Embedded Security in Automobilanwendungen

Prof. Dr.-Ing. Christof Paar
eurobits Kompetenzzentrum für IT-Sicherheit, Ruhr-Universität Bochum
und escrypt GmbH
cpaar@crypto.rub.de

published in Elektronik Automotive 01/2004

Zusammenfassung

Informations- und Kommunikationstechnik nimmt eine ständig wachsende Rolle im Automobil ein. Ein extrem wichtiger, aber oft übersehener, Aspekt hierbei ist IT-Sicherheit *im* Automobil. In diesem Beitrag werden die Besonderheiten der eingebetteten Sicherheit im Automobilkontext dargestellt. Es werden die jetzigen und zukünftigen Automobilfunktionen mit Sicherheitsbedarf diskutiert. Es werden neue Geschäftsmodelle, die durch IT-Sicherheit ermöglicht werden, beschrieben. Abschließend werden die spezifischen Kenntnisse und Schwierigkeiten bei der Erstellung von eingebetteten Sicherheitssystemen diskutiert.

1 Einleitung

Mit raschem Tempo gewinnt die Informationstechnologie (IT) in Kraftfahrzeugen als zentrale Komponente an Bedeutung für neue Anwendungen und Dienste. Schon heute sind ein Großteil der Innovationen im Automobilbereich Elektronik- und IT-basiert. Heutige Anwendungen umfassen grundlegende Fahrzeugfunktionen (Motorsteuerung, Bremsen, Lenkung), Sekundärfunktionen wie Wegfahrsperre, Airbag etc. und Infotainment-Anwendungen wie Navigationssysteme, Telematik, und in-car Entertainment. Ein Aspekt der modernen Informationstechnik, der in Zukunft dramatisch and 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 durchsetzt werden. Spätestens mit der Kommunikationsanbindung von Fahrzeugen an externe Einheiten, z.B. über das GSM oder UMTS-Netz, wireless-LAN Kanäle ("WiFi") oder Bluetooth-Verbindungen, wird das Gefahrenpotential sprunghaft ansteigen. Wir glauben, dass das Fehlen von ädequaten Sicherheitsmaßnamen ein ernsthafter Hinderungsgrund für die Einführung zukünftiger IT-Anwendungen sein kann, die große finanzielle und technische Bedeutung in Fahrzeugen der Zukunft haben kann. 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 dazu gefügt 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 weiter unten diskutiert werden wird, gibt es zahlreiche Anwendungsgebiete im Automobilkontext, bei denen eingebettete Sicherheit eine wichtige Rolle spielt. All diese Anwendungen können aber zu zwei übergreifende Funktionen zusammengefasst werden, die durch IT-Sicherheit ermöglicht werden. Dies sind eine erhöhte Zuverlässigkeit und die Absicherung neuere 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 kann ohne weiteres durch Dritte missbraucht werden, in dem Daten abgehört oder manipuliert werden. Die benötigten Schutzmechanismen werden durch Methoden der modernen IT-Sicherheit zur Verfügung gestellt.

2. **Neue Geschäftsmodelle** Die 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 hier aber extrem wichtig zu unterstreichen, dass praktisch alle IT-basierten Geschäftsmodelle ohne IT-Sicherheit zusammenbrechen. Zum einen muss Kommunikationssicherheit bereit gestellt werden, um die (geldwerten) digitalen Inhalt 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 sie durch physikalische Manipulation die kryptographische Funktionalität nicht umgangen wird.

Die gerade genannten beiden Grundfunktionalitäten von eingebetteter Sicherheit sollen im folgenden anhand einer Reihe konkreter Anwendungsdomänen konkretisiert werden.

Software-Integrität In den letzten Jahren ist das Thema "Flashen", d.h. Änderungen der eingebetteten Software, im Fahrzeug extrem 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 kommerzielle angeboten werden. Als absolut notwendiger Grundbaustein hierfür müssen Datensicherheitsfunktionen, z.B. digitales Signatur oder Nachrichtenauthentisierungscodes, eingesetzt werden.

Diebstahlschutz Dies ist wahrscheinlich in Form der Wegfahrsperre die bekannteste und älteste Anwendung in der Fahrzeugtechnik, in der moderne kryptographische Methoden zum Einsatz kommen. Die kryptographischen Schwächen der ersten Versionen der Wegfahrsperre (einfaches Aufzeichnen des Codes erlaubte Klonen des Schlüssels) betonen die Wichtigkeit eines sorgfältigen Systementwurfs. Weitergehender Diebstahlschutz, z.B. 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 Regel zu unterwerfen. Beispiele hierfür sind Kartendaten für Navigationssysteme oder in-car Entertainment (Musik, Film). Hier spielt 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 Missbrauchsszenarien vorstellen, die von dem relativ harmlosen "Stehlen" von Zustandsdaten des Fahrzeugs bis zur Manipulation des Bordcomputers oder anderer kritischer Steuergeräte reicht.

Anonymität Sobald 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 Navigationssysteme oder anderen Geoinformationsdiensten (beispielsweise Abfrage von Restaurants in der Nähe des Fahrzeugsstandortes) ist Anonymität eine wünschenswerte Eigenschaft.

Vertraulichkeit und Verlässlichkeit der Kommunikation Ein mit der Anonymität verwandtes Problem ist die Abhörsicherheit und Verlässlichkeit der Kommunikation zwischen Automobil und der Außenwelt. Auch hier sind mannigfaltige Missbrauchsszenarien denkbar, in denen ein Angreifer beispielsweise gefälschte Telematikdaten ausgibt. Ebenso müssen Zahlungsvorgänge (elektronische Maut!) gegen Abhören und Verfälschung gesichert sein.

Rechtliche Zwänge Ein weiteres Anwendungsgebiet moderner IT-Sicherheit sind solche Situationen, in denen der Gesetzgeber gewisse IT-Funktionen vorschreibt. Beispiele sind z.B. die elektronische Fahrtenschreiber in LKWs oder Maut-Systeme. Solche Systeme müssen gegen Manipulationen geschützt sein.

Diese Auflistung ließe sich sicherlich noch fortsetzen. Es sollte aber deutlich geworden werden, das 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 Ende der 90er Jahre hat sich innerhalb der IT-Sicherheitgemeinde das Gebiet der eingebetteten Sicherheit (embedded Security) — oft auch Security-Engineering oder Crypto-Engineering genannt — als eigenständige Disziplin herausgebildet. Dies 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 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 (s. Kasten).

Im folgenden beschreiben wir einige zentrale Themengebiet des modernen IT-Security-Engineerings, die im Kontext von eingebetteter Sicherheit im Automobil auftreten.

3.1 Digital Rights Management (DRM)

Das Thema DRM hat in den letzten Jahren für Anwendungen wie Musik- und Filmdistribution über das Internet eine zentrale Bedeutung erlangt. DRM-Systeme können Regeln, beispielsweise wie lange der Benutzter Zugang zu einem Musikfile hat oder wie viele Kopien eines Files angelegt werden dürfen, durchsetzen. Es ist vielleicht eine überraschende Entwicklung, dass DRM in der Zukunft ein extrem wichtiges Thema für Automobilanwendungen werden wird. DRM wird spätestens für Dienste, bei denen Daten einen Geldwert darstellen — z.B. Entertainment Inhalte, ortsbezogene Dienste oder Flash-Software — von zentraler Bedeutung. Für die Realisierung von DRM im Automobil bietet sich eine Erweiterung des zentralen Bordcomputer an. Für eine DRM-Plattform muss dieser im wesentlichen um physikalisch sichere Kryptokomponenten (u.a. sicherer Schlüsselspeicher, asymmetrischen Kryptoalgorithmen und ein physikalischer Zufallszahlengenerator) und eine sichere Betriebssystemkomponente erweitert werden.

Fallstudie: Der Kunde will für seinen Urlaub in Spanien mit viel Bergfahrten für drei Wochen einen stärkeren Motor. 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. Das DRM System, welches im Bordcomputer realisiert ist, stellt sicher, dass die Flash-Software und die Navigationsdaten nur für den 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, dass die zu schützende Einheit

(beispielsweise ein Fahrzeugsensor, Tachometer, oder Unterhaltungselektronik) einen *geheimen* kryptographischen Schlüssel besitzt, der durch Angreifer nicht ausgelesen werden kann. Da viele der potentiellen (Besitzer, Wartungspersonal etc.) Angreifer physikalischen Zugang zu den Einheiten haben, besteht die Gefahr, dass diese durch Seitenkanalangriffe in den Besitz des Schlüssel gelangen, und damit Teile manipulieren und klonen können. Seitenkanalattacken nutzen Information über den Verlauf des Stromverbrauchs oder des Zeitverhaltens von kryptographischen Algorithmen aus, um den Schlüssel zu rekonstruieren. Diese Attacken wurden gegen Ende der 90er Jahre das erste Mal vorgeschlagen, und es existieren zur Zeit eine Vielzahl von Gegenmaßnahmen einerseits und verbesserter Attacken andererseits. Viele der Ergebnisse in diesem Bereich wurden in den CHES Konferenzbänden dargestellt [KP99, KP00, KNP01, KKP02, WKP03].

Verwandt mit Seitenkanalattacken sind Angriffe, die durch Methoden des Reverse Engineering versuchen in den Besitz von geheimen kryptographischen Schlüsseln zu gelangen. Hierzu gehört beispielsweise das Auslesen von Speicherzellen in eingebetteten Prozessoren oder in integrierten Schaltungen. Entsprechende Gegenmaßnahmen fallen in den Bereich des "Tamper Resistance". Fallbeispiele zu diesem Thema und den damit verbundenen Schwierigkeiten sind in [And01] zu finden. Der Unterschied zum klassischen Reverse Engineering liegt darin, dass es hier schon reicht *eine* kritische Information auszulesen, oft ein kryptographischer Schlüssel zwischen 64–256 Bits. Das Auslesen und ggf. Verstehen des gesamten Codes ist nicht notwendig.

Fallstudie: Der Bordcomputer zeichnet Fahrzeugdaten auf (z.B. über den Zustand einzelner Komponenten oder Laufleistung) die über eine Telematikanbindung oder beim Warten ausgelesen werden. Um eine Manipulation der Daten durch den Fahrzeugbesitzer zu verhindern, werden diese Verschlüsselt und signiert abgespeichert. Es muss nun verhindert werden, dass der Halter durch Seitenkanalangriffe bzw. Reverse Engineering in den Besitz der kryptographischen Schlüssel kommt, und somit gefälschte Daten (z.B. niedrigere Laufleistung zur Garantiewahrung) weitergibt.

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 — so bilden Kryptoverfahren doch die atomaren Bausteine für jede Sicherheitsanwendung. Kryptographische Algorithmen werden in zwei Kategorien unterteilt: Symmetrische und asymmetrische Algorithmen. Die erste Gruppe kann insbesondere der eigentlichen Verschlüsselung der Daten und zur Überrufung der Integrität von übertragenen Daten dienen. Symmetrische Algorithmen lassen sich wiederum in zwei Gruppen klassifizieren: Stromchiffrierungen und Blockchiffrierungen. Erstere Gruppe verschlüsselt bitweise und die andere blockweise. Beispiele für Blockchiffren sind der Advanced Encryption Standard (AES) oder der DES. Die zweite Gruppe zeichnet sich im allgemeinen durch eine höhere Verschlüsselungseffizienz (gemessen in verschlüsselten Bits pro Prozessortakt) und durch geringeren Programm- und Datenspeicherbedarf (ROM, RAM) aus, und sind somit für eingebettete Anwendungen besonders attraktiv. Demgegenüber steht die Tatsache, dass die Theorie von Blockchiffren weiter entwickelt ist und es wenig sehr gut untersuchte Stromchiffren gibt.

Für Automobilanwendungen sind sehr oft allerdings asymmetrische Algorithmen die bessere (oder einzige) Möglichkeit komplexe Sicherheitslösungen — insbesondere mit sehr vielen Teilnehmern — zu realisieren. Grundsätzlich unterteilt man die in der Praxis angewandten asymmetrischen Algorithmen in drei Familien: Algorithmen basierend auf dem *Faktorisierungsproblem* (z.B. RSA), dem *diskreten Logarithmusproblem* (z.B. DSA) und elliptische Kurven (ECC). Eine Gemeinsamkeit der drei Familien ist die Durchführung von komplexen Operationen mit langen Zahlen, da alle drei auf schweren zahlentheoretischen Problemen basieren. 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, sog. 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 Mikrocontroller mit Taktraten von einigen 10 MHz, ausgestattet. Aufgrund der vergleichsweise kurzen Operandenlängen sind ECC am ehesten für kleine Prozessoren geeignet. Allerdings sind die atomaren Operationen (die sog. 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 sein. 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 sind. In der Grafik sind Laufzeiten und Komplexitäten von RSA und ECC auf eingebetteten Prozessoren verglichen.

`Grafik (Balkendiagramm) mit Komplexitätsvergleich RSA : ECC`

Fallstudie: Ein Steuergerät soll nur mit authorisierter Flash-Software aktualisiert werden dürfen. 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 hierbei ist, dass der Verifikationsschlüssel öffentlich ist, so dass einem Angreifer durch Bekanntwerden des Schlüssels des Steuergerätes nicht geholfen ist.

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.

4 Zusammenfassung: Herausforderung und Chancen für die KFZ-Elektronik Community

Zusammenfassend kann gesagt werden, dass die IT-Sicherheit sowohl gegen (neuartige) Gefahren schützt und die Zuverlässigkeit erhöht, 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. Abschließend sollen nachfolgend noch einmal die wichtigsten Aspekte der IT-Sicherheit im Automobil zusammengefasst werden:

- IT-Sicherheit wird ein **Muss** in Fahrzeugen der Zukunft (z.B. Televatikanwendungen).
- 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 wird “unsichtbar” in eingebettete Anwendungen integriert werden. Eingebette Sicherheit wird somit ein Thema, in dem Zulieferer und Hersteller Expertise durch externe oder interne Resscourcen aufzeigen müssen.
- Eingebette Sicherheit ist ein vergleichbar junges Thema, für das aber in anderen Anwendungsgebieten (z.B. Smart Cards) viele Lösungen gefunden wurden.
- Eingebettete Sicherheit im Automobil erfordert das Umgehen mit sehr speziellen Rahmenbedingungen, u.a. kleine Rechner und enger Kostenrahmen, Seitenkanalangriffe, Reverse-Engineering, komplexe Systeme.
- Neue Sicherheitssysteme müssen extrem sorgfältig entworfen werden. Ein einziger “kleiner” Fehler kann zum Zusammenbruch des gesamten Systems führen, und zum Beispiel neue Geschäftsmodelle gefährden. Da Nachbesserungen in Automobilanwendungen oft nur mit extrem hohen Kosten möglich sind (Rückrufaktion), ist hier besondere Sorgfalt notwendig.
- Die Zusammenführung der Automobil-IT Community und der Security/Crypto Community birgt große Chancen, bringt aber auch kulturelle Schwierigkeiten mit sich. 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.

5 Kasten: 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. CHES bildet heute das bedeutenste Forum für neue Resultate im Bereich der Ingenieuraspekte der IT-Sicherheit. Themenschwerpunkte sind u.a. effiziente Kryptoverfahren auf eingebetteten Prozessoren, Sicherheit gegen Seitenkanalattacken (s. Text) 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. 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.

Literatur

[And01] R. Anderson. Protecting embedded systems — the next ten years. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2001*, volume LNCS 2162, pages 1–2. Springer-Verlag, 2001. Invited Talk.

[KKP02] B. S. Kaliski, Jr., Ç. K. Koç, and C. Paar, editors. *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2002*, volume LNCS 2523, Berlin, Germany, August 13-15, 2002. Springer-Verlag.

[KNP01] Ç. K. Koç, D. Naccache, and C. Paar, editors. *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2001*, volume LNCS 2162, Berlin, Germany, May 13-16, 2001. Springer-Verlag.

[KP99] Ç. K. Koç and C. Paar, editors. *Workshop on Cryptographic Hardware and Embedded Systems — CHES'99*, volume LNCS 1717, Berlin, Germany, August 12-13, 1999. Springer-Verlag.

[KP00] Ç. K. Koç and C. Paar, editors. *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2000*, volume LNCS 1965, Berlin, Germany, August 17-18, 2000. Springer-Verlag.

[WKP03] C. Walter, Ç. K. Koç, and C. Paar, editors. *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2003*, volume LNCS 2779, Berlin, Germany, September 8–10 2003. Springer-Verlag.