diesem Kontext nicht nur mit seiner Stärke in der Kommunikation, sondern insbesondere auch im Bereich Security punkten. Dabei sind die sehr hohen Anforderungen letztlich dieselben wie in industriellen Anwendungen mit vergleichbarem Schutzbedarf. Sie teilen sich auf in Manipulationsschutz und Datenschutz, denn die Bewegungsdaten fallen als persönliche Daten unter die Datenschutz-Grundverordnung. Sie müssen bei der Übertragung und Speicherung besonders geschützt werden. Der Manipulationsschutz gliedert sich in den Schutz vor Angriffen aus dem Netzwerk und direkte Sabotageversuche am einzelnen Fahrzeug. Daraus ergeben sich einige Anforderungen, die letztlich unabhängig davon sind, welches Betriebssystem diese Aufgaben übernimmt:

Die zentrale Kommunikationseinheit sollte möglichst physisch von allen Fahrzeug-Bussen getrennt sein, über die kritische Funktionseinheiten angesteuert werden. Dadurch und durch weitere Maßnahmen der Separation sowie ein Rollen- und Berechtigungsmanagement wird verhindert, dass die mit der Außenwelt kommunizierenden Programme Schaden anrichten, falls sie doch durch einen Angreifer übernommen werden.

Das Linux-System darf lediglich autorisierte Verbindungen zulassen. Gegenstellen müssen sich also beim Verbindungsaufbau autorisieren. Sämtliche eingehenden Daten müssen auf Integrität geprüft werden. Zusätzlich sollte es insbesondere im AUTOSAR-System eine Plausibilitätsprüfung geben. Beispielsweise muss der Befehl, in einem Fahrzeug im Normalbetrieb die Bremse außer Kraft zu setzen, als ungültig abgelehnt werden.

Im Vergleich zu stationären Industrie-Gateways kommt beim Automobil als Anforderung hinzu, dass alle Vorgänge so ausgelegt und abgesichert sein müs-

sen, dass sie zu jedem Zeitpunkt mit einem Zusammenbruch der Kommunikationskanäle umgehen können. Wurden z.B. für einen Vorgang mit dem Back End Dienste deaktiviert, muss ein Timeout bei der Kommunikation erkannt werden, um diese wieder zu aktivieren. Aus dem gleichen Grund darf man sich etwa bei der Prüfung von Zertifikaten nicht ausschließlich auf OCSP (Online Certificate Status Protocol) verlassen. Um direkte Manipulationen an der Kommunikationseinheit zu verhindern, muss diese durch entsprechende Verfahren (Secure Boot) geschützt werden.

Fahrzeug initiiert die Kommunikation

Die eingesetzten Technologien sind im Linux-Kontext keineswegs neu, sondern etabliert und vielfältig im Einsatz. Für die Authentifizierung des Back End Server beim Verbindungsaufbau kann TLS (Transport Layer Security) genutzt werden. Der Verbindungsaufbau geht dabei idealerweise vom Fahrzeug aus, damit das Gerät keine von außen erreichbaren Dienste benötigt. Steht der verschlüsselte Kanal zur Verfügung, können Betriebsdaten übermittelt oder Updates und Steuerdaten empfangen werden. Alle übertragenen Daten und Software-Pakete werden vorher signiert, um auf Vertrauenswürdigkeit geprüft werden zu können. Auch hier können etablierte Technologien wie etwa GnuPG oder OpenSSL zum Einsatz kommen.

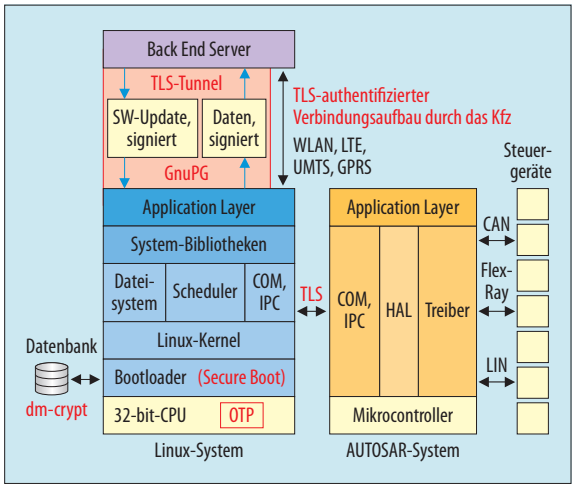
TLS bietet sich auch an, um die Kommunikation im Fahrzeug zwischen dem Linux-System der Kommunikationseinheit und dem AUTOSAR-System abzusichern. Gesprochen wird dabei – mangels Standard – jeweils ein proprietäres Protokoll. Für die gesicherte Ablage von Betriebs- und Bewegungsdaten in einem Datenspeicher auf dem Fahrzeug können etablierte Verfahren wie dm-crypt oder eCryptfs verwendet werden. Zertifikate und Schlüssel müssen dabei fahrzeugspezifisch sein und in einem von außen nicht einsehbaren Bereich liegen. Je nach Anwendungskontext kommen beliebig viele weitere, spezifische Anforderungen und Maßnahmen hinzu, wobei die wachsende Komplexität der Fahrzeugkommunikation ihre Absicherung nicht leichter macht.

Ohne Software-Ballast

Linux hat den Vorteil, dass es sich aufgrund seiner Transparenz und seines strikt modularen Aufbaus auf diejenigen Software-Komponenten begrenzen lässt, die wirklich benötigt werden – unter Umständen sind das recht wenige. In solchen gehärteten Systemen gibt es per se weniger Angriffspunkte; Wechselwirkungen zwischen den Modulen bleiben beherrschbar. Ebenso sind die eingesetzten Security-Technologien transparent. Geheim sind lediglich die verwendeten Schlüssel.

Der Aufwand für die Härtung des Linux-Systems und die sinnvolle Auswahl von Sicherheitstechnologien zahlen sich beim Security Lifecycle Management aus, ohne das keine Sicherheitslösung für ein netzwerkintegriertes Gerät – nichts anderes ist ein modernes Auto – auskommt. Entsprechende Prozesse und Werkzeuge für ein kontinuierliches Security Monitoring und das „Ausrollen" von Security Patches und Updates auf die Fahrzeuge gehören originär zu einem Sicherheitskonzept, denn eine Aufforderung an die Fahrzeughalter, in die Werkstatt zu kommen, kann es nur im Ausnahmefall geben.

Heike Jordan (Emlix) / jk



Das Linux-System stellt die Verbindung zwischen den AUTOSAR-Geräten im Fahrzeug und dem Netzwerk her. Der Back End Server stammt üblicherweise vom Fahrzeughersteller. Sensible Daten und Kommunikationsverbindungen sind abgesichert.