IT-Sicherheit im Automobil

Dr. André Weimerskirch

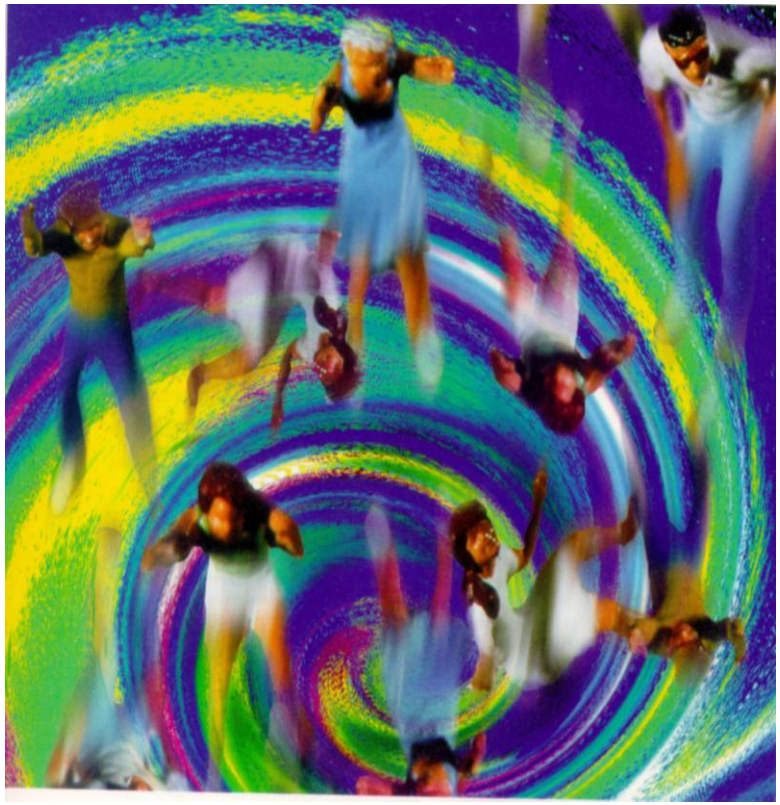
rub.de/autokongress2, Bochum, 1. Juni 2005

escrypt
Embedded Security

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

t: +49(0)234 43 870 209
f: +49(0)234 43 870 211

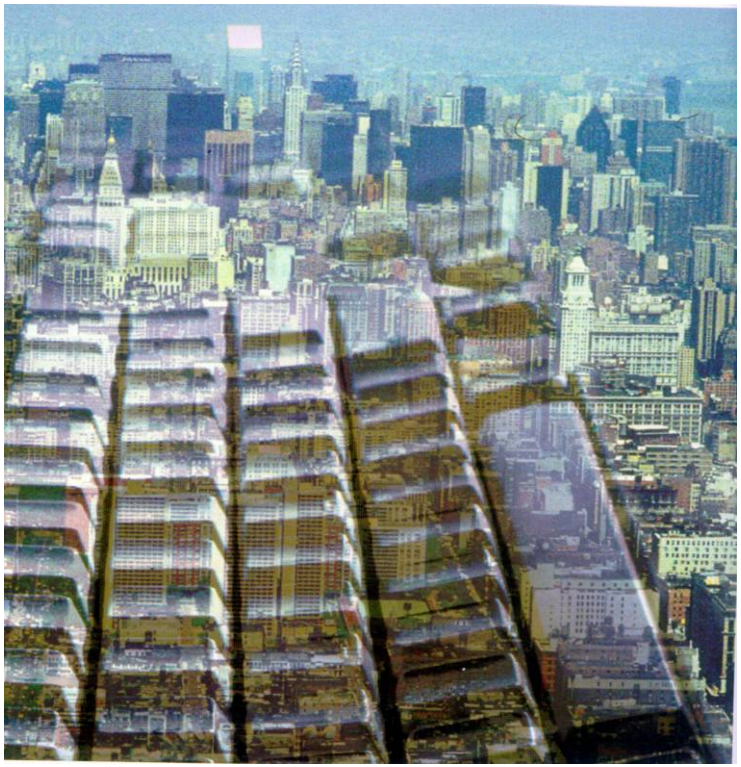
Status Quo



„Wenn das Auto die gleiche Entwicklung gemacht hätte wie der Computer, dann würde ein Rolls Royce heute 150 DM kosten, drei Milliliter auf 100 Kilometer verbrauchen und einmal im Jahr alle Insassen bei einer Explosion umbringen.“

ROBERT X. CRINGELY, INFOWORLD

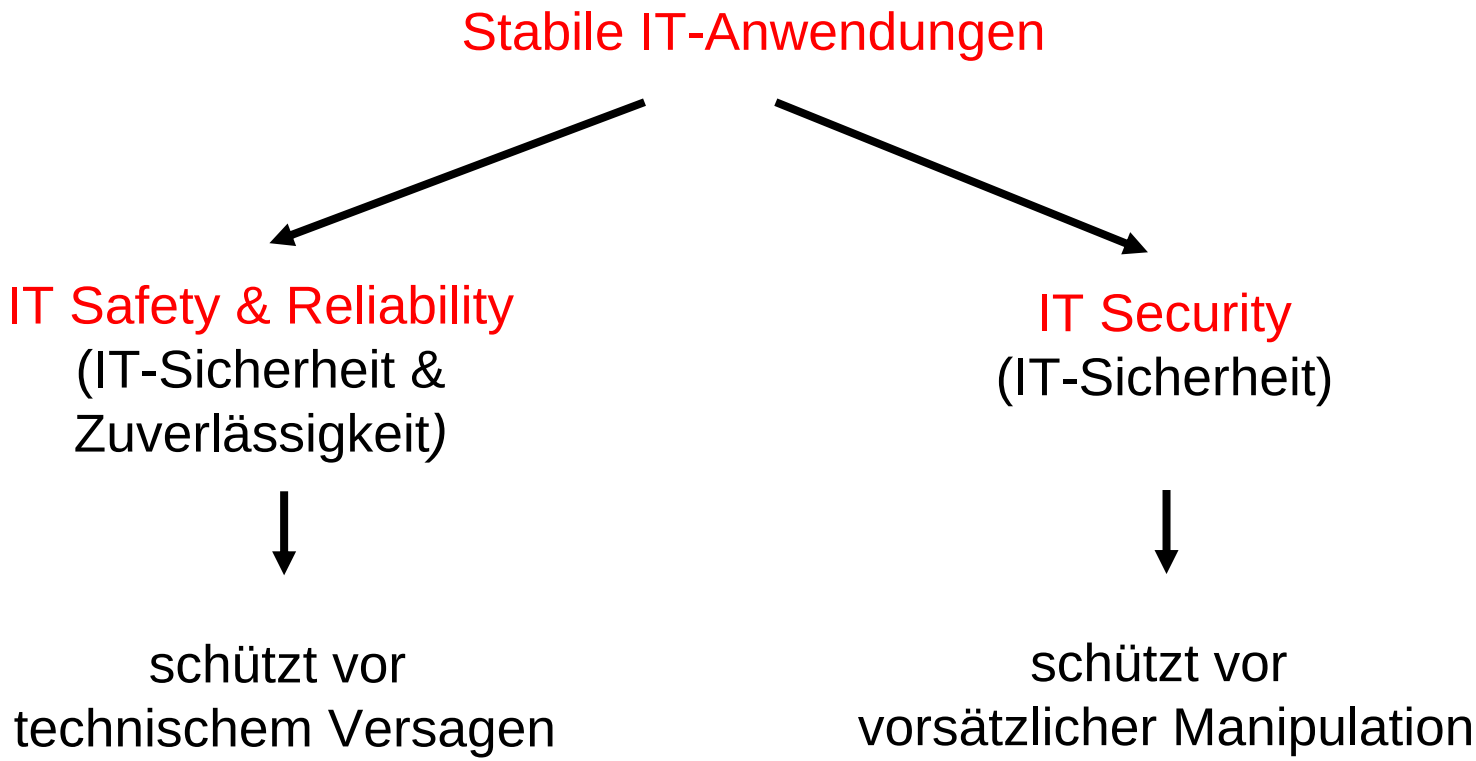
Status Quo



„Wenn das Auto die gleiche Entwicklung wie die Telekommunikation gemacht hätte, dann würde ein VW Käfer heute 10^{9} km/h schnell sein, 400 Millionen PS haben, und würde routinemäßig 4 Mal pro Jahr ausgeraubt, ohne dass der Fahrer es merkt.“

escrypt GmbH

Definition: IT Safety contra IT Security



Gliederung

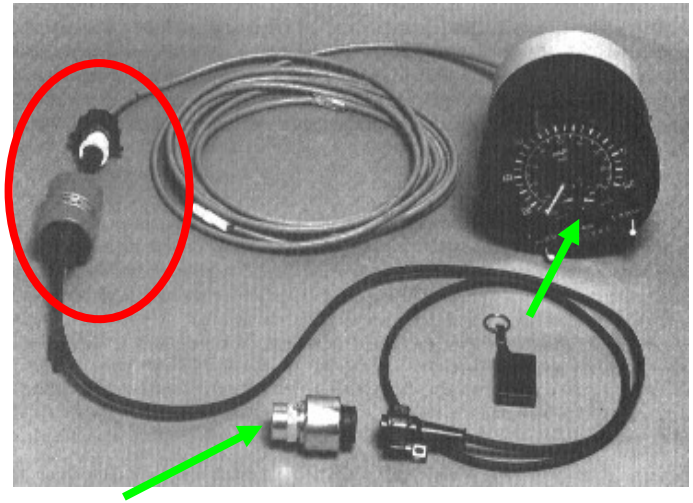
- **Fallstudie**
- Zukünftige Anwendungen mit Sicherheitsbedarf
- Wer sind die Angreifer?
- Warum IT-Sicherheit in eingebetteten Systemen schwierig ist
- Lösungsansätze
- Schlussfolgerungen

Fallstudie Kombiinstrumente

Tachograph

- LKW-Fahrer-Kontrolle per digitalem Tachograph: Sensor & Anzeigeinstrument

- Ausgeklügelte Manipulations-Vorrichtung ermöglicht Betrug



aus: R. Anderson “Security Engineering”, Wiley, 2001

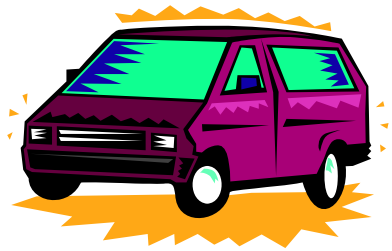
Aber: Kryptographische Mechanismen können solche Attacken verhindern

Fallstudie Diebstahlschutz im Automobil

Wegfahrsperre:

- wechselnder Code
  (zeitvariantes Passwort)

$code = f_k(T_i)$



wobei $f_k()$ eine kryptographische Einwegfunktion ist

Trotzdem werden immer noch zahlreiche Autos gestohlen!

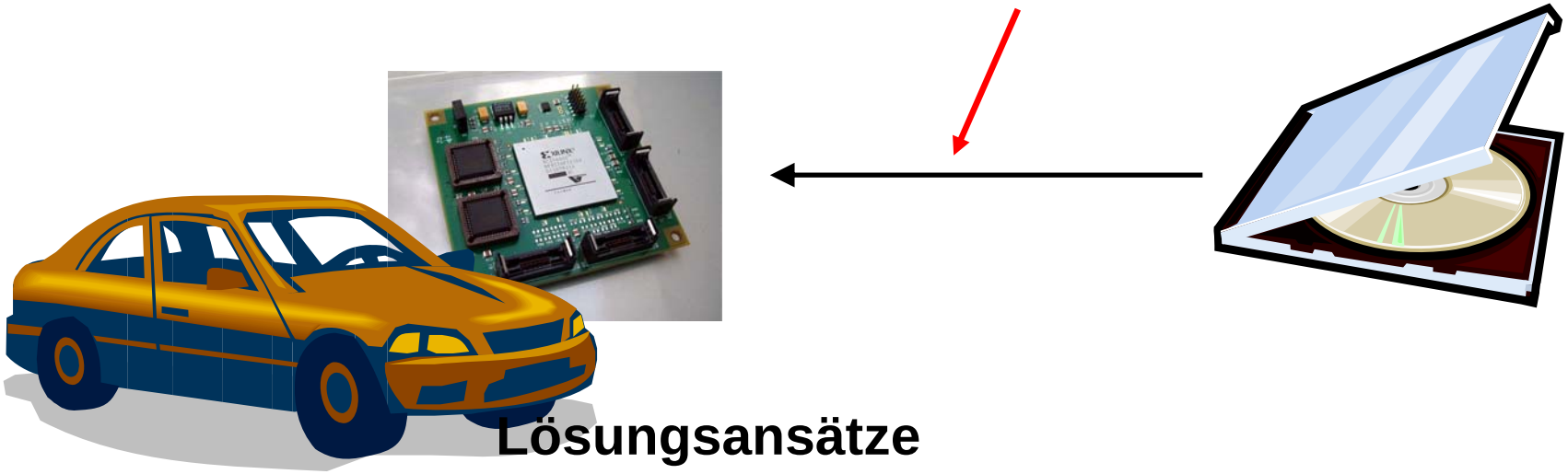
Fallstudie Bussystem im Automobil

Bangkok Post

Bangkok - May 13, 2003: Finance Minister Suchart Jaovisidha turned escape artist yesterday after the computer system in his BMW 520 failed, trapping him inside.

Fallstudie sicheres Flashen

Software wird manipuliert
und/oder mitgelesen



Lösungsansätze

- Kryptographische Verfahren im Bootloader
- Hürde: Einbindung in Prozessabläufe

Gliederung

- Fallstudie
- **Zukünftige Anwendungen mit Sicherheitsbedarf**
- Wer sind die Angreifer?
- Warum IT-Sicherheit in eingebetteten Systemen schwierig ist
- Lösungsansätze
- Schlussfolgerungen

Neue Geschäftsmodelle

Kooperation

- Notfallbremse
- Parkplatzsuche
- Vorfahrtsregelung

Vernetzte Systeme

- Elektronische Maut
- Traffic Management
- Car-to-car Kommunikation
- Notfallbremse
- …

Zukünftige Anwendungen mit Sicherheitsbedarf

- **Diebstahlschutz**
  - Komponentenidentifikation
- **Rechtl. & behördl. Einsatzbereiche**
  - Digitale Signatur Gesetz
  - Elektronisches Kennzeichen
- **Innovationslawine**

Gliederung

- Fallstudie
- Zukünftige Anwendungen mit Sicherheitsbedarf
- **Wer sind die Angreifer?**
- Warum IT-Sicherheit in eingebetteten Systemen schwierig ist
- Lösungsansätze
- Schlussfolgerungen

Wer sind die Angreifer?

Besitzer

- geringe bis mittlere Erfahrung
- Physikalischer Zugang

Mechaniker/Mitarbeiter

- Technisch ausgebildet
- Insiderwissen
- Physikalischer Zugang

Wettbewerber/Gruppe

- evtl. sehr große Resourcen
- evtl. physikalischer Zugang

Einige Beispiele für attraktive Angriffe

- **Besitzer** entzieht sich der **Zahlung von Mautgebühren**
- **Besitzer** zahlt nicht für digitale Angebote
- **Besitzer** erhöht **PS-Zahl** oder dreht den **Kilometerstand** zurück
- **Dritte** spielen böswillig **Software Updates** auf
- Die **Konkurrenz** beschafft sich technische Daten aus Telematiksystemen

Gliederung

- Fallstudie
- Zukünftige Anwendungen mit Sicherheitsbedarf
- Wer sind die Angreifer?
- **Warum IT-Sicherheit in eingebetteten Systemen schwierig ist**
- Lösungsansätze
- Schlussfolgerungen

Warum IT-Sicherheit schwierig ist

Moderne IT-Sicherheit bietet:

- Kommunikationssicherheit
- Manipulationsschutz
- Rechtemanagement (Digital Rights Management)

basierend auf kryptographischen Algorithmen und Protokollen …

⇒ **Alle Sicherheitsprobleme können (theoretisch) gelöst werden**

Warum IT-Sicherheit schwierig ist

Wo liegt das Problem?

Am häufigsten bei der

Embedded Security,

die sich stark von konventioneller Computersicherheit (Internetsicherheit, Firewalls, Anti-Viren SW, ...) unterscheidet!

Warum IT-Sicherheit schwierig ist

- **Beschränkte Umgebungen:**
  Oft nur 8 or 16 bit μP für rechenintensive Kryptoverfahren (Algorithmen mit 1024 Bit Arithmetik etc.)
- **Physikalischer Zugang der Angreifer**:
  Seitenkanalangriffe, Reverse Engineering, …
- **Komplexe Vernetzung**
  Externe Sicherheit (GSM etc.) interagiert mit interner Buskommunikation, ad-hoc Anbindungen, ...
- **Systemkomplexität**:
  Viele Ebenen sind involviert (Hersteller, 1…x-tier Zulieferer, Besitzer, Verwaltung): Wer hat kryptographische Privilegien? Rollenverteilung? ...
- **Historische Entwicklung:**
  Designer möchten, dass das System funktioniert, IT-Sicherheit ist zweitrangig
- **Kulturelle Probleme:**
  IT Ingenieure müssen interdisziplinär arbeiten: Kryptoalgorithmen, Kryptoprotokolle, physikalische Sicherheit, …

Gliederung

- Fallstudie
- Zukünftige Anwendungen mit Sicherheitsbedarf
- Wer sind die Angreifer?
- Warum IT-Sicherheit in eingebetteten Systemen schwierig ist
- **Lösungsansätze**
- Schlussfolgerungen

Lösungsansätze

- Effiziente kryptographische Mechanismen
  - Digitale Signaturen
  - Elliptische Kurven
- Contents Protection
  - Digital Rights Management
  - Trusted Computing
- Sicherer Systementwurf
  - Betrachtung der Gesamtheit

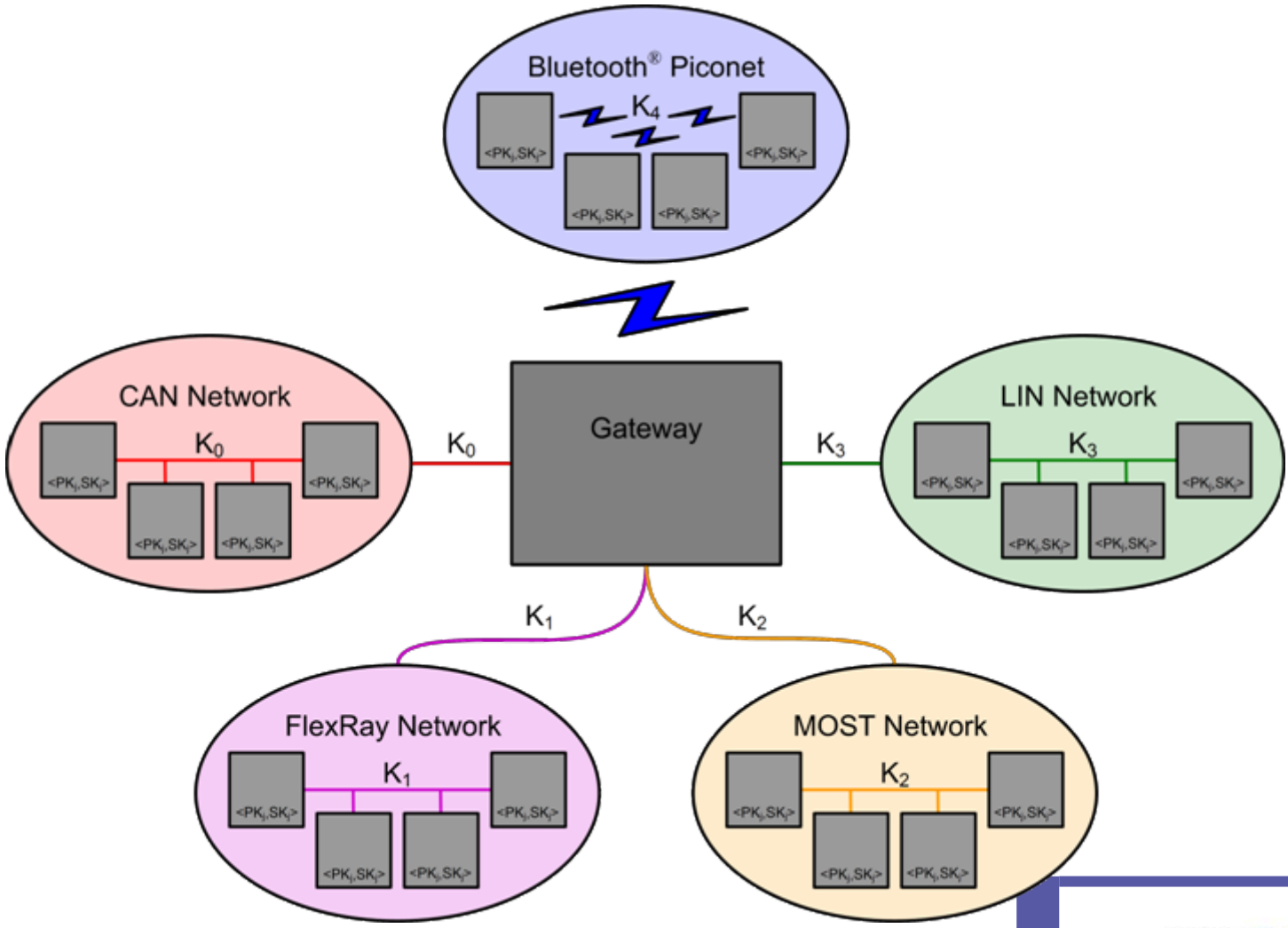
Komponentenidentifikation

- Auto und Komponente „kennen sich“

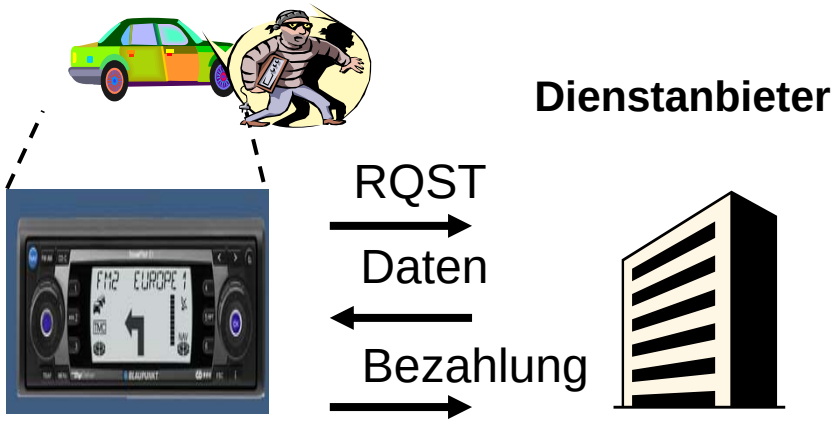
⇒ **Komponente wird an Auto „angekettet“**

- **Schutzziele**
  - Schutz vor gefälschten Teilen
  - Diebstahlschutz
  - Manipulationsschutz

Sichere Bussysteme im Automobil



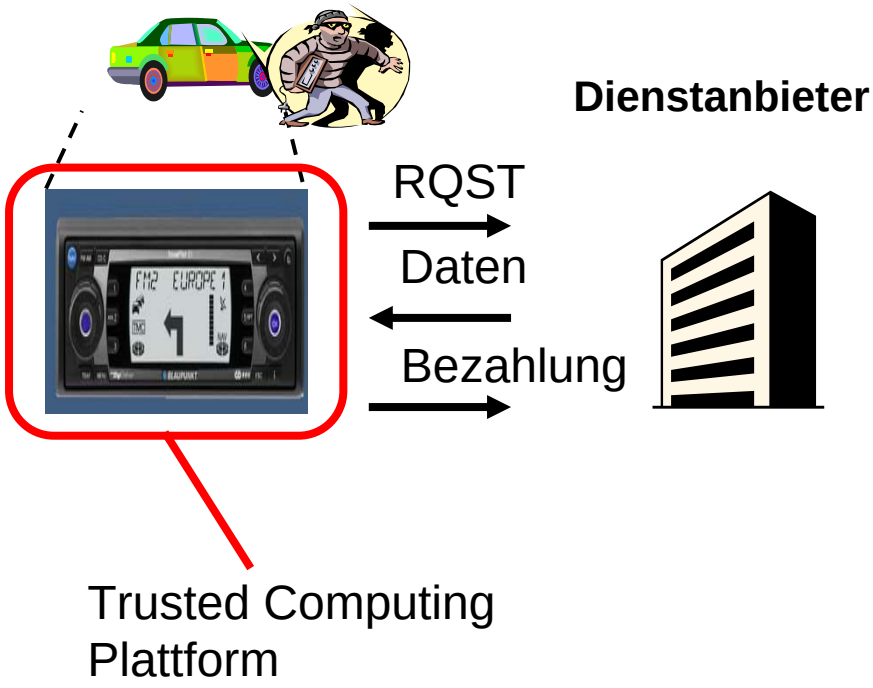
Digital Rights Management



Navigationsdaten

- Service on demand
- Neues Geschäftsmodell
- Basierend auf der Notwendigkeit, jede Navigationsroute neu zu erwerben

Digital Rights Management



Lösungsansätze

- Verschlüsselte und authentifizierte Kommunikation
- Verschlüsselte und authentifizierte Daten
- Sichere Hard- und Software
- Wohldefinierte Regeln
- Wasserzeichen
- Sicheres Systemdesign

Gliederung

- Fallstudie
- Zukünftige Anwendungen mit Sicherheitsbedarf
- Wer sind die Angreifer?
- Warum IT-Sicherheit in eingebetteten Systemen schwierig ist
- Lösungsansätze
- **Schlussfolgerungen**

Schlussfolgerungen

- **IT-Security** wird ein zentrales Thema für zukünftige Automobilgenerationen
- **„Embedded security“ hat ganz bestimmte Anforderungen**: beschränkte Umgebungen, Seitenkanalattacken, …
- **Neue Geschäftsfelder durch IT-Sicherheitslösungen**: besseres CRM, pay-per-view, neue Dienste

⇒ **Embedded Security ist *enabling Technologie* für zukünftige Anwendungen**

Vielen Dank!

Dr.-Ing. André Weimerskirch

Leiter Entwicklung, escrypt GmbH

aweimerskirch@escrypt.com

escrypt
Embedded Security

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

t: +49(0)234 43 870 209
f: +49(0)234 43 870 211

eurobits

Europäisches Kompetenzzentrum für IT- Sicherheit

Horst Görtz Institut für IT Sicherheit

Institut für Sicherheit im eBusiness

GITS AG
- Training
- Technologie-transfer

escrypt GmbH

Embedded Security

GITS Projekt GmbH
Haus für IT Sicherheit

escrypt – Auf einen Blick

- Profil: Systemhaus für eingebettete Sicherheit
- Leistungen:
  - Beratung
  - System-, Software- und Hardware-Entwicklung
- weltweit einziger Anbieter, der auf IT-Sicherheit im Automobil spezialisiert ist
- mit über 10 Jahren Erfahrung im Bereich eingebettete Sicherheit einmalige technologische Expertise
- Einbettung in eurobits (Europas größtes Kompetenzzentrum für Datensicherheit)
- Kunden: Alle großen deutschen Automobilhersteller & führende Zulieferer