Sicherheit und Privatsphäre in RFID-Systemen

Dirk Henrici, Jochen Müller, Paul Müller

AG Integrierte Kommunikationssysteme
Technische Universität Kaiserslautern
Gottlieb-Daimler-Straße
67663 Kaiserslautern
{henrici,jmueller,pmueller}@informatik.uni-kl.de

Zusammenfassung: RFID-Systeme sind in aller Munde: Sie sollen Warenwirtschaftssysteme revolutionieren und auch in einer Vielzahl anderer Anwendungsbereiche hilfreiche Dienste leisten. Für die damit verbundene Kostenersparnis und die neuen Möglichkeiten wird der Schutz von Daten und der Privatsphäre der Nutzer noch vernachlässigt. In diesem Beitrag werden die Bedrohungen dargestellt und einige bisher vorgeschlagene Lösungsansätze diskutiert. Zur Überwindung der identifizierten Schwachstellen wird ein anwendungsneutrales Framework für RFID-Systeme vorgestellt, mit dem der Schutz der Privatsphäre technisch verankert werden kann.

1 Motivation

Für RFID-Systeme gibt es eine Vielzahl von Anwendungen. Tags können beispielsweise an Waren angebracht werden, um damit auf einfachem Wege ein automatisch erstelltes Inventar pflegen zu können, indem die Waren beim Ein- und Ausgang automatisiert erfasst werden. Auch für Büchereien stellt die Technik einen bequemen Weg dar, Bestände zu erfassen und zu verwalten [Li03]. Post- und Lieferdienste können die zu versendenden Güter zur automatischen Verfolgung mit Tags bestücken [CW03]. Weitere Anwendungsgebiete sind neben vielen anderen Zutritts- und Zeiterfassungssysteme, Ticket- und Mautsysteme [EZ03] oder die Fälschungssicherung von Geldscheinen [Yo01] und Wertpapieren.

Die Grundfunktionalität der RFID-Systeme basiert darauf, dass die Tags eine eindeutige Kennung enthalten, mit der sie identifiziert und somit auch verfolgt werden können. Gemäß dem Vorschlag von EPCglobal Inc., einem Industriekonsortium [EG04], soll diese Kennung aus einem „Electronic Product Code“ (EPC), der die Nachfolge des UPC und des EAN-Codes [EI04] antreten soll, bestehen. Der EPC besteht aus Angabe des Herstellers, Produkttyp und einer eindeutigen Seriennummer und kann damit Produkte eindeutig identifizieren [TG02].

In dieser Grundfunktionalität wird die RFID-Technologie von Industrie und Handel als würdiger Nachfolger von optischen Barcodes angepriesen, weil ein Auslesen der Tags auch drahtlos ohne Sichtverbindung möglich ist und somit die Warenverfolgung ungleich einfacher und bequemer wird.

Aber auch ein Missbrauch der Technologie zur Erfassung des Kaufverhaltens und zur Erstellung von Kunden- und Bewegungsprofilen wird vereinfacht, weil Personen, die mit

Tags ausgestattete Objekte mit sich führen, ebenso leicht identifiziert und verfolgt werden können [Bl03, Ga02]. Die Ankündigungen von namhaften Firmen wie Metro, Wal-Mart [CN03], Benetton [BB03], Michelin [RJ03] oder Gillette [RJ02], um nur einige zu nennen, ihre Waren mittelfristig mit RFID-Tags kennzeichnen zu wollen, führte zu heftigen Reaktionen von Verbrauchern und Verbraucherschutzorganisationen [FV04], weil sie den Schutz von Daten und der Privatsphäre nicht mehr gegeben sehen. Die Skala reichte von Bedenken über Beschwerden bis hin zum Boykott einzelner Anbieter [BB03, SR04]. Metro erhielt für mangelnden Verbraucherschutz in 2003 einen „BigBrother-Award“ [FV04]. Die Befürchtungen reichen soweit, dass die Technologie eine Grundlage für eine vollkommene Überwachung [MC03] bieten könne, wie sie am ehesten aus Orwells „1984“ bekannt ist.

Mag derartiges Verhalten vieler Verbraucher auf den ersten Blick – gerade für die Nutznießer der Technik – auch technik- und fortschrittsfeindlich wirken, so muss bedacht werden, dass eine Einführung der RFID-Technik in der Warenwirtschaft nur ein erster Schritt ist. Kommen andere Anwendungen hinzu, beispielsweise eine Verwendung in Geldscheinen oder Ausweisen verbunden mit einem starken Anwachsen von Zahl und Vernetzung von Lesegeräten, so erscheinen die Bedenken, dass der Schutz der Privatsphäre ein zu geringes Gewicht bei der Einführung der Technik habe, mehr als berechtigt.

Der Schutz der Privatsphäre ist nämlich ein Bürgerrecht, das in der Gesetzgebung vieler Länder verwurzelt ist [EP03]. Beispielhaft sei die “Universal Declaration of Human Rights“ der UN aus dem Jahre 1948 angeführt, in der „no one shall be subjected to arbitrary interference with his privacy, . . . “ als Grundrecht beschrieben ist [UN48].

Aus diesem Grund muss der Schutz der Privatsphäre auch in der RFID-Technologie Berücksichtigung finden. Im Folgenden werden daher Verfahren vorgestellt, deren Zielsetzung es ist, den Schutz der Privatsphäre und Datenschutzaspekte technisch in RFID-Systemen zu verankern. Aspekte der Systemsicherheit werden, soweit sie RFID-Tags und die Funkschnittstelle zwischen Tags und Lesegerät betreffen, im Vorfeld ebenfalls betrachtet, weil sie als Grundlage für Techniken für den Schutz der Privatsphäre bedeutsam sind. Der Aufwand für die eingesetzten Verfahren und damit die Stückkosten der Tags sind von besonderer Relevanz, da RFID-Tags in großen Stückzahlen zum Einsatz kommen sollen. Verfahren, wie sie beispielsweise von Smartcards her bereits bekannt sind, sind daher meist wenig geeignet.

2 Sicherheit von RFID-Systemen

Es gibt eine Vielzahl möglicher Bedrohungen für die Sicherheit von RFID-Systemen. Die folgende Einführung ist an Informationen aus [We03] angelehnt, basiert jedoch auch auf anderen referenzierten Arbeiten. Ziel ist es aufzuzeigen, dass sich RFID-Systeme einer Vielzahl von Bedrohungen gegenüber sehen. Verfahren, die den Schutz der Privatsphäre sicherstellen sollen, müssen diesen Bedrohungen Rechnung tragen, um einen effektiven Schutz bieten zu können.

2.1 Physikalische Angriffe

Aufgrund der Beschränkung in den Stückkosten sind die meisten Tags passiv, d.h. sie beziehen die für deren Arbeit notwendige Energie aus dem vom Lesegerät generierten elektromagnetischen Feld. Diese Tags sind daher gegenüber Angriffen wie „fault induction“, „timing attacks“ oder „sudden power interruption“ machtlos [We00]. Andere Angriffsformen wie „power or EM analysis“ [Ag03] sind ebenfalls denkbar. Daneben sind auch direkte Angriffe wie das Einbringen von Strahlung, ätzenden Substanzen usw. möglich, um an auf dem Tag gespeicherte Daten zu gelangen. Weil eine Absicherung gegen derartige Angriffe durch entsprechende Schutzvorkehrungen, wie sie von entsprechend ausgestatteten Smartcards her bekannt sind, zu teuer ist, müssen RFID-Tags als physikalisch angreifbar eingestuft werden.

Aus diesem Grund dürfen auf einem Tag keine Daten abgelegt werden, deren Offenlegung ein hohes Risiko darstellt. Ein Beispiel dafür stellt unter einer Vielzahl von Tags gemeinsam verwendetes Schlüsselmaterial dar, etwa ein herstellerabhängiges „Kill-Kommando“ zum kontrollierten Zerstören oder Deaktivieren von Tags. Neben dem Kostenaspekt müssen bei der Implementierung kryptographischer Verfahren auf einem Tag auch die Angreifbarkeit durch physikalische Angriffe einbezogen werden.

2.2 Auswerten des Datenverkehrs

Sogar die Möglichkeit zu erkennen, dass RFID-Tags in der Umgebung vorhanden sind, kann eine Bedrohung darstellen. Dabei ist gerade diese Möglichkeit für viele Anwendungen wieder erwünscht [Ga02] und für das Arbeiten eines RFID-Systems notwendig.

Durch das Auswerten von Verkehrsmustern zwischen Tags und Lesegeräten, durch Zählen der Lesevorgänge, Messen der übertragenen Datenmenge oder ähnlichem, kann ein Angreifer in begrenztem Umfang Informationen extrahieren. Beispielsweise kann eine Person alleine dadurch erkannt werden, dass sie eine ungewöhnlich große Anzahl von Tags mit sich führt. Da der Datenverkehr selbst nur implizit und unter bestimmten Umständen Rückschlüsse zulässt, stellt er jedoch nur eine vergleichsweise geringe Bedrohung dar – insbesondere, wenn zwischen Lesegerät und verschiedenen Tags immer die gleiche Datenmenge ausgetauscht wird.

2.3 Abhören

Die Kommunikation zwischen RFID-Tag und den Lesegeräten läuft über die Luft und ist somit quasi öffentlich. Mit entsprechendem Equipment kann die Übertragung von Lesegeräten in Richtung zu passiven Tags aus relativ großen Entfernungen abgehört werden, die bis zu einem Kilometer bei 900MHz-Tags betragen können. Wird beispielsweise ein auf „Binary-Tree-Walking“ basierende Kollisionsvermeidungsstrategie verwendet, um ein Tag zu adressieren, so kann ein Angreifer daher die Adresse – in der Regel die Tag-Kennung – aus sicherer Entfernung ermitteln. Der Rückkanal der Übertragung von Tags hin zu Lesegeräten ist deutlich schwächer, doch ist ein Abhören für einen Angreifer auch hier nicht sonderlich schwierig.

Aus diesem Grund sollte die Kommunikation zwischen Tag und Lesegerät mittels Verschlüsselung oder Verfahren mit vergleichbarem Effekt abgesichert werden, damit keine wertvollen Daten im Klartext übermittelt werden.

2.4 Fälschen der Identität/ Spoofing

Ein Angreifer kann auch versuchen, sich entweder als Tag oder als Lesegerät auszugeben. Dazu werden im Regelfall aus dem Abhören der Verbindung gewonnene Daten verwendet. Eine Vielzahl von Angriffsszenarios ist damit denkbar. Zum Beispiel könnte ein Angreifer ein berechtigtes Lesegerät imitieren, um so an auf dem Tag gespeicherte, vertrauliche Informationen zu gelangen.

Durch das Abfangen von Nachrichten und Einbringen gefälschter Nachrichten auf den Kommunikationskanal kann ein Eingreifer die verwendeten Kommunikationsprotokolle zu stören suchen und gegebenenfalls nützliche Informationen zur Kompromittierung des Systems erlangen.

Diesen Angriffsmöglichkeiten kann entgegengewirkt werden, indem sowohl auf der Seite des Tags als auch auf der Seite des Lesegeräts eine Authentifizierung stattfindet. Weiterhin muss in irgendeiner Form Zustandsinformation gespeichert werden, um Replay-Angriffe auf die eingesetzten Protokolle zu verhindern.

2.5 Denial of Service – Angriffe

Es gibt viele Möglichkeiten, das ordnungsgemäße Arbeiten eine RFID-Systems zu stören, weil ein Tag auf eine Vielzahl von Dingen angewiesen ist: Seine eigene Integrität, die Verlässlichkeit der Funkschnittstelle, ein korrektes Arbeiten der verwendeten Protokolle etc.

Die „Holzhammer“-Methode für einen DoS-Angriff besteht in der Zerstörung eines Tags, häufig als „kill“ bezeichnet. Dies kann auf elektromagnetischem Wege geschehen, durch übermäßige mechanische Beanspruchung oder durch die Verwendung aggressiver Chemikalien. Im Gegensatz zu anderen Angriffsmethoden macht diese ein Tag permanent unbrauchbar.

Die Funkschnittstelle kann entweder abgeschirmt oder mittels Störsignalen gestört werden. Eine Abschirmung erfolgt durch Objekte, die als Faradayscher Käfig fungieren. Ein Beispiel dafür sind mit Metallstreifen versehene Handtaschen, die sogar bereits kommerziell verfügbar sind [MC04]. Ein einfacher Weg die Kommunikation zu stören ist die Aussendung eines Störsignals auf den verwendeten Frequenzen. Immerhin kann ein derartiges Vorgehen leicht detektiert werden.

Eine gezielte Störung der Adressierung von Tags ist ebenfalls möglich, ist jedoch von der eingesetzten Kollisionsvermeidungsstrategie abhängig. ALOHA-basierte Ansätze gehören in die Gruppe der probabilistischen Schemata, Binary-Tree-Walking in die Gruppe der deterministischen. Für letztgenanntes Verfahren gibt es einen Ansatz genannt „Blocker Tag“, das darauf abzielt die Privatsphäre zu schützen, indem das Binary-Tree-Walking Protokoll derart gestört wird, dass bestimmte Gruppen von Tags nicht mehr gefunden

werden. Im Allgemeinen ist eine Störung der Kollisionsvermeidungsalgorithmen leicht zu erkennen.

Denial of Service kann jedoch nicht nur ein Angriff sein, der legitime Anwendungen behindert (man stelle sich z.B. eine automatische Kasse vor), sondern stellt auch einen gangbaren Weg dar, den Schutz der Privatsphäre der Verbraucher sicherzustellen. Ein Beispiel wäre eine abgeschirmte Geldbörse, die somit ihren Inhalt nicht preisgibt.

3 Bedrohungen für die Privatsphäre

Verzahnt mit den genannten Bedrohungen im Hinblick auf die Sicherheit der Datenübertragung zwischen Tags und Lesegerät sind die Bedrohungen, die sich bei Nutzung der RFID-Technologie für die Privatsphäre der Nutzer ergeben. Zum einen ermöglicht die Tracking-Funktionalität die Erstellung von Bewegungsprofilen, zum anderen können auf RFID-Tags zusätzliche Daten gespeichert sein, die für Angreifer verwertbar sind. Von der Sicherheit des Systems insgesamt, z.B. in Bezug auf die Abhörsicherheit des Kommunikationskanals zwischen Tag und Lesegerät, hängt es mit ab, wie leicht ein Angreifer an Daten gelangen kann, deren Offenlegung und unberechtigte Auswertung die Privatsphäre der Nutzer verletzt. Somit ist ein sicheres System eine notwendige aber noch nicht hinreichende Bedingung, um den Schutz der Privatsphäre zu gewährleisten.

3.1 Erstellung von Bewegungsprofilen

Wie der Name „Radio Frequency Identification“ schon aussagt, enthalten RFID-Tags im Regelfall eine eindeutige Kennung, mit der sie identifiziert werden können. Im Falle von Tags für den Supermarkt bestünde diese Kennung aus dem „Electronic Product Code“ (EPC), der aus Herstellerangabe, Produkttyp und einer Seriennummer besteht. Mit einer eindeutigen Kennung ist es möglich, ein Tag und damit das Produkt, an dem es angebracht ist, („pars pro toto“) zu verfolgen – genau die Funktionalität, die für Supply-Chain-Management Anwendungen benötigt wird. Allerdings ist es auch genau diese Funktionalität, unter deren Verwendung Privatsphäre verletzt werden kann: Trägt eine Person ein Produkt, das ein RFID-Tag enthält, beispielsweise ein Kleidungsstück [BB03] oder eine Kreditkarte, so kann diese Person unter Einsatz der RFID-Technologie ebenfalls verfolgt werden (auch hier „pars pro toto“). Damit ergibt sich eine ähnliche Problematik wie bei der Verwendung von Cookies beim Webbrowser: Eine Person besucht eine Webseite und kann mit Hilfe des Cookies wieder erkannt werden. Parallele hierzu wäre beispielsweise ein Geschäft, das seine Kunden beim Besuch wieder erkennt. Jedoch verstärkt sich diese Problematik bei Verwendung von RFID-Technologie dadurch, dass die Trennung zwischen virtueller Welt und physikalischer Welt in viel größerem Maße aufgehoben wird: Ein Tag repräsentiert ein physikalisches Objekt in der virtuellen Welt und somit wird nicht nur ein relativ eng begrenzter Bereich wie das Surfverhalten erfassbar, sondern auch die Erstellung umfassenderer Kunden- und Bewegungsprofile möglich.

Beim Einsatz von RFID-Technik begibt man sich also in eine Konfliktsituation: Auf der einen Seite ist es für quasi alle legitimen Anwendungen nötig und somit erwünscht, dass Tags verfolgbar sind, auf der anderen Seite stellt die Verfolgbarkeit jedoch auch eine Bedrohung für die Privatsphäre da.

Von den Verfechtern der RFID-Technik, die auf eine baldige, kostengünstige Einführung drängen, wird diese Bedrohung im Regelfall in Kauf genommen. Dem stehen besorgte Bürger gegenüber, die ihre Privatsphäre bedroht fühlen und gegen eine breite Einführung der Technologie votieren. Wünschenswert wäre daher als Kompromiss eine Möglichkeit, die Trackingmöglichkeit von Tags auf bestimmte Personen/Parteien und auf einen bestimmten Kontext (Ort, Zeit und Grund des Auslesens) beschränken zu können.

3.2 Verwertbare Nutzerdaten

Neben einer eindeutigen Kennung, die zur Identifikation eines Tags benutzt werden kann, kann ein Tag je nach Anwendungszweck noch weitere Daten beinhalten. Je nachdem, was zusätzlich gespeichert wird, verdienen der Datenschutz und damit der Schutz der Privatsphäre besondere Beachtung. Bei der Verwendung eines Studierendenausweises mit RFID-Tag an einer Hochschule könnte beispielsweise die Matrikelnummer und eine Berechtigung für öffentliche Verkehrsmittel gespeichert sein. Enthält ein Tag einen „Electronic Product Code“ (EPC), so stellt dieser nicht nur eine willkürlich gewählte, eindeutige Kennung dar, sondern gibt auch Produkthersteller und Produkttyp als zusätzliche Informationen preis.

3.3 Mangelnde Transparenz und fehlende Kontrollmöglichkeit für Nutzer

In einem typischen Verwendungsszenario von RFID-Tags sind heute zwei Parteien involviert. Auf einer Seite stehen Firmen, die die RFID-Systeme verwenden, um bestimmte Anwendungen zu realisieren. Diese Firmen sind es auch, die Tags ausgeben und mit den Tags assoziierte Daten verwalten. Auf der anderen Seite steht jeweils der aktuelle Besitzer eines Tags, sei es eine Person in der Rolle eines Arbeitnehmers mit ID-Karte, eines ÖPNV-Nutzers mit einem Ticket, eines Kunden mit RFID-ausgezeichneter Ware oder in welcher Rolle auch immer.

Bezeichnend daran ist, dass es eine aktive und eine passive Partei gibt. Die aktive hat alle Daten und deren Verwendung unter ihrer Kontrolle, die passive ist zwar im Besitz des Tags, hat jedoch keinen Einfluss auf dessen Verwendung. Dabei ist es gerade diese passive Partei, deren Privatsphäre durch eine nicht legitime Nutzung des Tags wie z.B. die Möglichkeit der Erstellung von Bewegungsprofilen bedroht ist. Die passive Partei muss der aktiven in diesem Szenario also vertrauen, dass das Tag nur in einem genau definierten Anwendungsrahmen verwendet wird. Eine Möglichkeit, die Einhaltung des Verwendungsrahmens zu kontrollieren oder sofern nötig gar Sanktionen zu verhängen, gibt es für den Besitzer des Tags nicht. Dies wird auch von Verbraucherschützern oft moniert und daher für die Verbraucher tthe right to know when, where and why the tags are being read“ [Ga02] eingefordert.

4 Kurzer Überblick über vorgeschlagene Lösungsansätze

Um die Stückkosten niedrig zu halten, müssen Tags möglichst einfach aufgebaut sein. Aus diesem Grund bestehen die preiswertesten Tags nur aus einem kleinen, nur lesbaren Speicher, beispielsweise von 96 Bit [TG02]. Besser ausgestattete haben eine größere

Speicherkapazität, wieder beschreibbaren Speicher, integrierte Sensoren oder eine größere Zahl von Gates zur Durchführung von Berechnungen. Die Fähigkeiten sehr komplexer und damit teurer Tags schließen die Generierung „guter“ Zufallszahlen und die Unterstützung von symmetrischen und auch asymmetrischen Verschlüsselungsverfahren ein, dergestalt, wie es auch von einigen Smartcards her bekannt ist.

Aus diesen Gründen ist es offensichtlich so, dass jeglicher Aufwand für die Implementierung zusätzlicher Vorkehrungen zur Sicherung der Privatsphäre dem Ziel möglichst niedriger Stückkosten für Tags entgegensteht. Aus diesem Grund muss ein angemessener Kompromiss gefunden werden, mit dem bei optimalen Kosten das gewünschte Maß der Sicherung der Privatsphäre realisierbar ist. Dieses Maß hängt letztendlich von den Erfordernissen der Anwendung ab, sollte aber in jedem Fall den Kundenwünschen und gesetzlichen Erfordernissen entsprechen.

Im Folgenden werden einige Lösungsansätze, die in Publikationen vorgeschlagen worden sind, vorgestellt und kritisch betrachtet. Wie sich herausstellen wird, gibt es massive Unterschiede dahingehend, inwieweit die Privatsphäre effektiv geschützt wird und welcher Aufwand in den Tags betrieben werden muss. Es muss betont werden, dass es noch eine Vielzahl weiterer Vorschläge gibt, deren Sicherheit jedoch sehr von einem bestimmten Angreifermodell abhängt.

4.1 Einschränken des Funktionsumfangs

Eine nahe liegende Maßnahme ist das Zerstören von Tags, sobald sie nicht mehr benötigt werden. Im Falle der Verwendung des Electronic Product Code (EPC) als Tag Kennung gibt es eine abgeschwächte Lösung, bei der die Seriennummer bei der Übergabe an den Verbraucher entfernt wird, so dass nur Hersteller und Produkttyp lesbar bleiben. Beide Varianten stellen jedoch keine zufrieden stellende Lösung dar [Ju03]. Im zweiten Szenario ist ein nicht gewolltes Tracking durch die Konstellation von Produkten, die eine Person mit sich führt, noch immer sehr einfach möglich. Beide Verfahren lösen die Probleme nicht, so lange die Tags noch vollkommen intakt sind (Scannen von Tags durch Konkurrenten etc.), schränken aber nach Nutzung auch legitime Anwendungen ein oder machen sie unmöglich. Weiterhin muss es Schutzmaßnahmen gegen ein unautorisiertes Entfernen von Tag-Kennungen oder Zerstören von Tags geben, so dass die Maßnahmen nicht so einfach sind, wie sie auf den ersten Blick aussehen. Zusätzlich sind die Maßnahmen auch nicht transparent für den Verbraucher, eine umständliche Prüfung mit Lesegeräten wäre zur Kontrolle erforderlich.

Für Operationen, die den Austausch vertraulicher Informationen zwischen Lesegerät und Tag erfordern, könnte man die vergleichsweise unsichere Funkschnittstelle sperren und eine andere Verbindung fordern (Kabel oder optische Schnittstelle). Derartiges geht jedoch zu Lasten einer bequemen Handhabung, ist umständlich und erhöht Kosten und Größe der Tags.

4.2 Verhindern von Lauschangriffen

Einige Verfahren machen sich besondere Eigenschaften von RFID-Systemen zu nutze. Zum Beispiel nutzen Verfahren wie „Blinded Tree-Walking“ aus, dass der Rückkanal der

Funkschnittstelle bei der Nutzung passiver Tags deutlich schwächer als der Vorwärtskanal ist. Auf gleicher Grundlage funktioniert „Asymmetric Key Agreement“, bei welchem auf dem Tag Zufallszahlen generiert und über den sichereren Rückkanal an das Lesegerät gesendet werden. Letzteres kann dann Daten sicher jeweils als „<Wert> XOR <Zufallszahl>“ statt nur „<Wert>“ über den Vorwärtskanal an das Tag senden. Die genannten Verfahren tragen dafür Sorge, dass sensitive Daten nie über den Vorwärtskanal übertragen werden und geben damit eine gewisse Sicherheit gegenüber schwachen Angreifern. Trotz der eher begrenzten Sicherheit kann die Implementierung (z.B. Zufallszahlengenerator im Tag) aufwendig sein.

4.3 Komplexere Ansätze

Einer der komplexeren Ansätze ist das „Hash Lock“, mit dessen Hilfe unautorisiertes Lesen eines Tags verhindert werden soll. Ein Tag gibt gespeicherte Daten erst preis, nachdem es vom Lesegerät den Wert als Schlüssel erhalten hat, dessen Hashwert zuvor vom Tag gesendet worden ist. Das Verfahren erfordert die Implementierung einer Einweg-Hashfunktion auf dem Tag und ein Schlüsselmanagement im Backend. Dies wird für die nahe Zukunft als wirtschaftlich machbar angesehen [We03]. Leider schützt der Ansatz zwar auf dem Tag gespeicherte Daten, bietet jedoch keinerlei Schutz vor der Erstellung von Bewegungsprofilen (keine „location privacy“), weil ein Tag eindeutig durch den gesendeten Hashwert identifiziert werden kann. Ein weiterer Nachteil ist, dass der Schlüssel im Klartext über den Vorwärtskanal gesendet wird und damit relativ leicht aus größerer Entfernung abgehört werden kann.

Ein erweitertes Verfahren mit dem Namen „Randomized Hash Lock“ [WS03] bietet zwar „location privacy“, skaliert jedoch nicht. Weil im Backend eine große Anzahl von Hash-Operationen ausgeführt werden muss, ist es nicht für eine große Tagzahl anwendbar. Außerdem werden wieder Zufallszahlen im Tag benötigt, um die Tagantworten gegenüber einem Angreifer zufällig aussehen zu lassen.

“Blocker Tags“ [Ju03] zielen darauf ab, Lesegeräte zu stören, um damit die Privatsphäre von Verbraucher zu schützen. Das Verfahren beruht darauf, in die Kollisionsvermeidungsstrategie „Binary-Tree-Walking“, die bei einigen Tags verwendet wird, einzugreifen und damit Taggruppen unsichtbar zu machen. Die Tags selbst werden in keinerlei Weise verändert. Der Ansatz ist zwar einfallsreich, doch funktioniert er mit anderen verwendeten Kollisionsvermeidungsstrategien nicht, erfordert einheitliche Standards für unterschiedliche „Privatsphäre-Zonen“, ist für Verbraucher in hohem Maße intransparent und konnte die verlässliche, praktische Machbarkeit bisher nicht nachweisen. Aus diesem Grund und weil die eigentlichen Probleme nicht gelöst werden, wird der Ansatz von Verbraucherschutzorganisationen nicht befürwortet [FV04].

Ein Verfahren namens „Re-Encryption“ schützt die Privatsphäre, indem die Tag-Kennung bei jedem Lesen für einen Außenstehenden anders aussieht und ein Tag damit für ihn nicht verfolgt werden kann. Das Verfahren beruht darauf, dass es für einen Klartext (hier die Tag-Kennung) verschiedene verschlüsselte Varianten mit dem gleichen Dechiffrierschlüssel geben kann, die auch ohne den Klartext zu kennen ineinander überführt werden können. Das Verfahren ist sehr elegant, doch benötigen derartige Operationen Tags, die zu

komplexen Berechnungen in der Lage und damit teuer sind. Für die Nutzung in Banknoten, deren Authentizität nachgewiesen werden soll, jedoch aber keine verfolgbaren Kennungen enthalten sollen, wurde vorgeschlagen, diese Berechnungen extern durchzuführen [Ju02]. Problem ist jedoch, dass dann jeder die auf dem Tag gespeicherten Daten ändern kann und das Verfahren ohne weitere Vorkehrungen damit für die Praxis wertlos ist.

Mittels kryptographischer Verfahren ist es möglich, alle Probleme hinsichtlich Sicherheit und vom Grundsatz her auch vom Aspekt des Schutzes der Privatsphäre her zu lösen. Dabei muss jedoch vermieden werden, vertrauliche Informationen wie private Schlüssel auf Tags zu speichern. Die Problematik ist hier analog zu der bei Smartcards [We03, Ab91]. Techniken wie „Privacy Amplification“ [Be95] oder „Oblivious Transfer“ [Ra81] können verwendet werden, um Sitzungsschlüssel über einen unsicheren Kommunikationskanal zu erstellen. Leider ist die Implementierung kryptographischer Verfahren auf Tags teuer und bietet selbst wieder viele Angriffsmöglichkeiten [We00].

Ein Ansatz speziell zum Erlangen von „location privacy“ ist die Verwendung einer Liste von Pseudonymen auf einem Tag [Ju04]. Dabei verwendet ein Tag bei jeder Abfrage ein anderes seiner Pseudonyme als Tag-Kennung. Der Ansatz ist sehr einfach zu implementieren und bietet umso mehr Schutz, je größer die Zahl der verfügbaren Pseudonyme ist. Es muss sichergestellt werden, dass ein derartiges Tag nicht in zu kurzen Zeitabständen ausgelesen werden kann und sich die Kennungen wiederholen. Außerdem sollte die Pseudonymliste regelmäßig aktualisiert werden können, damit die Schutzfunktion auch auf Dauer wirksam bleibt.

5 Ein die Privatsphäre berücksichtigendes RFID-Framework

Wie aus dem letzten Abschnitt hervorgeht, gibt es noch kein sowohl skalierbares als auch in wirtschaftlichem Rahmen liegendes Verfahren, das in der Lage wäre, die Privatsphäre der Nutzer in vollem Umfang zu schützen und das dazu notwendige Maß an Systemsicherheit bereitzustellen. Im Folgenden stellen wir daher in groben Zügen einen aus drei Teilen bestehenden Lösungsansatz vor, der diesen Designkriterien zu entsprechen vermag. Ziel war die Schaffung eines offenen und flexiblen Frameworks, bei dessen Design Sicherheit und Schutz der Privatsphäre gewichtige Punkte waren.

5.1 Datenhaltung im Backend

Jegliche Daten, die auf einem RFID-Tag gespeichert sind, müssen entweder als öffentlich zugänglich angesehen oder mit einer Zugangskontrolle versehen werden. Öffentliche Daten ohne Zugriffsschutz widersprechen der Zielsetzung des Bundesdatenschutzgesetzes im Hinblick auf Datensparsamkeit und können darüber hinaus neben einer Tag-Kennung zur Identifikation und Verfolgung eines Tags verwendet werden. Dieses Szenario muss daher vermieden werden. Eine Zugangskontrolle zu auf dem Tag gespeicherten Daten löst die beiden genannten Probleme, es ergeben sich jedoch auch neue. Zum einen sind RFID-Tags aufgrund fehlender Schutzvorkehrungen gegen physikalische Angriffe zur Speicherung sensitiver Daten noch immer nicht geeignet. Zum anderen handelt es sich bei RFID-Tags um Systeme mit knappen Ressourcen: Zusätzlicher Speicher würde benötigt, um Zugangskontrolllisten zu speichern, und zusätzliche Logik und Rechenzeit, um das Lesegerät zu

authentifizieren und die Kommunikation mit dem Lesegerät gegen Angreifer abzusichern. Auch im Hinblick auf die Auslesegeschwindigkeit der Tags sollte die zwischen Tag und Lesegerät zu übertragende Datenmenge möglichst gering gehalten werden.

Da die Implementierung von Zugangskontrollmechanismen bei Speicherung zusätzlicher Daten aus den genannten Gründen zwar nötig, aber auch aufwendig und damit teuer zu realisieren ist, macht es Sinn, neben der eindeutigen Kennung keine weiteren Daten auf einem RFID-Tag abzulegen. Mit der Tag-Kennung als Schlüssel können die benötigten Daten in einer externen Datenbank, die sich in einer sicheren Umgebung befindet, abgelegt und flexible Zugriffsmechanismen für diese Datenbank implementiert werden. Dies bietet auch den weiteren Vorteil, dass mit einem Tag assoziierte Daten auch ohne Präsenz des Tags geändert werden können. Einziger Nachteil der Off-Tag-Datenspeicherung ist, dass zum Auslesen der mit einem Tag assoziierten Daten eine Verbindung zur speichernden Datenbank vorhanden sein muss. Aufgrund der Tatsache, dass dies mit der Verbreitung von Wireless-LAN und flächendeckendem Mobilfunk auch für mobile Anwendungen ein zunehmend kleineres Problem darstellt, wird dieser Nachteil aufgrund der vielfältigen und der damit weitaus überwiegenden Vorteile in Kauf genommen. Zu einem Tag zugehörige Daten werden daher bei praktisch allen publizierten Verfahren nicht auf dem Tag selbst sondern im Backend gespeichert, wo eine kostengünstigere und flexiblere Zugriffskontrolle möglich ist.

Wegen den genannten Vorteilen gehen viele Anwendungen von einer Datenhaltung im Backend aus. Auch die im vorherigen Kapitel vorgestellten Lösungsansätze anderer Forschergruppen setzen eine Datenhaltung im Backend voraus.

5.2 Wechselnde Tag-Kennung

Wie oben erklärt, können RFID-Tags mit statischen Kennungen zur Erstellung von Bewegungsprofilen missbraucht werden. Um dies zu vermeiden, muss eine dynamische Kennung verwendet werden. Mit den Worten des Bundesdatenschutzgesetzes ausgedrückt, muss eine „Pseudonymisierung“ stattfinden: Ein Tag muss wechselnde Pseudonyme haben, so dass Außenstehende nicht mehr auf die wahre Kennung und die dahinter stehende Person schließen können, sondern dies exklusiv für den Besitzer des Tags möglich ist.

Einige Möglichkeiten, dies zu tun, wie beispielsweise Re-Encryption sind oben bereits beschrieben worden. Da die Re-Encryption nur mit hohem Aufwand in einem Tag ausführbar ist bzw. die Validierung einer extern durchgeführten Re-Encryption nicht benutzerfreundlich möglich ist, ist dieses Verfahren für viele Anwendungen zu teuer oder zu schlecht handhabbar. Das Verfahren mit der Pseudonymliste im Tag, deren Einträge nacheinander verwendet werden, bietet nur dann wirklich Sicherheit für die Privatsphäre, wenn die Listeneinträge auf sicherem Wege regelmäßig geändert werden können.

Aus diesem Grund haben wir ein neues Verfahren entworfen, um die Kennung eines Tags regelmäßig zu ändern [He04, HM04]. Dieser basiert wie der „Hash Lock“-Ansatz auf einer in den Tags implementierten Einweg-Hashfunktion.

Das Tag sendet bei seiner Abfrage den Hashwert der aktuellen Tag-Kennung und einen Hashwert, in den die Tag-Kennung und eine Transaktionsnummer eingehen, zur Authentisierung (Nachricht A in Abbildung 1). Die Transaktionsnummer hat dabei die Aufgabe,

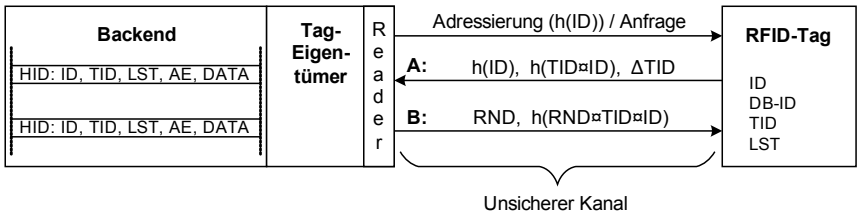

Abbildung 1: Protokoll zur Änderung der Tag-Kennung

Replay-Attacken auf das Protokoll abzuwehren. Als Antwort erhält das Tag eine Zahl, aus der unter zu Hilfenahme der alten Tag-Kennung eine neue errechnet wird. Die neue Tag-Kennung wird also nicht direkt im Klartext übertragen, um das Protokoll gegen Abhören der Verbindung zu sichern. Weiterhin erhält die Antwort an das Tag auch noch einen Hashwert, in den zur Validierung die genannte Zahl und zur Authentisierung auch hier die Tag-Kennung und die Transaktionsnummer eingehen. Die Hashwerte in den beiden Nachrichten dienen also zur Integritätsprüfung der Nachrichten und zur gegenseitigen Authentifizierung.

Auf diesem Weg ist es möglich, die Tag-Kennung bei jedem legitimen Lesen des Tags in sicherer Art und Weise zu ändern. Sicher bedeutet dabei, dass das Protokoll gegen Angriffe wie Abhören, Replay- und Spoofing-Attacken resistent ist. Eine detaillierte Beschreibung des Protokolls und eine Untersuchung der möglichen Angriffe finden sich in [He04]. Wesentliche Charakteristiken des Protokolls sind, dass es mit einem einzigen Nachrichtenaustausch auskommt und den Verlust von Nachrichten – verursacht durch Kommunikationsstörungen oder hervorgerufen durch Angreifer – ohne Probleme hinnimmt. Besonderes Augenmerk wurde beim Entwurf darauf gelegt, dass der Nachrichtenaustausch keine Informationen enthält, die ein Angreifer zur Verfolgung eines Tags verwenden könnte.

Das vorgeschlagene Verfahren kann sinnvoll mit dem Vorschlag der Pseudonymliste kombiniert werden, um auch bei nicht autorisierten Leseversuchen oder einem von Angreifern absichtlich verhinderten Nachrichtenaustausch eine Änderung der Tag-Kennung zu gewährleisten.

Als Protokoll für die regelmäßige Änderung der Tag-Kennung wurde in Anlehnung an das im vorherigen Abschnitt beschriebene Hash-Lock-Verfahren ein auf einer Hashfunktion basierendes Verfahren gewählt, da dies als wirtschaftlich machbar angesehen wird [We03]. Die Hashfunktion sollte dazu effizient in Hardware implementierbar sein. Als alternative technologische Basis für ein Protokoll, mit den erforderlichen Eigenschaften, bieten sich auf elliptischen Kurven basierende kryptographische Verfahren an, da diese ebenfalls effizient umsetzbar sind.

5.3 Divide et impera – Einbindung des Tag-Besitzers

Durch Nutzung dynamischer Tag-Kennungen, wie im vorigen Abschnitt beschrieben, ist es für einen außenstehenden Angreifer nicht mehr möglich, ein Tag zu verfolgen. Dies ist ein großer Gewinn für den Schutz der Privatsphäre des Tag-Besitzers. Allerdings liegt die

volle Kontrolle und die Möglichkeit der Tag-Verfolgung noch immer beim Tag-Eigentümer, so dass der Besitzer diesem im vollen Maße vertrauen muss, dass keine Tracking-Daten weitergegeben oder zur unberechtigten Erstellung von Bewegungsprofilen verwendet werden. Dem Besitzer fehlt jegliche Möglichkeit, den Tag-Eigentümer dahingehend zu kontrollieren. Der Tag-Besitzer erfährt auch nicht, wann, wo und wozu ein Tag ausgelesen wurde, so lange der Tag-Eigentümer ihm diese Informationen nicht freiwillig zukommen lässt.

Um diese Abhängigkeit des Tag-Besitzers vom Tag-Eigentümer zu vermeiden, ist es sinnvoll, die „Macht“ des Tag-Eigentümers auf mehrere Instanzen zu verteilen. Ziel ist es, dass der Tag-Eigentümer zwar volle Kontrolle über das Tag und damit direkt assoziierte Daten behält, jedoch der Tag-Besitzer in den Leseprozess als überwachende Instanz miteinbezogen wird.

Ein erster wichtiger Schritt in diese Richtung ist die logische Trennung von Tag-Eigentümer und lesewilliger Partei, die unter Verwendung eines Lesegerätes ein Tag ausliest und damit assoziierte Daten abfragen möchte. Zwar können Eigentümer und lesewillige Partei durchaus zusammenfallen, doch ist dies umso seltener der Fall, je verbreiteter die RFID-Technologie sein wird.

Eine abstrakte Darstellung des kompletten Frameworks findet sich in Abbildung 2. Dort wird auch die logische Trennung zwischen Eigentümer, dem das Tag gehört und der sich dafür verantwortlich zeichnet, und dem Besitzer, der das Tag mit sich führt, illustriert. Besitzer und Eigentümer können selbstverständlich auch wieder zusammenfallen.

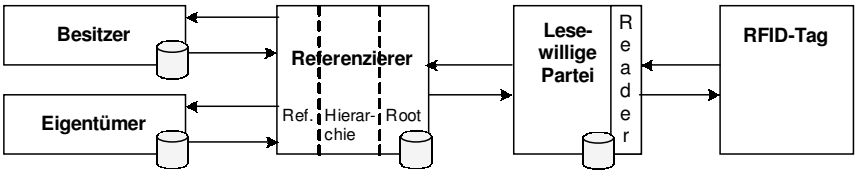

Abbildung 2: RFID-Framework

Die Umsetzung der Designkriterien, i.e. Schutz der Privatsphäre, Verteilung, gegenseitige Kontrolle und Transparenz, sowie das Zusammenspiel der in Abbildung 2 dargestellten Komponenten soll anhand eines Beispielszenarios erfolgen.

Beispiel sei die Verwendung einer mit einem RFID-Tag versehenen Kreditkarte. Eigentümer der Kreditkarte und damit des Tags ist die Kreditkartengesellschaft. Der Kunde, der Besitzer der Kreditkarte und damit des Tags ist, geht in ein Geschäft und möchte mit Hilfe seiner Kreditkarte bezahlen. Das Geschäft besitzt ein Lesegerät an der Kasse und ist somit die lesewillige Partei.

Das Geschäft liest mit Hilfe des Lesegeräts das Tag der Kreditkarte aus. Bis dahin unterscheidet sich das Verhalten des Geschäfts in keiner Hinsicht von einem möglichen Angreifer. Um dem Schutz der Privatsphäre gerecht zu werden und ein unberechtigtes Verfolgen

des Tags unmöglich zu machen, dürfen die gelesenen Tagdaten keinerlei dafür verwertbare Informationen erhalten, schon gar nicht den Besitzer oder den Eigentümer des Tags. Hier findet sich somit ein Konflikt: Ein Angreifer darf Besitzer oder Eigentümer nicht erfahren, ein legitimer Leser muss jedoch mit Besitzer und Eigentümer kommunizieren können, um die mit dem Tag assoziierten Daten abzufragen.

Hier kommt die als „Referenzierer“ bezeichnete in Abbildung 2 dargestellte Instanz ins Spiel. Es handelt sich dabei um ein am ehesten mit dem DNS-System vergleichbares hierarchisch aufgebautes System, das jedoch zusätzlich anonymisierende und entanonymisierende Funktion übernimmt.

Die gelesene, eventuell dynamische Tag-Kennung, mit der das Geschäft genauso wie ein potentieller Angreifer nichts anfangen kann wird zusammen mit einer Anfrage nach Daten durch das Kassensystem (etwa: „Ich bin das Kassensystem von Geschäft X und möchte Daten von Zahlungsmitteln auslesen“) an einen der Root-Server des Referenzierungssystems gesendet. Ein Root-Server ist in der Lage, aus der Tag-Kennung gerade soviel Information zu extrahieren, dass er weiß, an welchen Server der nächsten Hierarchieebene er die Anfrage weiterleiten muss. Dies funktioniert durch die weiteren Hierarchieebenen hindurch analog, bis die Anfrage auf der obersten Hierarchieebene angekommen ist. Hier ist nun verzeichnet, wer der Besitzer des Tags mit der angegebenen Kennung ist und die Anfrage wird an diesen weitergeleitet.

Da die oberste Hierarchieebene von der Vertrauensstellung her dem Tageigentümer nahe steht, kann durch den Besitzer optional noch ein Mix-System zwischengeschaltet werden. Dies ist jedoch nur für besondere Anwendungen relevant, bei denen der Besitzer dem Betreiber der obersten Hierarchieebene einen unerlaubten Datenaustausch mit dem Eigentümer unterstellt und gegenüber dem Eigentümer anonym bleiben möchte oder anderweitig eine besondere Stellung einnimmt.

Allein der Besitzer ist nun in der Lage, aus der empfangenen Tag-Kennung auf den Eigentümer zu schließen. Sofern die erhaltene Anfrage nach Tagdaten legitim und sinnvoll ist, wird die Anfrage über den Referenzierer an den Tageigentümer weitergeleitet und dort weiterverarbeitet. Entspricht die Anfrage nicht dem Datenschutzwünschen des Besitzers oder macht sie keinen Sinn (wenn das Kassensystem z.B. ein Tag eines Ausweises lesen möchte), so wird die Anfrage abgelehnt, ohne das die lesewillige Partei, also im Beispiel das Kassensystem, die Identität des Besitzers erfährt.

Sofern vom Besitzer als legitim eingestuft, erhält der Eigentümer nun die Anfrage und prüft sie. Er kann die Anfrage ablehnen, weitere Informationen anfordern oder mit den angefragten Daten antworten. Im Beispiel würde die Kreditkartenfirma beim Lesen des Tags der Kreditkarte mit der Firmenidentität und den vom Kassensystem benötigten Daten wie z.B. einer Kartennummer o.ä. antworten.

Anhand des beschriebenen Beispielszenarios wurden die Grundgedanken des vorgeschlagenen Frameworks in groben Zügen verdeutlicht: saubere Trennung der beteiligten Parteien und Einbezug all dieser Parteien in das Gesamtsystem. Jede der Parteien behält dabei die Kontrolle über die sie betreffenden Abläufe im System und kann gegebenenfalls Einfluss nehmen.

Für den Besitzer des Tags, d.h. den Träger, welcher im Regelfall der Verbraucher ist, wird transparent und überprüfbar, wann ein Tag zu welchem Zweck gelesen wird, wie es von Verbraucherschützern gefordert wird [FV04, Ga02]. Das vorgestellte Konzept erweitert eine mögliche freiwillige Selbstkontrolle bzw. an Lesegeräten angebrachte, möglicherweise irreführende, unvollständige und generell unkontrollierbare Informationstexte um eine technische, im System verankerte und somit kontrollierbare Einfluss- und Überprüfungsmöglichkeit für den Tagbesitzer. Da diese Überprüfung verpflichtend notwendig ist, um ein Tag auszulesen, kann sich kein Anbieter oder Angreifer darüber hinwegsetzen und Tags ohne Zustimmung des Besitzers auslesen.

Der Eigentümer eines Tags bleibt dabei in der Lage, dieses für legitimierte Anwendungen zu verwenden und im Rahmen des Bundesdatenschutzgesetzes beliebige Daten damit zu assoziieren.

Die Partei, die ein Tag auszulesen versucht, erhält vom Tageigentümer nur die Daten, die sie auch wirklich benötigt. Dies entspricht dem Grundsatz der Datensparsamkeit. Im Gegensatz zu anderen Ansätzen gehen wir grundsätzlich davon aus, dass diese Partei nicht oder nur eingeschränkt vertrauenswürdig ist.

Der Referenzierer stellt eine von Providern und Dienstleistern unterhaltene, hierarchische Infrastruktur dar, wie sie vom Namensauflösungssystem des Internet (DNS) her bereits bekannt ist. Genauso, wie das Internet ohne ein funktionierendes DNS nicht nutzbar wäre, baut das vorgestellte Framework auf einem funktionierenden Referenziererdienst auf.

Aufgrund Tatsache, dass die betroffenen Parteien im Framework voneinander getrennt sind, ergibt sich die Möglichkeit der gegenseitigen Überwachung und Kontrolle, beispielsweise auf Einhaltung gesetzlicher Regelungen oder getroffener Abmachungen hin.

6 Zusammenfassung

Im vorliegenden Beitrag wurden die Probleme, die eine Einführung von RFID-Systemen in Bezug auf den Schutz der Privatsphäre mit sich zieht, dargestellt. Bei der Vorstellung bisher vorgeschlagener Lösungsansätze wurde deutlich, dass es noch keine praktisch umsetzbaren Verfahren gibt, die in der Lage wären, all diese Probleme wirtschaftlich zu lösen. Sogar wenn man die Einschränkung des „wirtschaftlich“ wegfallen lässt, sieht das kaum anders aus.

Daraufhin haben wir die Grundideen eines Frameworks erläutert, das generisch für eine Vielzahl von Anwendungen eine Möglichkeit bietet, den Schutz der Privatsphäre beim Einsatz von RFID-Systemen technisch zu verankern.

Das Framework basiert dabei im Wesentlichen aus drei Teilbausteinen: Erstens die Verlagerung der Datenspeicherung vom Tag ins Backend, wie es auch von vielen anderen Ansätzen vorausgesetzt wird. Zweitens die Nutzung einer Tag-Kennung, die mit einem sicheren Protokoll regelmäßig geändert wird, um ein unberechtigtes Verfolgen eines Tags wirksam zu unterbinden. Und drittens schließlich die Trennung der einzelnen beteiligten Parteien, um somit Transparenz und gegenseitige Kontrollmöglichkeiten zu schaffen.

Das Framework ist dabei offen und flexibel genug, um eine Vielzahl auch besonderer Anwendungen zu unterstützen. Beispielsweise ist es möglich, dass der Tagbesitzer gegenüber

dem Tageigentümer anonym bleibt, jedoch ein Auslesen des Tags vom Tagbesitzer erfasst und ggf. unterbunden werden kann. Derartiges macht z.B. bei einem S-Bahn-Ticket Sinn, wo die Identität des Fahrgastes den Verkehrsbetrieben als Fahrkarteneigentümer nicht offen gelegt werden muss.

Es ist damit ein Verfahren kurz vorgestellt worden, das die Forderungen von Daten- und Verbraucherschützern hinsichtlich des Schutzes der Privatsphäre erfüllt, legitime und innovative Anwendungen aber nicht beeinträchtigt.

Literatur

[Ab91] Abadi, M. et al.: Authentication and Delegation with Smart-cards. Theoretical Aspects of Computer Software, Seiten 326-345, 1991

[Ag03] Agrawal. D. et al.: Advances in Side-Channel Cryptanalysis. RSA Cryptobytes Vol. 6, Nr. 1, 2003

[Ba95] Bakhtiari, S. et al.: Cryptographic Hash Functions: A Survey. Technical Report 95-09, Department of Computer Science, University of Wollongong, 1995

[Ba96] Bakhtiari, S. et al.: Keyed Hash Functions, Cryptography: Policy and Algorithms. E. Dawson and Jovan Golic (Eds), Lecture Notes in Computer Science, Vol. 1029, Seiten 201-214, Springer, 1996

[BB03] Consumer Group Calls for Immediate Worldwide Boycott of Benetton. 2003, Web: http://www.boycottbenetton.org/PR_030313a.html, 2004

[Be94] Berson, T. et el.: Secure, Keyed, and Collisionful Hash Functions. Technical Report SRI-CSL-94-08, SRI International, 1994

[Be95] Bennett, C. H. et al.: Generalized Privacy Amplification. IEEE Transaction on Information Theory, Vol. 41, Seiten 1915-1923, 1995

[Be03] Beresford, A. R.; Stajano, F.: Location Privacy in Pervasive Computing; IEEE Pervasive Computing, Januar-März 2003, Seiten 46-55, 2003

[Bl03] Black, J.: Playing Tag with Shoppers Anonymity. BusinessWeek online, 2003, Web: http://www.businessweek.com/technology/content/jul2003/tc20030721_8408_tc073.htm

[Ca98] Canetti, R. et al.: Perfectly One-Way Probabilistic Hash Functions. 30th Annual Symposium on Theory of Computing, Seiten 131-140, 1998

[Ch81] Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, Vol. 24(2), Seiten 24-88, 1981

[CN03] CNET News: Wal-Mart to throw its weight behind RFID. Web: http://news.com.com, 2003

[Cr03] Crane, J.: Benetton Clothing to Carry Tiny Tracking Transmitters. Associated Press, 2003

[CW03] Computerworld: Sidebar: UPS Sees RFID In Its Future but Isn't Ready to Deploy Devices. Web: http://www.computerworld.com, 2003

[EG04] EPCglobal Inc. Web: http://www.epcglobalinc.org, 2004

[EI04] EAN International, Web: http://www.ean-int.org, 2004

[EP03] Electronic Privacy Information Center / Privacy International: Privacy and Human Rights 2003, An International Survey of Privacy Laws and Developments. epic.org, 2003

[EZ03] E-ZPass, Web: see http://www.ezpass.com, 2003

[FV04] FoeBuD e.V., Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. Web: http://www.foebud.de, 2004

[Ga02] Garfinkel, S.: An RFID Bill of Rights. Technology Review, 2002, Web: http://www.technologyreview.com/articles/garfinkel1002.asp, 2003

[He04] Henrici, D. et al.: Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. PerSec'04 at IEEE PerCom, 2004

[HM04] Henrici, D.; Müller, P.: Tackling Security and Privacy Issues in Radio Frequency Identification Devices, 2nd International Conference on Pervasive Computing (Pervasive), 2004

[Ju02] Juels, A.; Pappu, R.: Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. Financial Cryptography, 2002

[Ju03] Juels, A. et al.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. 10th ACM Conference on Computer and Communications Security, 2003

[Ju04] Juels, A.: Minimalist Cryptography for RFID Tags, 2003. In submission. Web: http://www.rsasecurity.com/rsalabs/node.asp?id=2033, 2004

[Li03] Lindquist, M.: RFID in libraries – introduction to the issues. World Library and Information Congress: 69th IFLA General Conference and Council, 2003

[MC03] McCullagh, D.: RFID tags: Big Brother in small packages. CNET, 2003, Web: http://news.com.com/2010-1069-980325.html, 2004

[MC04] Mobilecloak. Web: http://www.mobilecloak.com, 2004

[Ra81] Rabin, M..: How to Exchange Secrets by Oblivious Transfer. Technical Memo TR-81, Aiken Computation Laboratory, Harvard University, 1981

[RJ02] RFID Journal: Gillette to Buy 500 Million EPC Tags. Web: http://www.rfidjournal.com, 2002

[RJ03] RFID Journal: Michelin Embeds RFID Tags in Tires. Web: http://www.rfidjournal.com, 2003

[Sa02] Sarma, S. et al.: RFID Systems and Security and Privacy Implications. Workshop on Cryptographic Hardware and Embedded Systems, Seiten 454-470, Lecture Notes in Computer Science, 2002

[Sa03] Sarma, S. et al.: Radio-Frequency Identification: Security Risks and Challenges. RSA Laboratories Cryptobytes, Vol. 6, Nr. 1, 2003

[SR04] Web: http://www.stoprfid.org/, 2004

[TG02] Auto-ID Center: Technology Guide. Web: http://www.autoidcenter.org/aboutthetech.asp, 2003

[UN48] United Nations: Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution, 217 A(III), 1948

[We00] Weingart, S.: Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. Cryptographic Hardware and Embedded Systems – CHES 2000, Vol. 1965, Seiten 302-317, Springer LNCS, 2000

[We03] Weis, S.: Security and Privacy in Radio-Frequency Identification Devices. Massachusetts Institute of Technology, 2003

[WS03] Weis, S. et al.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. First International Conference on Security in Pervasive Computing (SPC), 2003

[Yo01] Yohida, J.: Euro bank notes to embed RFID chips by 2005. EE Times, 2001, Web: http://www.eetimes.com/story/OEG20011219s0016, 2003