secunet Security Networks AG

Automotive Spezifische Herausforderungen bei Online Zugängen im Fahrzeug

„Automotive Software Engineering“ - Kolloquium, TU Darmstadt

23. Juni 2009

Dr. Marc Lindlbauer, Leiter embedded Security

Das Unternehmen im Überblick

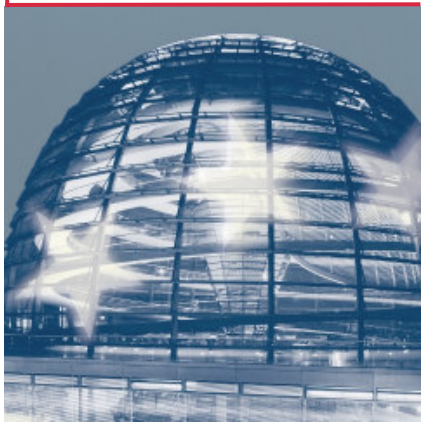
- Der führende deutsche Spezialist für komplexe IT-Sicherheitslösungen
- Sicherheitspartner der Bundesrepublik Deutschland
- Projekte in Industrie, bei Behörden und internationalen Organisationen im In- und Ausland
- Umfassende Kompetenz – kundennah
  - 4 Geschäftsbereiche
  - 7 Standorte in D, Tochterunternehmen in CH und CZ
  - 230 hoch qualifizierte Mitarbeiter
- secunet Security Networks AG
  - Gegründet 1996, börsennotiert seit 1999
  - Umsatz 2008: 52,08 Mio. Euro
  - Anteilseigner: G&D 50 % + 1 Aktie, RWTÜV 26,4 %

secunet Geschäftsbereiche

Hochsicherheit

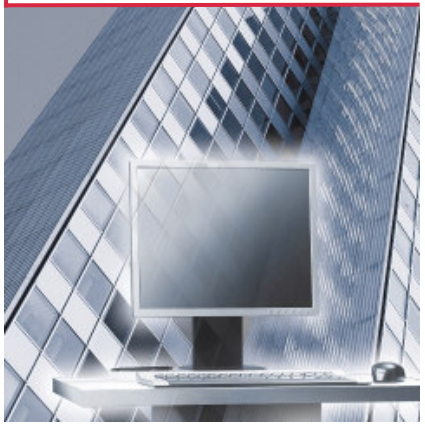
- SINA
- Beratung
- Integration

Government



- E-Government
- Biometrie
- Hoheitliche Dokumente
- Gesundheitswesen
- Sicherheitsvalidierung
- Prüfstelle IT-Konformität

Business Security



- Security Consulting
- Network Security
- Identity Management
- Managed Security Services

Automotive

- Funktionsfreischaltung
- Flashdatensicherheit
- Advanced Engineering
- Online Security

Portfolio
Business Unit Automotive Security

- **Function Enabling**

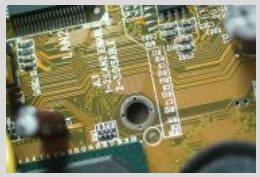
  Design, development and integration of a secure solution for Function Enabling.

- **Flash Ware Protection**

  Design, development and integration of mechanisms to protect ECUs against unauthorized access and programming

- **Advanced Engineering**

  New topics in the context of car2X-/X2car-communication and vehicular network architecture

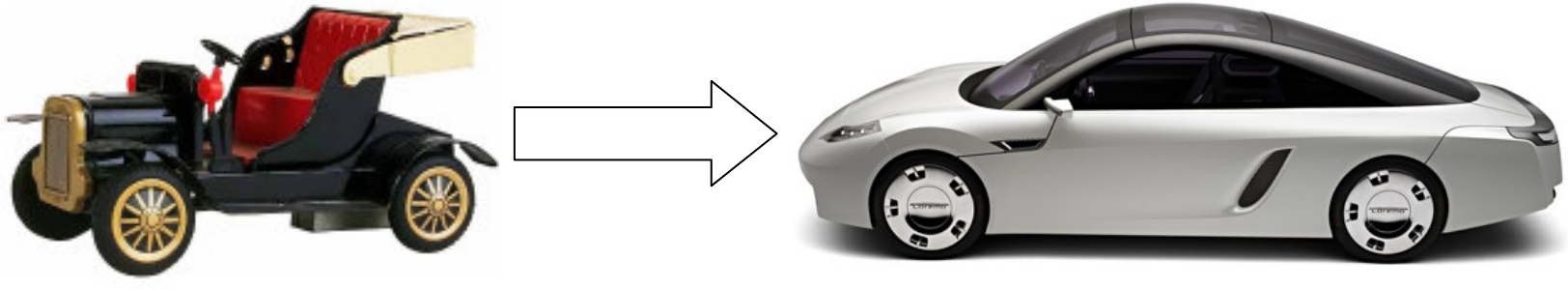


- **Online Security**

  Solutions to protect online access in cars at network / application layer

Verschiebung der Anteile
Mechanik zu Elektronik im Fahrzeug

Der Software Anteil im Auto steigt rapide



Beispiel: Anteil Herstellungskosten (Elektronik / Software)

1900	2000	2010
0% / **0 %**	**22%** / **4 %**	**35%** / **13 %**

Quelle: HVB/Mercer

Elektronischer Datenaustausch im Automobil Heute und in der Zukunft

Fahrzeug - Fahrer

Fahrzeug - Infrastruktur

Fahrzeug - Bordnetz

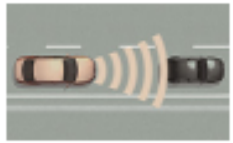
Fahrzeug - Stromnetz

Fahrzeug - Hersteller

Fahrzeug - Fahrzeug

Security relevante Anwendungen im Automobil Heute und in der Zukunft

Bezahlfunktionen



Assistenz-Systeme

Online Content

Wegfahrsperre

Flash-Update

Tuningschutz

Komponenten-Schutz

DRM / Individualisierung

Unterschiede Auto vs. klassische IT

Massive Unterschiede in Bereichen wie:

Connectivity

Bandbreite

Rechenleistung

KnowHow Bediener

Fehlertoleranz

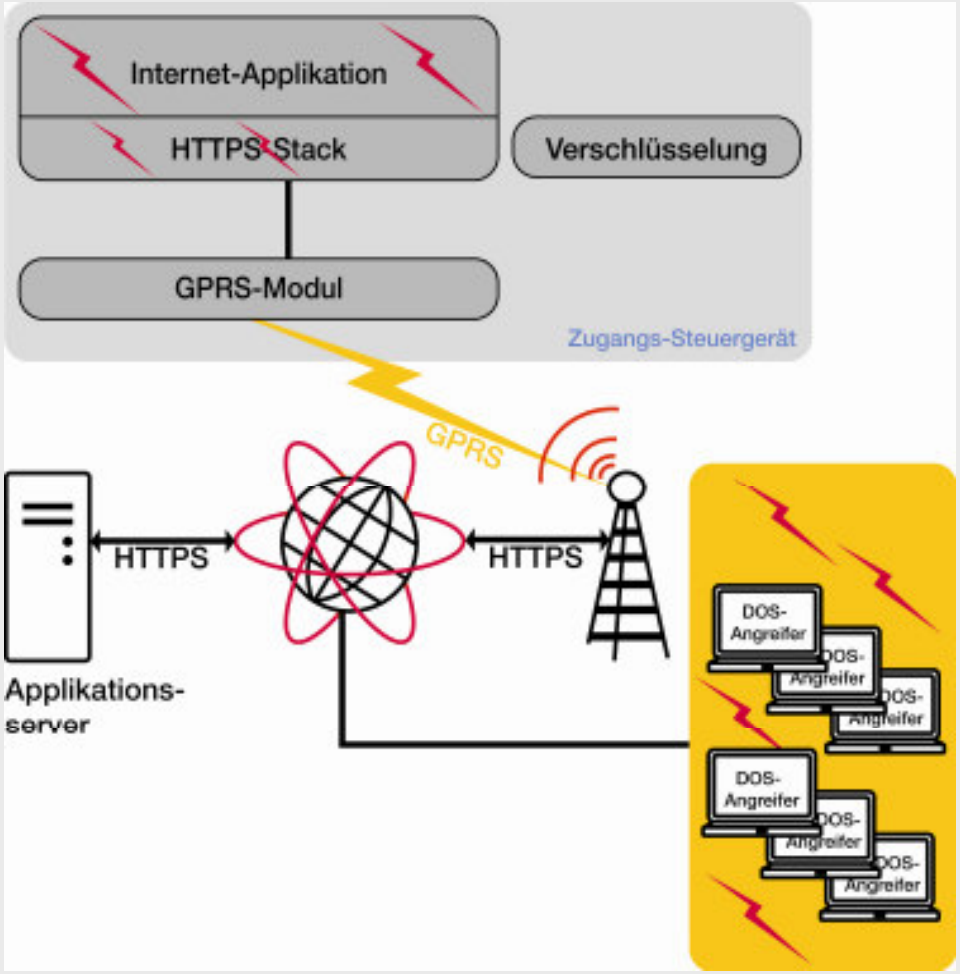
Sicherer Speicher / Sichere Hardware

Entwicklungszyklen

Produkt-Lebenszyklen

…

Angriffe auf Übertragungsebene – Denial of Service (DoS)



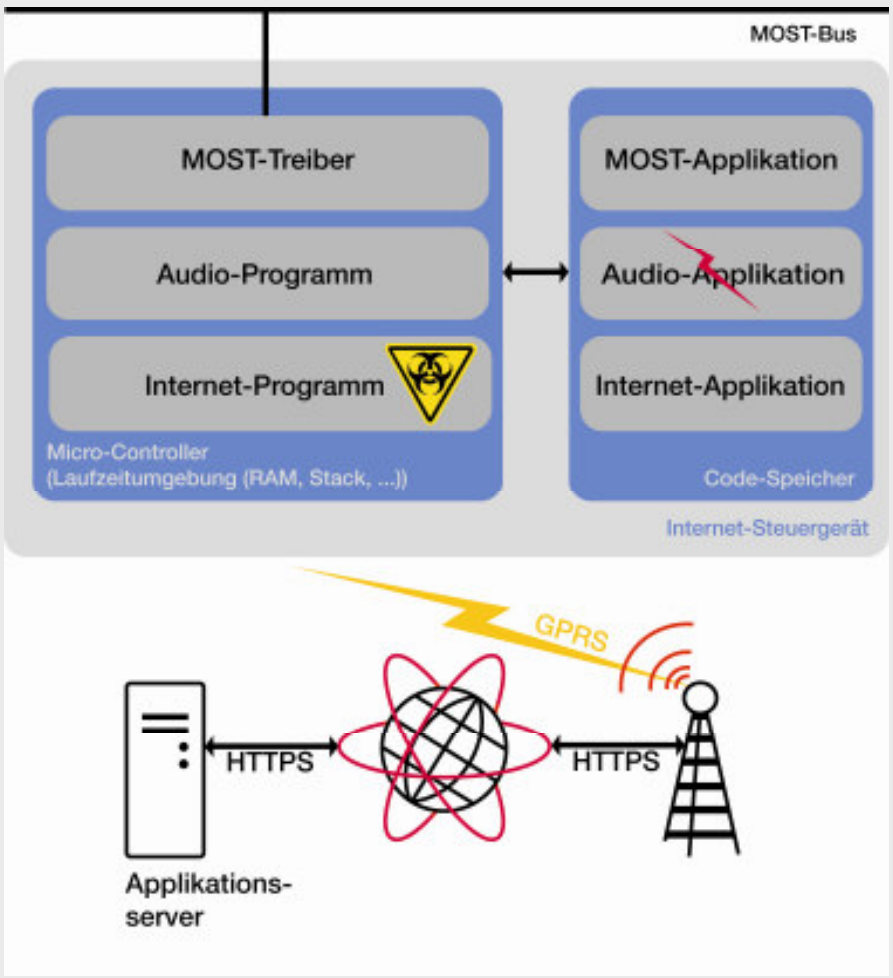
Herausforderung

- Das Fahrzeug ist ein Knoten des globalen Internets
- Die Adresse des Fahrzeugs (z.B. IP-Adresse) ist nicht geheim

Bedrohungsszenario

- Angreifer können die IP-Adresse eines Fahrzeugs ausfindig machen
- Über die bekannten Methoden zur Zusammenschaltung von Rechnern im Internet kann ein mächtiger Strom von Verbindungsanfragen auf das Fahrzeug gelenkt werden.
- Potentiell kann die gesamte Applikation abstürzen ohne wieder gestartet werden zu können.
- Eine authentischer Verbindung hilft nicht als Gegenmaßnahme, da der Verbindungsaufbau vor der Authentisierung stattfindet

Angriffe auf Applikationsebene – Viren



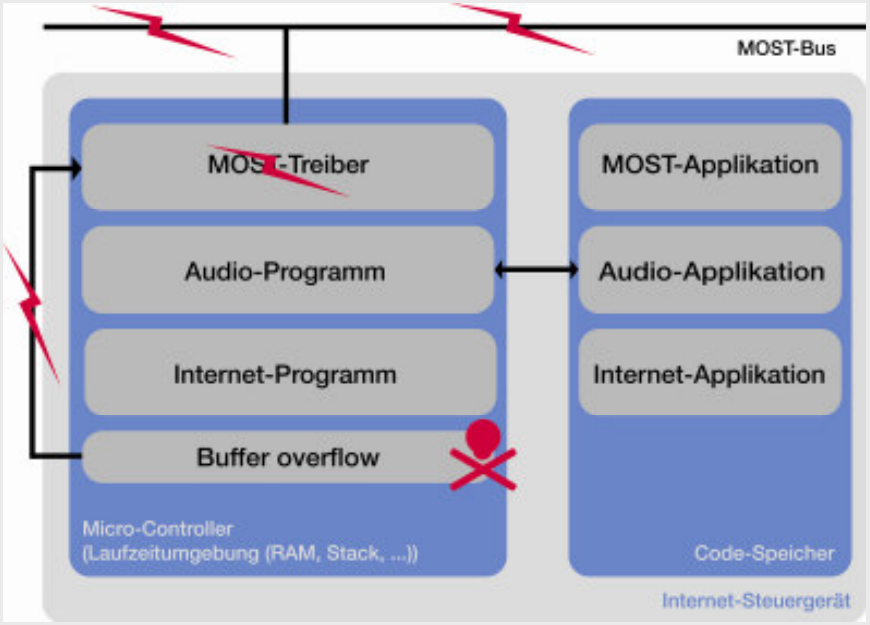
Herausforderung

- Fahrzeug ist nicht immer online
- Herkömmliche Virenscanner können also nicht aktuell gehalten werden
- Nutzer sollen Applikationen ins Fahzeug laden können, die nicht von einem OEM kontrolliert werden

Bedrohungsszenario

- Das Steuergerät bringt infiziert Dateien zur Ausführung
- Benutzer lädt eine infiziert Datei in das Internet-Programm
- Die infiziere Datei ändert die Einstellung der maximalen Lautstärke
- Beim nächsten Start des Fahrzeugs wird der Fahrer durch ein überlautes Radio beeinträchtigt

Angriffe auf Applikationsebene – Buffer-Over-Flow



Herausforderung

- Fahrzeug ist nicht immer online
- Patches für die Steuergeräte-Software können nicht unter allen Umständen zeitnah in das Fahrzeug eingespielt werden.
- Nutzer sollen Applikationen ins Fahzeug laden können, die nicht von einem OEM kontrolliert werden

Bedrohungsszenario

- Durch Programmierlücken wird bösartiger Code in die Laufzeitumgebung der Steuergeräte-CPU geschrieben
- Benutzer lädt infizierte Datei herunter
- Durch eine Programmierlücke wird Code zur Ausführung gebracht, der Nachrichten auf den MOST Bus legt.
- Als Konsequenz ist eine Störung oder ein Zusammenbrechen des MOST Busses denkbar.

Online Access in Cars

Secunet Approach to the Challenges – Security Sensors and Actuators

- Learn e.g. from air back systems
- Identify attack Sensors that do not vary, that react as early as possible, that are easy to implement
- Define Rules for “attack present”
- Rely on simple and stable information → efficient production / service of the car with security functions
- Define Automotive Response (Actuators) to end attack

Priority of Protecting the Vehicle Network

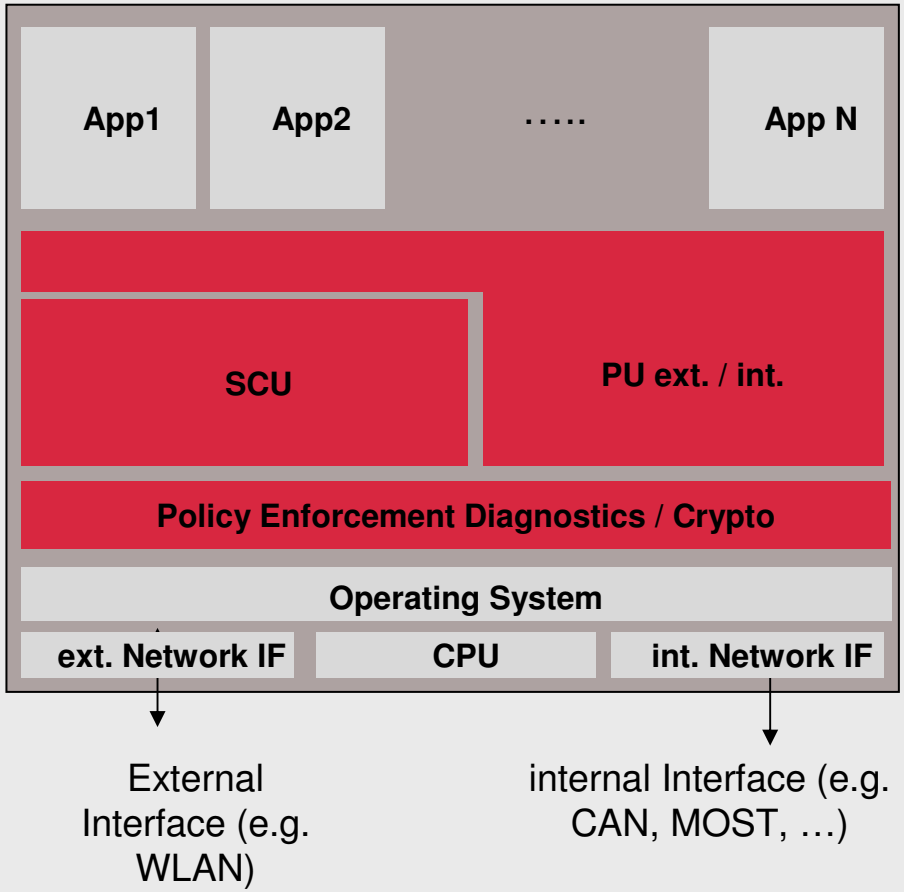
Communication oriented Measures

- Separate network security from Application Security on ECU (cf. corporate Firewalls and Client in the LAN → Client is not responsible for network security)
- Augment OS responsible for connectivity with Decision Function / Actor
- Eventually modify existing Security Sensors or add new ones at network / transport layer
- Optional: OS with RT capabilities / Use dedicated Hardware

Secure Communication Unit / Protection Unit

General Approach – without Sandboxing / Virtualization

Architecture (Module view)



Functionality

- **SCU**
  - Detection of Attacks over externel Interface
  - Adresses Network-/Transport Layer
  - IPSec (Tunnel-) Functionality
- **PU ext. / int.**
  - Detection of abnormal App Behavior
  - Monitoring of communication towards car
- **Policy Enforcement (SCU / PU)**
  - Actively remove car from attack
- **Diagnostics (SCU / PU)**
  - Configuration of the SCU / PU
  - status queries by applications
- **Crypto**
  - Crypto-Primitives (En-/Decryption, Verify / Sign)