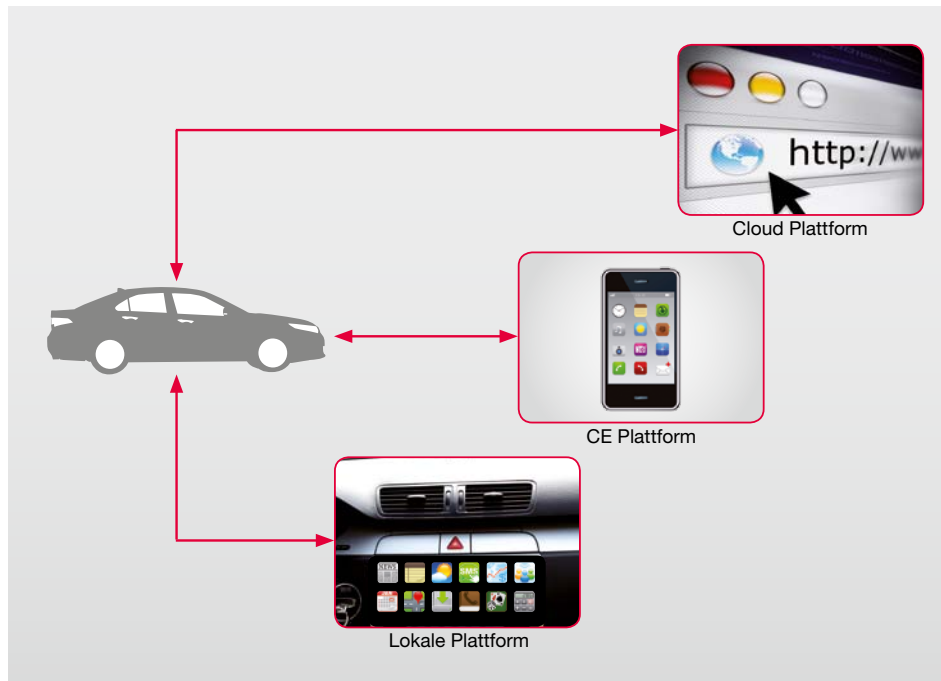


Die Application Control Unit implementiert Sicherheit für vernetzte Fahrzeuge



Ihre Vorteile:

- » **Schnelle und sichere Umsetzung neuer Kundenwünsche**
- » **Einfache Wartung der Infotainment Plattform, da die Safety des Fahrzeugs nicht vom regelmäßigen Patchen von Applikationen abhängt**
- » **Keine spezielle Hardware für die sichere Ablage von kryptographischen Schlüsseln und Routinen**

Neue und flexible Anwendungen und Dienste über Internet Applikationen im modernen Fahrzeug machen das Fahrerlebnis noch attraktiver. Die Apps laufen im Fahrzeug auf den gängigen Betriebssystemen aus dem Consumer Umfeld wie Linux oder Android. Damit sind aber auch alle existierenden Schwachstellen dieser Betriebssysteme im Fahrzeug präsent und können von bösartigen Anwendungen und Services ausgenutzt werden, um Zugriff auf das Bordnetz zu erlangen.

Um den Schutz der Automobilelektronik zu gewährleisten, hat secunet die Application Control Unit entwickelt. Deren Security Mechanismen sind unabhängig von Anwendungen und eingesetzten Betriebssystemen und schützen das Fahrzeugbordnetz sogar dann, wenn unbekannte Malware versucht, darauf zuzugreifen.

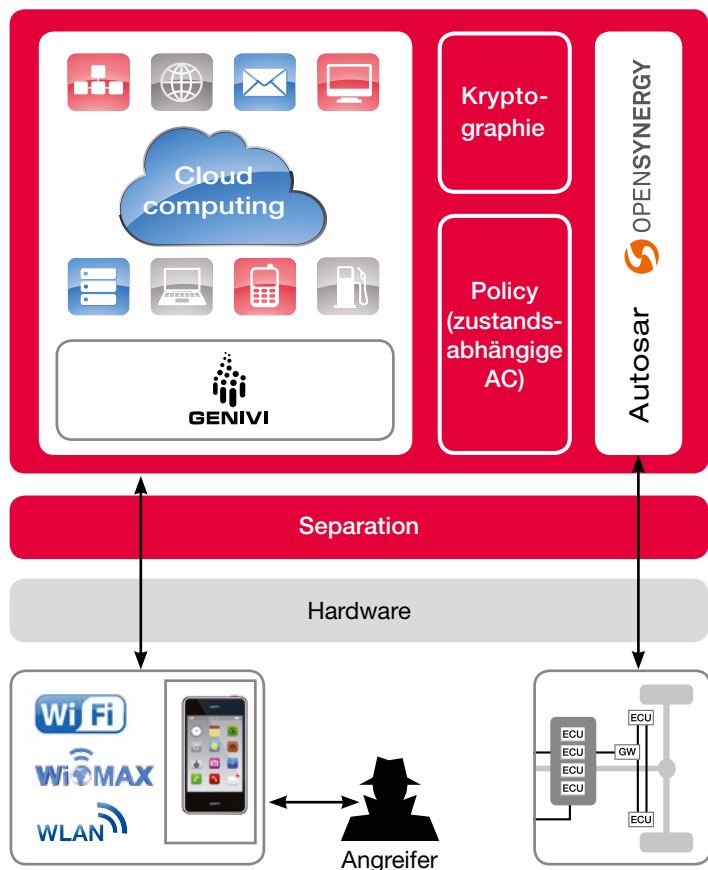
Features:

- **Policy Check:** Aus der Spezifikation der Bordnetzfunktionen wird ein Regelwerk, das vom Fahrzeugzustand abhängt, für die Kommunikation der Apps ins Bordnetz abgeleitet. Falls eine Regel verletzt wird, werden die Kommandos nicht an das Fahrzeugbordnetz weitergeleitet.
- **Aktive Gegenmaßnahmen:** Falls ein Angriff registriert wird, führt die Policy Maßnahmen durch, um die Applikation, die die Regelverletzung verursacht hat, unschädlich zu machen. Die Policy kann z. B. das Gastbetriebssystem neu starten oder von einem vertrauenswürdigen Image neu booten.
- **Policy Update:** Falls das Bordnetz geändert oder eine neue Generation von Applikationen eingeführt wird, können verschlüsselte und signierte

Policy Files ausgerollt werden, um die Security an die neuen Anforderungen anzupassen.

- **Kryptographie:** Eine Schnittstelle stellt Standardverschlüsselungsdienste zur Verfügung, wie z. B. Signaturverifikation, sichere Schlüssel-Speicherung oder Unterstützung für kryptographische Tunnel. Sie umfasst Schnittstellen für Signaturprüfung, Hashwertberechnung sowie Ver- und Entschlüsselung.
- **Separierung:** Dabei handelt es sich um eine softwarebasierte Isolationstechnologie mit einer hohen Verlässlichkeit hinsichtlich der Sicherheit der gegenseitigen Abschottung von Rechen- und Hardware-Ressourcen. Infotainmentbetriebssysteme haben nur auf solche Peripheriegeräte Zugriff, die ihnen beim Kompilieren der Plattform-Software explizit zugeteilt wurden.

Architektur



Nutzen der secunet ACU

- Unterstützt modulare Plattformarchitekturen
- Sichere Integration Browser-basierter Head Units und mobiler Endgeräte ins Fahrzeug
- Verhindert die Ausbreitung von Malware und Fehlern in den Infotainment-Betriebssystemen und -Applikationen
- Keine Beeinflussung der Schutzmechanismen der ACU durch Malware, denn Policy, kryptographische Schlüssel und Routinen sind unabhängig von den Applikationen
- Sichert Plattform-Updates, neue Bordnetzfeatures oder die Abwehr neuer Angriffsvektoren durch die Updatefähigkeit der Policy
- Ermöglicht eine zentrale Implementierung sicherer kryptographischer Routinen und stellt Applikationen kryptographische Services zur Verfügung, ohne dass Geheimnisse mit übergeben werden müssen
- Verbessert die Sicherheit bei der Einbindung von vielen IVI Applikationen und weniger vertrauenswürdigen Applikationen
- Unterstützt auch 2-Prozessor Architekturen zur Umsetzung der Separation

Kommunikationsmodell:

- » Die ACU verwendet Sockets für die Kommunikation zwischen Infotainment und Bordnetz

Mikrobetriebssystemplattform:

- » COQOS von OpenSynergy; zertifizierbar nach Safety-Standards wie DO178B und Security-Standards wie Common Criteria bis zu EAL7
- » Weitere POSIX kompatible Micro OS und Separation Kernels auf Anfrage

Hardware:

- » ARM Cortex A8
- » Andere Hardware auf Anfrage

Unterstützte Boards:

- » Freescale i.MX51
- » Freescale i.MX53

Gastbetriebssysteme:

- » Android 2.1
- » Weitere Betriebssysteme wie z. B. ein Genivi-kompatibles Linux auf Anfrage

Unterstützte Kryptographie:

- » OpenSSL, andere Kryptobibliotheken auf Anfrage
- » RSA mit Schlüsseln bis zu 4096 bit
- » SHA1 (Android kompatibel), längere Hashwerte auf Anfrage
- » AES 128-bit-CBC, längere Schlüssellängen auf Anfrage

Technologie Provider:

Weitere Informationen:
www.secunet.com

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