Mobile Sicherheit

In immer mehr Geräten unseres Alltags arbeiten auf den ersten Blick unsichtbare IT-Komponenten. Schleichend durchdringt diese stille Revolution mehr und mehr unser Leben und hält neben vielen segensreichen Funktionen auch ein allgegenwärtiges Risiko bereit: Denn all die vernetzten kleinen elektronischen Helfer verlangen auch nach Sicherheitslösungen, die uns vor dem Bruch der Vertraulichkeit und vor Manipulationen schützen sollen. Dieser Beitrag betrachtet verschiedene Aspekte der eingebetteten und besonders der mobilen Sicherheit in einem Überblick. Dr.-Ing. Jan Pelzl, Dr.-Ing. Thomas Wollinger

Mobile und eingebettete Systeme sind in Zukunft ganz sicher eines der großen Schlachtfelder, auf denen der Kampf um die Sicherheit der IT ausgetragen wird. Die Bedeutung dieses Bereichs kann man kaum überschätzen, wie folgende Fakten belegen: Nur 2 Prozent aller im Jahr 2000 hergestellten 32-Bit-Mikrorechner landeten in interaktiven, also herkömmlichen Computern. Die restlichen 98 Prozent kamen in eingebetteten Anwendungen zum Einsatz. Betrachten wir nicht nur die 32-Bit-Mikrorechner, sondern zusätzlich 4/8/16-Bit-Mikrorechner, dann verbauen die Hersteller sogar nur 0,2 Prozent aller CPUs in konventionellen PCs.

Unter einem eingebetteten System versteht man dabei ein Gerät mit folgenden Eigenschaften:

- es ist im Wesentlichen für eine Anwendung konzipiert (wie Waschmaschine oder Auto).
- es ist mit Intelligenz, das heißt mit einem Mikrocontroller, ausgestattet.
- die Rechenfunktion ist nicht direkt sichtbar, es gibt also keine klassischen Computer-Benutzer-Schnittstellen wie Bildschirm oder Tastatur. Nach dieser Definition fallen praktisch alle Alltagsgeräte, die mit einem Mikroprozessor ausgestattet sind, unter den Begriff eingebettetes System (**Abbildung 1**). Damit sind auch alle mobilen Endgeräte eine Teilmenge der eingebetteten Geräte.

Die Brisanz der mobilen Datensicherheit steht einem klar vor Augen, wenn man bedenkt, dass die meisten Anwendungen in diesem Bereich zudem kabellos kommunizieren und diese Drahtlosverbindungen um einiges leichter von einem Angreifer abzuhören, zu stören oder zu manipulieren sind. Die technischen Voraussetzungen für einen solchen Angriff stellen heute kein Hindernis mehr dar.

Kurz: Wir sind schon jetzt von einer Vielzahl an eingebetteten und mobilen Geräten mit Rechnern umgeben. Eine oft vorhergesagte Zukunftsvision prophezeit, dass die nächste IT-Revolution in der Vernetzung solcher Systeme besteht. Man spricht hier oft von Szenarien mit pervasiven (alles durchdringenden) oder ubiquitären (allgegenwärtigen) Computern.

Mobile Anwendungen

Ganz im Gegensatz zur wachsenden Rolle der Embedded Security ist sie als eigenständiges Gebiet bisher kaum betrachtet worden. Dabei unterscheidet sich die eingebettete Sicherheit stark von der IT-Sicherheitsproblematik in herkömmlichen Computernetzen. Dort stehen Standardlösungen wie beispielsweise Verschlüsselungssoftware, Firewalls, Intrusion-Detection-Systeme und anderes mehr zur Verfügung. Aber diese Lösungen sind zum großen Teil nicht übertragbar. Und zwar aus folgenden Gründen:

- Ressourcen-Beschränkung. Viele der zu schützenden Systeme arbeiten mit vergleichsweise schwachen Prozessoren. Für Sicherheitsanwendungen sind aber oft asymmetrische, extrem arithmetikintensive Algorithmen nötig.
- Drahtlose Schnittstellen. Mobile Endgeräte verfügen oft über drahtlose Schnittstellen wie Bluetooth, Infrarot, WLAN, ZigBee, GSM oder UMTS. Eine ausschließlich drahtlose Anbindung ist prinzipiell anfällig gegenüber Störungen – so lässt sich beispielsweise das absichtliche Blockieren einer Funkverbindung nicht verhindern. Kryptographische Standardprotokolle sind deshalb den Bedingungen der drahtlosen Kommunikation erst anzupassen oder neu zu entwerfen.
- Seitenkanalattacken. 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 (das mobile Endgerät) einen geheimen kryptographischen Schlüssel besitzt, den Angreifer nicht auslesen können. Da der potenzielle Angreifer physikalischen Zugang zu den Einheiten hat, besteht aber die Gefahr, dass er durch Seitenkanalangriffe

Abbildung 1: Der SerCHo Showroom mit dem 4Star Cooking Assistant demonstriert vielleicht die Küche von morgen mit dem Kochbuch-Computer, der auch den Herd steuert.

doch in den Besitz des Schlüssels gelangt und damit Teile des Systems manipulieren oder klonen kann. Seitenkanalangriffe nutzen beispielsweise Informationen über den Verlauf des Stromverbrauchs um den Schlüssel zu rekonstruieren. Inzwischen existiert eine Vielzahl dieser, gegen Ende der 90er Jahre das erste Mal vorgeschlagener Attacken. Neueste wissenschaftliche Erkenntnisse und die Ergebnisse bei der Verbesserung von Angriffen sowie von Gegenmaßnahmen stellt unter anderem die jährlich stattfindenden CHES-Konferenz vor (1).

- Reverse Engineering. Verwandt mit Seitenkanalattacken sind Angriffe, die durch Methoden des Reverse Engineerings 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 der sogenannten Tamper Resistance.
- Eingeschränkte Wartungsmöglichkeit. Im Allgemeinen ist es bei eingebetteten Systemen sehr schwer, bekannt gewordene Sicherheitsprobleme mit nachträglichen Änderungen zu verhindern, wie das bei konventionellen Computeranwendungen der Alltag ist. Nachdem eine neue Lücke bekannt geworden ist, installieren die Anwender beispielsweise Software-Updates oder neue Virensignaturen. Ein vergleichbarer Ansatz ist in den meisten eingebetteten Anwendungen nicht möglich, weil sie sich beispielsweise prinzipiell nicht mehr aktualisieren lassen. Darüber hinaus realisieren die Entwickler in manchen Fällen Sicherheitsfunktionen in Hardware. Ein Software-Update ist unter diesen Umständen oft unmöglich oder zu aufwendig oder zu teuer. Dies unterstreicht die Bedeutung eines einwandfreien Security-Engineerings in der Entwurfsphase.

Verantwortung für IT-Sicherheit

Durch die schon erwähnte schlechte Aktualisierbarkeit von eingebetteten Anwendungen können die Anbieter von Sicherheitslösungen ihre Produkte in der Regel nicht direkt an den Benutzer verkaufen. Stattdessen integrieren sie ihre Lösungen in das Gerät. Dies bedeutet für die Hersteller, dass sie die Verantwortung für die Sicherheit des Produktes selbst übernehmen müssen und es nicht – wie beim PC – dem Kunden überlassen können, durch Firewalls oder Anti-Viren-Software für den eigenen Schutz zu sorgen.

Eine weitere Besonderheit kann in den komplexen Fertigungsprozessen für moderne Systeme liegen. So sind beispielsweise bei komplexen Geräten viele verschiedene Parteien (Zulieferer, Hersteller, Händler) beteiligt. Hier ist es besonders wichtig zu untersuchen, wer als vertrauenswürdig gilt, und wer Funktionen wie kryptographische Initialisierung oder das Schlüsselmanagement und Zugriffsrechte auf entsprechende Sicherheitsfunktionen erhält.

Seitenkanal-Attacken im Detail

Die Entwickler kryptographischer Algorithmen gingen bisher immer davon aus, dass Implementierungen sicher und in sich geschlossen sind und keine Informationen über zugrunde liegende Verarbeitungsvorgänge preisgeben. Dem ist leider nicht so: Die schon erwähnten Seitenkanalangriffe basieren auf der Tatsache, dass unbeabsichtigte Informationen wie zum Beispiel Ausführungsdauer, Stromverbrauch sowie elektromagnetische Abstrahlung direkt von den durchgeführten Rechenoperationen und den verwendeten Operanden abhängen.

Im Jahr 1998 zeigten Paul Kocher et al., dass alle zu diesem Zeitpunkt erhältlichen Smartcards durch Seitenkanal-Attacken zu brechen waren. Allerdings enthalten nahezu alle heutigen Smartcards auf Hardware basierende Gegenmaßnahmen.

Der Stromverbrauch einer Chipkarte lässt sich messen, indem ein geringer Reihenwiderstand zwischen dem Massekontakt der Chipkarte und die externe Masse der Spannungsquelle geschaltet wird und ein digitales Speicheroszilloskop die über dem Widerstand abfallende Spannung misst. Die beiden meistverbreiteten Angriffe, die den Stromverbrauch eines Mikrocontrollers analysieren, sind die einfache Stromprofilanalyse, Simple Power Analysis (SPA), und die differenzielle Stromprofilanalyse, Differential Power Analysis (DPA).

Bei der SPA analysiert ein potenzieller Angreifer das Stromprofil zu einem festen Zeitpunkt »t« unter der Annahme, dass die untersuchte Instruktion oder ein verarbeiteter Operand direkt mit dem geheimen Schlüssel korreliert. Die wissenschaftliche Literatur hat mehrfach gezeigt, dass insbesondere Carry-Flag-abhän-

gige Verzweigungsbefehle, Rotationsbefehle sowie Instruktionen, die das Hamming-Gewicht (Anzahl der gesetzten Bits) des Akkumulators verändern, durch die einfache Stromprofilanalyse zu erkennen sind. Die SPA setzt allerdings detaillierte Kenntnisse der zu untersuchenden Hardware und des implementierten Algorithmus voraus und ist damit in der Praxis nicht immer anwendbar.

Die differenzielle Stromprofilanalyse DPA basiert auf einer statistischen Auswertung der gemessenen Kurven. Dazu stellt ein Angreifer zunächst eine Hypothese bezüglich des geheimen Schlüssels auf. Im Falle des Data Encryption Standard (DES) lässt sich beispielsweise während einer Verschlüsselung der Ausgang einer S-Box in der ersten Runde vorhersagen, da der Angreifer den Klartext kennt und mithilfe einer 6-Bit-Schlüsselhypothese der Ausgang einer S-Box bestimmbar ist.

Verschlüsselt der Angreifer »n« randomisierte Klartexte, so lassen sich die entsprechenden Stromprofilmessungen in zwei Summensignale aufaddieren: Ein Summensignal enthält genau die Messungen, für die ein festgelegtes Ausgangsbit der S-Box den Wert »0« hat, das andere Summensignal enthält genau die Messungen, für die das Ausgangsbit den Wert »1« hat.

Als Nächstes subtrahiert der Angreifer die beiden Summensignale und untersucht das entsprechende Differenzsignal. Bei einer falschen Schlüsselhypothese sind die aufsummierten Messkurven in allen Punkten aufgrund der randomisierten Operanden miteinander unkorreliert, daher strebt das Differenzsignal gegen Null. Bei einer korrekten Schlüsselhypothese sind die aufsummierten Messkurven zu genau dem Zeitpunkt miteinander korreliert, wenn Instruktionen den Ausgang der untersuchten S-Box bestimmen. In dem Differenzsignal ist dies an deutlichen Ausschlägen zu erkennen. Der Angreifer probiert solange alle möglichen Schlüsselhypothesen aus, bis das entsprechende Differenzsignal deutliche Spitzen aufweist.

Im Vergleich zur SPA bietet die DPA zwei deutliche Vorteile: der Angreifer benötigt weder genaue Kenntnisse über die eingesetzte Hardware noch über den implementierten Algorithmus. Die Angriffe sind übertragbar auf nahezu alle kryptographischen Algorithmen. Es existiert mittlerweile eine Vielzahl von Angriffen, gegen die allerdings eine Kombinationen entsprechender Gegenmaßnahmen schützt.

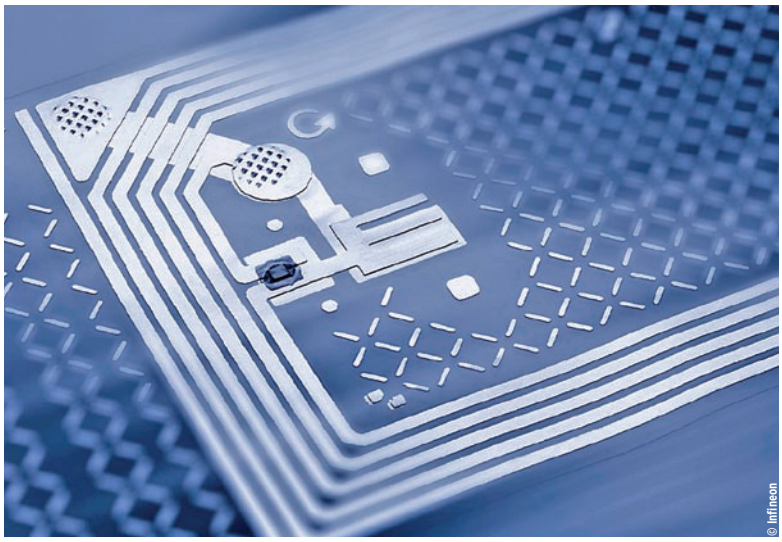

Abbildung 2: RFID-Tags haben vielfältige Anwendungsmöglichkeiten, beispielsweise in der Logistik.

Die Verwendung von Gegenmaßnahmen in Software und Hardware bedeutet neben dem erhöhten Schutz vor Seitenkanalangriffen aber auch immer einen erhöhten Aufwand und damit höhere Kosten.

Asymmetrische Verfahren

Ein Großteil der aktuellen Forschung konzentriert sich auf die Entwicklung effizienter Algorithmen für kryptographische Anwendungen. Leider gibt es wenige Publikationen, die die schnelle Implementierung von Kryptosystemen auf speziellen Plattformen wie etwa den eingebetteten Prozessoren untersuchen. Solche eingebetteten Systeme kommen zudem in Applikationen zum Einsatz, bei denen der angestrebte niedrige Energieverbrauch die Laufzeit limitiert. Die zentrale Aufgabe ist es daher, einen bestmöglichen Kompromiss zwischen allen diesen Eigenschaften zu finden.

Zur Realisierung von asymmetrischen Algorithmen bieten sich kryptographische Einwegfunktionen an, deren Sicherheit auf dem Faktorisierungsproblem (RSA) oder auf dem Lösen des Diskreten Logarithmus beziehungsweise des Diffie-Hellman-Problems (DL, DH) beruhen. Letztere lassen sich auf Gruppen von elliptischen und hyperelliptischen Kurven übertragen (ECC, HECC).

RSA und DL sind seit mehr als 20 Jahren die meistverwendeten asymmetrischen Algorithmen, zunehmend lösen sie aber neuere, auf elliptischen Kurven (EC) basierende Algorithmen

ab. Der Grund hierfür liegt in der Komplexität von RSA und DL gegenüber ECC: Für gängige Sicherheitsniveaus sind RSA- und DL-Operanden 1024 Bit groß, wohingegen ECC mit Operanden von rund 160 Bit auskommt. Hyperelliptische Kurven-Kryptosysteme (HECC) erlauben sogar noch geringere Bitlängen bei gleichbleibender Sicherheit. Einen Vergleich von Bitlängen bei gleicher Sicherheit für die genannten Verfahren zeigt **Tabelle 1. (2)**.

Hyperelliptische Kurven sind potenziell noch besser für eingebettete Anwendungen geeignet als elliptische Kurven, da Berechnungen mit Zahlen erfolgen können, die nur 40-80 Bit lang sind. Der Nachteil von HEC liegt in der gegenüber EC erheblich komplexeren Arithmetik. Das heißt, es sind für eine Gruppenoperation mehr Berechnungen über dem Grundkörper nötig. Aus diesem Grund hielt man bisher das hyperelliptische Kryptosystem dem elliptischen Kryptosystem in puncto Geschwindigkeit für unterlegen.

Mobile IT-Sicherheit durch Trusted Computing

Die Technologien des Trusted Computing sind gerade für mobile Anwendung von großem Interesse. So lässt sich beispielsweise die Integrität einer Plattform feststellen und die sichere Ausführung von Funktionen gewährleisten. Im Jahr 2003 gründeten führende IT-Unternehmen eine gemeinnützige Organisation, die offene Standards für sichere Hardware- und Software-Produkte erarbeiten soll. Unter dem Namen Trusted Computing Group (TCG) versuchen die beteiligten Unternehmen, ihre Sicherheitsinitiativen zu koordinieren.

Den Kern der Arbeit der TCG bildet die Spezifikation eines Moduls, auf dem das gesamte Sicherheitskonzept aufbaut: Das Trusted Platform Module (TPM), das es mittlerweile auch für mobile Anwendungen gibt (Mobile Trusted Module – MTM). Das TPM ist ein passiver Chip, der einen Mikrokontroller enthält und fest mit dem Mainboard oder dem Prozessor verbunden ist. Es ist von seiner Architektur her mit einer Prozessor-Chipkarte vergleichbar. Eine wesentliche Funktion des TPM ist die Bereitstellung eines speziellen Schlüssels, mit dessen Hilfe Dritte sowohl die Plattform als auch eine bestimmte Systemkonfiguration als vertrauenswürdig erkennen können.

TPM-Module sind für gängige PC-Plattformen verfügbar. Die Schlüssel selbst sind in einem geschützten Speicherbereich abgelegt, sodass Angreifern – selbst bei Zugang zur Hardware – kein Zugriff auf die Schlüssel und damit mittelbar auf die damit verschlüsselten Informationen gelingt.

Tabelle 1: Bitlängen bei gleichem Sicherheitslevel

	Operandengröße in Bit		
symmetrisch	RSA/DAS/DSS	ECC	HECC (g=2)
80 (SKIPJACK)	1024	160	80
112 (3DES)	2048	224	112
128 (AES-128)	3072	256	128
192 (AES-192)	8192	384	192
256 (AES-256)	15360	512	256

Anwendungen für TPM

Die Anwendungsfälle für den Einsatz von Trusted Computing in eingebetteten und mobilen Anwendungen sind vielseitig und beschränken sich keinesfalls auf DRM und Durchsetzung diverser Lizenzmodelle. So bietet eine entsprechend geschützte Plattform Schutz vor Malware jeglicher Art. Ferner lassen sich Software-

Abbildung 3: Das Smartphone Neo FreeRunner von OpenMoko hat einen Mikrokernel als Sicherheitsschicht.

Updates sicher durchführen und Prozesse sicher voneinander separieren. Letzteres ist besonders interessant, wenn Nutzer Zugriff auf das Gerät haben und eigene Software aufspielen können: Benutzerbereich und die essenziellen, zum Betrieb des Gerätes notwendigen Prozesse lassen sich mit einer entsprechenden Sicherheitsarchitektur separieren. Ist der Benutzerbereich durch Malware befallen, so sind die davon sicher separierten Prozesse nicht betroffen.
Weiter sind innovative und faire Lizenzmodelle wie etwa die Superdistribution möglich. In diesem Fall lassen sich Lizenzen einfach von Gerät zu Gerät übertragen. Findet ein Kunde Gefallen, so kann er über sein Gerät eine dauerhafte Lizenz erwerben. Eine sofortige Nutzung, aber spätere Zahlung ist möglich. Auch braucht man den Rechteinhaber erst zu einem späterem Zeitpunkt zu informieren. Die Grundlage für ein solches Modell ist die Feststellung der Integrität der Zielplattform, damit der Anwender Inhalte nur gemäß der Lizenz nutzen kann.

TPM embedded

Trusted Computing auf eingebetteten Systemen unterscheidet sich insofern von Standard-PC-Plattformen, als es hier um sehr unterschiedliche Hardware-Ausstattungen geht, für die zum Teil spezielle Treiber erforderlich sind. Ferner sind solche Plattformen aus Kosten- und Platzgründen oftmals nicht sehr leistungsfähig, sodass entsprechende Optimierungen notwendig sind. Der Einsatz von herkömmlichen TPMs ist bei eingebetteten Systemen in der Regel nicht sinnvoll, da die üblicherweise extern angebundenen TPMs lediglich vor Software-Angriffen schützen, nicht aber vor Hardware-Angriffen. Bei einem Angriff auf Hardware-Ebene (etwa durch Kontaktieren der Datenverbindung zwischen TPM und Prozessor), bietet ein herkömmliches TPM keinen Schutz.(3) Grundlage einer Sicherheitsarchitektur (**Abbildung 4**) ist der Sicherheitsanker (root of trust), den eine entsprechende Sicherheitserweiterung in Hardware gewährleistet (zum Beispiel TPM, Sicherheits-IC, integrierte Sicherheitsfunktionen, etc.). Darauf aufbauend sorgt eine Sicherheitsschicht in Form eines Mikrokernels (z.B. L4-Kern) für die entsprechende Trennung der einzelnen Compartments oder Prozesse von der Hardware. Zugriffe eines Prozesses auf die Hardware regelt so immer der Sicherheits-Kernel, der die Integrität der Plattform sicherstellt (**Abbildung 3**).

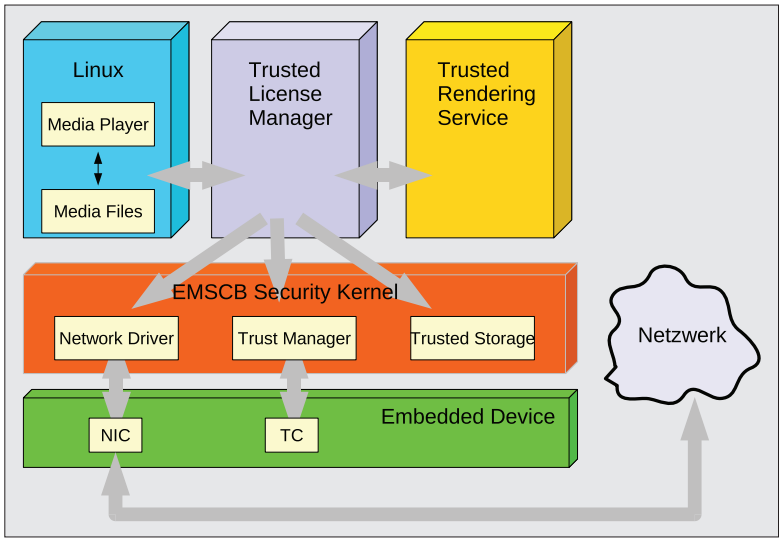

Abbildung 4: Architektur einer mobilen Sicherheitsplattform.

Schützenswerte Inhalte, etwa Schlüssel oder geschützte Daten, speichert man separat vom Benutzer-Compartment. Die Darstellung von Inhalten kann ebenfalls über einen gesicherten Prozess erfolgen, um den Benutzer beispielsweise vor Phishing-Angriffen zu schützen.

Mobile IT-Sicherheit in pervasiven Netzen

In Zukunft werden Mikrochips in nahezu alle Geräte wie beispielsweise Kaffeemaschinen, Thermostate oder Radiowecker eingebaut. Stattet man diese Geräte zusätzlich mit drahtloser Kommunikation aus, so entsteht zusammen mit schon vorhandenen Rechnern wie Mobiltelefonen und PCs ein weitverzweigtes drahtloses Netzwerk. Da es möglich ist, diesem Netzwerk Geräte kontinuierlich hinzuzufügen oder sie zu entfernen, muss es selbstorganisierend sein und darf keine zentrale Infrastruktur voraussetzen.
Jeder Knoten in dem Netzwerk verlässt sich in einem solchen Fall auf seine Nachbarn, denen er seine Dienste anbietet und deren Dienste er in Anspruch nimmt, etwa bei der Weiterleitung und dem Senden von Datenpaketen. Ein solches Ad-hoc-Netz kennt keine zentralen Angriffspunkte, da es keine zentralen Server gibt. In vielen Fällen ist zu erwarten, dass Basisstationen den Zugang zum Internet ermöglichen.

Ad-hoc-Netze

Typische Beispiele von Ad-hoc-Netzen sind Bluetooth, HiperLAN2, und eingeschränkt auch WLAN (802.11). Ad-hoc-Netze entstanden ur-

sprünglich in den 70er Jahren im Rahmen militärischer Forschung (DARPA). Daher sieht man entsprechende Anwendungen auch häufig im militärischen Bereich oder in Katastrophengebieten, etwa beim Wiederaufbau eines ausgefallenen Telefonnetzwerks. Weitere Beispiele sind Multi-Hop-Netzwerke mobiler Telefone mithilfe von Bluetooth oder WLAN, um kostenlos telefonieren zu können, oder auch Sensornetzwerke.

Einen ersten Eindruck, wie winzige Mikrochips als Sensoren in solch einem Sensornetzwerk fungieren können, geben die Smartdust-Geräte, die die Berkeley University entwickelt **(5)**. Schon nahezu alltagstauglich sind die Radio-Frequency-Identification-Etiketten (RFID) (**Abbildung 2**), kleinste passive Elemente, die einen kurzen Bitstring speichern können und die Energie zum Betrieb einem von außen angelegten elektromagnetischen Feld entnehmen.

Es ist derzeit vorstellbar, dass RFID-Etiketten bald die Barcodes ablösen. Dann bräuchte man an der Supermarktkasse nicht mehr jedes Produkt aus dem Einkaufswagen zu nehmen und zu scannen, sondern alle Waren ließen sich gleichzeitig erfassen (**Abbildung 5**).

Diese Technologie kann zu riesigen Einsparungen in allen Bereichen der Logistik führen. Weiterhin ist denkbar, dass zum Beispiel Tablettenpackungen ein RFID-Etikett erhalten, das den Anwender automatisch vor Nebenwirkungen warnt, wenn er miteinander nicht verträgliche Tabletten einnimmt.

Abbildung 5: RFID-Etiketten könnten an der Supermarktkasse schon bald die Barcodes ablösen. Dann lässt sich der Inhalt des Einkaufswagens mit einem Mal erfassen.

Herausforderungen

Wegen der beschränkten Rechenleistung, Speicherkapazität und Batterieleistung mobiler Geräte, müssen Ad-hoc-Netze Sicherheitsanforderungen auf andere Weise entsprechen als statische Netze. So ist es zum Beispiel nicht möglich, jedes Datenpaket im Interesse eines sicheren Routings zu signieren. Das scheitert an der beschränkten Rechenleistung und der Notwendigkeit einer Public-Key-Infrastruktur (PKI), die sich im Grundsatz nicht mit dem dezentralen Charakter eines Ad-hoc-Netzes verträgt.

Das sichere Routing von Datenpaketen ist ein wichtiges, aber bisher nicht grundsätzlich gelöstes Forschungsthema. Da in einem Ad-hoc-Netzwerk jeder Knoten potenziell ein Router ist, braucht es sichere und zuverlässige Verfahren. Aufgrund der mangelnden physikalischen Sicherheit ist es in Ad-hoc-Netzen zudem wichtig, dass einige bösartige Knoten die Funktionsweise des Netzes nicht gefährden.

Die Gefahren mangelnder Sicherheit machen insbesondere Szenarien sichtbar, in denen Alltagsgegenstände mit Sensoren ausgestattet sind. So können die oben erwähnten RFID-Etiketten nicht nur Logistikabläufe beschleunigen, sondern lassen sich auch zur Erstellung von Kundenprofilen nutzen.

Überhaupt liegen Nutzen und Gefahren oft dicht beieinander. So gibt es Überlegungen, winzige RFID-Etiketten in Geldscheine einzubetten, um diese fälschungssicher zu machen. Dies bedeutet allerdings auch, dass ein Taschendieb mit einem einfachen Gerät sofort feststellen kann, wer große Geldmengen bei sich trägt.

Lösungsansätze für Ad-hoc-Netze

Die folgenden Szenarien beschreiben mögliche Lösungsansätze für einzelne Kategorien von Ad-hoc-Netzen:

- Militärische Anwendungen. Es gibt nur eine Autorität, der alle Knoten unterstellt sind. Weiterhin sind Kostenfragen hier weniger bedeutend. Daher sind nicht nur Lösungen mit (kostengünstigerer) symmetrischer Kryptographie vorstellbar, sondern auch Public-Key-Techniken. Da es nur eine Autorität gibt, scheint eine verteilte PKI realisierbar. Dabei kann sich die Erstellung und Erneuerung von Zertifikaten auf viele Knoten verteilen, was eine Manipulation erschwert.

- Heterogene pervasive Netze. Hier betreiben viele Autoritäten das Netz aus heterogenen Knoten. Falls das Netz eine Verbindung zum Internet hat, lassen sich Sicherheitsmechanismen wie zum Beispiel ein Kerberos-Server nutzen. Andernfalls ist es notwendig, ein Vertrauensnetz aufzubauen. Dieses Prinzip findet in ähnlicher Form Anwendung im Web-of-Trust von PGP.
- Sensornetzwerke. In Sensornetzwerken ist die Benutzung asymmetrischer Kryptographie aufgrund der beschränkten Rechenleistung der Sensoren nahezu ausgeschlossen, jedoch ist die Gefahr physikalischer Angriffe sehr hoch, sodass eine einfache symmetrische Lösung unzureichend ist.
  Aufgrund der unterschiedlichen Auslegungen solcher Netzwerke existiert keine einheitliche Lösung, die die Sicherheit in Ad-hoc-Netzwerken sicherstellt. Die Ansätze basieren größtenteils auf symmetrischer Kryptographie, um teure Rechenoperationen zu vermeiden. Außerdem ist wegen der großen Anzahl an Knoten eines pervasiven Netzwerkes immer davon auszugehen, dass es möglich ist, einen Teil der Knoten zu manipulieren. Dies sollte jedoch keinen merkbaren Einfluss auf das Gesamtnetzwerk haben.

Zusammenfassung

Bisher stellte die zunehmende Vernetzung von Computern ein gravierendes Sicherheitsproblem für Firmen und Organisationen dar. Durch den massiven Einsatz mobiler Kleinst-Computer in allen Lebensbereichen überträgt sich diese Problematik aber auf viele Bereiche des alltäglichen Lebens. Das dadurch entstehende Bedrohungspotenzial wird zurzeit in Industrie und Forschung unterschätzt.

In vielen eingebetteten Anwendungen unterscheiden sich die Bedrohungsszenarien stark von konventioneller Internetsicherheit. Dies kann zu grundsätzlich anderen Annahmen und Systemkonzepten führen. Eine saubere Untersuchung der Angriffspotenziale für ausgesuchte eingebettete Anwendungsdomänen erscheint hier lohnenswert. Offene Fragen ergeben sich insbesondere bei folgenden Themen:

- Resistenz gegen Seitenkanalangriffe: In den letzten Jahren hat sich die Forschung hauptsächlich mit softwarebasierten Gegenmaßnahmen beschäftigt. Wichtige Beiträge stehen hier im Bereich der Hardware-Gegenmaßnahmen und der automatischen Generierung von Gegenmaßnahmen durch Entwurfswerkzeuge aus.
- Symmetrische Ultra-low-cost-Algorithmen: Der Einsatz von symmetrischen Algorithmen in eingebetteten Systemen ist wichtig für die Authentisierung und Verschlüsselung.
  Für Systeme mit besonders stark limitierten Ressourcen (wie beispielsweise RFID Tags) wäre es notwendig, Algorithmen zu entwickeln, welche weniger als 1000 Gatter für ihre Realisierung benötigen. Solche Algorithmen gibt es bereits vereinzelt, ihre theoretischen Grundlagen sind allerdings noch weitestgehend unerforscht.
- Public-Key-Kryptographie: Flaschenhals jeder Realisierung von kryptographischen Protokollen sind Public-Key-Algorithmen. Für Anwendungen in einer pervasiven Umgebung müsste man die Komplexität dieser Algorithmengruppe um mindestens eine Größenordung senken.
- Protokolle für Ad-hoc-Netze: Die klassischen kryptographischen Protokolle sind wenig geeignet für die Anforderungen in Ad-hoc Netzwerken. Obwohl es schon eine Reihe Protokolle für Ad-hoc-Netze gibt, sind sie bisher sehr wenig hinsichtlich ihrer Praxistauglichkeit getestet worden.
- Low-cost Tamper Resistance: Die bestehenden Maßnahmen gegen physikalische Angriffe (Tamper Resistance) sind aus Kostengründen nicht ohne Weiteres in eingebettete Low-Cost-Chips integrierbar. Hier wären kostengünstigere Alternativen gefragt. *(jcb)* ■■■

Infos

(1) Workshop on Cryptographic Hardware and Embedded Systems: (http://www.chesworkshop.org)

(2) J. Pelzl, Practical Aspects of Curve-Based Cryptography and Cryptanalysis, Doktorarbeit, Europäischer Universitätsverlag 2006, ISBN: 3899661893

(3) European Multilaterally Secure Computing Base: (http://www.emscb.de)

(4) escrypt Publikationen, erhältlich unter (http://www.escrypt.com/10_20.html)

(5) Smart Dust: (http://robotics.eecs.berkeley.edu/~pister/SmartDust/Kontakt)

Die Autoren

Dr. Jan Pelzl arbeitet seit 1999 auf dem gebiet der eingebetteten Sicherheit. er führte viele nationale und internationale Projekte und veröffentlichte zahlreiche Publikationen zu diesem Thema. Heute ist er Geschäftsführer der escrypt GmbH

Dr. Thomas Wollinger ist seit 1997 in Forschung und Industrie im Umfeld der eigebetteten Sicherheit tätig. Seit 2005 bei der escrypt GmbH beschäftigt hat er dort heute die Stelle eines Geschäftsführers inne.