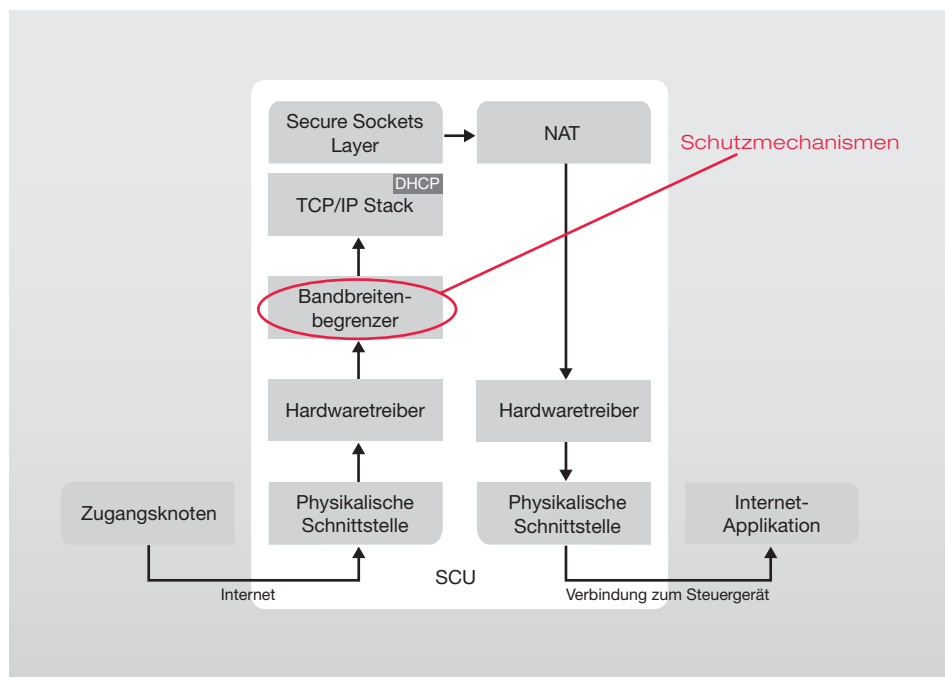


Die Secure Communication Unit sorgt für sichere Online-Zugänge im Fahrzeug



Ihre Vorteile:

- » Ausfallsichere Online-Zugänge im Fahrzeug
- » Schutz vor Flooding Attacken
- » Schutz vor Bot-Netzen
- » Erhöhte Verfügbarkeit von Online-Applikationen

Freie Internetzugänge in modernen Automobilen sind bereits heute Wirklichkeit. Sie werden zukünftig stark zunehmen. Durch den Anschluss an das Internet und die Möglichkeit nicht vertrauenswürdige Software herunter zu laden, steigen die Sicherheitsanforderungen an Fahrzeuge. Denn das Fahrzeugbordnetz muss zuverlässig vor Online-Angriffen geschützt werden.

Vor diesem Hintergrund hat secunet ein Verfahren entwickelt, das Online-Schnittstellen in Fahrzeugen wirkungsvoll gegen Angriffe aus dem Internet absichert.

Schutz vor Angriffen auf Übertragungsebene

Die Secure Communication Unit (SCU) ist ein Verfahren, das ausfallsichere Kommunikationsverbindungen vom und ins Fahrzeug gewährleistet. Die SCU stellt im Falle eines Angriffs auf die Kommunikationsschnittstelle des Fahrzeugs sicher, dass die restlichen Applikationen unbeschadet weiter betrieben werden können. Um die Online-Zugänge zu schützen, überwacht die SCU die Bandbreite der Internetverbindung. Dadurch werden Flooding Angriffe neutralisiert, Bot-Netz Angriffe erfolgreich abgewehrt.

Architektur der Secure Communication Unit

Die oben genannten Schutzmaßnahmen agieren auf der Schnittstelle zwischen physikalischem Zugang und TCP/IP Stack. Damit greifen die Schutzmaßnahmen auf unterster Ebene und wirken auf alle darüber liegenden Software-Schichten. Alle IP-betriebsnotwendigen Protokolle (ARP, DHCP, TCP/IP und ICMP) sind im TCP/IP-Stack-Block zusammengefasst. Der Router übernimmt die NAT-Funktionalität (Network Address Translation).

Übersicht der Funktionen der Secure Communication Unit

Aufbau einer Internetverbindung

Um eine Internetverbindung aus dem Fahrzeug heraus aufzubauen, wird über den Zugangsknoten eine dynamische IP-Adresse abgerufen. Das geschieht automatisiert über das Dynamic Host Configuration Protocol (DHCP). Diese zugewiesene dynamische IP-Adresse wird dann über NAT auf eine interne statische IP-Adresse übertragen. Über diese statische IP-Adresse wird anschließend der interne Kommunikationsknoten angesprochen. Um eine sichere Verbindung zu einem vertrauenswürdigen Server aufbauen zu können, verfügt die SCU über eine IPSec-Funktionalität, d. h. sie kann einen sicheren VPN-Tunnel aufbauen.

Schutz vor Flooding-Attacken (Bandwidth Limitation)

Zum Schutz vor Flooding-Angriffen wird die Bandbreite nach der Peak-(Anzahl pro Sekunde) und der Average-Anzahl der IP-Pakete je Zeitfenster begrenzt. Die Zeitfenster können dabei variabel gesetzt werden. Dieser sogenannte Bandbreitenbegrenzer wirkt auf IP-Ebene ohne spezifische Berücksichtigung der Protokolle ICMP, ARP, DHCP, IP HTTPS, IP HTTP etc. und ermöglicht so eine einfache und zukunftssichere Realisierung der SCU.

Sobald die Bandbreite bestimmte Schwellwerte überschreitet, baut die SCU die logische IP-Verbindung ab. Die nachgeschaltete Internetanwendung bleibt davon unberührt und kann so nicht abstürzen. Anschließend

wird die Internetverbindung mit einer neuen IP-Adresse wieder aufgebaut (Autoreload). Durch die Verwendung einer neuen IP-Adresse sind für den Angreifer die SCU und das Fahrzeug nicht mehr sichtbar. Durch die Bandbreitenbegrenzung ist ebenfalls sichergestellt, dass die SCU zu jedem Zeitpunkt über genügend Rechenleistung verfügt, um den Autoreload durchzuführen.

Konfiguration der SCU (Diagnose)

Die Konfiguration der SCU erfolgt aktuell über SNMP-Kommandos (Simple Network Management Protocol). Folgende Kommandos sind verfügbar:

- Setzen und Auslesen der Schwellwerte für den Bandbreitenbegrenzer
- Setzen und Auslesen der statischen IP-Adresse im Zusammenhang mit NAT
- Abfrage der aktuellen Bandbreite
- Abfrage, ob ein Autoreload stattgefunden hat

Verfügbarkeit der SCU Funktionen

Die Funktionen der SCU sind in Software realisiert. Sie werden unter Linux und auf Basis eines Freescale MPC5200 implementiert. Als Zugangsknoten kommt WLAN zum Einsatz, welches über USB mit dem Prozessorboard verknüpft ist. Die Internet-Applikation ist über Ethernet an die SCU angebunden.

Warum secunet?

secunet bietet OEMs und Zulieferern bei der Einführung von sicheren Online-Plattformen den entscheidenden Wettbewerbsvorteil in Form von Time to Market: Sie konzentrieren sich auf die Entwicklung der Kundenfunktionen ihrer Plattform und wir liefern die notwendigen Sicherheitsmechanismen. Das bedeutet für unsere Kunden weniger Kosten bei schnellerer Einführung.

Unser Kunde profitiert von erstklassigem Know-how: Wir verbinden langjährige Projekterfahrung aus der Automobilwelt mit klassischer IT und Telekommunikation.

Bei der Entwicklung angepasster Sicherheitsmechanismen zum Schutz von Online-Plattformen greifen wir u. a. auf folgende Projekte zurück:

- Einführung von sicheren Bezahlvorgängen über mobile Endgeräte in der Telekommunikationsindustrie
- Einführung von Absicherungsmechanismen für Fernwartungszugänge in der Automobilindustrie
- Analyse der Browsersicherheit in Head Units und der Sicherheitsmodule für die Onboard Units eines Mautsystems
- Netzwerksicherheit bei der Umsetzung mehrstufiger Firewall-Konzepte und dem Betrieb von Managed Security Services

Animation und Whitepaper finden Sie hier:
www.secunet.com/onlinesecurity

secunet

secunet Security Networks AG
Kronprinzenstraße 30
45128 Essen

Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com