

Sichere Datenkommunikation im Automobil

Kompetenztreffen ZVEI e.V.

Kronberg, den 16. Januar 2004

Willi Mannheims, Vorstandsvorsitzender GITS AG

Inhalt

- **Motivation: Warum Autos IT- Sicherheit benötigen.**
- Wer sind die Angreifer?
- Warum IT- Sicherheit in Autos schwierig ist
- Schlussfolgerungen
- Eurobits

IT- Sicherheit und Autos – WARUM ?

Autodiebstahl: Beispiele

- In GB stehlen Jugendliche Autos, um z.B. Mutproben durchzuführen oder Airbag Systeme aus Spaß zu testen.
- Taschenrechner mit einer IR Oberfläche und einem speziellen Programm können französische Autos öffnen.
- Während ein Gastredner in einer Fernsehshow über Autodiebstahl referiert wird sein Mercedes gestohlen
- Ein Lese/Schreib- Wiedergabegerät wird durch eine Kopie ersetzt (gleicher Anbieter)
- Ehemalige Auto Kontrolleure pflegen neue Automodelle zu stehlen
- Mit bestimmten Zusatzsteckern lassen sich Autos starten.

IT- Sicherheit und Autos – WARUM ?

Autodiebstahl: Deutschland

<u>Jahr</u>	<u>Anzahl</u>	<u>Schaden / Mio DM</u>		
1990	39.935	260.0		
1991	55.288	368.2	←	Neue Bundesländer
1992	90.020	656.8		
1993	105.543	800.0	←	Einführung neuer elektronischer Wegfahrsperren
1994	104.890	766.6		
1995	89.072	587.4		
1996	76.266	496.5		
1997	65.861	427.5		
1998	58.646	378.0		
1999	48.742	332.9		
2000	42.560	316.2		
2001	37.549	307.5		
2002	34.775	300.9		

Quelle: Gesamtverband Deutscher
Versicherungsgesellschaften

IT- Sicherheit und Autos – WARUM ?

Autodiebstahl: Deutschland

<u>Marke</u>	<u>abs. Anzahl</u>	<u>Marke</u>	<u>rel. Anzahl</u>
VW	10.697	Trabant	3.1
Audi	5.580	Ssangyong	2.9
Mercedes	4.994	Audi	2.8
Opel	3.193	Porsche	1.8
BMW	2.986	Mercedes	1.8
Ford	1.555	VW	1.6
Fiat	784	Chrysler	1.6
Renault	691	BMW	1.5
Nissan	597	GM (USA)	1.4

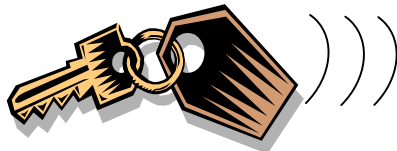
Jahr 2002, Quelle: GDV

pro 1000 Autos

IT- Sicherheit und Autos – WARUM ?

Wegfahrsperre:

- frühe Diebstahl-Kontrolle: einheitlicher Code (Passwort)
- Lauscher kopiert Schlüssel



code



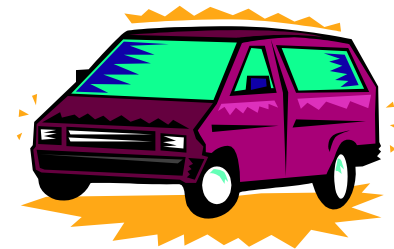
IT- Sicherheit und Autos – WARUM ?

Wegfahrsperre:

- weiter entwickelte Diebstahl-Kontrolle: wechselnder Code (Passwort)



$$\text{code} = f_k(T_i)$$



wobei $f_k()$ eine kryptographische one-way-Funktion ist

Frage: Nur begrenzter Anwendungsbereich mit Sicherheitsbedarf?

IT- Sicherheit und Autos – WARUM ?

Verhinderung der Manipulation von Betriebsdaten

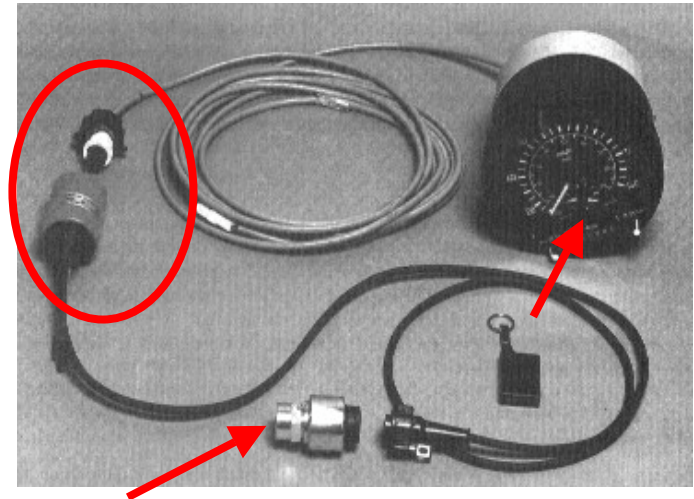
- Moderne Fahrzeuge speichern Betriebsdaten elektronisch
- Daten der Laufleistung (z.B. Tachometer) werden elektronisch abgelegt
- Manipulation (nicht autorisiertes Verändern) der Daten einfach:
 - Vielzahl von Angeboten im Internet, Tages- oder Fachzeitungen
 - Kosten (einmalig) zwischen 100-200 Euro¹
 - Gerät zur Programmierung ca. 5.000 Euro¹

¹ Quelle: www.tachodreh.de, 2003

IT- Sicherheit und Autos – WARUM ?

Tachomanipulation:

- LKW-Fahrer-Kontrolle per digitalem Tachograph:
Sensor & Anzeigeeinstrument
- Ausgeklügelte **Manipulations-Vorrichtung** ermöglicht Betrug



aus: R. Anderson "Security Engineering", Wiley, 2001

Anmerkung: Kryptografische Mechanismen können solche Attacken verhindern

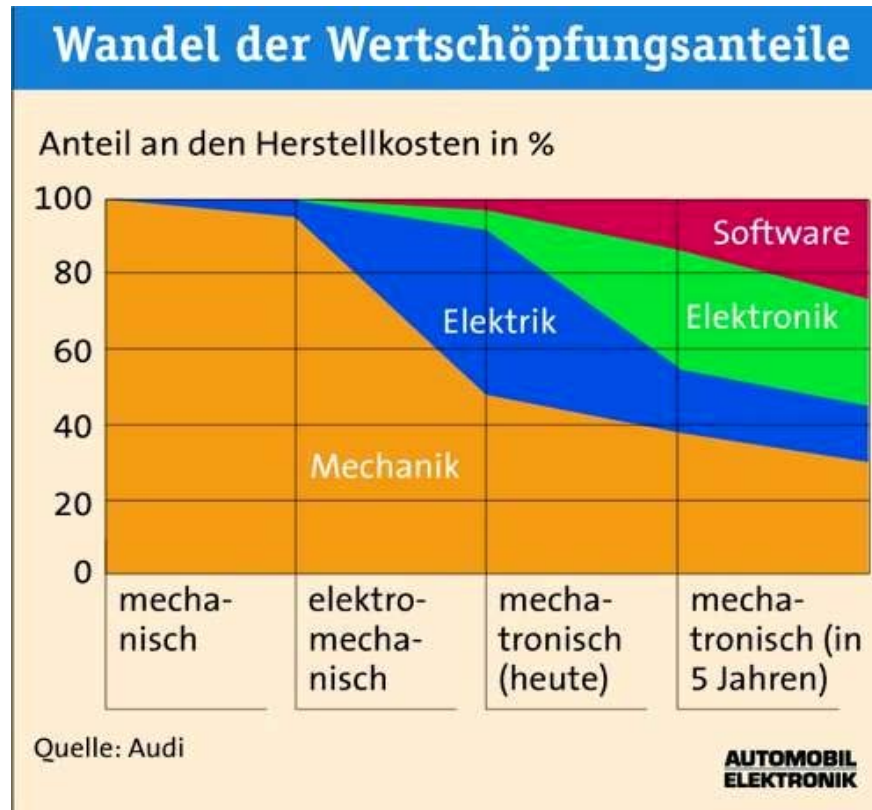
IT- Sicherheit und Autos – WARUM ?

Verhinderung der Manipulation von Steuerungssoftware

Auszug aus einem Werbeschreiben eines Chiptuning Anbieters:

- ...eine garantiert fehlerfreie Tuningsoftware, welche sich bei Wartungsarbeiten in den Fachwerkstätten am Diagnoseanschluss vollständig neutral und unverändert wie im Serienstand verhält.
- ...somit meldet sich Ihr Fahrzeug bei der Fahrzeugdiagnose auch mit seiner korrekten Fahrzeugidentitätsnummer, der originalen Motornummer, der korrekten Getriebeversion, allen originalen Ausstattungskodierungen, sowie allen sonstigen korrekten fahrzeugspezifischen Eigenheiten.
- ...Es ist ja Ihre Originalsoftware - nur eben optimiert.
- ...Der Nachweis, dass in Ihrem Fahrzeug eine optimierte Tuningsoftware zum Einsatz kommt, kann über die Fahrzeugdiagnose seitens der Fachwerkstätten zumeist auch nicht geführt werden

Automotive – Wie sieht die Zukunft aus?



} IT > 45%

Zukünftige Anwendungen mit Sicherheitsbedarf

- Per Netzwerk betriebenes Auto (GSM, 3G, WiFi):
 - In Luxusfahrzeugen sind bis zu 90 vernetzte Kleinrechner (bis zu 3 Km Kabel)
 - Zugriff-Kontrolle des Auto-Netzwerks (Hacker im ABS?)
 - Sicherung & Integrität der Kommunikation
 - Anonymität (Datenschutz von Standort- & Auto-Angaben)
- Schutz der digitalen Inhalte (Navigationsdaten, Musik, Video, ...)
- Diebstahl-Schutz
- Rechtl. & Behördl. Einsatzbereiche (Geschwindigkeitskontrolle, Inspektion zur Mobilitätsgarantie, ...)
- Innovationslawine (Breake-by-Wine, Steer-by-Wine)

Inhalt

- Motivation: Warum Autos IT- Sicherheit benötigen
- **Wer sind die Angreifer?**
- Warum IT- Sicherheit in Autos schwierig ist
- Schlussfolgerungen
- Eurobits

Ein paar Beispiele attraktiver Angriffe

- **Besitzer** entzieht sich der **Zahlung von Mautgebühren**
- **Dritte** spielen böswillig **software updates** auf
- Die Konkurrenz verursacht (regelmäßig & nicht böswillig) den **Ausfall des Bordrechners**
- Besitzer dreht den **Kilometerstand zurück**
- **Die Konkurrenz** beschafft sich techn. Daten
- **Besitzer** zahlt nicht für digitale Angebote
- Dritte werden zum **Attentäter** wenn das ABS System ausfällt

Die Angreifer und Ihre Fähigkeiten

Die Angreifer \	Technische Kenntnisse	Physikalischer Zugang	Kryptografische Privilegien
Besitzer	variieren (in der Regel wenig)	ja	wenig
Mitarbeiter	hoch	ja	einige
Externe	variieren (kann hoch sein)	nein	keine

Mitarbeiter sind eine äußerst ernst zu nehmende Angreifergruppe

Inhalt

- Motivation: Warum Autos IT- Sicherheit benötigen
- Wer sind die Angreifer?
- **Warum IT- Sicherheit in Autos schwierig ist**
- Schlussfolgerungen
- Eurobits

IT-Sicherheit

Moderne IT-Sicherheit bietet:

- Kommunikationssicherheit
- Manipulationsschutz
- Rechtemanagement (digital rights management)

Basierend auf kryptografische Algorithmen und Protokolle ...

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

Wo liegt das Problem?

Anmerkung:

Am häufigsten bei **Embedded Security**, da sie sich zu sehr von alltäglicher Computersicherheit unterscheidet!

Warum IT-Sicherheit im Auto schwer ist

- **Historische Entwicklung:**
Designer möchten, dass das System funktioniert, die IT-Sicherheit ist zweitrangig
- **Kulturelle Probleme:**
Car SW Ingenieure müssen interdisziplinär arbeiten: crypto algorithms, crypto protocols, physical security, ...
- **Beschränkte Mittel:**
Normalerweise sind nur 8 or 16 bit μ P für rechenintensive public-key Verfahren vorhanden (Oft Algorithmen mit 1024 Bit)
- **Physikalischer Zugang der Angreifer:**
Seiten Kanal Attacken, reverse engineering, ...
- **System Komplexität:**
Viele Ebenen sind involviert (Hersteller, 1...x-tier OEM, Besitzer, Verwaltung):
Wer hat kryptografische Privilegien?

Inhalt

- Motivation: Warum Autos IT- Sicherheit benötigen
- Wer sind die Angreifer?
- Warum IT- Sicherheit in Autos schwierig ist
- **Schlussfolgerungen**
- Eurobits

Sichere Datenkommunikation im Auto - Schlussfolgerungen

- **IT-Sicherheit** wird ein MUSS werden für Autos (z.B. telematic appl.)
 - **Security wird tendentiell schwieriger**: Die Vergangenheit zeigt genügend Beispiele für „schwache Lösungen“
 - **„Embedded security“ hat ganz bestimmte Anforderungen**: komplexe Umgebung, side-channel attacks, ...
 - **Neue Geschäftsfelder durch IT-Sicherheitslösungen**: besseres CRM, pay-per-view, ...
 - **Die Zusammenführung der car-SW Community und der security/crypto community** bietet gute Chancen, bringt aber auch kulturelle Schwierigkeiten mit sich.
- ⇒ **Embedded security ist eine mögliche Technologie für viele zukünftige Anwendungen & Geschäftsmodelle**

Inhalt

- Motivation: Warum Autos IT- Sicherheit benötigen
- Wer sind die Angreifer?
- Warum IT- Sicherheit in Autos schwierig ist
- Schlussfolgerungen
- **Eurobits**

EUROBITS

Europäisches Zentrum für IT-Sicherheit



Horst Görtz Institut

Lehrstuhl
für Kommu-
nikations-
sicherheit

Lehrstuhl für
Informations-
sicherheit
und
Kryptologie

Lehrstuhl
für Netz-
werk und
Daten-
sicherheit

Lehrstuhl:
Institut für
Sicherheit
im
E-Business

Assoziierte
Lehrstühle

Wirtschafts-
wissenschaften
Elektrotechnik
Soziologie

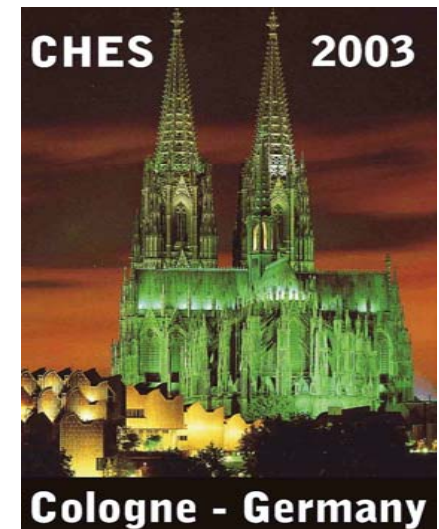
Assoziierte Unternehmen

GITS AG
Training
Consulting

escrypt GmbH
Embedded
Security

Veranstaltungen EUROBITS (www.crypto.rub.de)

- **Cryptographic Hardware and Embedded Systems (CHES)**
August 2003
- **ESCAR (Embedded Security in Cars)**
November 2003
(1st conference ever about this topic)
- **Elliptic Curves Cryptography (ECC 2004)**
September 2004



Vielen Dank für Ihre Aufmerksamkeit!

Willi Mannheims, Vorstandsvorsitzender GITS AG

mannheims@gits-ag.de