Eingebettete Sicherheit und Kryptographie im Automobil: Eine Einführung

Christof Paar und Thomas Wollinger
Horst Görtz Institut für IT-Sicherheit
Fak. für Elektrotechnik & Informationstechnik, Ruhr-Universität Bochum
www.crypto.rub.de

Presented at Workshop Automotive SW Engineering & Concepts, GI-Jahrestagung 2003, University of Frankfurt, Sept 29-Oct 2, 2003

Abstract: Informations- und Kommunikationstechnik nimmt eine ständig wachsende Rolle im Automobil ein. Der vorliegende Artikel soll das erste Mal einen Überblick über den wichtigen Themenkreis der IT-Sicherheit *im* Automobil geben. Es werden die jetzigen und zukünftigen Automobilfunktionen mit Sicherheitsbedarf diskutiert, eine Bedrohungsanalyse erstellt und Besonderheiten der eingebetteten Sicherheit im Automobilkontext erläutert. Anschließend wird über einige relevante Ergebnisse im Bereich von Kryptoverfahren in eingebetteten Umgebungen berichtet.

1 Einleitung

Es wird zunehmend deutlich, dass die Informationstechnik innerhalb von Automobilen rapide an Bedeutung gewinnt. Zum einen wird die Informationstechnik für grundlegende Fahrzeugfunktionen (Motorsteuerung, Bremsen, Lenkung) eingesetzt, daneben für Sekundärfunktionen wie Wegfahrsperre oder Airbag und letztlich für Anwendungen wie online Streckenführung und in-car Entertainment. Ein Aspekt der modernen Informationstechnik, der bisher nicht systematisch 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, UMTS-Netz oder wireless-LAN (”WiFi”) wird das Gefahrenpotential sprunghaft ansteigen. Das Fehlen adäquater Sicherheitsmaßnamen kann ein ernsthafter Hinderungsgrund für die Einführung neuer IT-Anwendungen sein. Der vorliegende Artikel soll das erste Mal einen Überblick über diesen extrem wichtigen Themenkreis geben.

2 IT-Sicherheit im Auto — Warum?

Dieser Abschnitt stellt eine Reihe von jetzigen und zukünftigen IT-basierten Funktionen vor, bei denen Sicherheit eine wichtige Rolle spielen wird.

Zugangskontrolle: Sobald Fahrzeuge in irgendeiner Form externe Kommunikation erlauben (z.B. UMTS oder wirless LAN), wird das Problem der Zugangsberechtigung akut. Man kann sich hier zahlreiche Missbrauchsszenarien vorstellen, die von dem vergleichsweise harmlosen "Stehlen" von Zustandsdaten des Fahrzeugs bis zur Manipulation des Bordcomputers oder kritischer Steuergeräte reicht.

Diebstahlschutz: Dies ist in Form der Wegfahrsperre die bekannteste und älteste Anwendung in der Fahrzeugtechnik, in der moderne Kryptographie zum Einsatz kommt. 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. durch Fahrzeuglokalisierung, ist ebenfalls schon realisiert worden.

Anonymität: Sobald eine Vernetzung des Automobils stattfindet, bei der dieses Daten sendet, ist das Problem der Verletzung der Privatsphäre zu beachten. Insbesondere bei Anwendungen wie z.B. Navigationssystemen oder anderen Geoinformationsdiensten (beispielsweise Abfrage von Restaurants in der Nähe des Fahrzeugsstandortes) ist Anonymität eine wünschenswerte Eigenschaft.

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

Contents Protection: In der Zukunft wird es zunehmend Anwendungen geben, bei denen es gilt, digitale Inhalte im Automobil zu schützen. Beispiele hierfür sind Kartendaten für Navigationssysteme oder in-car Entertainment (Musik, Film).

Rechtliche Zwänge: Ein weiteres Anwendungsgebiet sind solche Situationen, in denen gesetzgeberische Vorschriften durch IT realisiert werden. Beispiele sind z.B. die elektronischen Fahrtenschreiber in LKWs, die die Einhaltung von Ruhezeiten sicherstellen. Solche Systeme müssen gegen Manipulationen geschützt sein.

3 Bedrohungsanalyse

Fahrzeugbesitzer: Diese haben oft ein Interesse, sich unehrlich zu verhalten. Beispielsweise durch Manipulation der Automobildaten (z.B. Laufleistung zur Garantiewahrung) oder Umgehung des Kopierschutzes von Infotainment-Inhalten. Da der Fahrzeugbesitzer per Definition physikalischen Zugang zu allen Komponenten hat, kann er auch entsprechende Attacken (Seitenkanalangriffe etc.) durchführen. Das technische Wissen und Können der Besitzer ist sehr unterschiedlich, obwohl für die Mehrzahl der Besitzer keine

Spezialgeräte zur Manipulation zur Verfügung stehen werden.

Wartungspersonal: Dieses könnte die gleichen Motive zur Manipulation wie die obere Gruppe aber auch andere haben, z.B. Weitergabe von vertraulichen Fahrzeugdaten oder unehrliches Verhalten gegenüber dem Hersteller und Besitzer zur persönlichen Bereicherung. Das Wartungspersonal stellt eine besonders kritische Gruppe dar, da es sowohl über den physikalischen Zugang, das Fachwissen und die notwendigen Geräten verfügt. Im Fall von Vertragswerkstätten können zusätzlich noch gewisse kryptographische Zugangsprivilegien vorliegen.

Externe Dritte: Dies ist in sich eine sehr heterogene Gruppe. Als Beispiele von Angreifern und Motiven sei genannt: Es kann sich um eine Person handeln, die dem Besitzer schaden möchte (z.B. Manipulation von Bordfunktionen), um Kriminelle, die sich persönlich bereichern wollen (Diebstahl von geldwerten Daten, z.B. für Autobahngebühren), oder um Konkurrenten des Fahrzeugherstellers, der z.B. durch periodische Fehlfunktionen Kosten und Unzufriedenheit des Besitzers erzeugen möchte. Einige dieser Angreifer verfügen über sehr gutes Fachwissen und Ressourcen (konkurrierenden Hersteller!), aber per Definition nicht über physikalischen Zugang zum Fahrzeug.

4 Besonderheiten der IT-Sicherheit im Automobil

Es handelt sich hier um Probleme der *eingebetteten* Sicherheit, die sich stark von der IT-Sicherheit (ITS) in konventionellen Computernetzen unterscheiden [An01b]. Im folgenden werden die Besonderheiten der ITS im Automobil aufgezeigt.

Ressourcenbeschränkung: Die Mehrzahl der zu schützenden Systeme ist mit vergleichbar schwachen eingebetteten Prozessoren (z.B. 8 oder 16 Bit Mikrocontroller) ausgestattet. Für Sicherheitsanwendungen sind oft asymmetrische Algorithmen erforderlich, die extrem arithmetikintensiv sind und für solche Prozessoren ein grosses Problem darstellen. In Abschnitt 5 wird diese Problematik weiter diskutiert.

Seitenkanalattacken: Eine zentrale Komponente für ITS-Anwendungen sind kryptographische Algorithmen. Alle Lösungen basieren darauf, dass die zu schützende Einheit (z.b. Steuergerät oder Infotainment-Einheit) einen *geheimen* kryptographischen Schlüssel besitzt. Da viele der Angreifer physikalischen Zugang zu den Einheiten haben, besteht die Gefahr, dass diese durch Seitenkanalangriffe in den Besitz des Schlüssels gelangen. Seitenkanalattacken nutzen Informationen über den Stromverbrauch oder das Zeitverhalten von kryptographischen Algorithmen aus, um den Schlüssel zu rekonstruieren. Siehe die CHES-Konferenzbände zu Lösungen in diesem Bereich ([KKP02] u.a.).

Reverse Engineering: 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 Prozessoren oder in integrierten Schaltungen. Fallbeispiele und die damit verbundenen Schwierigkeiten sind in [An01a] beschrieben.

Beschränkte Wartungsmöglichkeiten: Es wird sehr schwer sein, bekannt gewordene Sicherheitslücken mit nachträglichen Änderungen zu schließen. Dies ist leider aber der Alltag in konventionellen Computeranwendungen, bei denen beispielsweise der Virusscanner die Signaturen neuer Viren erhält. Ein vergleichbarer Ansatz wird durch das (weitgehende) Fehlen von online Verbindungen und der Tatsache, dass viele Funktionen in Hardware realisiert sind, oft nicht möglich sein. Dies unterstreicht die Bedeutung eines einwandfreien Security-Engineerings in der Entwurfsphase.

Systemkomplexität: Eine weitere Besonderheit liegt in dem komplexen Fertigungsprozess moderner Automobile, bei dem viele verschiedene Parteien (Zulieferer verschiedener Ebenen, Hersteller, Händler) beteiligt sind. Hier ist es besonders wichtig zu untersuchen, wer als "vertrauenswürdig" gilt und wer Funktionen wie kryptographische Initialisierung, Schlüsselmanagement und Zugriffsrechte auf Kryptomodule erhält.

5 Sicherheit durch Kryptographie

Die bisher aufgeführten Automobilanwendungen mit Schutzbedarf lassen sich prinzipiell mit Methoden der modernen IT-Sicherheit (ITS) realisieren. Es stehen insb. die folgenden Sicherheitsdienste zur Verfügung: Identifikation von Personen und Geräten, Verschlüsselung, Zugangsberechtigungen, Contents Protection Systems und Anonymität. Wir gehen im Nachfolgenden auf einen besonders wichtigen Aspekt der eingebetteten ITS ein, nämlich auf kryptographische Algorithmen auf eingebetteten Plattformen. Obwohl symmetrische Kryptoverfahren wesentlich effizienter und von daher für eingebette Anwendungen attraktiv sind, reichen sie oftmals nicht aus, da sie Nachteile bezüglich Schlüsselverteilung (über einen geheimen Kanal), Skalierbarkeit (Systeme mit sehr vielen Teilnehmern) und Systemsicherheit (single point of failure) besitzen. Daher sind asymmetrische Algorithmen oft die bessere bzw. einzige Möglichkeit komplexe Sicherheitslösungen zu realisieren. Da ihre Realisierung durch den hohen Rechenaufwand aber in vielen eingebetteten Anwendungen sehr schwer ist, gehen wir im folgenden insbesondere auf diese Problematik ein.

Für die Praxis relevant sind drei Algorithmusfamilien: Algorithmen basierend auf dem *Integer Faktorisierungsproblem* (z.B. RSA), dem *diskreten Logarithmusproblem* (DLP) (z.B. DSA) und *elliptische Kurven* (EC). Ein grosser Nachteil ist, dass alle Familien extrem arithmetikintensiv sind. Typischerweise erfordern die Verfahren Operanden der Länge 1024–2048 Bit für RSA und dem DLP, und 160–256 Bit für EC. Eine Verallgemeinerung von EC, sog. hyperelliptische Kurven, benötigen lediglich Operanden von 40–128 Bit. Im folgenden werden wir beispielhaft einige Implementierungsergebnisse von asymmetrischen Algorithmen auf eingebetteten Plattformen aufführen. Außerdem stellen wir die zur Zeit besten Ergebnisse zur Implementierung von hyperelliptischen Kurven vor, welche unlängst in unserer Gruppe durchgeführt wurden. Als Metrik wird die Zeit für eine sog. Punktmultiplikation benutzt, welche eine atomare Operation in einem Sicherheitsprotokol darstellt.

In [ITT+99] wurden mehrere Methoden vorgestellt, asymmetrische Algorithmen auf ei-

nem (relativ rechenstarken) DSP, dem 200 MHz TI TMS320C6201, zu implementieren. Die Autoren erhielten eine 1024-bit RSA Signatur in 11,7 ms und eine Verifikation in 1,2 ms. 192-bit ECDSA Signaturen dauern 1.67 ms und die Verifikationen 6.28 ms. Am anderen Ende des Prozessorspektrums sind 8 Bit Mikrocontroller. Die besten Zeit auf dem verbreiteten 8051 ohne Coprozessor wird in [WBP00] beschrieben, wobei Zeiten von 1,95 s für eine 134-bit Punktmultiplikation mit Vorberechnungen und 8,37 s für einen zufälligen Punkt erreicht werden. In einen mittleren Leistungsbereich fällt der Motorola Dragonball mit 16 MHz (populär in Palmpilots u.ä.). In [WPS01] werden ECC unter Verwendung von sog. Koblitzkurven derart implementiert, dass eine ECDSA Signatur in weniger als 0,9 s und die Verifikation in weniger als 2,4 s möglich ist. Hyperelliptische Kurven sind potentiell noch besser für eingebettete Anwendungen geeignet, da Berechnungen mit Zahlen erfolgen können, die nur 40–128 Bit lang sind. Ihr Nachteil ist, dass das Auswerten von Formeln erforderlich ist, die erheblich komplexer als die von elliptischen Kurven sind. Uns ist es gelungen, die Anzahl der Berechungen für Kryptoverfahren mit hyperelliptischen Kurven auf ein Drittel des zuvor bekannten Wertes zu senken. Tabelle 1 zeigt einige unserer Ergebnis für low-cost public-key Security auf einem StrongARM Prozessor. Unsere Untersuchungen zeigten, dass hyperelliptische Kurven bei geeigneter Parameterwahl elliptischen Kurven in punkto Geschwindigkeit überlegen sind.

Tabelle 1: Hyperelliptische Kurven auf dem ARM7TDMI@80MHz [PWP03]

Geschlecht	Körper	Gruppenordnung	Add. [μs]	Verdoppel. [μs]	Punktmult. [ms]
4	$\mathbb{F}_{2^{32}}$	2^{128}	441	260	49.07
3	$\mathbb{F}_{2^{43}}$	2^{129}	603	199	47.13
2	$\mathbb{F}_{2^{63}}$	2^{126}	450	443	71.54

Literatur

[An01a] Anderson, R.: Protecting embedded systems — the next ten years. In: Ç. K. Koç, Naccache, D., und Paar, C. (Hrsg.), *Workshop on Cryptographic Hardware and Embedded Systems — CHES 2001*. volume LNCS 2162. S. 1–2. Springer-Verlag. 2001. Invited Talk.

[An01b] Anderson, R.: *Security Engineering: A Guide to Building Dependable Distributed Systems*. John Wiley and Sons. 2001.

[ITT+99] Itoh, K., Takenaka, M., Torii, N., Temma, S., und Kurihara, Y.: Fast Implemenation of Public-Key Cryptography on a DSP TMS320C6201. In: Çetin K. Koç und Paar, C. (Hrsg.), *Workshop on Cryptographic Hardware and Embedded Systems — CHES'99*. volume LNCS 1717. S. 61–72. Berlin, Germany. August 1999. Springer-Verlag.

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

[PWP03] Pelzl, J., Wollinger, T., und Paar, C.: Low Cost Security: Explicit Formulae for Genus-4 Hyperelliptic Curves. In: *Tenth Annual Workshop on Selected Areas in Cryptography — SAC 2003*. Springer-Verlag. 2003.

[WBP00] Woodbury, A., Bailey, D. V., und Paar, C.: Elliptic curve cryptography on smart cards without coprocessors. In: *IFIP CARDIS 2000, Fourth Smart Card Research and Advanced Application Conference*. Bristol, UK. September 20–22 2000. Kluwer.

[WPS01] Weimerskirch, A., Paar, C., und Shantz, S. C.: Elliptic Curve Cryptography on a Palm OS Device. In: Varadharajan, V. und Mu, Y. (Hrsg.), *The 6th Australasian Conference on Information Security and Privacy — ACISP 2001*. volume LNCS 2119. S. 502–513. Berlin. 2001. Springer-Verlag.