

Sicherheit und Privatsphäre in RFID-Systemen: Ein Blick hinter die Kulissen

Dirk Henrici¹, Tino Fleuren², Paul Müller³

Kurzfassung:

Die RFID-Technologie erhält Einzug in immer mehr Anwendungsbereiche und wird künftig in unserem täglichen Leben ein ständiger Begleiter sein. Die wirtschaftliche Bedeutung der Technologie ist immens, doch sind die mit ihr verbundenen Probleme bezüglich Sicherheit und Schutz der Privatsphäre trotz intensiver Bemühungen noch nicht zufriedenstellend gelöst. Dies weckt Ängste in der Bevölkerung und führt zu Akzeptanzproblemen.

Die Herausforderung ist es, Lösungen zu finden, die einerseits die vielen sinnvollen Anwendungen der RFID-Technologie nicht behindern, andererseits den Menschen jedoch informationelle Selbstbestimmung ermöglichen.

Ziel dieses Beitrages ist es, einen interdisziplinär gehaltenen Überblick über den aktuellen Sachstand in der öffentlichen Diskussion, der Forschung und der praktischen Anwendungen zu geben.

Stichworte: RFID, Sicherheit, Privatsphäre, Diskussion

1. Einführung in Sicherheit und Schutz der Privatsphäre

RFID, i.e. „Radio-Frequency Identification“, ist eine Technologie zur berührungslosen Identifikation von Objekten. Im Gegensatz zu optischen Barcodes können RFID-Label, sogenannte „Transponder“ oder „Tags“, kontaktlos ausgelesen werden und über erweiterte Fähigkeiten verfügen. Die meisten Transponder vermögen zumindest eine weltweit eindeutige Seriennummer zu speichern. Teurere Exemplare haben noch mehr Speicher, zusätzliche Logik, einen Mikroprozessor und/oder Sensoren und integrieren damit die Funktionalität von Smartcards und Telemetriekomponenten (z.B. Transponder mit Temperatursensoren zur Überwachung von Kühlketten).

RFID-Systeme können die Produktivität von Warenwirtschaftsprozessen steigern, werden in Zeiterfassungs-, Abrechnungs- und Zutrittskontrollsystemen eingesetzt und dringen in eine Vielzahl weiterer Bereiche vor. Die RFID-Technologie wird als ein Wegbereiter hin zur Vision des „Internet der Dinge“ und des sogenannten „Pervasive Computing“ gesehen – Visionen einer Welt aus vernetzten Alltagsgegenständen. Das wirtschaftliche Potential der RFID-Technologie und die jährlichen Wachstumsraten

¹ Technische Universität Kaiserslautern

² Technische Universität Kaiserslautern

³ Technische Universität Kaiserslautern

sind enorm, sodass die RFID-Technologie erhebliche volkswirtschaftliche Bedeutung hat bzw. erlangt. Dass die RFID-Technologie dank der Vielzahl möglicher Anwendungen weiter Einzug in unseren Alltag erhalten wird, erscheint sicher und unabwendbar.

Die Technologie kann neben den vielen positiven (höhere Produktivität, mehr Komfort etc.) jedoch auch extrem negative Wirkungen haben. Verbraucherschützer und informierte Bürger stehen der RFID-Technologie daher auch mit Skepsis gegenüber. Die Möglichkeiten, wie etwa den Inhalt verschlossener Handtaschen im Vorbeigehen unbemerkt erfassen zu können oder gar Bewegungsprofile erstellen zu können, erfüllen viele Menschen mit Unbehagen. In der Presse ist teilweise gar reißerisch von „Schnüffelchips“ und „Überwachung von der Wiege bis zur Bahre“ die Rede. Vorschläge wie die Deaktivierung von RFID-Transpondern an der Kasse sind keine nachhaltige Lösung, da sie nicht universell einsetzbar sind (z.B. bei Leihbüchern in der Bibliothek) und auch sinnvolle Anwendungen nach dem Kauf (Warenrücknahmen, intelligentes Wohnen, „Ambient Intelligence“ usw.) verhindern. Auch rein legislative Lösungen oder freiwillige Selbstverpflichtungen, die nicht technisch verankert oder durch geeignete Anreizsysteme gestützt sind, bieten keine Lösung. Dies lässt sich mit einem Alltagsbeispiel belegen: Der Versand unerwünschter Emails („SPAM“) ist verboten, und dennoch sind unsere Postfächer voll davon, weil es weder technischen Schutz gibt, noch die Verursacher ermittelt werden können.

Neben dem Schutz der Privatsphäre ist auch die Thematik „Sicherheit“ wichtig. Störungen ihrer RFID-Systeme können Unternehmen beträchtlichen finanziellen Schaden sowie Imageverlust zufügen. Darüber hinaus ist auch Fälschungssicherheit von großer Bedeutung. So führen etwa Plagiate von Medikamenten nicht nur zu entgangenem Gewinn, sondern können eine Gefahr für Leib und Leben der Konsumenten darstellen. RFID-Technologie kann zur Lösung dieses Problems beitragen.

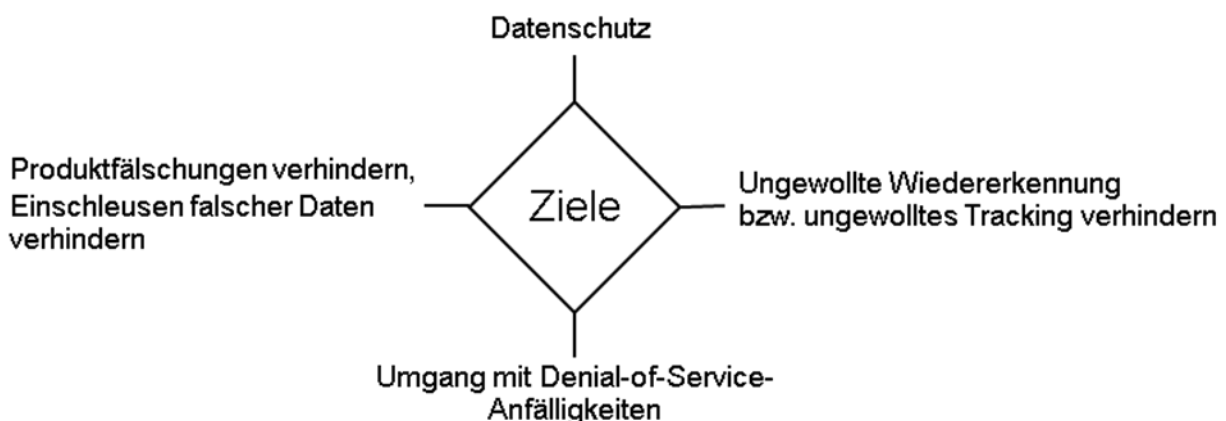


Abbildung 1: Übergeordnete Schutzziele

Aus der Vogelperspektive ergeben sich für Sicherheit und den Schutz der Privatsphäre die in Abbildung 1 dargestellten übergeordneten Schutzziele.

„*Datenschutz*“: Hier geht es darum, dass RFID-Systeme schützenswerte Daten speichern und verarbeiten. Diese Daten sollen vor dem Zugriff unberechtigter Dritter geschützt werden. Daten auf Transpondern müssen nicht unbedingt direkten Personenbezug haben, um datenschutzrechtlich relevant zu sein. Dadurch, dass Personen Transponder mit sich führen und damit einer jeweiligen Person zugeordnet werden können, können Daten leicht personenbeziehbar werden. Natürlich kann auch für nicht datenschutzrechtlich relevante Daten ein Schutzinteresse bestehen, z.B. bei Daten, deren Kenntnis Wettbewerbsvorteile verschafft (Industriespionage).

„*Produktfälschungen verhindern, Einschleusen falscher Daten verhindern*“: Durch den Einsatz von RFID-Tags sollen Produktfälschungen erschwert werden. Ideal wären RFID-Transponder, die nicht kopiert werden und ihre Echtheit nachweisen könnten. Außerdem gilt es zu vermeiden, dass Angreifer falsche Daten in ein RFID-System einspeisen können. So soll ein Angreifer nicht vorgeben können, ein RFID-Transponder sei an einem bestimmten Ort, obwohl er das gar nicht ist.

„*Umgang mit Denial-of-Service-Anfälligkeiten*“: Es ist mit einfachen Mitteln möglich, ein RFID-System zu stören. Beispielsweise können viele Arten von RFID-Transponder mit Aluminiumfolie abgeschirmt werden, sodass sie nicht mehr ausgelesen werden können. Derartiges kann in der Praxis kaum verhindert werden, doch sollte es zumindest die Möglichkeit geben, unerwünschtes Verhalten zu erkennen, um es danach sanktionieren zu können. Außerdem ist es wichtig, dass RFID-Lösungen keine zusätzlichen Angriffspunkte einführen.

„*Ungewollte Wiedererkennung bzw. ungewolltes Tracking verhindern*“: Zum Schutz der Privatsphäre soll verhindert werden, dass Personen oder Objekte ungewollt wiedererkannt oder verfolgt werden können. Hier gilt es, einen Zielkonflikt zu lösen: In Lieferketten ist es gewünscht, dass Objekte (z.B. Pakete) mit Hilfe von RFID-Transpondern erkannt und verfolgt werden können. Sobald Personen ins Spiel kommen, steht der Schutz der Privatsphäre im Vordergrund, und die betroffene Person soll selbst bestimmen können, ob sie wiedererkannt werden möchte oder nicht. Besonders relevant wird das Schutzziel, sobald RFID-Transponder und -Lesegeräte allgegenwärtig werden.

2. Die öffentliche Diskussion

In Politik, Verbänden, Presse und auch bei vielen Bürgern ist die RFID-Technologie in den letzten Jahren in die Diskussion gekommen. Auf der einen Seite stehen viele Vorteile, auf der anderen aber auch Bedenken oder gar Ängste. In Veröffentlichungen findet man viele Allgemeinplätze, Halbwahrheiten, einseitige Sichtweisen und leider nur selten sachliche, fundierte aber trotzdem verständliche Informationen.

Ein wesentlicher Grund dafür ist die Komplexität der Thematik. Zwar ist das Prinzip der RFID-Technologie an sich geradezu trivial, doch bei genauerer Betrachtung wird es schwer überschaubar. Einige Gründe dafür sind: 1) Die RFID-Technologie ist in der Güte ihrer Funktion von vielfältigen Umgebungseinflüssen abhängig. 2) Die

Technologie findet zusammen mit vielen anderen Technologien und informationstechnischen Systemen in unterschiedlichsten Lebensbereichen Anwendung. 3) RFID ist oftmals Teil eines komplexen Anwendungsszenarios oder einer Prozesskette. 4) Sicherheitseigenschaften sind ohne detaillierte informatische/mathematische Kenntnisse der verwendeten Algorithmen und möglicher Angriffstechniken in Funktion und Güte kaum zu überblicken. 5) Die Erklärung von Privatsphäreigenschaften fällt ohne psychologischen/soziologischen Hintergrund schwer. 6) Die korrekte Anwendung und Interpretation von Datenschutzbestimmungen erfordert juristische Kenntnisse.

Das Zusammenspiel und die Auswirkungen der RFID-Technologie sind hochgradig interdisziplinär und umspannen ein breites Spektrum von Wissenschaften. Hinzu kommt, dass es einen ständigen Wandel (technisch, gesellschaftlich,...) und damit Veränderungen gibt, währenddessen die RFID-Technologie mehr und mehr ubiquitär wird. Dementsprechend fällt eine Technologiefolgenabschätzung sehr schwer.

Gerade bezüglich der Punkte Sicherheit und Schutz der Privatsphäre gibt es noch einen weiteren Grund, warum die öffentliche Diskussion keinen gemeinsamen Nenner zu finden scheint: Es wird geredet, ohne sich darüber im Klaren zu sein, auf welcher Ebene gerade argumentiert wird und ohne eine gemeinsame Basis zu haben.

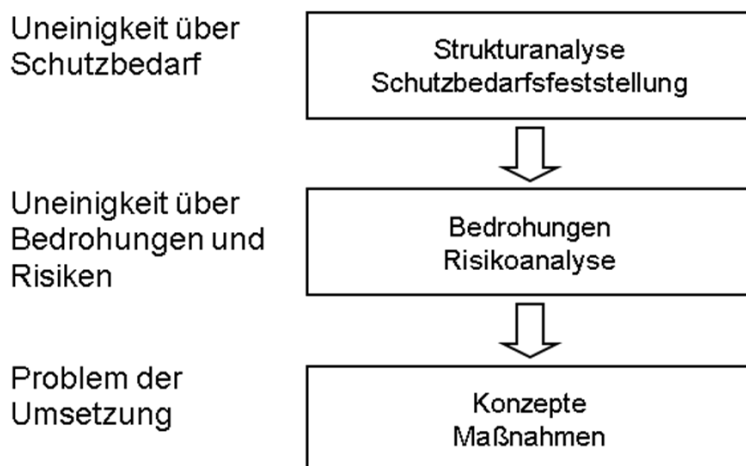


Abbildung 2: Erklärung der Uneinigkeit anhand einer Grafik aus den BSI-Grundschatzkatalogen [1]

Ein Beispiel dafür ist in Abbildung 2 dargestellt und wird im Folgenden anhand eines Beispiels erläutert. Es ist eine zurzeit heiß geführte Debatte, ob im Handel eine freiwillige Selbstverpflichtung als Schutzmaßnahme ausreicht (Deaktivierung der Transponder an der Kasse) oder ob gesetzliche Reglementierungen getroffen werden müssen. Hier wird über Verbraucherschutzmaßnahmen diskutiert, die die Privatsphäre schützen sollen. Aber was ist Privatsphäre überhaupt, was bedeutet sie für den Menschen? Wann ist sie geschützt, wann nicht? Inwiefern wird sie bedroht, von welchen Angreifern, Angriffstechniken, in welchen Szenarien/Kontexten, mit welchen Auswirkungen? Bezogen auf die in Abbildung 2 dargestellte Vorgehensweise besteht also sowohl über den Schutzbedarf als auch über Bedrohungen und das Risiko bei den

diskutierenden Parteien höchstens eine individuelle Ahnung, jedoch kaum eine fundierte Betrachtung, die allgemeinen Konsens findet. Dass dann letztendlich über die zu ergreifenden Maßnahmen Uneinigkeit herrscht, ist dann kaum noch verwunderlich.

Statt solider inhaltlicher Diskussion geht es somit oftmals eher darum, keinen Boden zu verlieren und eine strategisch günstige Ausgangsposition für die nächste Diskussionsrunde zu erhalten. Wirtschaftsvertreter fürchten, dass der Gesetzgeber den RFID-Einsatz reglementieren könnte oder Maßnahmen für den Datenschutz fordert, die zu merklich höheren Kosten führen würden. Daten- und Verbraucherschützer hingegen fordern einen besseren Schutz der Rechte der Bevölkerung und einen verantwortungsbewussten Umgang mit den Risiken der Technologie.

Die Diskussionen und Lobbyaktivitäten haben ein Ausmaß angenommen, das ein Finden eines allgemeinen Konsenses sehr unwahrscheinlich erscheinen lässt. Dabei sind die Standpunkte aus der Distanz betrachtet gar nicht so unvereinbar: Die „Wirtschaft“ heißt Datenschutz gut, solange er zu entsprechend erhöhter Akzeptanz der RFID-Technologie führt und letztendlich kostenneutral zu realisieren ist. Daten- und Verbraucherschützern ist auch nicht daran gelegen, die wirtschaftliche Entwicklung zu behindern und Kosten zu verursachen, die letztendlich wieder durch die Verbraucher getragen werden müssen. Es soll nur eine effektive Berücksichtigung der schutzwürdigen Interessen gegeben sein. Was also benötigt wird, sind kostenneutrale Maßnahmen zur Verbesserung des Datenschutzes.

Die bereits oben angesprochene Debatte, ob im Handel eine freiwillige Selbstverpflichtung als Schutzmaßnahme ausreicht oder gesetzliche Reglementierungen getroffen werden müssen, erscheint jedenfalls nicht zielführend und ihr Ausgang damit letztendlich für den Verbraucher nahezu unerheblich.

Problem ist, dass die Debatte (erst mal) nur den Handel betrifft, der Einsatz der RFID-Technologie an anderer Stelle, z.B. in Leihbüchern, Pässen usw., davon unberührt bleibt. Dort können RFID-Transponder beim Übergang in die Sphäre des Verbrauchers nicht deaktiviert werden, weil sie noch benötigt werden. Darüber hinaus ist eine Deaktivierung von Transpondern an der Kasse keine nachhaltige Lösung, weil die Transponder in Zukunft auch in anderen Lebensbereichen, etwa zu Hause, eine sinnvolle Verwendung finden werden.

Das Ausmaß der öffentlichen Diskussion ist verständlich, wenn man den zu erwartenden Einzug der RFID-Technologie in unterschiedlichste Lebensbereiche berücksichtigt. Vielfach werden jedoch nur Randaspekte betrachtet, statt die grundlegenden Probleme zu erfassen und Lösungen dafür zu suchen. Solange nicht geklärt ist, was wovor geschützt werden muss, darf man sich nicht wundern, dass kein Konsens über die umzusetzenden Maßnahmen erzielt werden kann. Eine Diskussion über allgemeine, anwendungsneutrale Schutzmaßnahmen, die dem Verbraucher konkreten und nachhaltigen Nutzen schaffen würden, geht im Zuge der mit dem Handel geführten Debatte „Selbstverpflichtung vs. gesetzliche Regelung“ leider unter.

3. Die wissenschaftliche Forschung

In diesem Abschnitt wird dargestellt, mit welchen Ansätzen üblicherweise versucht wird, die oben dargestellten Schutzziele zu erreichen. Basierend auf dieser Einführung wird ein kurzer, pauschalisierter Überblick über den bisherigen Forschungsstand auf dem Gebiet der RFID-Sicherheit gegeben. Detailliertere Informationen sind in [2] zu finden.

Grundlagen

Eine Vielzahl von Forschern beschäftigte sich in den letzten Jahren mit Verfahren für Sicherheit und Schutz der Privatsphäre in RFID-Systemen. Die meisten der vorgeschlagenen Lösungen implementieren das gleiche Grundkonzept, das im Folgenden vorgestellt wird.

Für RFID-Transponder werden üblicherweise drei Grundfunktionalitäten benötigt: Ein Transponder muss in der Lage sein, sich gegenüber berechtigten Lesern zu identifizieren, sich zu authentisieren und seinen Identifier regelmäßig zu modifizieren.

Die Identifikationsmöglichkeit ist die Basisfunktionalität von RFID-Systemen und wird daher in jedem Fall benötigt. Die einfachste Implementierungsmöglichkeit besteht darin, dass jeder Transponder dazu eine weltweit eindeutige Seriennummer/Identifier enthält.

Sich zu authentisieren bedeutet, dass ein Transponder seine Echtheit glaubhaft nachweist. Ziel ist es hier zu verhindern, dass Transponder einfach kopiert oder imitiert werden können und Angreifer falsche Daten in das RFID-System einspeisen können. Wie auch in anderen Bereichen der IT-Sicherheit wird das oft so gelöst, dass der sich ausweisende Kommunikationspartner unter Nutzung kryptographischer Primitiven nachweist, im Besitz eines Geheimnisses zu sein, ohne dieses Geheimnis dabei preiszugeben.

Ein häufig verfolgter Ansatz, um ungewollte Wiedererkennung und ungewolltes Tracking zu verhindern, ist es, die Transponder-Identifier regelmäßig zu ändern („modifizieren“), wobei nur berechtigte Parteien in der Lage sind, die Zuordnung zwischen einem bestimmten Transponder und seinem aktuellem Identifier herzustellen. Zum Erreichen des genannten Schutzzieles gibt es, insbesondere anwendungsspezifisch, aber auch noch weitere Ansätze wie die Einführung unterschiedlicher Transponder-Zustände.

Einfacher Ansatz: Anlehnung an Barcodesysteme

In RFID-Systemen werden Daten unter Verwendung elektromagnetischer Felder oder Wellen über die Luft ausgetauscht, d.h. ein Medium, das leicht abhörbar ist und auf das jeder Zugriff hat (siehe Abbildung 3). Daraus resultieren viele der Sicherheits- und Privatsphäreprobleme im Zusammenhang mit der RFID-Technologie. Der einfachste, direkte Ansatz ist es, den unsicheren Kommunikationskanal abzusichern.

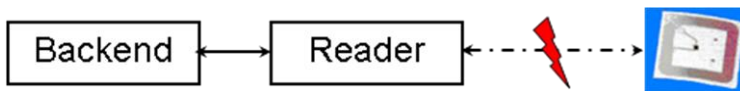


Abbildung 3: RFID-System mit angreifbarem Kommunikationskanal

Es wird folglich an geeigneten Kommunikationsprotokollen geforscht, die die Luftschnittstelle zwischen RFID-Transpondern und Lesegeräten absichern und die drei genannten Grundfunktionalitäten implementieren. Erste Protokolle wurden bereits im Jahr 2002 vorgeschlagen [3], doch auch noch in jüngerer Zeit werden derartige Kommunikationsprotokolle auf namhaften Konferenzen vorgestellt [4].

Es muss bei den Protokollen berücksichtigt werden, dass RFID-Transponder nur wenige Ressourcen verbrauchen dürfen, damit sie weiterhin kostengünstig in großen Stückzahlen herstellbar sind. Es wird daher versucht, die benötigte Funktionalität mit möglichst einfachen Primitiven zu implementieren. In der Praxis führt das oftmals dazu, dass im Bereich der Forschung symmetrische und asymmetrische Verschlüsselungsverfahren gemieden werden. Stattdessen wird die Funktionalität ausschließlich mit Einweg-Hashfunktionen implementiert.

Erweiterter Ansatz: Neue Architekturprinzipien

Der vorgestellte einfache Ansatz übernimmt die Architektur von Barcode-Systemen und ergänzt Maßnahmen zur Absicherung der Kommunikation. Der grundlegende Aufbau und die Datenpfade sind die gleichen. Leider vermag es dieser Ansatz bzw. die klassische Barcodearchitektur konzeptionell nicht, alle Anforderungen an gute Lösungen (Sicherheit und Privatsphäre, Ressourcenbedarf, Performanz, Skalierbarkeit, Verfügbarkeit, Benutzerfreundlichkeit, Nachhaltigkeit, Allgemeinheit, Dimension, Praktikabilität; siehe [5] zur Erläuterung) gleichzeitig zu erfüllen. Hier muss zum Beispiel auch berücksichtigt werden, dass die RFID-Technologie in naher Zukunft in eine Vielzahl von Lebensbereichen Einzug finden werden. Durch die Ubiquität von Transpondern und Lesegeräten steigen die Anforderungen.

Die bisherige Architektur fokussiert etwa hinsichtlich Sicherheit auf die Absicherung der Kommunikation zwischen Transpondern und Lesegeräten. Dabei wird jedoch wichtigen praktischen Anforderungen nur ungenügend Rechnung getragen. Die Anforderungen und Defizite werden in den folgenden Abschnitten erläutert.

Ein erster Punkt ist, dass Systeme benötigt werden, die firmen- und organisationsübergreifend arbeiten können. Das globale Wirtschaften benötigt Systeme von hoher Skalierbarkeit, die auch in globalem Maßstab einsetzbar sind. Es muss möglich sein, Zugriffs- und Leserechte an Zulieferer und Unterauftragsnehmer zu delegieren. Darüber hinaus wird ein firmenübergreifender Datenaustausch benötigt. Diese Anforderungen stehen im Widerspruch zum Schutz der Privatsphäre, der eine regelmäßige Änderung der Transponder-Identifizier erfordert, um ein unerwünschtes Wiedererkennen zu verhindern. Reine Erweiterungen und Ergänzungen, wie die Absicherung der Kommunikation, bieten keine zufriedenstellende Lösung.

Ein zweiter Punkt ist, dass in der bisherigen Architektur bezüglich Sicherheit und Privatsphäre nur die Interessen der Eigentümer der RFID-Transponder (üblicherweise die ausgebende Stelle, z.B. Bibliothek, Verkehrsbetrieb, Arbeitgeber, Staat etc.) in technischer Hinsicht berücksichtigt werden. Bezüglich der Privatsphäre- und Datenschutzprobleme sind jedoch in der Regel die Personen betroffen, die die Transponder mit sich führen (Bibliotheksbenutzer, Fahrgäste, Arbeitnehmer, Bürger etc.). Deren Interessen werden in der bisherigen Architektur nicht berücksichtigt.

Ein dritter Punkt ist, dass sich viele Forschungsarbeiten auf technische Schutzmaßnahmen versteifen und die nicht-technischen Randbedingungen zu wenig berücksichtigen. Technische Maßnahmen sind jedoch nur als eine Säule zu sehen und müssen im wirtschaftlichen, legislativen und sozialen Kontext betrachtet werden.

Unter anderem aus den genannten Gründen bedarf eine umfassend zufriedenstellende Lösung einer neuen Architektur, die sich vom Ansatz her in einigen wesentlichen Punkten von der jetzigen, wie sie von Barcode-Systemen direkt übernommen ist, unterscheidet. Auch derartige neue Architekturkonzepte sind Forschungsgegenstand. Eine ausführlichere Motivation und ein möglicher Ansatz finden sich in [2].

4. Die Praxis

Im vorherigen Abschnitt wurde gezeigt, dass sich die Forschung in den letzten Jahren dem Thema „Sicherheit und Schutz der Privatsphäre“ angenommen hat. Praktikable, standardisierte Lösungen sind allerdings in nächster Zeit nicht zu erwarten, insbesondere auch, weil – wie im zweiten Abschnitt dargestellt – in der öffentlichen Diskussion derartige Lösungen nicht vehement eingefordert werden.

Wie sollte nun jemand, der ein RFID-System implementieren soll oder die Sicherheit eines Systems einschätzen möchte, praktisch mit der Thematik umgehen? Diese Frage ist gar nicht so einfach zu beantworten. Daher hat sich beispielsweise das BSI mit den „Technischen Richtlinien für den sicheren RFID-Einsatz“ [6] vorgenommen, zumindest für einige Anwendungsbereiche, z.B. eTicketing, Empfehlungen zu geben. In den folgenden Abschnitten werden einige allgemeine Punkte diskutiert, bezüglich derer es häufig zu Missverständnissen kommt oder bei denen „alte“ Fehler in der Praxis leider regelmäßig wiederholt werden.

Meiden von „Security by obscurity“

Informiert man sich regelmäßig zu die Sicherheit betreffenden Themen, so hört man immer wieder von Produkten, bei denen Sicherheit zumindest teilweise auf der Geheimhaltung der Arbeitsweise beruht. Beispiele dazu finden sich in unterschiedlichsten Bereichen. Zu den weithin bekannt gewordenen Beispielen gehören die Verarbeitung von PINs bei Geldautomaten, unsichere mathematische Algorithmen bei Wegfahrsperrern oder in jüngerer Zeit das Brechen der proprietären Verschlüsselung der weit verbreiteten „Mifare Classic“.

Basiert die Sicherheit eines Systems auf der Geheimhaltung seiner Funktionsweise, sogenannte „security by obscurity“, erweisen sich die Systeme oftmals als unsicher. Dies hat bereits im 19. Jahrhundert Auguste Kerckhoffs erkannt und formuliert, dass die Sicherheit eines kryptographischen Systems auf der Geheimhaltung des Schlüssels beruhen sollte und nicht auf der Geheimhaltung des Algorithmus. Dies ist in der modernen Kryptographie als das „Kerckhoffs'sche Prinzip“ bekannt und weithin anerkannt.

Neben der in der Praxis gemachten Erfahrung, z.B. dass sich viele nicht offen gelegte Verfahren als schwach erweisen, gibt es viele weitere Argumente, das Kerckhoffs'sche Prinzip zu beachten. So ist es schwieriger, einen Algorithmus geheim zu halten als einen Schlüssel, und es ist schwieriger, einen kompromittierten Algorithmus auszutauschen als einen kompromittierten Schlüssel. Daneben gibt es noch die qualitativen Aspekte, dass Fehler in offen gelegten Algorithmen im Allgemeinen schneller entdeckt werden als in geheim gehaltenen, und dass Hersteller, die die genutzten Verfahren nicht offenlegen, leichter Hintertüren in ihre Produkte einbauen können.

Trotz der Bekanntheit des Problems und der vielen Negativbeispiele wird immer wieder der Fehler wiederholt, das Nicht-Offenlegen technischer Abläufe und Verfahren als Mittel zur Erlangung von Sicherheit anzusehen. Dabei kann Geheimhaltung von Verfahren allerhöchstens eine zusätzliche Maßnahme sein.

Handlungsempfehlung: Anbieter, die bezüglich Sicherheit auf die Geheimhaltung der verwendeten Algorithmen und der genutzten Abläufe setzen, sollte man meiden bzw. sich zumindest im Klaren sein, dass das jeweilige Produkt nicht längere Zeit als sicher angesehen werden kann.

Tatsächliche Sicherheit versus Marketing

Im Marketing werden häufig die positiven Eigenschaften eines Angebotes hervorgehoben und negative Eigenschaften verschwiegen. Es setzt einen fundiert informierten Kunden oder Verbraucher voraus, zu beurteilen, wie die Charakteristika objektiv einzuschätzen sind. Bezüglich Sicherheit ist es oftmals so, dass nicht die technisch beste/sicherste Lösung die sinnvollste ist, sondern eine, die bei möglichst geringen Kosten das für den konkreten Anwendungsfall benötigte Maß an Sicherheit gewährleisten kann. Sowohl dieses benötigte Maß an Sicherheit als auch die Sicherheit, die ein gegebenes Produkt/Verfahren zu bieten vermag, werden in der Praxis leider häufig falsch eingeschätzt – unter anderem bedingt durch Marketing.

Ein Beispiel hierzu ist die Erhöhung von Fälschungssicherheit unter Zuhilfenahme von RFID-Transpondern. Anwendungen finden sich etwa bei Zutrittskontrollsystemen und der Eindämmung von Produktpiraterie. Problem ist hier, dass einfache Transponder sehr leicht kopierbar oder zumindest imitierbar sind. Die dazu notwendigen Bausteine sind für einen zweistelligen Eurobetrag in jedem Elektronikladen zu beziehen. Selbst implantierbare Transponder, die zur Zutrittskontrolle für Sicherheitsbereiche eingesetzt werden und sowohl vom Marketing als auch von den vorgeschlagenen Einsatzgebieten

her eine hohe Sicherheit suggerieren, bewegen sich auf diesem erschreckend niedrigen Sicherheitsniveau. Für den Einsatz in der Logistik promotet GS1 das sogenannte „Track & Trace“. Hier ist das Ziel, Schutz gegen Produktfälschungen zu erreichen. Zwar sind sowohl Barcodes und auch handelsübliche RFID-Transponder leicht kopierbar oder zumindest imitierbar, doch kann man durch Führen einer Produkthistorie entlang der Lieferkette Plausibilitätstests durchführen, die Produktfälschungen entlarven können. Die Barcodes/RFIDs müssen dazu nur eindeutige, nicht erratbare Seriennummern besitzen, damit das jeweilige Produkt eindeutig identifiziert werden kann und ein Angreifer gültige Nummern nicht erraten kann. Der Erfolg dieses Ansatzes setzt jedoch eine im Idealfall lückenlose Überwachung der Lieferkette voraus, d.h. die Verwendung von Lesegeräten bei allen Akteuren und das Zusammenführen der Daten zentral zu einer Produkthistorie. Diese Voraussetzung macht in vielerlei Hinsicht Probleme, angefangen bei der Standardisierung des Datenaustauschs bis hin zu den Interessen der Beteiligten, die evtl. ihre Lieferketten nicht offen legen möchten. Die sicherste Möglichkeit, Schutz vor Fälschungen zu erreichen und die genannten Probleme zu vermeiden, ist es, die RFIDs mit Zusatzfunktionalität auszustatten, die dafür sorgt, dass RFIDs nicht mehr auf einfache Weise kopiert werden können. Grundidee ist, dass jeder RFID-Transponder einen Transponder-spezifischen geheimen Schlüssel in sich trägt. Kann der Transponder nachweisen, dass er im Besitz des korrekten Schlüssels ist, so sind der Transponder und damit das Produkt echt. Bei diesem Nachweis wird der Schlüssel nicht preisgegeben, damit ein Kopieren nicht ermöglicht wird. Es gibt unterschiedlichste Möglichkeiten, diesen Nachweis zu führen. Je nach Anwendung muss der passende Kompromiss zwischen Sicherheit und Aufwand gefunden werden.

Ein anderes Beispiel für die Wahrnehmung von Sicherheit ist die Reichweite von Lesegeräten. Die erzielbare Reichweite ist von vielen Faktoren abhängig, insbesondere davon, welche Frequenzen verwendet werden und wie die Transponder mit Energie versorgt werden. Aber auch eine Vielzahl von Umgebungseinflüssen, wie etwa die Ausrichtung der Transponder zum Lesegerät, spielt eine Rolle. In der Wahrnehmung von Sicherheit wird die praktisch gegebene Reichweite als Sicherheitsmaßstab angesehen und durch Marketing und Lobbyisten bekräftigt: „Probieren Sie es selbst, es funktioniert nur aus bis zu 10cm Entfernung“. Im Gegensatz dazu wird in einigen Veröffentlichungen von Reichweiten von hunderten von Metern berichtet, teilweise ohne auf die Einschränkungen und praktische Bedeutung einzugehen. Die Wahrheit liegt, wie so oft, auch hier irgendwo in der Mitte: Zum einen muss man technische und physikalische Limits unterscheiden, zum anderen Standardlesegeräte im Unterschied zu speziellen Lesegeräten. Drittens ist jeweils die Frage, worauf sich die Reichweitenangabe bezieht. In jedem Fall ist die Kommunikationsrichtung ein ausschlaggebender Faktor. Bei passiven Transpondern kommt es noch auf die Energiequelle an, d.h. ob das genutzte Lesegerät einen Transponder auch mit Energie versorgen muss oder nur die Kommunikation zwischen anderen Kommunikationspartnern belauscht wird. Eine interessante Veröffentlichung, die einen erahnen lässt, was technisch mit einigen Kniffen möglich ist, ist [7]. Dort geht es um die technische

Umsetzung eines sog. „Relay-Angriffs“. Dieser Angriff zeigt, dass die grundsätzliche und naheliegende Annahme, dass räumliche Nähe die Kommunikationspartner ausweist, falsch ist. Die Möglichkeit derartiger Angriffe mag für bestimmte Anwendungsszenarien in Kauf genommen werden können, in anderen, z.B. Bezahlssystemen, sollten bekannte Möglichkeiten der Abwehr (Latenzmessungen) Anwendung finden.

Handlungsempfehlung: Marketingversprechen bezüglich Sicherheit sollten stets kritisch hinterfragt werden. Nichts ist 100%ig sicher. Man muss sich im Klaren sein, welche Sicherheit ein Produkt/Verfahren bietet und welche nicht und darauf basierend für den gegebenen Anwendungsfall eine geeignete Wahl treffen.

Die „einfachen Dinge“: Nutzen technischer Gestaltungsspielräume

Im Abschnitt zur Forschung wurde eine Reihe von Entwicklungstendenzen in der Forschung dargestellt. Derartige Ansätze funktionieren zwar, doch werden die Anstrengungen in der Praxis durch unüberlegte Designentscheidungen oder das Begehen „alter Fehler“ wieder zunichte gemacht.

Obwohl in jedem Anfängerprogrammierkurs gepredigt wird, alle Eingaben zu prüfen, wurde die Möglichkeit von Buffer-Overflow-Angriffen mit RFID-Transpondern als Datenquelle nachgewiesen. In der Presse war reißerisch von „RFID-Viren“ die Rede. Derartige Lücken wären mit einer oder wenigen Zeilen Programmcode effektiv zu schließen und würden auch die Zuverlässigkeit des Systems beim Auftreten zufälliger Fehler erhöhen.

Nur mit großem Aufwand zu beheben und daher möglichst schon im Vorhinein zu vermeiden, ist hingegen ein schlechtes Design der Systemarchitektur. Technische Gestaltungsspielräume sollten so genutzt werden, dass ein optimales Ergebnis entsteht.

Ein Beispiel hierfür stellt die Datenspeicherung in RFID-Systemen dar. Grundsätzlich gibt es zwei mögliche Speicherorte für zu einem Objekt gehörige Daten: Den Transponder selbst und Datenbanken im Hintergrund, d.h. Datenspeicherung im sogenannten Backend.

Welche Daten wo gespeichert werden, stellt einen Gestaltungsspielraum für die technische Implementierung dar. Bezüglich der Anwendungsmöglichkeiten ist der Speicherort inzwischen praktisch unerheblich, die Wahl schränkt die Möglichkeiten nicht ein. Jedoch ergeben sich grundlegende Unterschiede, die sich auf Randbedingungen wie Kosten, Flexibilität und Datenschutz auswirken.

Bei optischen Barcodes hatte man vielfach kaum eine Wahl, da die Speicherkapazität bei eindimensionalen Codes sehr begrenzt ist. So umfasst der bekannte EAN-Code (European Article Number) nur 13 Ziffern. Dies reicht nicht aus, um Waren eindeutig zu identifizieren oder gar noch weitere Daten zu hinterlegen, sodass dieser Code nur jeweils eine Kennung für den Hersteller und das Produkt enthält. Alle weiteren Daten müssen somit im Backend gespeichert werden. Mit dem höheren Speichervermögen

von RFID-Transpondern (kostenabhängig), entsteht eine Wahlmöglichkeit, da auch direkt auf Transpondern Daten abgelegt werden können.

Es gibt unterschiedliche Ausgestaltungen, die Auswirkungen auf praxisrelevante Kriterien wie Lesegeschwindigkeit, Fehlerrate, Flexibilität, allgemeine Sicherheit, Datensicherheit, Schutz der Privatsphäre und Kosten haben. Trotz dieser vielschichtigen Auswirkungen, wird die Entscheidung, welche Daten wo gespeichert werden, vielfach nur an einzelnen Kriterien getroffen und die anderen Auswirkungen übersehen. Eine ausführliche Vorstellung der technischen Möglichkeiten mit Diskussion und Bewertung findet sich in [8].

Es liegt gedanklich nahe, Produktbeschreibungen direkt auf den Tags am Objekt zu speichern. Insbesondere in der Fertigung wird diese Möglichkeit als Innovation angepriesen und damit versucht, einen Markt zu schaffen. Mit der steigenden Vernetzung, die ebenfalls mehr und mehr zum Standard wird, greifen jedoch viele der Argumente für diese Lösung nicht mehr. Die Informatik ist schon einige Schritte weiter und fordert im „Pervasive Computing“ und „Internet der Dinge“ Vernetzung und Flexibilität. Insgesamt kann Entscheidern und Entwicklern für die meisten Anwendungsfälle die Empfehlung gegeben werden, RFID-Systeme dergestalt zu fordern und zu entwickeln, dass nur eine minimale Datenmenge direkt auf den Transpondern gespeichert wird. Die Begründung dieser Empfehlung ist ebenfalls in [8] dargestellt.

Handlungsempfehlung: Es bringt nichts, sich über komplexe kryptographische Ansätze Gedanken zu machen, solange selbst einfachste Dinge nicht berücksichtigt werden. „Alte Fehler“ werden wiederholt, statt dass aus Fehlern gelernt wird. Technische Gestaltungsspielräume sollten genutzt werden. Schon kleine Änderungen am Design können beträchtliche Auswirkungen auf die Charakteristika des Systems haben.

5. Zusammenfassung

Die RFID-Technologie wird aller Voraussicht nach in absehbarer Zukunft aus unserem Alltag nicht mehr wegzudenken sein. Zu vielfältig sind die Anwendungsmöglichkeiten, die u.a. die Produktivität steigern. Die Interessen des Menschen sollten dabei jedoch besondere Berücksichtigung finden, da es für niemanden mehr möglich sein wird, sich der Technologie zu entziehen.

Zurzeit wird intensiv diskutiert, wie die schutzwürdigen Interessen der Menschen berücksichtigt werden können. Etwa die Frage, ob im Handel eine freiwillige Selbstverpflichtung ausreichend ist oder gesetzliche Regelungen erforderlich sind, wird in die Medien thematisiert. In diesem Beitrag wurde hinterfragt, was in der öffentlichen Diskussion vor sich geht und wie es zu bewerten ist.

Ziel der Forschung ist es, Konzepte und Verfahren zu entwerfen, die es ermöglichen, Sicherheit und Schutz der Privatsphäre in RFID-Systemen zu gewährleisten. Es wurde im Beitrag vorgestellt, woran geforscht wird und inwieweit es heute Lösungen für die vielfältigen Probleme gibt. Ausgehend von der vorherrschenden Forschungsrichtung

wurde aufgezeigt, welche praktischen Herausforderungen in der heutigen Forschung noch Berücksichtigung finden müssen.

Im dritten Teil wurde besprochen, was sich für die Praxis ableiten lässt. Es wurde anhand einiger Beispiele aufgezeigt, in welche Richtung sich orientiert werden sollte und welche grundlegenden Fehler es zu vermeiden gilt.

Literaturhinweise

- [1] BSI: IT-Grundschutz-Kataloge; BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise; 2005/2008; online verfügbar unter <http://www.bsi.bund.de/gshb/>
- [2] Dirk Henrici: RFID Security and Privacy - Concepts, Protocols and Architectures; Lecture Notes in Electrical Engineering, Nr. 17; Springer-Verlag; 2008; ISBN 978-3-540-79075-4
- [3] Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels: RFID Systems and Security and Privacy Implications; Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science, Nr. 2523, S. 454-469, Springer-Verlag; 2002
- [4] Dirk Henrici, Paul Müller: Providing Security and Privacy in RFID Systems Using Triggered Hash Chains; Sixth Annual IEEE International Conference on Pervasive Computing and Communications, PerCom 2008; Kowloon, Hongkong, China; 2008
- [5] Vedran Kordic (ed.): Development and Implementation of RFID Technology; Dirk Henrici, Aneta Kabzeva, Paul Müller: RFID System Architecture Reconsidered; I-Tech Education and Publishing, Wien; to appear 2009
- [6] BSI: Technische Richtlinie für den sicheren RFID-Einsatz (TR RFID, TR 03126); online verfügbar unter <http://www.bsi.bund.de/literat/tr/tr03126/>
- [7] Ziv Kfir, Avishai Wool: Picking virtual pockets using relay attacks on contactless smartcard systems, Proceedings of SecureComm 2005, IEEE, 2005
- [8] Dirk Henrici, Tino Fleuren: RFID-Technologie: Verbesserung des Datenschutzes durch Nutzung des technischen Gestaltungsspielraums; 16. DFN-Workshop "Sicherheit in vernetzten Systemen"; to appear 2009