Ethernet-Security

AUTOREN

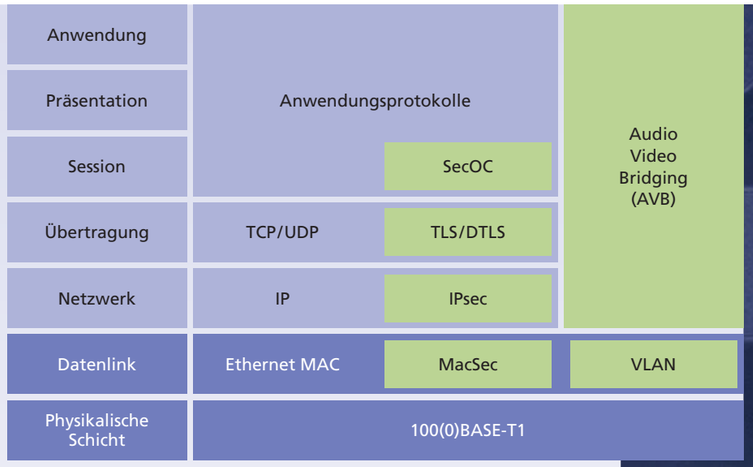
Norbert Fabritius und **Ramona Jung** sind Security Engineers bei der **ESCRYPT GmbH**.

Dr. Jan Holle ist Security Engineer und Produktmanager bei der **ESCRYPT GmbH**.

ESCRYPT ist eine hundertprozentige Tochtergesellschaft von ETAS und bietet Sicherheitslösungen im Bereich Embedded Security an.

Sicheres Ethernet – eine Chance für die Fahrzeug-IT

Seit über 40 Jahren ist der Ethernet-Standard in der klassischen IT etabliert. In Rechenzentren und im Consumer-Bereich ist er eine feste Größe. Nun erobert er moderne Fahrzeuge. Nach ersten Einsätzen in Systemen ohne domänenübergreifende Kommunikation folgt nun der Ausbau in der E/E-Architektur über Domänengrenzen hinweg. Das wirft Fragen zu Security, Safety und zuverlässigem Zeitverhalten auf. Praktikable Ethernet-Lösungen sind gefragt.



Einordnung der verschiedenen sicherheitsrelevanten Protokolle (grün).

Die Datenraten im Automobil steigen rasant. Um sie bewältigen zu können, bekommen klassische Bussysteme wie CAN und FlexRay Gesellschaft: Ethernet. Was im Infotainment-Bereich begann, setzt sich mittlerweile in domänenübergreifenden Systemen fort.
Für ein sicheres Neben- und Miteinander der Datenbusse sind durchdachte Lösungen gefragt. Neben der Kommunikation der Ethernet-Komponenten untereinander ist der reibungslose Datenaustausch mit den konventionellen Bussystemen zu gewährleisten. Zudem gilt es, Ethernet-Standards – wo nötig – den fahrzeugspezifischen Anforderungen anzupassen. Teils lassen sich Lösungen aus der klassischen IT übertragen oder nach geringfügiger Modifikation implementieren. Teils sind neue Entwicklungen nötig. Die Entscheidung darüber steht und fällt mit der Frage, wie ein Höchstmaß an Security, Safety und ein zuverlässiges Zeitverhalten, auch in Anbetracht großer Datenmengen wie bei Videosignalen, zu erreichen ist.

Probleme und Lösungen der klassischen IT

Im dezentralen Aufbau von Ethernet lässt sich mithilfe eingebauter Redundanzen und der Nutzung dynamischer Netzwerkpfade eine zentrale Kontrollinstanz vermeiden – und somit ein Single Point of Failure. Doch eben dieser verteilte Aufbau sorgt für Zweifel: Wenn alle Mitglieder in Ethernet-Netzwerken gleichberechtigt sind, wie können unerwünschte Netzwerkteilnehmer erkannt und verbannt werden? Wie werden Manipulationen am Netzwerk festgestellt und verhindert?
Dafür gibt es etablierte Lösungen. Etwa virtuelle Netzwerke, sogenannte VLANs, zur Trennung des Netzwerk-Traffics. Ursprünglich wurden die Netzwerk-Ports der verbauten Switches verschiedenen VLANs zugewiesen. Mittlerweile ist es auch möglich, Ethernet-Frames und Port-unabhängige VLANs zu markieren. Dieses „Taggen" ist im Standard IEEE 802.1Q definiert.
Die logische Trennung von Netzwerkverkehr allein verhindert aber nicht die Teilnahme unerwünschter Geräte. Auch schützt sie den Traffic nur bedingt vor Manipulation und Ausspähung. Dafür braucht es kryptografische Authentisierung oder Verschlüsselung. Auch hierfür sind Lösungen in der klassischen IT etabliert: Was auf den oberen Protokollschichten mit Datenformaten und Standards wie Transport Layer Security (TLS) begann, wurde später durch Sicherheitsmechanismen für die tieferen Layer ergänzt. Dazu zählen die Verschlüsselung von IP-Paketen (Layer 3) durch IPsec und von Ethernet-Frames (Layer 2) per MACsec (IEEE 802.1AE). Es handelt sich ebenfalls um standardisierte Lösungen.
Hinzukommen Sicherheitskomponenten: Klassische Firewalls kontrollieren anhand von Filterregeln, welche Pakete zwischen verschiedenen Netzen oder Endpunkten erlaubt sind. Moderne Varianten können den Traffic mittels Deep Packet Inspection bis hin zu den Nutzdaten der Pakete analysieren und bewerten. Darauf bauen wiederum Intrusion-Detection- bzw. -Prevention-Systeme (IDS bzw. IPS) auf – und erweitern die Kontrollmöglichkeiten der Administratoren.

Sicherheitsanforderungen moderner Fahrzeugnetzwerke

Netzwerkarchitekturen moderner Fahrzeuge und in der klassischen IT haben viele Parallelen. Doch die technischen Randbedingungen und Schutzziele unterscheiden sich teils deutlich. Im Fahrzeug hat das Abwenden von Schaden an Mensch und Maschine oberste Priorität. Das rückt die Authentizität des Netzwerkverkehrs und die Systemverfügbarkeit in den Fokus. Dort finden sich zudem die hohen Echtzeitanforderungen im Fahrzeugbetrieb: Nahezu verzögerungsfreies, deterministisches Verhalten der Netzwerkkomponenten wird voraussetzt.
Diese Erfordernisse stehen vermeintlich im Widerspruch dazu, dass Ethernet als paketbasiertes Best-Effort-Medium keine harten Garantien für die Zustelldauer von Datenpaketen kennt. Zusätzlich wird das Erfüllen der Schutzziele und Echtzeitanforderungen dadurch erschwert, dass in Fahrzeugen meist eher Komponenten mit limitierter Rechenleistung verbaut werden. Aus diesen Gründen finden etablierte Sicherheitstechnologien häufig nur in abgewandelter Form den Weg in Fahrzeugnetzwerke. Etwa, wenn VLANs zur Erhöhung der Ausfallsicherheit genutzt werden. Das Netzwerk wird dazu in virtuelle Zonen mit unterschiedlichem Schutzbedarf eingeteilt, über die der Netzwerkverkehr sicherheitsrelevanter Komponenten in Echtzeit identifizierbar wird. Bei Bedarf kann er so priorisiert und isoliert werden. Fluten beispielsweise ein Denial-of-Service-Angriff oder eine fehlerhafte Komponente das Netzwerk mit Paketen, lassen sich diese am nächsten Switch per Rate Limiting aufhalten, um der Kommunikation im priorisierten VLAN Vorrang zu geben.
Mithilfe von Firewalls oder leistungsfähigeren IDS-/IPS-Systemen lassen sich angrenzende IP-Netze mit unterschiedlichem Schutzbedarf noch schärfer voneinander trennen und genauer überwachen. Dagegen erlauben klassische Automotive-Bussysteme als Broadcast-Medium an sich keine logische Trennung – es sei denn, es wird ein zusätzlicher physikalischer Bus verbaut.

Bestehende und neue Security-Lösungen

Vorsicht war bisher beim etablierten IT-Sicherheitsprotokoll TLS geboten. Da hier Konflikte mit den Echtzeitanforderungen im Fahrzeug drohten, kamen sie nur für die zeitlich unkritische Kommunikation mit Backend-Systemen oder Testgeräten infrage. TLS 1.3 bringt hier substanzielle Neuerungen: Dank der Optimierung im Verbindungsaufbau (Zero-RTT Handshakes) lassen sich TLS-gesicherte Daten bereits im Handshake im ersten Paket unterbringen. Zusätzliche Paketumlaufzeiten bzw. Round Trip Times (RTTs) beim TLS-Einsatz entfallen. Da durch den Einsatz von Pre-Shared Keys (TLS-PSK) obendrein asymmetrische Verfahren verzichtbar werden, lässt sich der Overhead von TLS dramatisch reduzieren. Noch gilt es jedoch, die Möglichkeiten mit Blick auf die mögliche Abschwächung der TLS-Sicherheitsgarantien sorgfältig zu evaluieren.
Die Echtzeitanforderungen im Automobil stehen dem Einsatz kryptografischer Signaturen auf Basis asymmetrischer Verfahren entgegen. Zum Schutz der Authentizität von Datenpaketen wurde daher 2014 das Secure-On-board-Communication-Modul (SecOC) als Teil von AUTOSAR 4.2 spezifiziert. Die Spezifikation ist so flexibel, dass sich SecOC auch für den Ethernet-/IP-basierten Verkehr eignet.
Gleiches gilt für diverse Standards des Time-Sensitive Networking (TSN). Darunter das ursprünglich für die Übertragung zeitkritischer Videodaten entwickelte Audio Video Bridging (AVB). Es setzt auf Ethernet auf und definiert eigene Mechanismen, die die Reservierung von Netzwerkressourcen, die Synchronisierung von Zeitsignalen oder die Priorisierung von Datenströmen regeln. Zudem erlaubt AVB die Übertragung konventioneller Busdaten. Das trägt den Anforderungen in Umgebungen mit Echtzeitanforderung Rechnung, ohne auf Ethernet als Basistechnologie zu verzichten. Die neueste Fassung des AVB-Transportprotokolls (Ende 2016) unterstützt zudem optional die Verschlüsselung übertragener Nutzdaten – mit vergleichsweise geringen Hardware-Anforderungen.

Ethernet-Security im Fahrzeug – Entwicklung und Integration

Die Integration von Ethernet-basierten Lösungen in Fahrzeugnetzwerke ist in vollem Gange. Der Standard macht die Funktionen möglich, die von künftigen Fahrzeugen erwartet werden. Dabei steht die Entwicklung keineswegs im Widerspruch zu den Sicherheitsanforderungen im Automobil. Mit sachkundiger Begleitung durch Security-Experten und passgenauen Sicherheitslösungen gelingt die Implementierung sicherer Ethernet-Architekturen trotz aller Komplexität. ESCRYPT kann hierfür auf langjährige Erfahrungen im Ethernet-Security- wie im Automotive-Bereich zurückgreifen. Mit diesem Know-how werden Kunden in allen Phasen der Ethernet-Integration unterstützt: Von der Erarbeitung tragfähiger Sicherheitskonzepte und -analysen bis zur individuellen Implementierung von Soft- und Hardwarelösungen aus einem breiten, exakt auf die Automobilindustrie zugeschnittenen Portfolio. Abgesichert durch intelligente Security-Lösungen und -Produkte wird der Ethernet-Standard seine über 40-jährige Erfolgsgeschichte fortschreiben – auch und erst recht in der Automobilindustrie.