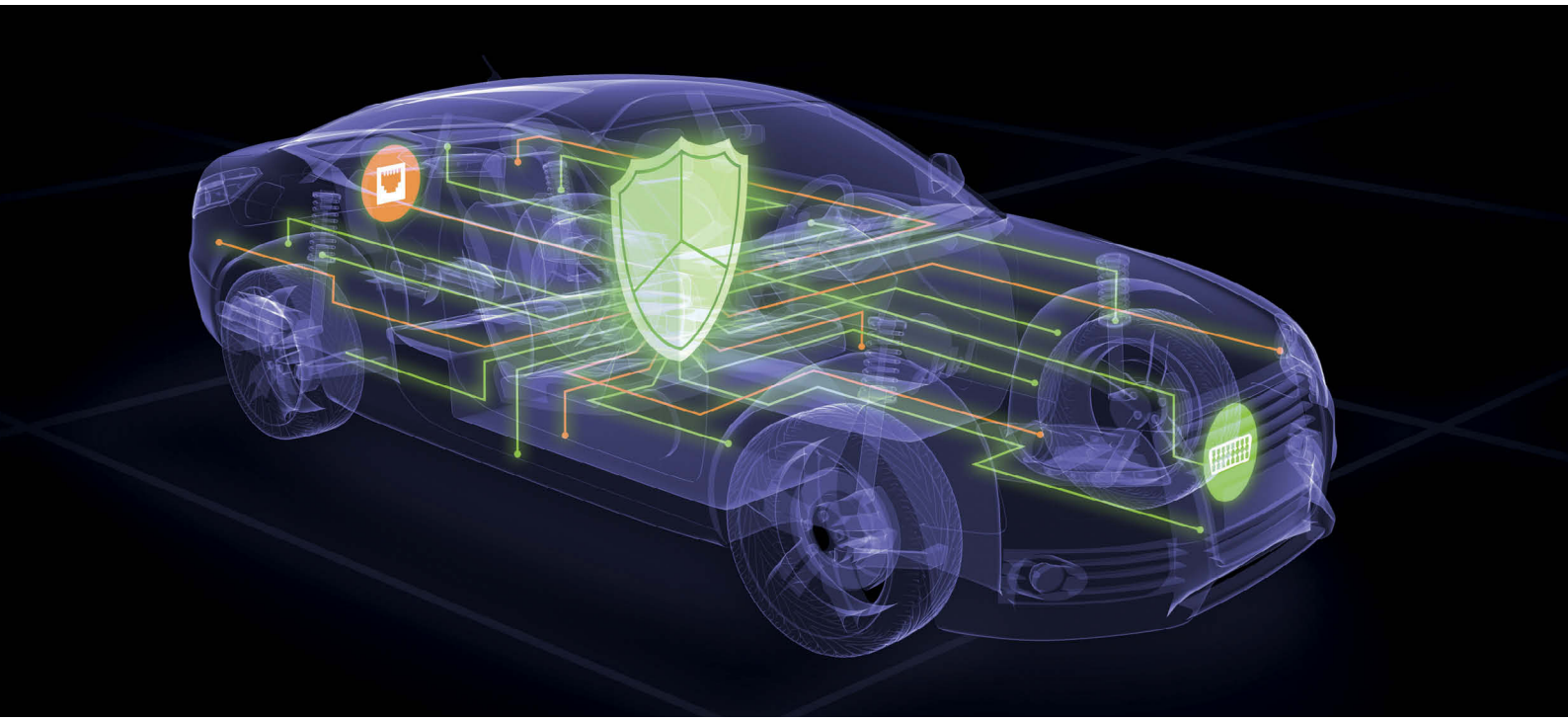
Angriffserkennung für hybride CAN-Ethernet-Netzwerke

Automotive Cybersecurity zielgenau auf beide Welten abstimmen



Heutige dezentrale E/E-Architekturen werden den vernetzten, automatisierten Fahrzeugen der nahen Zukunft nicht mehr gerecht. Daher werden Vehicle Computer und Automotive Ethernet herkömmliche Steuergeräte und CAN-Busse ergänzen. Solche hybriden Fahrzeugnetzwerke brauchen Schutz durch zielgenaue Angriffserkennung und Überwachung des Datenverkehrs.

Bald schon werden Vehicle Computer (VCs) und breitbandiges Automotive Ethernet heutige Bordnetze mit ihren dutzenden, durch CAN-, LIN- und FlexRay-Datenbusse verbundenen Steuergeräten ergänzen. Letztere bleiben gefragt, wo es hohe Echtzeitanforderungen und zyklisch wiederkehrende Funktionen umzusetzen gilt. Ansonsten übernehmen Mikroprozessor-basierte, in Virtual Machines partitionierte Zentralrechner. Denn sie sind den Herausforderungen vernetzter, automatisierter Fahrzeuge besser gewachsen.

Doch wie lassen sich die hybriden CAN-Ethernet-Architekturen und deren Datenprozesse effektiv absichern? Grundsätzlich bleibt es bei zwei Prinzipien: Abschirmung der Kommunikation sowie Partitionierung. Lückenlose Überwachung der Kommunikation ist geboten, um Cyberattacken frühzeitig zu erkennen. Domänenspezifische virtuelle Teilnetze (VLANs) minimieren im Fall eines Angriffs die Eindringtiefe. Beides ist in hybriden Bordnetzen machbar, erfordert allerdings für die CAN- und die Ethernet-Welt verschiedene methodische Ansätze.

Effiziente Angriffserkennung für CAN

Zur Überwachung der CAN-Busse lässt sich ein Intrusion Detection System (IDS) in Gateways oder zentrale Steuergeräte integrieren. Anomalien im CAN-Datenverkehr erkennt es im Abgleich mit dem vom OEM spezifizierten „Normalverhalten". Die eingebettete Security-Komponente erkennt beispielsweise Anomalien bei

zyklischen Botschaften sowie missbräuchliche Diagnose-Anforderungen, die es jeweils als potenzielle Angriffe klassifiziert und loggt bzw. meldet (Bild 1).

Die Leistungsfähigkeit des CAN-IDS (CycurIDS) hängt direkt von der Qualität seiner Konfiguration ab. Daher sollten effiziente initiale Regeln des OEM kontinuierlich durch neue Erkennungsmechanismen auf Basis von Analysen aktueller Angriffsvektoren ergänzt werden, um eine hohe Erkennungsrate bei möglichst wenigen Fehlalarmen zu erreichen. Die Umsetzung steht und fällt mit der Qualität des Werkzeugkastens, der bei der initialen Konfiguration und der kontinuierlichen Weiterentwicklung der Regelsätze zum Einsatz kommt. Als Ready-to-use-Software ist das IDS (CycurIDS) als CAN-Angriffserkennung in hybriden Bordnetzen jederzeit einsatzbereit.

Automotive Firewall im Ethernet Switch

Für die sichere, reibungslose Ethernet-Kommunikation in hybriden Bordnetzen hingegen ist eine Automotive Ethernet Firewall (CycurGATE) das Mittel der Wahl. Wird diese direkt im Ethernet Switch implementiert, kann sie den kompletten Packet Flow überwachen, ohne dass Interferenzen mit Steuergeräten oder dem Host Controller drohen. Durch ausbalanciertes Co-Design von Hard- und Software kann die Firewall die Hardwarebeschleunigung auf dem Switch optimal nutzen. Das Gros der Datenpakete wird so mit Wirespeed verarbeitet. Hauptaufgabe ist die Abwehr von Denial-of-Service-Attacken. Doch indem die Firewall die Partitionierung in allen Netzwerkschichten aufrechterhält, unterstützt sie auch den sicheren Datenaustausch zwischen partitionierten Domänen. Hierfür filtert ein „Packet Filter" die ein- und ausgehenden Daten, die jeweils per „Stateful Packet Inspection" und vertiefter „Deep Packet Inspection" überprüft werden.

Die Automotive Ethernet Firewall (CycurGATE) schützt das Bordnetz also nicht nur vor unbefugtem Zugriff und Manipulation, sondern dient obendrein zur Steuerung der Onboard-Kommunikation (Bild 2). Sie deckt den Ethernet/IP Stack inklusive der gängigen Automotive-Protokolle (zum Beispiel SOME/IP) vollständig ab und überwacht die Zugänge zu Netzen und VLANs. Gefiltert wird die

```
…
0.010000 1  100  Rx  d 8 8A FF FF 0C 42 5F FD 97
0.011000 1  110  Rx  d 8 03 3E 3E E2 10 FF 4A 3F
0.012000 1  120  Rx  d 8 03 F7 30 27 C7 7E D9 9C
0.020000 1  100  Rx  d 8 11 F4 00 3E E2 60 6C B9
0.021000 1  110  Rx  d 8 1F AA 00 00 00 00 C0 00
0.022000 1  120  Rx  d 8 02 AA 00 00 00 00 C0 00
0.031000 1  110  Rx  d 8 86 4A 2F 01 81 05 80 7F
0.031500 1  110  Rx  d 8 E5 2B 41 0C 00 00 00 00
0.032000 1  120  Rx  d 8 02 04 78 00 FF 00 00 30
0.041000 1  110  Rx  d 8 6E 7B FF FF 3F FF 1F 8B
0.042000 1  120  Rx  d 8 00 5A 00 00 0F 55 02 00
0.043000 1  7DF  Rx  d 8 02 10 03 00 00 00 00 00
0.044000 1  7E8  Rx  d 8 02 50 03 AA AA AA AA AA
0.051000 1  110  Rx  d 8 FE 4B 2F 01 81 07 80 7F
0.052000 1  120  Rx  d 8 68 05 78 00 FF 00 00 30
…
```

Timings
- Frequenzabweichung
- Nachrichteneinschleusung
- Timeouts

Diagnose
- Art des Services
- Servicebedingungen

Bild 1: Das CAN-IDS erkennt Anomalien bei zyklischen Botschaften und den Missbrauch von Diagnose-Anforderungen.

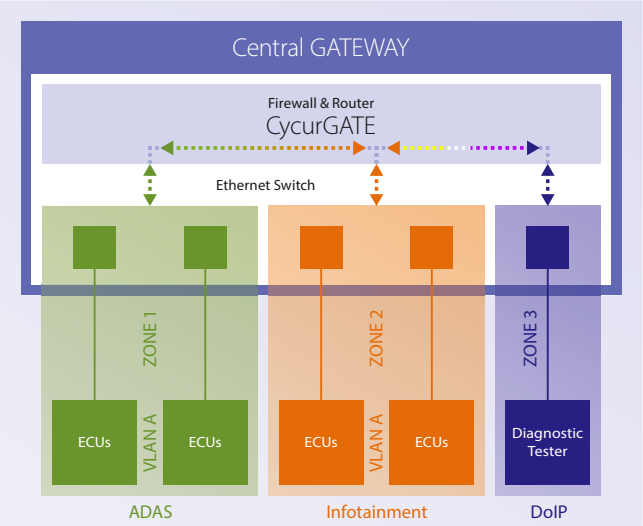


Bild 2: Automotive Ethernet Firewall übernimmt Gatekeeper- und Routerfunktionen.

Kommunikation anhand von jederzeit aktualisierbaren White- oder Blacklists, was die schnelle, wirksame Reaktion auf neue Angriffsmuster gewährleistet.

Intelligente Lastenverteilung

Neben der Implementierung im zentralen Ethernet Switch ist es möglich, hostbasierte Firewalls direkt in Steuergeräte zu integrieren. Das setzt hochperformante Lösungen voraus. Die Firewall muss leistungsstark genug sein, um in Echtzeit zu prüfen und zu entscheiden, ob und wohin sie einzelne Datenpakete routet. Komplexe Angriffserkennungsmuster, etwa über die Frequenz der zustandsorientierten SOME/IP-Kommunikation, kann die Firewall nicht abdecken. Hier ist ein zusätzliches Ethernet-IDS geboten, das Muster von Anomalien anhand der Nachrichtenfrequenz, Sequenz, Nutzlastdaten und Services erkennt und als Angriffsversuche loggt bzw. meldet. Im Sinne optimaler Performance bedarf dieser Ansatz intelligenter Lastenverteilung zwischen Switch und Mikrocontroller. Firewalling und Intrusion Detection können teils im Switch und teils im Zielsteuergerät erfolgen.

Im Zusammenspiel können CAN-IDS, Automotive Ethernet Firewall und Ethernet-IDS hybride E/E-Architekturen zuverlässig und ohne merkliche Latenzen schützen. Eingebettet in ganzheitliche Security-Konzepte sind sie zentrale Bausteine der Risikoabwehr und der funktionalen Sicherheit im vernetzten und zunehmend automatisierten Fahrzeug der Zukunft. ■

Autoren

Dr. Jan Holle ist Produktmanager Intrusion Detection Systems bei ESCRYPT. **M.Sc. Siddharth Shukla** ist Produktmanager Automotive Firewall bei ESCRYPT.