

## **Automotive Security: Absicherung des Gesamtsystems Kraftfahrzeug durch eingebettete Hard- und Software**

### **Abstrakt**

Die Informations- und Kommunikationstechnik im Automobil der Neuzeit nimmt eine stetig wachsende Rolle ein. Es existieren starke Indikatoren, dass eingebettete Sicherheit in diesem Feld von größter Bedeutung sein wird. Trotzdem fand sie als eigenständiges Gebiet bisher zu wenig Beachtung, so dass der extrem wichtige Aspekt der IT-Sicherheit im Automobil oft übergangen wurde. In diesem Beitrag werden die Besonderheiten der eingebetteten Sicherheit im Automobilkontext dargestellt. Es werden die jetzigen und zukünftigen Automobilfunktionen mit Sicherheitsbedarf diskutiert. Außerdem werden neue Geschäftsmodelle, die durch IT-Sicherheit ermöglicht werden, beschrieben. Abschließend werden die spezifischen Kenntnisse und Schwierigkeiten, die bei der Erstellung von eingebetteten Sicherheitssystemen entstehen, diskutiert.

### **Stichworte**

Automotive Security, IT-Sicherheit, Eingebettete Systeme, Software, Hardware, Diebstahlschutz, Sicheres Update, Sicheres Freischalten, Sicheres Flashen, neue Geschäftsmodelle, DRM, Anonymität, Integrität, physikalische Sicherheit

# **Automotive Security: How to secure automotive systems with embedded hardware and software**

## **Abstract**

Information and communication technologies in modern automobiles increasingly gained in importance over the last years. There is a strong indication for the crucial role of embedded security in this area. However, this topic has been insufficiently considered so far, even though IT-security in the automotive domain is extremely important. Therefore we will describe the special role of embedded security within the automotive context in this article. We will discuss recent and future functionalities of automobiles which are subjected to security. New business models enabled by embedded security will be described. We will also discuss specific aspects and problems of embedded security systems.

## **Keywords**

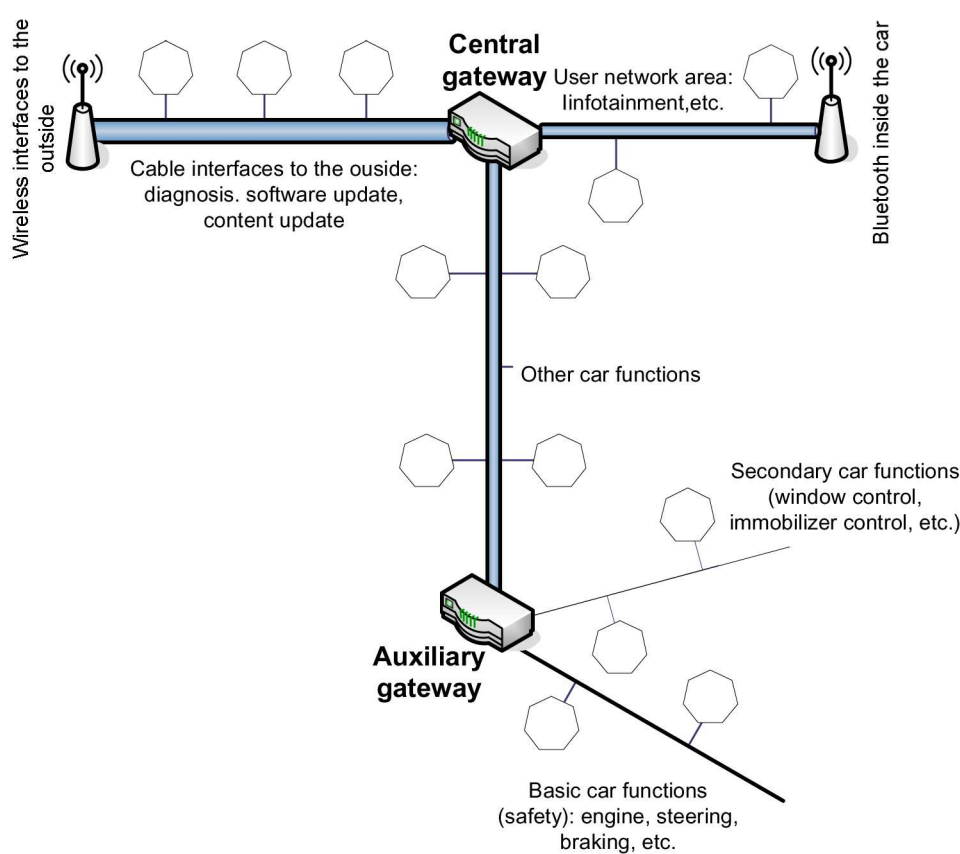
Automotive Security, IT-Security, Embedded Systems, Software, Hardware, Theft Protection, Secure Update, Secure Activation, Secure Flashing, new Business Models, DRM, Anonymity, Integrity, Physical Security

## **1. Einleitung**

Es wird vielfach angenommen, dass die nächste Revolution in der IT-Landschaft durch die Vernetzung von eingebetteten Systemen erfolgen wird. IT-Sicherheit spielt in allgegenwärtigen Computeranwendungen, wie z.B. im Automobil, bereits eine extrem wichtige Rolle. Ziel des vorliegenden Beitrages ist es, verschiedene Aspekte der eingebetteten Sicherheit im Automobil in einer Gesamtdarstellung näher zu beleuchten. Insbesondere auf die spezifischen Probleme der eingebetteten Sicherheit im Automobil wird näher eingegangen. Anhand von Fallbeispielen im Automobil sollen zukünftige Probleme und Möglichkeiten von IT-Sicherheit in eingebetteten Anwendungen verdeutlicht werden.

Mit raschem Tempo gewinnt die Informationstechnologie (IT) in Kraftfahrzeugen an Bedeutung. Schließlich ist sie die zentrale Komponente 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 Wegfahrsperre, Airbag etc., als auch Infotainment-Anwendungen wie Navigationssysteme, Telematik, und in-car Entertainment. IT-Sicherheit wird im Umfeld der modernen Informationstechnik in Zukunft dramatisch an Bedeutung gewinnen.

Ein großer Themenbereich, der bisher kaum behandelt wurde, ist die Absicherung der IT-Anwendungen. Er wird jedoch in dem Maße an Bedeutung gewinnen, in dem Automobile mit IT-Funktionalität ausgestattet werden. Spätestens mit der Kommunikationsanbindung von Fahrzeugen an externe Einheiten, z.B. über das GSM oder UMTS-Netz, Wireless LAN ("WiFi") oder Bluetooth-Verbindungen, wird das Gefahrenpotential sprunghaft ansteigen.



**Abbildung 1: Fahrzeugnetzwerk mit internen und externen Schnittstellen**

Wir glauben, dass das Fehlen von adäquaten Sicherheitsmaßnahmen einen ernsthaften Hinderungsgrund für die Einführung zukünftiger IT-Anwendungen darstellen kann. Diese sind in den Fahrzeugen der Zukunft jedoch von enormer finanzieller und technischer Bedeutung. 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 spielt, 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 Sekundärgedanke war, der oft erst in sehr späten Phasen einer Anwendung hinzugefügt wurde. Ein Beispiel par excellence ist das Internet, das erst zum jetzigen Zeitpunkt mit rudimentären Sicherheitsfunktionen versehen wird.

## **2. Anwendungsbereiche von IT-Sicherheit im KFZ**

Wie nachfolgend noch diskutiert wird, existieren zahlreiche Anwendungsgebiete im Automobilkontext, bei denen eingebettete Sicherheit bereits eine wichtige Rolle

spielt. Alle diese Anwendungen können aber zu zwei übergreifenden Funktionen zusammengefasst werden, die durch IT-Sicherheit ermöglicht werden. Diese sind eine erhöhte Zuverlässigkeit und die Absicherung neuer Geschäftsmodelle:

#### 1. Zuverlässigkeit (Reliability)

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 kann ohne weiteres durch Dritte missbraucht werden, indem Daten abgehört oder manipuliert werden. Die benötigten Schutzmechanismen werden durch Methoden der modernen IT-Sicherheit zur Verfügung gestellt.

#### 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. Hier ist es jedoch extrem wichtig zu unterstreichen, dass praktisch alle IT-basierten Geschäftsmodelle ohne IT-Sicherheit zusammenbrechen würden. Zum einen muss Kommunikationssicherheit bereitgestellt werden, um die (geldwerten) digitalen Inhalte zum Kunden zu übertragen und zum anderen muss der Kunde durch Methoden des Digital Right Managements am unerlaubten Kopieren und Weitergeben der Inhalte gehindert werden. Letztlich müssen die Hardware-Komponenten so ausgelegt werden, dass durch physikalische Manipulation die kryptographische Funktionalität nicht beeinflusst werden kann.

Im Folgenden werden die gerade genannten beiden Grundfunktionalitäten von eingebetteter Sicherheit anhand einer Reihe konkreter Anwendungs-Domänen konkretisiert.

### ***Software-Integrität***

In den letzten Jahren gewann das Thema „Flashen“, d.h. Änderungen der eingebetteten Software, im Fahrzeug an enormer Bedeutung. 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 müssen hier Datensicherheitsfunktionen fungieren, wie z.B. digitale Signaturen oder Nachrichtenauthentisierungs-codes.

### ***Diebstahlschutz***

Die Wegfahrsperre ist in diesem Bereich wohl die bekannteste und auch älteste Anwendung in der Fahrzeugtechnik, in der moderne kryptographische Methoden zum Einsatz kommen. Die kryptographischen Schwächen der ersten Versionen der Wegfahrsperre (ein einfaches Aufzeichnen des Codes erlaubte ein Klonen des Schlüssels) betonen die Wichtigkeit eines sorgfältigen Systementwurfs. Weitergehender Diebstahlschutz, z.B. von Komponenten, durch Kryptographie ist sicherlich machbar und erstrebenswert.

### ***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 spielt sowohl der Kopierschutz als auch die 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 Missbrauchsszenarien vorstellen, die von dem relativ harmlosen „Stehlen“ von Zustandsdaten des Fahrzeugs bis hin zur Manipulation des Bordcomputers oder anderer kritischer Steuergeräte reichen.

### ***Anonymität***

Sobald Vernetzungen des Automobils stattfinden, bei denen Daten gesendet werden, ist das Problem der Verletzung der Privatsphäre zu beachten. Insbesondere bei Anwendungen wie off-board Navigationssysteme oder anderen gängigen Geoinformationsdiensten (beispielsweise Abfrage von Restaurants in der Nähe des Fahrzeugstandortes) ist Anonymität eine wünschenswerte Eigenschaft.

### ***Vertraulichkeit und Verlässlichkeit der Kommunikation***

Die Abhörsicherheit und Verlässlichkeit der Kommunikation zwischen Automobil und der Außenwelt ist ein Problem, dass mit der Anonymität verwandt ist. Auch hier sind mannigfaltige Missbrauchsszenarien denkbar: Angreifer können beispielsweise gefälschte Telematikdaten ausgeben. Auch Zahlungsvorgänge (elektronische Maut!) bieten Angriffsfläche für Abhören und Verfälschungen.

### ***Rechtliche Zwänge***

Ein weiteres Anwendungsgebiet moderner IT-Sicherheit sind Situationen, in denen der Gesetzgeber gewisse IT-Funktionen vorschreibt. Als Beispiel seien hier die elektronischen Fahrtenschreiber in LKWs oder Maut-Systemen angemerkt. Solche Systeme müssen per Gesetz gegen Manipulationen geschützt sein.

Diese Auflistung ließe sich sicherlich noch fortsetzen. Es sollte aber deutlich geworden werden, dass eingebettete Sicherheit ein Querschnittsthema ist, dass in nahezu jeder IT-Anwendung im KFZ von Bedeutung ist. Zusammenfassend kann gesagt werden, dass moderne IT-Sicherheit die Rolle einer „enabling Technologie“ spielt.

## **3. Technologien der eingebetteten Sicherheit im Automobil**

Seit dem Ende der 90er Jahre hat sich das Gebiet der eingebetteten Sicherheit (Embedded Security) - oft auch Security-Engineering oder Crypto-Engineering genannt - innerhalb der IT-Sicherheitsgemeinde, als eigenständige Disziplin

herausgebildet. Die eingebettete Sicherheit unterscheidet sich im Allgemeinen stark von der IT-Sicherheitsproblematik in Computernetzen (z.B. LAN- oder Internet-Sicherheit), welche relativ vertraut sind und für Lösungen wie beispielsweise Verschlüsselungssoftware, Firewalls, Intrusion Detection Systems u.a. zur Verfügung stehen. Die zentrale Veranstaltung für Anwender und Wissenschaftler, die sich mit eingebetteter Sicherheit beschäftigen, ist die jährlich stattfindende CHES Konferenz [1].

Im Folgenden werden einige zentrale Themengebiete des modernen IT-Security-Engineerings beschrieben, welche im Rahmen von eingebetteter Sicherheit im Automobil auftreten können.

### **3.1 Digital Rights Management (DRM)**

Durch gängige Anwendungen wie Musik- und Filmdistribution über das Internet, hat das Thema DRM in den letzten Jahren eine zentrale Bedeutung erlangt. DRM-Systeme sind in der Lage Regeln durchzusetzen, die beispielsweise den Zugangszeitraum eines Nutzers zu einem Musikfile oder die Anzahl möglicher Kopien eines Files kontrollieren. Die Bedeutung des DRM in diesem Feld liegt auf der Hand. Jedoch scheint es zunächst überraschend, dass DRM in der Zukunft auch ein extrem wichtiges Thema für Automobilanwendungen sein wird. Spätestens für Dienste, bei denen Daten einen Geldwert darstellen - z.B. Inhalte im Entertainment-Bereich, ortsbezogene Dienste oder Flash-Software – wird sich die zentrale Bedeutung herausstellen. Für die Realisierung von DRM im Automobil bietet sich eine Erweiterung des zentralen Bordcomputers an. Für eine DRM-Plattform muss dieser im Wesentlichen um physikalisch sichere Kryptokomponenten (u.a. sicherer Schlüsselspeicher, asymmetrische Kryptoalgorithmen und ein physikalischer Zufallszahlengenerator) und eine sichere Betriebssystemkomponente erweitert werden.

**Fallstudie:** Ein Kunde plant seinen dreiwöchigen Urlaub in Spanien in dem er viele Bergfahrten haben wird, so dass er sich für diesen Zeitraum eine höhere

Motorleistung wünscht. Gleichzeitig benötigt er für diesen Zeitraum Navigationsdaten für Frankreich und Spanien. Er bestellt sich die entsprechenden Daten, d.h. Flash-Software für die Motorsteuerung und digitale Karten, über eine Telematikverbindung. An dieser Stelle setzt das DRM System ein, welches im Bordcomputer realisiert ist, und stellt sicher, dass die Flash-Software und die Navigationsdaten nur für den Mietzeitraum zur Verfügung stehen und nicht an andere Fahrzeuge des gleichen Modells weitergegeben werden können.

### **3.2 Physikalische Sicherheit: Seitenkanalattacken und Reverse Engineering**

Eine zentrale Komponente für die Absicherung einer IT-Anwendung sind kryptographische Algorithmen. Sowohl symmetrische als auch asymmetrische Verfahren basieren darauf, die zu schützende Einheit (beispielsweise ein Fahrzeugsensor, ein Tachometer, oder Unterhaltungselektronik) mit einem *geheimen* kryptographischen Schlüssel auszustatten, der durch Angreifer nicht ausgelesen werden kann. Da viele der potentiellen Angreifer (Besitzer, Wartungspersonal etc.) physikalischen Zugang zu den Einheiten besitzen, besteht die Gefahr, dass sie durch Seitenkanalangriffe in den Besitz des Schlüssels gelangen, so dass sie Teile manipulieren und klonen können. Seitenkanalattacken nutzen Informationen über den Verlauf des Stromverbrauchs oder des Zeitverhaltens von kryptographischen Algorithmen, um eine Rekonstruktion des Schlüssels zu erstellen. Solche Attacken traten erstmals gegen Ende der 90er Jahre auf, woraufhin sich auf der einen Seite eine Vielzahl von Gegenmaßnahmen entwickelt hat, sich die Attacken auf der anderen Seite aber auch extrem verbessert haben. Viele der Ergebnisse in diesem Bereich wurden in den bisherigen CHES Konferenzbänden dargestellt [1].

Angriffe, die durch Methoden des Reverse Engineering versuchen in den Besitz von geheimen kryptographischen Schlüsseln zu gelangen, sind mit Seitenkanalattacken verwandt. Dazu zählt beispielsweise das Auslesen von Speicherzellen in eingebetteten Prozessoren oder in integrierten Schaltungen. Entsprechende Gegenmaßnahmen fallen in den Bereich der „Tamper Resistance“. Fallbeispiele zu

diesem Thema und den damit verbundenen Schwierigkeiten sind in [4] zu finden. Der Unterschied zum klassischen Reverse Engineering liegt darin, dass es hier schon genügt *eine* kritische Information auszulesen, oft einen kryptographischen Schlüssel zwischen 64-256 Bits. Das Auslesen und ggf. das Verstehen des gesamten Codes ist nicht notwendig.

**Fallstudie:** Der Bordcomputer zeichnet Fahrzeugdaten auf (z.B. über den Zustand einzelner Komponenten oder die Laufleistung), die über eine Telematikanbindung oder beim Warten ausgelesen werden. Es muss nun verhindert werden, dass der Fahrzeughalter durch Seitenkanalangriffe bzw. Reverse Engineering in den Besitz der kryptographischen Schlüssel kommt, womit er gefälschte Daten (z.B. niedrigere Laufleistung zur Garantiewahrung) weitergeben könnte. Damit eine solche Manipulation der Fahrzeugdaten verhindert wird, müssen diese verschlüsselt und signiert abgespeichert werden.

### 3.3 Kryptoverfahren in beschränkten Umgebungen

Obwohl sich IT-Sicherheit nicht allein durch kryptographische Algorithmen erreichen lässt (man braucht auch starke Protokolle und einen soliden Systementwurf), bilden Kryptoverfahren doch die atomaren Bausteine für jede Sicherheitsanwendung. Kryptographische Algorithmen werden in zwei Kategorien unterteilt: Symmetrische und asymmetrische Algorithmen.

Symmetrische Algorithmen dienen im Wesentlichen der eigentlichen Verschlüsselung der Daten und der Überprüfung der Integrität übertragener Daten. Sie lassen sich wiederum in zwei Gruppen klassifizieren: Stromchiffrierungen und Blockchiffrierungen.

Erstere Gruppe verschlüsselt bitweise und die andere blockweise. Stromchiffrierungen sind weniger gut untersucht und schlechter entwickelt als

Blockchiffren. Beispiele für Blockchiffren stellen der Advanced Encryption Standard (AES) [2] oder der Data Encryption Standard (DES) [3] dar. Blockchiffren zeichnen sich im Allgemeinen durch eine höhere Verschlüsselungseffizienz (gemessen in verschlüsselten Bits pro Prozessortakt) und durch einen geringeren Programm- und Datenspeicherbedarf (ROM, RAM) aus, wodurch sie besonders für eingebettete Anwendungen attraktiv werden.

Asymmetrische Algorithmen sind hingegen oft die bessere (oder auch die einzige) Möglichkeit komplexe Sicherheitslösungen für Automobilanwendungen - insbesondere bei sehr vielen Teilnehmern - zu realisieren. Diese Algorithmen führen in der Regel komplexe Operationen mit langen Zahlen durch. Die Länge der Zahlen ist typischer Weise 1024-2048 Bit für RSA und DL-Verfahren. ECC Systeme benötigen Operanden der Länge 160-256 Bit. Eine Verallgemeinerung von ECC, so genannte hyperelliptische Kurven, benötigen nur Operandenlängen von 40-128 Bit. Die Mehrzahl der zu schützenden Systeme wird mit vergleichbar schwachen eingebetteten Prozessoren, z.B. 8 oder 16-Bit Mikrocontrollern mit Taktraten von einigen 10 MHz, ausgestattet. Aufgrund der relativ kurzen Operandenlängen sind ECC am ehesten für kleine Prozessoren geeignet. Allerdings sind die atomaren Operationen (die so genannte Gruppenoperation) in einem ECC System wesentlich komplexer als bei RSA oder DL-Verfahren. Aus diesem Grund ist es nicht direkt deutlich, welches Verfahren tatsächlich besser geeignet ist. Nach intensiven Forschungen auf diesem Gebiet während der letzten fünf Jahre, ist es aber zunehmend deutlich geworden, dass ECC tatsächlich in den meisten Fällen das geeignete Verfahren für eingebettete Prozessoren darstellt.

**Fallstudie:** Ein Steuergerät soll aktualisiert werden, allerdings nur mit autorisierter Flash-Software. Hierfür wird jedes Software-Modul mit einem digitalen Signaturalgorithmus, einem asymmetrischen Verfahren, signiert. Bevor das Steuergerät ein Update durchführt, wird die Signatur durch den Verifikationsalgorithmus überprüft. Der Vorteil von asymmetrischen Algorithmen ist hierbei, dass der Verifikationsschlüssel öffentlich ist. Das heißt, selbst wenn der Angreifer den Schlüssel des Steuergerätes kennt, bringt ihm das keinen Vorteil.

### 3.4 Weitere Themen

Die oben stehenden Themen stellen nicht das gesamte Spektrum der eingebetteten Sicherheit im Automobilkontext dar. Insbesondere sind noch die Bereiche Mobilfunksicherheit und Systemsicherheit zu nennen. Beides sind wichtige Themengruppen, die aber wegen Ihrer Breite in diesem Artikel nicht behandelt werden können.

## 4. Zusammenfassung: Herausforderung und Chancen für die KFZ-Elektronik

Zusammenfassend kann gesagt werden, dass die IT-Sicherheit sowohl gegen (neuartige) Gefahren schützt und Zuverlässigkeit bietet, als auch den Aufbau neuer Geschäftsmodelle ermöglicht. Gleichzeitig gilt es gewisse technische Hürden zu nehmen und interdisziplinäres Know-how aufzubauen, um ausgereifte Lösungen im Bereich der eingebetteten Sicherheit zu entwickeln. Zum Abschluss werden nachfolgend noch einmal die wichtigsten Aspekte der IT-Sicherheit im Automobil zusammengefasst:

- IT-Sicherheit wird ein *Muss* in Fahrzeugen der Zukunft sein (z.B. Telematikanwendungen).
- Neue Geschäftsmodelle benötigen solide IT-Sicherheitslösungen als „enabling Technology“: Kommerzielles Flashen, neue Dienste (pay-per-view, location-aware services,...), besseres CRM, u.v.a.m.
- IT-Sicherheit kann „unsichtbar“ in eingebettete Anwendungen integriert werden. Eingebettete Sicherheit wird somit ein Thema, in dem Zulieferer und Hersteller Expertise durch externe oder interne Ressourcen aufzeigen müssen.
- Eingebettete Sicherheit ist ein relativ junges Thema, für das aber in anderen Anwendungsgebieten (z.B. Smart Cards) bereits viele Lösungen gefunden wurden.

- Eingebettete Sicherheit im Automobil erfordert die Auseinandersetzung mit sehr speziellen Rahmenbedingungen. Dazu zählen u.a. kleine Rechner und enge Kostenrahmen, Seitenkanalangriffe, Reverse-Engineering und komplexe Systeme.
- Neue Sicherheitssysteme müssen extrem sorgfältig entworfen werden. Ein einziger „kleiner“ Fehler kann zum Zusammenbruch des gesamten Systems führen und damit auch zur Gefährdung von z.B. neuen Geschäftsmodellen. Dies wird besonders deutlich, wenn man bedenkt, dass Nachbesserungen in Automobilanwendungen oft nur mit extrem hohen Kosten möglich sind (Rückrufaktion). Besondere Sorgfalt ist also von höchster Priorität.
- Die Zusammenführung der Automobil-IT-Community und der Security-/Crypto-Community birgt zwar große Chancen, geht aber auch mit kulturellen Schwierigkeiten einher. Hier sollte beachtet werden, dass IT-Sicherheit historisch von Theoretikern (Mathematikern und theoretischen Informatikern) behandelt wurde. Es gibt nur wenig Experten, die sowohl den Ingenieurkontext als auch die Datensicherheit verstehen.

### **Infobox (CHES Konferenz)**

Die CHES (Cryptographic Hardware and Embedded Systems) Konferenzreihe ist 1999 von Prof. Cetin Koc (Oregon State University, USA) und Prof. Christof Paar (Ruhr-Universität Bochum) ins Leben gerufen worden. CHES bildet heute das bedeutendste Forum für neue Resultate im Bereich der Ingenieur Aspekte der IT-Sicherheit. Themenschwerpunkte sind u.a. effiziente Kryptoverfahren auf eingebetteten Prozessoren, Sicherheit gegen Seitenkanalattacken und neue Anwendungsgebiete im Ingenieurbereich mit Sicherheitsbedarf. Als Beispiele für den letzten Punkt werden z.B. Sicherheit für RFID (Radio Frequency Identifications) Tags oder Sicherheit in pervasive Computing Anwendungen behandelt.

### **Literaturverzeichnis**

- [1] Webseite der CHES (Cryptographic Hardware and Embedded Systems) Konferenz: <http://www.chesworkshop.org>.
- [2] *NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES)*, U.S. Department of Commerce/National Institute of Standard and Technology, November 2001, Quelle: <http://csrc.nist.gov/encryption/aes>.
- [3] *NIST FIPS PUB 46-3, Data Encryption Standard (DES)*, Federal Information Processing Standards, National Bureau of Standards, U.S. Department of Commerce, 1977.
- [4] R. Anderson, *Protecting Embedded Systems --- The Next Ten Years*, Workshop on Cryptographic Hardware and Embedded Systems - CHES 2001, Springer-Verlag, 2001, LNCS 2162, Invited Talk.