

Mit raschem Tempo gewinnt die Informationstechnologie (IT) in Kraftfahrzeugen als zentrale Komponente an Bedeutung für neue Anwendungen und Dienste. Schon heute ist ein Großteil der Innovationen im Automobilbereich Elektronik- und IT-basiert. Heutige Anwendungen umfassen grundlegende Fahrzeugfunktionen (Motorsteuerung, Bremsen, Lenkung), Sekundärfunktionen wie Wegfahrsperrung, Airbag etc. und Infotainment-Anwendungen wie Navigationssysteme, Telematik und In-car-Entertainment. Ein Aspekt der modernen Informationstechnik, der in Zukunft dramatisch an Bedeutung gewinnen wird, ist IT-Sicherheit.

Ein großer Themenbereich, der bisher kaum behandelt wurde, ist die Absicherung der IT-Anwendungen. Dieses Thema wird in dem gleichen Maße an Bedeutung gewinnen, in dem Automobile mit IT-Funktionalität durchgesetzt werden. Wir glauben, dass das Fehlen von adäquaten Sicherheitsmaßnahmen ein ernsthafter Hinderungsgrund für die Einführung zukünftiger IT-Anwendungen sein kann, die möglicherweise große finanzielle und technische Bedeutung in Fahrzeugen der Zukunft haben wird. Man denke hier nur an das „Flashen“ von Steuergeräten über eine externe Vernetzung, welche sowohl dem Hersteller als auch dem Fahrzeugbesitzer eine große Anzahl von neuen Diensten ermöglichen wird. Trotz der Bedeutung, die IT-Sicherheit in der modernen Automobiltechnik spielen wird, ist dieses Thema bisher kaum diskutiert worden und die wenigen existierenden Lösungen sind zumeist Ad-hoc-Ansätze. Diese Entwicklung ist keinesfalls überraschend, wenn man bedenkt, dass in praktisch allen historisch gewachsenen IT-Anwendungen Sicherheit nur ein Nachgedanke war, der erst in späteren Phasen einer Anwendung hinzugefügt wurde. Ein Beispiel par excellence ist das Internet, das erst zum jetzigen Zeitpunkt mit rudimentären Sicherheitsfunktionen versehen wird.

► Anwendungsbereiche von IT-Sicherheit im Kfz

Wie weiter unten diskutiert wird, gibt es zahlreiche Anwendungsgebiete im

Embedded Security in Automobilanwendungen

IT-Applikationen im Fahrzeug müssen vor gezielten Manipulationen geschützt werden

Die Informations- und Kommunikationstechnik nimmt eine ständig wachsende Rolle im Automobil ein. Ein extrem wichtiger, aber oft übersehener Aspekt hierbei ist IT-Sicherheit im Automobil. Dieser Beitrag stellt die Besonderheiten der eingebetteten Sicherheit in Fahrzeugen dar, diskutiert die jetzigen und zukünftigen Funktionen mit Sicherheitsbedarf sowie die Schwierigkeiten bei der Erstellung von Sicherheitssystemen.

Von Christof Paar

Automobilkontext, bei denen eingebettete Sicherheit eine wichtige Rolle spielt. All diese Anwendungen lassen sich aber zu zwei übergreifenden Funktionen zusammenfassen, die durch IT-Sicherheit ermöglicht werden. Dies sind eine erhöhte Zuverlässigkeit und die Absicherung neuer Geschäftsmodelle:

1. Zuverlässigkeit: Innovative IT-Anwendungen müssen gegen gezielte Manipulationsversuche geschützt werden. Beispielsweise kann eine robust ausgelegte Motorsteuerung durch unautorisiertes Flashen zu einem sehr unzuverlässigen Motor (kurze Lebensdauer etc.) führen. Oder ein ansonsten hochgradig ausfallsicheres Telematiksystem lässt sich ohne weiteres durch Dritte

missbrauchen, wenn diese die Daten abhören oder manipulieren. Die benötigten Schutzmechanismen gründen auf Methoden der modernen IT-Sicherheit.

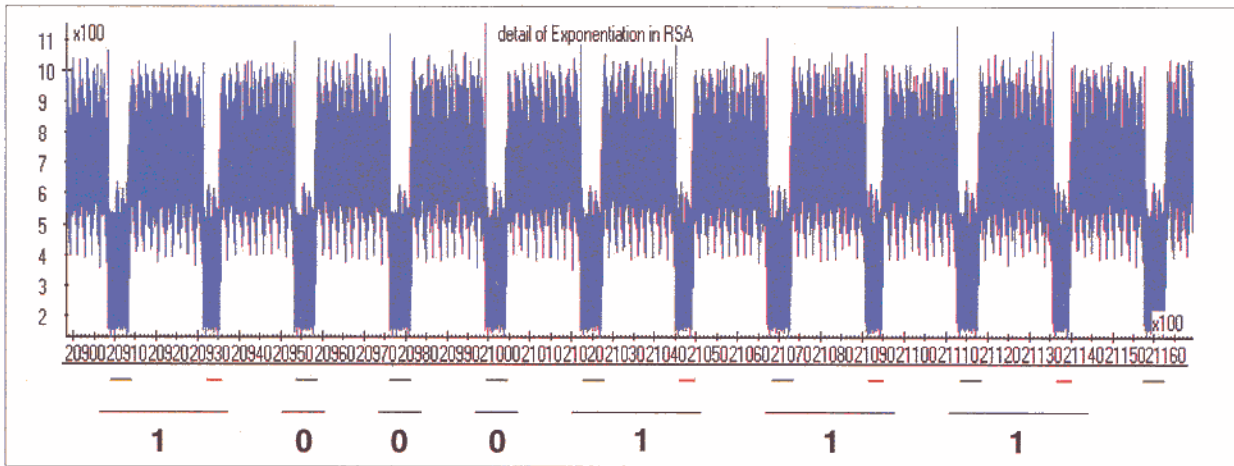
2. Neue Geschäftsmodelle: Den Möglichkeiten für neue Geschäftsmodelle in einem von Informationstechnik durchsetzten Fahrzeug sind nahezu keine Grenzen gesetzt. Beispielhaft seien hier Vermarktung von Flash-Software oder kommerzielle Infotainment-Inhalte, z.B. Navigationsdaten oder Pay-per-View, genannt. Es ist hier aber wichtig zu unterstreichen, dass praktisch alle IT-basierten Geschäftsmodelle ohne IT-Sicherheit zusammenbrechen. Zum einen muss Kommunikationssicherheit bereitgestellt werden,

■ CHES-Konferenz

Die CHES-(Cryptographic Hardware and Embedded Systems)-Konferenzreihe ist 1999 von Prof. Cetin Koc (Oregon State University, USA) und Prof. Christof Paar ins Leben gerufen worden. Sie bietet ein Forum für neue Resultate im Bereich der Ingenieur Aspekte der IT-Sicherheit. Themenschwerpunkte sind u.a. effiziente Kryptoverfahren auf eingebetteten Prozessoren, Sicherheit gegen Seitenkanalattacken (siehe Text) und neue Anwendungsgebiete

im Ingenieurbereich mit Sicherheitsbedarf. Als Beispiele für den letzten Punkt werden z.B. Sicherheit für RFID-Tags (Radio Frequency Identification) oder Sicherheit in „Pervasive Computing“-Anwendungen behandelt. CHES alterniert jährlich zwischen Europa und den USA. Nachdem die CHES 2003 in Köln stattgefunden hat, wird sie dieses Jahr im August in Boston sein. Mehr Info gibt es unter www.chesworkshop.org.

Bild 1.
Die Stromkurve einer ungesicherten RSA-Implementierung auf einem eingebetteten Prozessor erlaubt das direkte Erkennen der „geheimen“ Schlüsselbits.



um die (geldwerten) digitalen Inhalte zum Kunden zu übertragen. Dann muss der Kunde durch Methoden des Digital Right Managements an dem unerlaubten Kopieren und Weitergeben der Inhalte gehindert werden. Letztlich müssen die Hardware-Komponenten so ausgelegt werden, dass durch physikalische Manipulation die kryptographische Funktionalität nicht umgangen wird.

Die gerade genannten beiden Grundfunktionalitäten von eingebetteter Sicherheit werden im Folgenden anhand einer Reihe konkreter Anwendungsfällen deutlich gemacht.

● **Software-Integrität:** In den letzten Jahren ist das Thema „Flashen“, d.h. Änderungen der eingebetteten Software im Fahrzeug, wichtig geworden. IT-Sicherheit spielt hier direkt aus zwei Gründen eine extrem wichtige Rolle. Zum einen soll unautorisiertes Chip-Tuning verhindert werden, zum anderen möchten Hersteller gerne neue Geschäftsmodelle kreieren, in denen Software-Updates kommerziell angeboten werden. Als absolut notwendiger Grundbaustein hierfür müssen Datensicherheitsfunktionen, z.B. digitale Signatur oder Nachrichtenauthentifizierungs-codes, eingesetzt werden.

● **Diebstahlschutz:** Dies ist wahrscheinlich in Form der Wegfahrsperrung die bekannteste und älteste Anwendung in der Fahrzeugtechnik, in der moderne kryptographische Methoden zum Einsatz kommen. Die kryptographischen Schwächen der ersten Versionen der Wegfahrsperrung (einfaches Aufzeichnen des Codes erlaubte Klone des Schlüssels) betonen die Wichtigkeit

eines sorgfältigen Systementwurfs. Weitergehender Diebstahlschutz, etwa von Komponenten, durch Kryptographie ist sicherlich im Bereich des Machbaren.

● **Digital Rights Management:** In der Zukunft wird es zunehmend Anwendungen geben, bei denen es gilt, digitale Inhalte im Automobil gewissen Regeln zu unterwerfen. Beispiele hierfür sind Kartendaten für Navigationssysteme oder In-car-Entertainment (Musik, Film). Hier spielen sowohl der Kopierschutz als auch Zugangsberechtigung eine Rolle.

● **Zugangskontrolle:** Sobald Fahrzeuge in irgendeiner Form externe Kommunikation erlauben (z.B. UMTS oder Bluetooth), wird das Problem der Zugangsberechtigung akut. Man kann sich hier zahlreiche Missbrauchs-Szenarien vorstellen, die von dem relativ harmlosen „Stehlen“ von Zustandsdaten des Fahrzeugs bis zur Manipulation des Bordcomputers oder anderer kritischer Steuergeräte reicht.

● **Anonymität:** Wenn eine Vernetzung des Automobils stattfindet, bei dem dieses Daten sendet, ist das Problem der Verletzung der Privatsphäre zu beachten. Insbesondere bei Anwendungen wie Off-board-Navigationssystemen oder anderen Geoinformationssystemen (beispielsweise Abfrage von Restaurants in der Nähe des Fahrzeugstandortes) ist Anonymität eine wünschenswerte Eigenschaft.

● **Vertraulichkeit und Verlässlichkeit der Kommunikation:** Ein weiteres Problem ist die Abhörsicherheit und Verlässlichkeit der Kommunikation zwischen Automobil und der Außenwelt. Auch hier sind mannigfaltige

Missbrauchs-Szenarien denkbar, in denen ein Angreifer beispielsweise gefälschte Telematikdaten ausgibt. Ebenso müssen Zahlungsvorgänge (elektronische Maut!) gegen Abhören und Verfälschung gesichert sein.

● **Rechtliche Zwänge:** Ein neues Anwendungsgebiet moderner IT-Sicherheit sind Situationen, in denen der Gesetzgeber gewisse IT-Funktionen vorschreibt. Beispiele sind elektronische Fahrtenschreiber in LKWs oder Maut-Systemen. Solche Systeme müssen gegen Manipulationen geschützt sein.

Diese Auflistung ließe sich sicherlich noch fortsetzen. Es sollte aber deutlich werden, dass eingebettete Sicherheit ein Querschnittsthema ist, das in nahezu jeder Elektronik- und Software-Anwendung im Kfz von Bedeutung ist. Zusammenfassend lässt sich sagen, dass moderne IT-Sicherheit die Rolle einer „enabling Technologie“ spielt.

Technologien der eingebetteten Sicherheit im Automobil

Seit Ende der 90er Jahre hat sich innerhalb der IT-Sicherheitsgemeinde das Gebiet der eingebetteten Sicherheit (Embedded Security) – oft auch Security-Engineering oder Crypto-Engineering genannt – als eigenständige Disziplin herausgebildet. Diese unterscheidet sich im Allgemeinen stark von der IT-Sicherheitsproblematik in Computernetzen (z.B. LAN- oder Internet-Sicherheit), die relativ vertraut sind und für die Lösungen wie beispielsweise Verschlüsselungssoftware, Firewalls, Intrusion Detection Systeme u.a. zur

