Die Sicherheit der Verbraucher in vernetzten Fahrzeugen

7. NRW-Workshop Verbraucherforschung

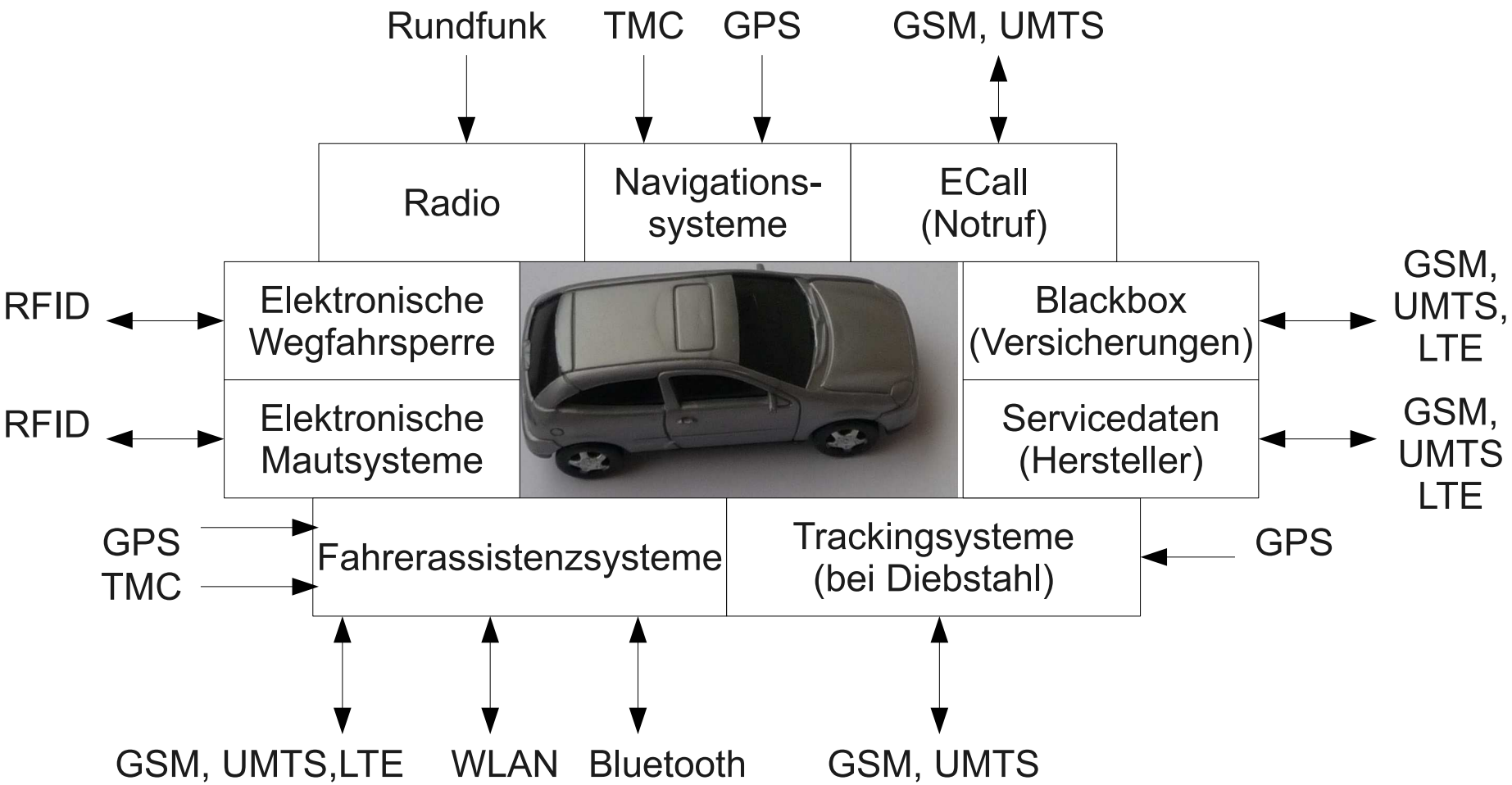
Prof. Dr.-Ing. Kerstin Lemke-Rust

Hochschule Bonn-Rhein-Sieg

15. Juni 2015

Hochschule
Bonn-Rhein-Sieg

Ist-Zustand: Vernetzte Fahrzeuge



Zukunft: Vernetzte Fahrzeuge in mobilen Ad-Hoc Netzwerken

1. Car-to-Infrastruktur/Infrastruktur-to-Car Kommunikation (C2X)
2. Car-to-Car Kommunikation (C2C)

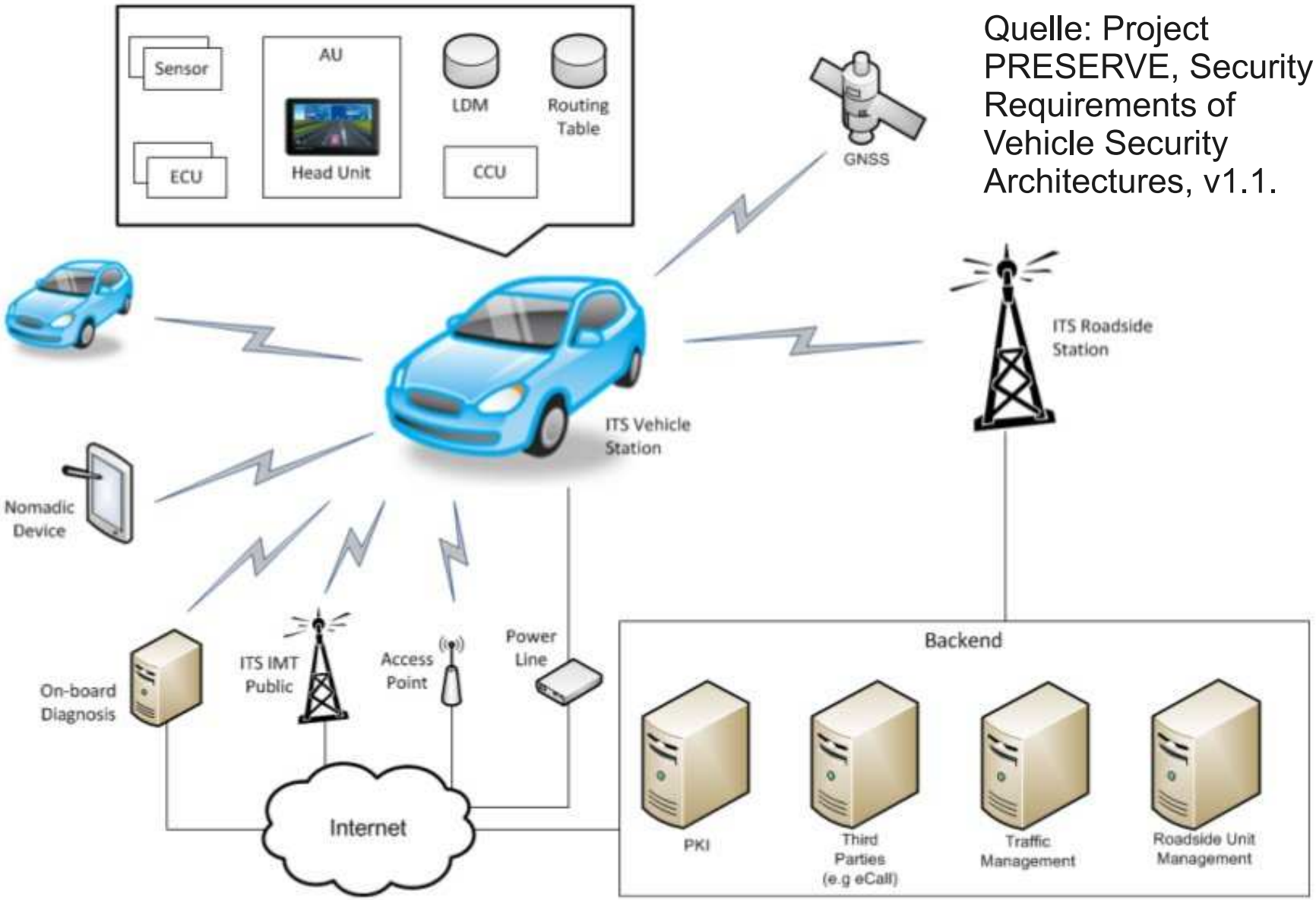
Ziele

1. Erhöhung der Verkehrssicherheit.
2. Bereitstellung aktueller Verkehrsflussinformationen.
3. Bereitstellung von Mehrwertdiensten.

Kommunikationsprotokolle

ITS-G5A (safety), ITS-G5B (non-safety), WLAN.

System: Vernetzte Fahrzeuge mit Infrastruktur



Quelle: Project PRESERVE, Security Requirements of Vehicle Security Architectures, v1.1.

Beispiele für Erhöhung der Verkehrssicherheit

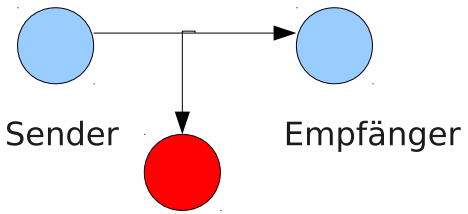
- Warnung herannahendes Rettungsfahrzeug
- Elektronisches Bremslicht
- Warnung langsames Fahrzeug
- Warnung Unfall
- Stauwarnung
- Baustellenwarnung
- usw.

Beispielszenarien

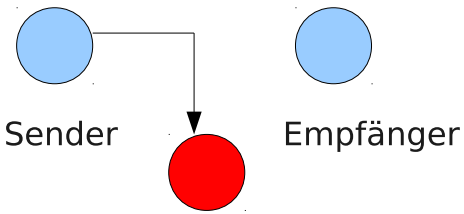
Warnung Unfall

Unautorisiertes Generieren einer Nachricht

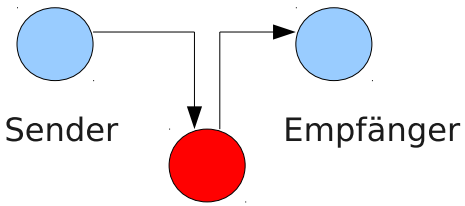
Generische Angriffe auf Funkkommunikation



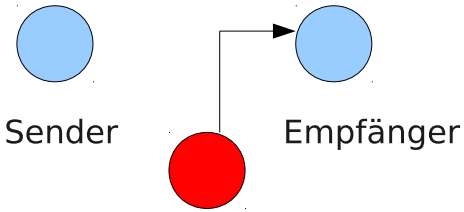
a) Abhören



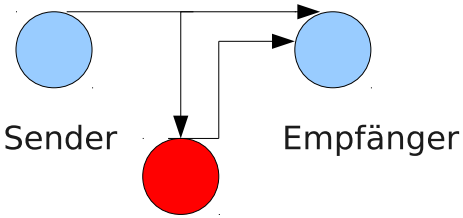
b) Denial-of-Service



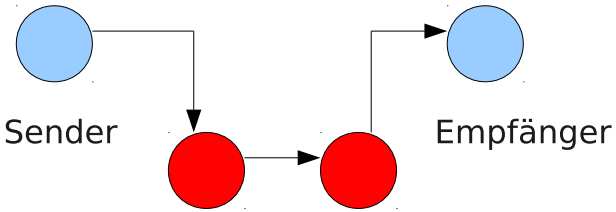
c) Manipulation



d) Generation

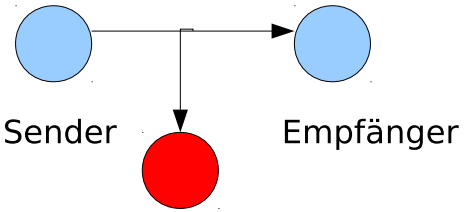


e) Wiedereinspielen



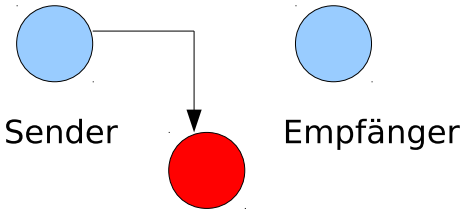
f) Relay

Gegenmaßnahmen



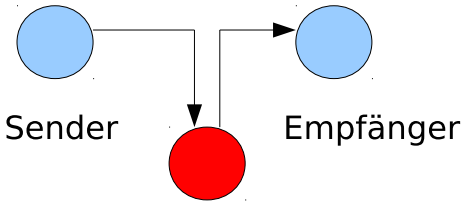
a) Abhören

Verschlüsselung



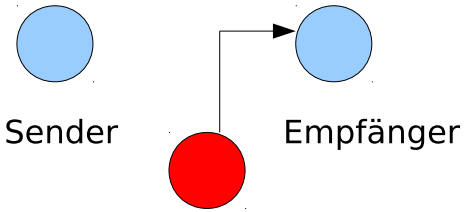
b) Denial-of-Service

Redundanz



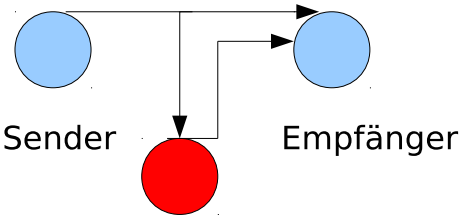
c) Manipulation

Digitale Signatur



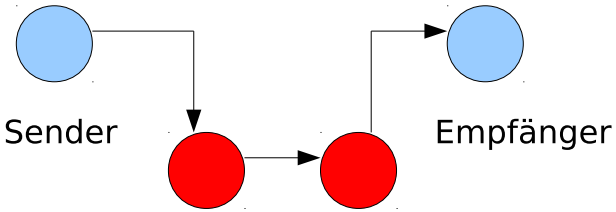
d) Generation

Digitale Signatur



e) Wiedereinspielen

Echte Zeitkoordinaten



f) Relay

Echte Ortskoordinaten

sim^{TD}: Feldversuch

1 sim^{TD}: Einzigartig und erfolgreich

In dem bislang größten Feldversuch zur Car-to-X Kommunikation wurde erstmals mit dem DRIVE Center eine kooperative Verkehrszentrale aufgebaut. Diese war mit den Verkehrszentralen des Landes Hessen und der Stadt Frankfurt am Main über eine standardisierte Schnittstelle vernetzt und kommunizierte über mehr als 100 ITS Roadside Stations (IRS) mittels Car-to-X Technologie mit 120 Fahrzeugen.

Abbildung 1: Platzierung der IRS an einer Verkehrszeichenbrücke

Quelle:
http://www.simtd.de/index.dhtml/deDE/backup_publications/Projektergebnisse.html,
TP5-Abschlussbericht – Teil A

sim^{TD}: Echtzeitanforderungen vs. Kryptographie

3.4 IT-Sicherheit

Im sim^{TD}-Feldversuch konnten aus Performancegründen keine kryptografischen IT-Sicherheitsmaßnahmen eingesetzt und getestet werden. Die kryptografischen Operationen wie Signierung und Verifikation bzw. Verschlüsselung und Entschlüsselung sind sehr rechenaufwendig da sie asymmetrische Schlüssel verwenden. Es hat sich herausgestellt, dass die sim^{TD}-Hardware nicht in der Lage ist, die geforderte Anzahl eingehender Nachrichten kryptografisch zu verarbeiten. Aus diesem Grund wurden in Absprache mit den Beteiligten die entsprechenden IT-Sicherheitsfunktionen nicht im Feldtest eingesetzt.

Quelle:
http://www.simtd.de/index.dhtml/deDE/backup_publications/Projektergebnisse.html,
TP5-Abschlussbericht -- Teil B-3, Version 1.0, 9.12.2013, Seite 130

EU-Projekt: PRESERVE

Hardware Security Module

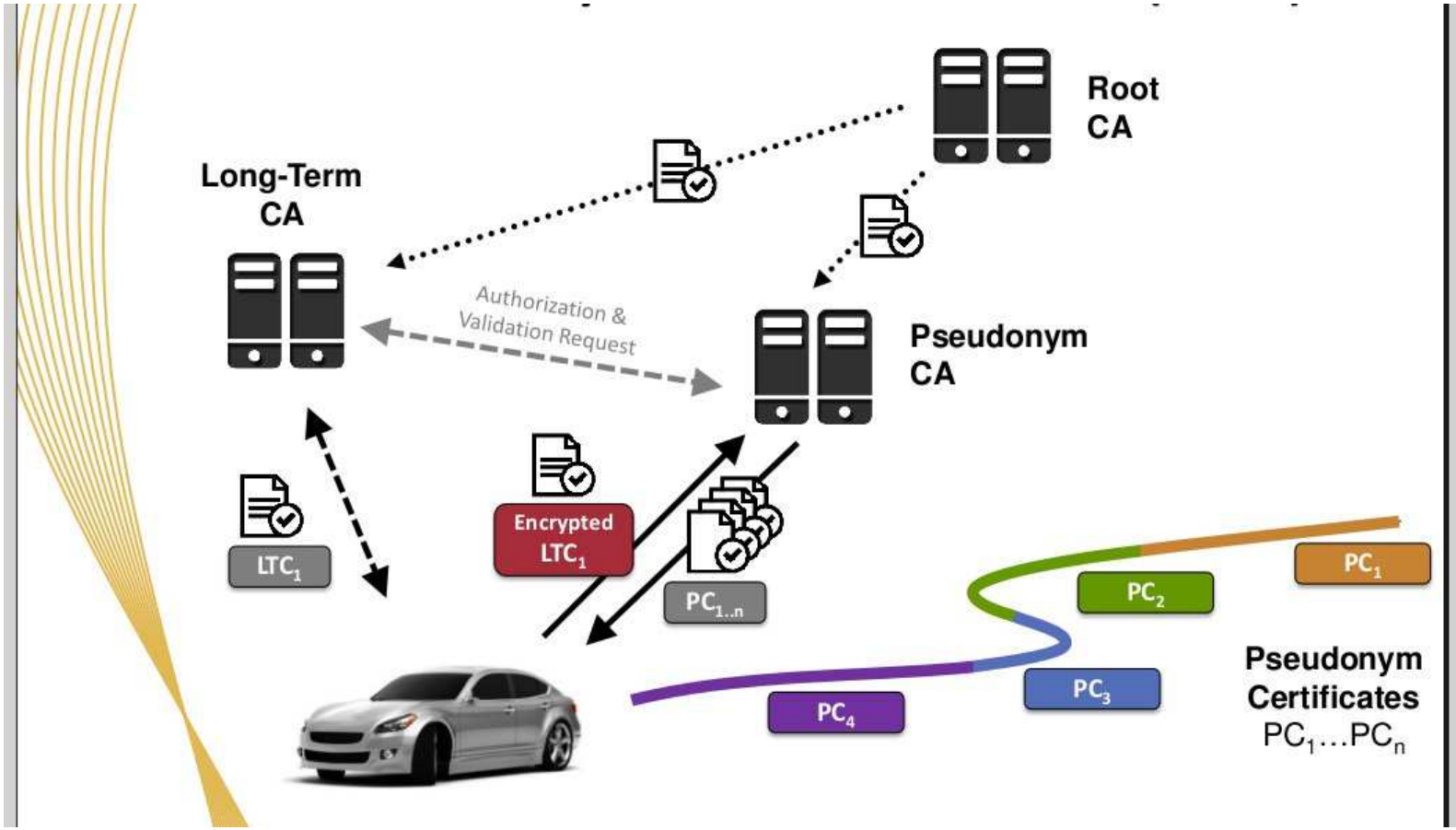
- ASIC ("currently in development")
- Krypto-Algorithmen: ECC, AES, "SHA"
- echter Zufallszahlengenerator
- Vertrauensanker für Secure Boot und Plattformintegrität.

Performance:

- 1000 ECC Verifikationen pro Sekunde

Quelle: http://docbox.etsi.org/Workshop/2013/201301_SECURITYWORKSHOP/06_INTELLIGENTTRANSPORTSYSTEMS/Preserve_BISSMEYER.pdf

EU-Projekt PRESERVE: PKI



Quelle:
http://docbox.etsi.org/Workshop/2013/201301_SECURITYWORKSHOP/06_INTELLIGENTTRANSPORTSYSTEMS/Preserve_BISSMEYER.pdf

Hoch komplexe Fahrzeug-interne Komponenten

In einem Fahrzeug der Luxusklasse sind heute zwischen 70 und 120 Steuergeräte zu finden.

Ein modernes Premium-Auto verfügt über 100 Millionen Zeilen Software-Code.

Bis zum Jahr 2020 wird mit rund 300 Millionen LOC im Auto gerechnet.

In tausend Zeilen Code können im Durchschnitt 20 bis 30 Bugs enthalten sein.

Quelle: `http://www.elektroniknet.de/automotive/tools/artikel/117489/1`

Angreifbarkeit Fahrzeug-interne Bussysteme

http://www.autosec.org/publications.html

Wenn ein Angreifer Zugang auf einen Fahrzeug-internen CAN Bus hat, so kann er praktisch alle Fahrzeug-Komponenten (Motor, Bremsen, Heizung, Licht, Instrumentenanzeige, Radio, Türschloss, etc.) kontrollieren.
Nachgewiesene Zugangsmöglichkeiten:

- Werkstattzugang (OBD-II),
- Kommunikationsschnittstellen der Telematik Einheit von Fahrzeugen.

> *We believe that car owners today should not be overly concerned at this time. It requires significant sophistication to develop the capabilities described in our papers and we are unaware of any attackers who are even targeting automobiles at this time.*
>
> Quelle: `http://www.autosec.org/faq.html`

Weitere Schwierigkeiten ...

Organisatorische Rahmenbedingungen

- Lange Lebensdauer eines PKW (mehr als 20 Jahre).
- Länderübergreifende PKI erforderlich.

Organisatorische Fragestellungen

- Langzeit Wartung der Software/Hardware?
- Rückruf von Langzeitzertifikaten (z.B. von Unfallfahrzeugen)?
- Vertrauenswürdiges Werkstattpersonal?

C2C und C2X Kommunikationssysteme stehen noch vor großen Herausforderungen, bevor sie großflächig eingeführt werden können.

Was ist aus Verbrauchersicht wünschenswert? 1/2

- Gesetzliche Sicherheitsanforderungen und unabhängige Evaluierung von sicherheitssensitiven Telematikeinrichtungen und der elektronischen Wegfahrsperre.
- Öffentlich verfügbare Spezifikation von Telematikeinrichtungen inkl. Kommunikationsschnittstellen.
- Kontrolle und Analysemöglichkeit der übertragenen Fahrtinformationsdaten für den Fahrzeugführer.
- Ende-zu-Ende Verschlüsselung und Integritätssicherung von Kommunikationsdaten in Telematikanwendungen.
- Kosten/Nutzen Betrachtung bei jeder C2C/C2X Anwendung.
- Benutzerfreundlichkeit von Telematikeinrichtungen.
- Automatische Reaktionen im Fahrzeug durch empfangene C2C/C2X Nachrichten sollten bei aktuellem Stand der Technik unterbleiben.

Was ist aus Verbrauchersicht wünschenswert? 2/2

Die IT nimmt im Fahrzeug einen immer höheren Stellenwert ein.
Die Komplexität der IT ist hoch, die Verletzlichkeit durch die IT auch.
Zudem ist die interne Fahrzeug-Architektur grundsätzlich offen und nicht speziell geschützt gegen Angriffe.

- Verfügbarkeit des Fahrzeugs auch bei Störungen in Telematikeinheiten.
- Garantie einer langen Lebensdauer von Hardware-Komponenten.
- Integre Soft- und Hardwarekomponenten.
- Erkennungs- und Entfernungsmöglichkeit von Schadsoftware im Auto.
- Verifizierte Software-Updates.
- Spezielle Abschirmung von sicherheitsrelevanten Komponenten im Fahrzeug-internen Netzwerk gegen Zugriff vom allgemeinen CAN-Bus.

Im Auto hat Safety Priorität vor Security.