Sicherheit und Privatsphäre in RFID-Systemen

Dipl.-Ing. Dirk Henrici, Technische Universität Kaiserslautern, Deutschland
Prof. Dr. Paul Müller, , Technische Universität Kaiserslautern, Deutschland

Kurzfassung

RFID-Technik hat ein enormes Potential, es gibt bereits jetzt eine Vielzahl von Anwendungen. Der Schutz der Privatsphäre hat in Entwicklung und Vermarktung der Technologie jedoch noch einen geringen Stellenwert. Im Rahmen des Beitrags wird in die mit der RFID-Technik zusammenhängenden Probleme in Bezug auf Systemsicherheit und Privatsphäre eingeführt und daraus abgeleitet, welche Maßnahmen ergriffen werden müssen.

1 Einführung und Motivation

Der Radio-Frequency Identification (RFID) Technologie wird eine glänzende Zukunft vorhergesagt: Als Nachfolger für optische Barcodes, deren Erfassung eine direkte Sichtverbindung voraussetzt, ermöglichen RFID-Labels (auch Tags oder Transponder genannt) eine drahtlose Identifikation und Verfolgung von Produkten. Die Technik soll damit eine neue Ära für Logistik, Inventarisierung und Lieferkettenmanagement einläuten.

Konzerne wie Wal-Mart und Metro aber auch andere bekannte Firmen wie Gillette oder Benetton drängen daher auf eine Einführung in den Massenmarkt. Ähnlich wie heute mit optischen Barcodes sollen erst Paletten, später auch einzelne Produkte mit Labels ausgestattet werden.

Auch für Büchereien stellt die Technik einen bequemen Weg dar, Bestände zu erfassen und zu verwalten [1], und Post- und Lieferdienste können die zu versendenden Güter zur automatischen Verfolgung mit Labels bestücken. Neben vielen anderen sind anvisierte Anwendungsgebiete auch Zutritts- und Zeiterfassungssysteme, Ticket- und Mautsysteme [2] und die Fälschungssicherung beispielsweise von Geldscheinen.

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 [3], soll diese Kennung für die Warenwirtschaft aus einem “Electronic Product Code” (EPC), der die Nachfolge des UPC und des EAN-Codes [4] antreten soll, bestehen. Der EPC setzt sich zusammen aus einem Herstellercode, einem Code für den Produkttyp und einer eindeutigen Seriennummer und kann damit Produkte eindeutig identifizieren. Aus Datenbanken im Backend können mittels dieser Produktkennung dann weitere Informationen zu den jeweiligen Produkten abgerufen werden.

In anderen Anwendungsbereichen werden – zumindest zurzeit – proprietäre Nummerierungsschemata verwendet und zuweilen neben der eindeutigen Tagidentifikation auch noch weitere Daten auf den Tags abgelegt. Für Reisepässe sind beispielsweise Tags angedacht, auf denen zusätzlich biometrische Daten des sich Ausweisenden abgelegt werden [5].

Die vielfältigen Möglichkeiten, die die RFID-Technik bietet, können leider auch zum Schaden der Menschen eingesetzt werden. Insbesondere die Möglichkeit der quasi unbemerkten Verfolgung von Gütern bereitet auch Probleme.

Denn es können nicht nur die Güter verfolgt werden, sondern indirekt auch die Personen, die diese Güter mit sich führen. In anderen Anwendungen, beispielsweise zur Zutrittskontrolle oder bei Ausweisen, wird sogar eine direkte Zuordnung von Labels und Personen vorgenommen.

Die Befürchtungen gehen soweit, dass ein Netz von miteinander verbundenen Lesegeräten es möglich machen wird, alles und jeden zu verfolgen. Dieser Möglichkeit wird sich ein Individuum bei Nutzung der RFID-Technologie auf breiter Front nicht mehr entziehen können („opt-out“), und bei Missbrauch kann der Albtraum eines Orwellschen „1984“ oder gar ein noch schlimmeres Szenario Wirklichkeit werden [6].

Aus diesen Gründen haben einige Unternehmen auch schon massiven Druck von Verbrauchern und Verbraucherschützern zu spüren bekommen: Einzelne Anbieter wurden bereits boykottiert [7, 8] und Metro, bekannt durch den „Future-Store“, erhielt für mangelnden Verbraucherschutz in 2003 einen „BigBrother-Award“ [9].

Doch muss nicht nur mit dem Akzeptanzproblem bei den Verbrauchern umgegangen werden, auch für die Unternehmen, die die RFID-Technologie einsetzen, können sich fehlende Vorkehrungen für die Gewährleistung von Datensicherheit oder gegen ungewolltes Tracking – beispielsweise durch die Konkurrenz – als heikel erweisen.

Im Rahmen der Forschung wird daher aktuell nach Verfahren gesucht, mit möglichst wenig Aufwand in den Labels – um die Kosten gering zu halten – die System- und Datensicherheit zu erhöhen und

die Privatsphäre der Verbraucher und Unternehmen zu schützen.
Die Bedrohungen, der sich die RFID-Technik dabei gegenüber sieht, sind sehr vielfältig. Dies wird in den nächsten Abschnitten dargestellt und verdeutlicht. Im Anschluss werden Designkriterien für RFID-Systeme abgeleitet, und es wird auf mögliche Lösungswege verwiesen.

2 Systemsicherheit

Aufgrund der Vielfalt der möglichen Anwendungsbereiche für RFID-Systeme kann davon ausgegangen werden, dass die Technik auch in geschäftskritischen Systemen Verwendung finden wird, deren Ausfall oder Störung betriebliche Abläufe beeinträchtigt und teilweise erhebliche Kosten verursacht.
Es muss daher dafür Sorge getragen werden, dass ein ordnungsgemäßes Funktionieren der RFID-Systeme für die gegebenen Anwendungen auch bei Beeinträchtigungen von Außen gewährleistet ist. Wie im Folgenden dargestellt wird, sind eine Vielzahl von Angriffspunkten denkbar. Die folgende Darstellung erhebt keinen Anspruch auf Vollständigkeit, sondern soll nur dazu dienen, für das Thema zu sensibilisieren.

2.1 Tags

RFID-Tags bestehen im einfachsten Fall aus einem Mikrochip und einer mit ihm verbundenen Antenne. Im Regelfall besitzen sie keine eigene Stromversorgung, sondern beziehen die für ihre Arbeit benötigte Energie aus dem elektromagnetischen Feld eines Lesegerätes.
Der trivialste Weg, ein RFID-System zu stören, stellt die Zerstörung von Tags da. Dies kann durch übermäßige mechanische Beanspruchung, durch Einbringen von Strahlung oder auf chemischem Wege, beispielsweise durch ätzende Substanzen, erfolgen. Ausgefeilter ist ein teilweises Unbrauchbarmachen oder eine gezielte Änderung von auf dem Tag gespeicherten Daten. Dieses wird evtl. nicht direkt erkannt und kann die Tag-Logik oder die eingesetzten Kommunikationsprotokolle - insbesondere, wenn sie einen zwischen Tag und Backend-Datenbank synchronisierten Zustand voraussetzen, beeinträchtigen. Solche undefinierten Zustände können auch durch ein plötzliches Ausbleiben oder schwankende Energieversorgung [10] hervorgerufen werden, wogegen passive Tags besonders anfällig sind. Die Tag-Logik muss entsprechend ausgelegt sein, damit Transaktionen, die den internen Zustand eines Tags ändern, vollständig oder gar nicht durchgeführt werden.
Mittels physikalischer Verfahren ist es – ähnlich wie bei Smartcards – möglich, unter Umgehung der normalen Sicherheitsmechanismen eines regulären Zugriffs an alle auf dem Tag gespeicherten Daten zu gelangen. Der Aufwand mag recht hoch sein, doch insbesondere in dem Fall, dass Kommunikationsschlüssel oder Kennwörter, die für mehr als ein Label gelten oder längerfristig Gültigkeit haben, auf dem Tag gespeichert sind, stellt ein derartiger Angriff ein großes Gefahrenpotential dar. Beispiel wäre ein „Kill-Kommando“ für die gezielte Zerstörung von Tags: Hat nicht jedes Tag ein individuelles Kill-Kommando, können durch ein ungewolltes bekannt werden des Kommandos eine große Zahl von Tags durch einen Angreifer unbrauchbar gemacht werden.
Für viele Anwendungsgebiete darf es nicht möglich sein, dass ein Tag ohne weiteres kopiert oder imitiert werden kann, beispielsweise wenn Tags zur Erhöhung der Fälschungssicherheit oder als Ausweis genutzt werden. Ein Kopieren oder Imitieren ist dann besonders einfach, wenn ein Tag seine komplette „Identität“ nach Außen preisgibt, d.h. keine Zustandsinformation, Zugriffschlüssel o.ä. einbehalten wird.

2.2 Funkschnittstelle

Tags und Lesegeräte kommunizieren drahtlos über die Luft, die ein „shared medium“ ist, auf das jeder zugreifen kann.
Am einfachsten ist es, die Funkschnittstelle entweder abzuschirmen oder mittels Störsignalen zu stören. Eine Abschirmung erfolgt durch Objekte, die als Faradayscher Käfig fungieren. Ein Beispiel dafür sind mit Metallstreifen versehene Handtaschen, die sogar bereits kommerziell verfügbar sind [11]. Auch aus größeren Entfernungen möglich, aber leichter detektierbar, ist ein Stören der Kommunikation durch Aussendung eines Störsignals auf den zur Kommunikation verwendeten Frequenzen.
Eine gezielte Störung der Adressierung von Tags ist ebenfalls möglich. Für Tags, die Binary-Tree-Walking als Kollisionsvermeidungsstrategie verwenden, gibt es beispielsweise „Blocker Tags“ [12], die dafür sorgen, dass bestimmte Gruppen von Tags nicht mehr gefunden werden. Während in diesem Fall die Störung der Kommunikation zum Schutz der Privatsphäre eingesetzt werden soll, sind in gleicher Weise jedoch auch nicht gewollte Denial-of-Service-Angriffe möglich.
Die offene Funkschnittstelle macht auch ausgefeilte Angriffe auf andere benutzte Kommunikationsprotokolle möglich. Zu den Möglichkeiten dafür gehören Replay-Angriffe. Ein besonderes Problem der RFID-Technik gibt es dahingehend, dass ein Ab-

fangen von Nachrichten und ein späteres Weiterleiten an ein Tag erst durch eine Antwortnachricht bemerkt werden kann, weil RFID-Tags „zeitlos“ sind: Sie haben keine innere Uhr und einige Standardmethoden des Umgangs mit verspäteten Nachrichten aus der Netzwerkwelt (wie etwa Zeitstempel) können daher nicht angewandt werden. Auf derartige Angriffsmöglichkeiten muss daher beim Protokolldesign besonderes Augenmerk gelegt werden.
Durch ein Abhören des Funkkanals kann ein Angreifer versuchen, an verwertbare Informationen zu gelangen, die ihm aktive Angriffe erleichtern oder gar erst ermöglichen. Beispielsweise muss vor Replay-Angriffen die Kommunikation aufgezeichnet worden sein.
Es soll noch einmal explizit erwähnt werden, dass Konzepte des Denial-of-Service in bestimmten Fällen bewusst und sinnvoll angewendet werden können. Ein Beispiel wäre eine Geldbörse für RFID-Geldscheine, die dank Abschirmung zum Schutz der Privatsphäre ihren Inhalt nicht preisgibt.

2.3 Lesegeräte und Backend

Für Lesegeräte und Systeme im Backend wie beispielsweise Datenbanken sind die aus der Netzwerkwelt bekannten Konzepte des AAAA (Authentication, Authorization, Accounting und Auditing) anzuwenden, um Systemsicherheit zu gewährleisten. Ein Augenmerk muss darauf gelegt werden, dass exponierte Lesegeräte gegen Vandalismus und sonstige Störungen entsprechend gesichert sind.
Weiterhin ist es erforderlich, dass ein Fälschen der Identität nicht möglich ist, also dass ein Lesegerät eines Angreifers nicht als ein legitimes agieren und beispielsweise die zwischen Tag und Lesegerät/Backend verwendeten Kommunikationsprotokolle beeinträchtigen kann.

3 Datenschutz und Privatsphäre

Datenschutz und Privatsphäre der Benutzer sind Punkte, die in der Öffentlichkeit im Hinblick auf einen großflächigen Einsatz der RFID-Technologie ausgiebig und auch heiß diskutiert werden.
Die Diskussion beginnt beim Schutz zu speichernder oder zu verarbeitender Daten und geht über Bedenken, dass riesige Datenbanken mit nicht zweckgebundenen Datenbeständen (Vorratsdatenspeicherung) entstehen, bis hin zu Ängsten, dass die Möglichkeiten des Trackings von Personen und Gütern von der Erstellung von Kunden- und Bewegungsprofilen zu Marketingzwecken bis hin zur totalen Überwachung Orwellschen Ausmaßes führen könnte.

3.1 Datenschutz allgemein

Wie bereits im Abschnitt zur Systemsicherheit dargestellt, sind auf dem Tag gespeicherte unverschlüsselte Daten nicht sehr sicher aufgehoben. Aus diesem Grund kann nur davon abgeraten werden, sensitive Daten unverschlüsselt auf einem Tag abzulegen. Für auf einem Tag abgelegte Daten muss es geeignete Mechanismen zur Zugriffkontrolle geben, damit nur authorisierte Personen bzw. Systeme Zugriff auf diese Daten erlangen können (Datensicherheit).
Die Verbindung zwischen Tag und Lesegeräten kann recht einfach, mit entsprechender Ausrüstung auch aus größerer Entfernung, abgehört werden. Erwähnenswert ist dabei, dass bei Verwendung von passiven Tags Kommunikation in Richtung von Lesegerät zum Tag aus größerer Entfernung abgehört werden kann als in der umgekehrten Richtung. Dies liegt daran, dass das elektromagnetische Feld des Lesegerätes vergleichsweise stark sein muss, weil ja darüber auch das Tag mit Energie versorgt wird.
Wegen den Möglichkeiten eines Lauschangriffs dürfen sensitive Daten nicht im Klartext übermittelt werden. Wie im Abschnitt zur Privatsphäre noch erklärt werden wird, sind alle übertragenen Daten einschließlich Protokollinformationen als sensitiv einzustufen, wenn ein ungewolltes Tracking verhindert werden soll.
Die Speicherung und Verarbeitung von Daten im Backend kann datenschutzrechtlich schnell problematisch werden. Daher sind insbesondere Prinzipien der Datensparsamkeit zu beachten, d.h. dass im Gegensatz zur Vorratsdatenspeicherung Daten nur zweckgebunden und nur im wirklich notwendigen Umfang gespeichert werden. Zunehmende offenere und vernetztere Systeme machen einen effektiven Schutz der gespeicherten Daten zu einer Herausforderung. Neben dem „üblichen“ AAAA beim Datenzugriff gewinnt daher ein zuverlässiges Datenmanagement an Bedeutung, um den erhöhten Anforderungen Rechnung tragen zu können.

3.2 Tracking und Privatsphäre

Mit der RFID-Technologie kann nicht nur der Weg von Waren zurückverfolgt werden, sondern auch drahtlos ermittelt werden, was für Produkte eine Person mit sich führt. Weiterhin kann eine Person anhand der Produkte, die sie mit sich trägt, unbemerkt identifiziert und verfolgt werden. Dies stellt einen schwerwiegenden Eingriff in die Persönlich-

keitsrechte dar, wie sie Bestandteil der Verfassungen vieler Nationen sind [13].
Problem ist nun, dass auf der einen Seite die Möglichkeit von Tracking erwünscht sein kann (z.B. Warenwirtschaft), auf der anderen Seite aber auch häufig unerwünscht ist. Ziel ist es daher, einen Weg zu finden, der gewolltes Tracking ermöglicht, ungewolltes aber unumstößlich unterbindet.
Dazu muss es erst einmal möglich sein, Tracking überhaupt zu unterbinden. Zum anderen muss gewolltes Tracking dann wieder kontrolliert ermöglicht werden können.

Tracking - Dateninhalt

Die Möglichkeit des Tracking von Tags und damit von Waren und Produkten ist die Triebfeder für den Einsatz der RFID-Technik in der Warenwirtschaft. Um die gewünschte Funktion zu realisieren, enthalten die Tags eine eindeutige Kennung, beispielsweise einen EPC (Electronic Product Code) [3]. Mittels einer derartigen Kennung kann ein Tag eindeutig identifiziert werden.
Für die Entwicklung von Verfahren für den Schutz der Privatsphäre ist es von Interesse, dass eine derartige eindeutige Kennung nicht die einzige Möglichkeit darstellt, um Tags und damit ihren Träger verfolgen zu können.
So wurde beispielsweise vorgeschlagen, beim Kauf eines Produktes im Supermarkt die eindeutige Seriennummer zu löschen und nur noch die Herstellerangabe und den Produkttyp intakt zu lassen [15]. Doch stellt dies keinen wirksamen Schutz gegen Tracking dar, weil Personen dadurch identifiziert werden können, dass sie eine bestimme Konstellation von Produkten mit sich führen. Beispielsweise eine Armbanduhr von Hersteller X und Schuhe vom Hersteller Y. Zwar sind derartige Konstellationen nicht notwendigerweise eindeutig, doch steigt die Wahrscheinlichkeit dafür mit der Anzahl der getragenen Produkte. Sofern noch weitere Nutzdaten auf einem Tag gespeichert werden, bei einem Supermarktprodukt beispielsweise ein Mindesthaltbarkeitsdatum, können auch diese zu Trackingzwecken genutzt werden.
Es wird also umso einfacher möglich, ein Tag und damit dessen Träger zu verfolgen, je unterschiedlicher die Daten auf den Tags sind. Dies ist umso mehr der Fall, je umfangreicher die von einem Tag extrahierbaren Daten sind.
Zum Schutz der Privatsphäre sollte die Menge der von einem Tag abrufbaren Daten also möglichst gering sein. Und alles, was abrufbar ist, sollte für einen Außenstehenden zufällig erscheinen, damit es nicht für ein ungewolltes Tracking nutzbar ist.

Tracking – Taganzahl/ Datenmenge

Doch nicht nur die auf den Tags gespeicherten Daten können zu Trackingzwecken verwendet werden. Ein erster Ansatzpunkt für einen Angreifer kann schon die Anzahl der Tags, die eine Person mit sich führt, sein: Ist sie ungewöhnlich hoch (oder in Zukunft auch niedrig), kann alleine dadurch eine Person wieder erkannt werden. In der Praxis ist die Zahl der Tags alleine jedoch zu unspezifisch.
Spezifischer ist jedoch die Menge der Nutzdaten, die von einem Tag ausgelesen werden kann, sofern sie nicht konstant ist. Unter Nutzung dieser Zusatzinformation können selbst Personen, die die gleiche Anzahl von Tags mit sich führen, unterschieden werden selbst ohne den eigentlichen Inhalt der Datenpakete zu kennen.

3.3 Vertrauen

In den meisten Arbeiten auf dem Gebiet der RFID-Technik werden Betreiber des Lesegerätes und die zu einer Anwendung gehörenden Tags als zusammengehörig angesehen und dann auf die Absicherung der Kommunikation und das Ausschließen einer Trackingmöglichkeit durch außen stehende Parteien fokussiert. Damit wird jedoch Vertrauen zwischen einem Nutzer, der Tags trägt oder mit Tags behaftete Gegenstände mit sich führt, und den Parteien, die die Tags ausgegeben haben und verwalten, vorausgesetzt. Denn selbst bei Implementierung der in diesen Arbeiten vorgeschlagenen Verfahren zur Erhöhung von Sicherheit und dem Schutz der Privatsphäre obliegt die Entscheidung und die Kontrolle, wer ein Tag auslesen und tracken darf, alleine der Partei, der das das Tag gehört, und der Nutzer bleibt außen vor. Dies muss für umfassenden Schutz geändert werden.

4 Designkriterien

In den vorherigen Abschnitten wurde deutlich, dass es eine Vielzahl von Bedrohungen für Systemsicherheit, Datenschutz und Privatsphäre gibt. Insbesondere das Problem, ein ungewolltes Tracking zu unterbinden, ist nicht einfach zu lösen: Eine Lösung setzt nicht nur ein sicheres System und Beachtung des Datenschutzes beim Tag voraus, sondern erfordert auch umfassende Berücksichtigung beim Systemdesign. Die Implikationen dahingehend sind so umfangreich, dass ein nachträgliches Hinzufügen einer technischen Schutzfunktion für die Privatsphäre in ein bestehendes System kaum mehr möglich ist.

Technische Verankerung

Es wurde vorgeschlagen, dass die Industrie zum Schutz der Privatsphäre der Verbraucher eine Art freiwillige Selbstverpflichtung eingeht, d.h. u.a. Waren mit Tags entsprechend kennzeichnet, Kunden, die auf Tags verzichten wollen, nicht benachteiligt usw. [16] Derartiges klingt in der Theorie zwar gut, ist jedoch in der Praxis unzureichend.
Auch rein legislative Beschränkungen, z.B. dass Tags nur zu bestimmten Zwecken verwendet werden dürfen, müssen als unzureichend angesehen werden.
Dass Systemsicherheit und Schutz der Privatsphäre technisch verankert werden müssen, zeigt sich beispielsweise am SPAM-Problem: Bei der Entwicklung der Mailprotokolle wurde auf die Absicherung des Systems gegen Missbrauch zu wenig Wert gelegt. Gesetzliche Verbote sind nicht auf ihre Einhaltung zu kontrollieren und greifen nicht, was heute zu großem volkswirtschaftlichem Schaden führt. Es sollte daher aus vergangenen Fehlern eine Lehre gezogen werden, und Schutzmaßnahmen von Anfang an technisch in den RFID-Systemen verankert werden.

Effizient implementierbar

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. Mit dieser Minimalausstattung lassen sich jedoch keine Schutzfunktionen implementieren.
Je mehr Funktionalität integriert werden muss, desto mehr steigen aber auch die Kosten. Es macht daher Sinn, mit vergleichsweise einfachen symmetrischen Verschlüsselungsverfahren oder kryptographischen Hash-Funktionen auszukommen und für diese nach effizienten Implementierungen in Hardware zu forschen. Es wurde bereits gezeigt, dass sich alleine mit einer Implementierung einer solchen Hash-Funktion auf den Tags die benötigten Schutzfunktionen realisieren lassen [17]. Eine derartige Voraussetzung wird als wirtschaftlich machbar angesehen [15].
Eine Implementierung komplexerer asymmetrischer Verschlüsselungsoperationen auf den Tags oder die Erzeugung „guter“ Zufallszahlen auf den Tags sind also nicht erforderlich. Damit können in Massenproduktion die Mehrkosten für die Implementierung der Schutzfunktion im Verhältnis zu den Gesamtherstellungskosten eines Tags gering werden.

Generische Tags

Wie im vorherigen Abschnitt angesprochen, müssen Tags in Massenproduktion hergestellt werden, um geringe Stückkosten erreichen zu können. Ziel sollte es daher sein, „generische“ Tags herzustellen, die für eine Vielzahl von Anwendungen nutzbar sind, um nicht viele verschiedene Arten von Tags und damit kleinere Stückzahlen zu haben.
Auch die von den Tags zurück gelieferte Datenmenge muss, wie oben beschrieben, möglichst konstant sein, damit Tags nicht darüber verfolgbar werden. Auch dies spricht für generische Tags oder zumindest für eine Standardisierung der Länge der Tagantworten.
Ein weiterer Grund für generische Tags besteht in der Transparenz für die Anwender: Die Vorstellung, in verschiedenen Produkten und Anwendungen grundverschiedene Tags zu verwenden, mag zwar aus technischer Sicht einfach handhabbar sein. Doch ist es einem Anwender nicht zuzumuten, den Überblick über verschiedene Tagarten zu behalten, die ihm einen unterschiedlichen Schutz für Daten und Privatsphäre bieten.

System- und Datensicherheit

Um die erforderliche Sicherheit gewährleisten zu können, müssen geeignete Mechanismen dazu implementiert werden. Es dürfen keine Daten im Klartext übermittelt werden, Tags und Backend müssen sich beidseitig authentifizieren, und ein Tag darf nicht einfach kopiert werden können, was durch Speicherung interner Zustandsdaten realisierbar ist.
Von Spezialanwendungen, in denen zentrale Datenbanken ein Risiko darstellen, abgesehen, sollten darüber hinaus Nutzdaten nur im Backend gespeichert werden, weil dort eine Zugriffskontrolle effektiver, flexibler und kostengünstiger realisierbar ist und die Kosten für die Tags geringer werden, weil weniger Speicher benötigt wird.

Default: Nicht verfolgbar

Ein Tag soll nur dann verfolgt werden können, wenn dies auch für die gegebene Anwendung erforderlich ist. Für einen Außenstehenden sollte die Tagantwort beim Auslesen zufällig und unvorhersagbar erscheinen und sich bei erneutem Auslesen so von der vorherigen unterscheiden, dass kein Zusammenhang erkennbar ist. Das kann mit Tag-Kennungen realisiert werden, die sich bei jedem Lesen ändern [18]. Andererseits muss es für legitime Anwendungen möglich sein, das Tag zu verfolgen.

Auch ein Henne-Ei-Problem ist zu lösen: Vor erfolgreicher Prüfung, dass eine Partei berechtigt ist, ein Tag auszulesen, darf sie nichts Verwertbares über das Tag erfahren. Andererseits muss für diese Berechtigungsprüfung bekannt sein, für was überhaupt eine Autorisierung erbeten wird.
Dies sind beides erstmal vollkommen widersprüchliche Anforderungen, die jedoch mit entsprechender Infrastruktur unter einen Hut gebracht werden können [14].

Einbindung Betroffener

Die meisten bisherigen Forschungsarbeiten betrachten nur die Tags und deren Eigentümer. Die eigentlichen Träger der Tags, deren Privatsphäre beispielsweise durch die Trackingmöglichkeit gefährdet ist, bleiben außen vor und müssen den Tag-Eigentümern vertrauen, dass die gewonnen Daten ausschließlich zweckgebunden verwendet werden. Ein derartiges Vertrauen ist jedoch unrealistisch: Ein Verbraucher möchte selbst bestimmen können und wissen, wem er wann wozu Informationen preisgibt. So fordern Verbraucherschützer "the right to know when, where and why the tags are being read“ [16] ein. Ziel muss es also sein, alle beteiligten Parteien in das System einzubinden und mehr Transparenz und gegenseitige Kontrollmöglichkeiten zu schaffen.

5 Zusammenfassung

Auf den vorherigen Seiten wurde ein Überblick über die Herausforderungen gegeben, denen sich die Forschung gegenübersieht, um Sicherheit und Schutz der Privatsphäre beim Einsatz der RFID-Technik zu gewährleisten. Die Auflistungen waren keineswegs umfassend und vollständig; Ziel war es lediglich, ein wenig Gespür für die Problematik zu vermitteln.
Einen Überblick und kurzen Vergleich über die vorgeschlagenen Verfahren zum Schutz der Privatsphäre, auf den aus Platzgründen in diesem Beitrag verzichtet werden musste, ist beispielsweise in [14] zu finden. Dort wird weiterhin ein offenes Framework vorgestellt, dass sich an den im vorherigen Abschnitt dargestellten Designkriterien orientiert und einen allgemeinen Lösungsansatz vorstellt.
Da aufgrund der Anwendungsvielfalt von künftiger Allgegenwärtigkeit der RFID-Systeme ausgegangen werden kann, der sich niemand mehr entziehen kann, ist es erforderlich, dass der Systemsicherheit, dem Datenschutz und dem Schutz der Privatsphäre bei der Anwendung der RFID-Technologie das notwendige Gewicht zukommt.

Literatur

[1] Lindquist, M.: RFID in libraries – introduction to the issues. World Library and Information Congress: 69th IFLA General Conference and Council, 2003
[2] E-ZPass, Web: http://www.ezpass.com, 2003
[3] EPCglobal Inc. Web: http://www.epcglobalinc.org, 2004
[4] EAN International, Web: http://www.ean-int.org, 2004
[5] Reisepass mit RFID-Chip; Heise, 2004; Web: http://www.heise.de/newsticker/meldung/45780
[6] McCullagh, D.: RFID tags: Big Brother in small packages. CNET, 2003, Web: http://news.com.com/2010-1069-980325.html, 2004
[7] Consumer Group Calls for Immediate Worldwide Boycott of Benetton. 2003, Web: http://www.boycottbenetton.org/PR_030313a.html, 2004
[8] Web: http://www.stoprfid.org/, 2004
[9] FoeBuD e.V., Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. Web: http://www.foebud.de, 2004
[10] Weingart, S.: Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. CHES 2000, Vol. 1965, Seiten 302-317, Springer LNCS, 2000
[11] Web: http://www.mobilecloak.com, 2004
[12] Juels, A. et al.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, 10th ACM Conference on Computer and Communications Security, 2003
[13] Electronic Privacy Information Center / Privacy International: Privacy and Human Rights 2003, An International Survey of Privacy Laws and Developments. epic.org, 2003
[14] Henrici, D. et al.: Sicherheit und Privatsphäre in RFID-Systemen, 18. DFN-Arbeitstagung, LNIC, Springer, 2004
[15] Weis, S.: Security and Privacy in Radio-Frequency Identification Devices. Massachusetts Institute of Technology, 2003
[16] Garfinkel, S.: An RFID Bill of Rights. Technology Review, 2002, Web: http://www.technologyreview.com/articles/garfinkel1002.asp, 2003
[17] Henrici, D. et al.: Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. PerSec'04 at IEEE PerCom, 2004
[18] Henrici, D.; Müller, P.: Tackling Security and Privacy Issues in Radio Frequency Identification Devices, 2nd International Conference on Pervasive Computing (Pervasive), 2004