Kleine Chips mit großer Wirkung – Über die Akzeptanzprobleme der RFID-Technologie

Matthias Handy, Dirk Timmermann

Institut für Angewandte Mikroelektronik und Datentechnik
Universität Rostock
matthias.handy@etechnik.uni-rostock.de

Die RFID-Technologie (Radio Frequency Identification) setzt an zum Sprung eine Massentechnologie zu werden. Doch bei vielen der angestrebten Anwendungen regt sich öffentlicher Widerstand. Besonders die kurz bevorstehende Einführung elektronischer Produktkennzeichnung mittels RFID-Technologie ruft Verbraucherschützer auf den Plan. Diese Arbeit gibt einen Überblick des Standes bei der Einführung der RFID-Technologie in Bereiche des täglichen Lebens und geht dabei insbesondere auf die elektronische Produktkennzeichnung ein. Überdies werden Ursachen der Akzeptanzprobleme genannt sowie Bestrebungen angeführt, die RFID-Technologie sicherer zu machen.

Einleitung

Am 28. Februar 2004 erregte eine kleine Demonstration im nordrhein-westfälischen Rheinberg weltweites Aufsehen. Obgleich die – zumindest deutschlandweit – erste Demonstration gegen die flächendeckende Einführung der RFID-Technologie im Einzelhandel lediglich eine kleine Schar von empörten Bürgern und Bürgerrechtlern zusammenbrachte, war die Botschaft unmißverständlich und löste ein (mit Bezug auf die Teilnehmerzahl) überproportional großes Presseecho aus [1].

Im April 2003 eröffnete Metro in eben diesem Rheinberg den „Extra Future Store“, der einen Ausblick auf die Zukunft des Einkaufens ermöglichen soll [2]. Verschiedene Artikel im Future Store sind mit RFID-Marken versehen. An jeden Einkaufswagen kann ein so genannter PSA, ein Personal Shopping Assistant, geklemmt werden, der unter anderem ein RFID-Lesegerät und ein tastsensitives Display enthält. Führt ein Kunde, bevor er einen funk-etikettierten Artikel in den Einkaufswagen legt, diesen in die Nähe des PSA, so registriert das integrierte Lesegerät Artikel, Menge und Preis. An der Kasse, so die Vorstellung der Future-Store-Betreiber, braucht der Kunde seine Einkäufe nicht mehr auf ein Transportband zu legen. Die Artikeldaten des PSA werden automatisch ausgelesen. Auch Kundenkarten, die im Future Store verteilt werden, enthalten RFID-Marken. Damit kann jeder Kunde bereits am Eingang des Supermarktes identifiziert werden. Für Marketing-Experten wird somit der Traum von der perfekt personalisierten Werbung Wirklichkeit.

In anderen Branchen werden RFID-Systeme bereits eingesetzt. In einigen Großwäschereien wird in jedes Wäschestück eine münzgroße RFID-Marke eingenäht, mit der

es sich genau einem Kunden zuordnen läßt [3]. Die Marke liefert dabei auf Anfrage lediglich eine Identifikationsnummer zurück, die über eine Datenbank mit einer Person verknüpft werden kann. Mehrere Fluggesellschaften erwägen den Einsatz von RFID-Systemen bei der Gepäckabfertigung [4]. Auch bei der Fußball-WM 2006 in Deutschland sollen RFID-Systeme zum Einsatz kommen [5]. So ist geplant, jede Eintrittskarte mit einer RFID-Marke zu versehen, womit zum einen die Fälschungssicherheit der Tickets erhöht, zum anderen eine einfache Zugangskontrolle zu den Stadien ermöglicht wird. Überdies verspricht man sich von den personalisierten Eintrittskarten eine Eindämmung der Hooligan-Problematik.

Daß eine Vision einer Welt des Ubiquitous Computing inklusive RFID-Systemen als ihre Vorboten nicht nur positive Reaktionen auslöst, läßt sich an den Verlautbarungen verschiedener gesellschaftlicher Gruppen auf die geplante Ablösung von Strichcodes durch RFID-Marken bei der Kennzeichnung von Konsumgütern ablesen [6],[7]. Bei der Verleihung der BigBrother-Awards 2003 – einer Art Pranger für Institutionen und Unternehmen, die private Datenschutzbelange nur unzureichend berücksichtigen – ging einer der Preise an die Metro-Gruppe und ihren Rheinberger Future Store [8].

Grundlegendes

RFID-Systeme

Ein RFID-System besteht in seiner einfachsten Form aus einem Lesegerät und aktiven bzw. passiven Transpondern (RFID-Marken) [9]. RFID-Lesegeräte setzen sich aus einer Steuerungseinheit und einer Hochfrequenzeinheit zusammen. Die Steuerungseinheit koordiniert und überwacht den Kommunikationsablauf mit dem Transponder, ist für die Signalcodierung und -decodierung verantwortlich und kommuniziert bei Bedarf mit einer Applikationssoftware auf einem angeschlossenen PC. Überdies wird die Steuerungseinheit zur Durchführung von Sicherheits- und Antikollisionsverfahren verwendet. Die Hochfrequenzeinheit erzeugt die Trägerfrequenz und übernimmt die Aufgabe der Modulation bzw. Demodulation.

Eine passive RFID-Marke besteht üblicherweise aus einem Mikrochip (RFID-Chip) und einem Koppelelement (Antennenspule und Kondensator). Die erforderliche Energie wird dem magnetischen Wechselfeld des Lesegerätes entzogen. Handelsübliche passive Transponder in Etikettenform sind zum Beispiel die von Texas Instruments angebotenen Tag-it HF-I Inlays [10] oder die I-Code-SLI-Familie [11] von Philips. Bei diesen auch als Smart Labels bezeichneten RFID-Marken sind Koppelelement und Mikrochip (RFID-Chip) auf einer PET-Folie aufgebracht. Die Firma Hitachi stellte im Jahr 2001 einen extrem kleinen RFID-Chip mit einer Kantenlänge von 0.4 mm vor [12]. Der nicht wieder beschreibbare µ-chip versendet auf Anfrage eine 128-bit lange Identifikation und erreicht mit einer externen Antenne eine Reichweite von maximal 30 cm. Eine neuere Version des µ-chip integriert die Antenne bereits auf dem Chip [13]. Der µ-chip ist auf Grund seiner geringen Ausmaße dafür geeignet, in besonders kleine oder hauchdünne Objekte wie Papier oder Banknoten integriert zu werden.

Elektronische Produktkennzeichnung

Weltweit federführend bei der Entwicklung RFID-basierter Produktkennzeichnung ist EPCglobal, ein Gemeinschaftsunternehmen der europäischen EAN international und des US-amerikanischen Uniform Code Council (UCC) [14]. EPCglobal soll einen weltweiten Standard zur Produktkennzeichnung per RFID entwickeln. Kern dieser Produktkennzeichnung ist der Elektronische Produkt-Code (EPC), eine weltweit eindeutige Nummer, die einem Produkt zugewiesen wird und anhand derer es auf der gesamten Versorgungskette identifizierbar ist. Der EPC ist auf einem RFID-Chip gespeichert und kann von kompatiblen Lesegeräten ausgelesen werden. Der EPC ist eingebettet in das so genannte EPCglobal Network, einer Sammelbezeichnung für verschiedene Technologien, die mit der elektronischen Produktkennzeichnung verbunden sind (EPC tags, Lesegeräte, Object Name Service (ONS), Physical Markup Language (PML), Savant). Der Object Name Service gibt Auskunft darüber, wo Informationen zu dem entsprechenden Produktcode zu finden sind. Die Physical Markup Language ist eine standardisierte Form zur Beschreibung von Produktinformationen. Savant verwaltet und transportiert sämtliche Informationen des Systems. Aktuell ist die Version 1 der EPC-Spezifikation verfügbar [15].

Was Daten- und Verbraucherschützer befürchten

Daten- und Verbraucherschützer sehen in der RFID-Technik vor allem eine Gefahr für die Privatsphäre und beschwören das Zukunftsbild einer nahezu perfekten Überwachung [16]:

„Marion Z. bekommt einen Bußgeldbescheid der Stadt Duisburg. Das Papier eines von ihr gekauften Mars-Riegels wurde im Ententeich des Stadtparks gefunden. Marion Z. grübelt und kommt darauf, daß sie den Riegel einem Kind beim Martins-Singen geschenkt hat. Zähneknirschend zahlt sie 10 Euro Bußgeld."

Der oben angeführte Textausschnitt beschreibt zwar keine Gefahr, die speziell von der RFID-Technologie allein und ihren physikalischen Eigenschaften ausgeht, er adressiert jedoch die Hauptanliegen bei der Einführung der elektronischen Produktkennzeichnung. So soll nach Bekunden des EPCglobal-Konsortiums jeder Artikel in einem Kaufhaus eine weltweit eindeutige Seriennummer erhalten. Diese Nummer soll bereits bei der Herstellung verwendet werden und den Artikel auf seinem Weg entlang der Versorgungskette eindeutig identifizieren. Die heute verwendete Strichcode-Kennzeichnung kann dagegen lediglich eine Artikelklasse identifizieren. Jede Dose Cola eines Herstellers trägt den gleichen Strichcode. Daher wird die elektronische Produktkennzeichnung per RFID auch mit dem Begriff *„item-level tagging"* belegt, womit die Möglichkeit der weltweit eindeutigen Identifizierung (genau *einer* Dose Cola) ausgedrückt werden soll.

Heutige Strichcodes können nur bei Sichtkontakt zwischen Lesegerät und Marke ausgelesen werden. Das spezielle Ausbreitungsverhalten von Funkwellen ermöglicht bei RFID-Marken dagegen auch ein Auslesen oder Beschreiben ohne Sichtkontakt.

Diese Tatsache begünstigt ein unbemerktes Auslesen von RFID-Marken, etwa bei Waren in einer Einkaufstasche. Der Verbraucher verliert damit die Kontrolle über Ort und Zeitpunkt des Auslesens der von ihm getragenen RFID-Marken.

Kombiniert man die Eigenschaft der weltweit eindeutigen Identifizierung mit der des unbemerkten Auslesens der RFID-Marken, so zeichnet sich ein weiteres Bedrohungsbild ab. Sobald die Möglichkeit besteht, die Ausleseinformationen mehrerer Lesegeräte zentral auszuwerten, lassen sich Bewegungsprofile von Personen erstellen. Angenommen Herr X kauft in einer Filiale eines Warenhauses in Rostock einen Anzug, der mit einer RFID-Marke und einer eindeutigen Seriennummer versehen ist. Betritt Herr X mit diesem Anzug zwei Tage später eine Filiale derselben Handelskette in Hamburg, so registrieren die Lesegeräte den gekennzeichneten Anzug (und zwar genau diesen einen) und können so ein grobes Bewegungsprofil von Herrn X konstruieren (auch wenn sie die wahre Identität des Herrn X nicht kennen). Hier kann der Einwand geltend gemacht werden, daß eine derartige Profilerstellung nur möglich ist, wenn die Betreiber von RFID-Lesegeräten kooperieren und ihre Daten abgleichen. Nichts anderes geschieht jedoch schon heute bei Bonuspunkte-Systemen: mehrere Einzelhandelsunternehmen erstellen eine zentrale Datenbank der Kaufgewohnheiten ihrer Kunden. Werden überdies auch Kunden- oder Kreditkarten mit RFID-Marken versehen, so läßt sich zu einem Bewegungsprofil auch eine Person zuordnen.

Verbraucherschützer fordern deshalb eine Kontrolle der Aktivitäten rund um die Einführung von RFID-Systemen, die von einem speziell dafür zu schaffenden Gremium bestehend aus Datenschützern, Verbraucherorganisationen und Arbeitnehmervertretern ausgeübt werden soll [17].

Wie kann die RFID-Technologie sicherer gemacht werden?

Eines haben Verbraucherschützer bereits erreicht: Es wird derzeit erheblicher Forschungsaufwand betrieben, um die RFID-Technologie sicherer zu machen. So löscht der *Kill-Befehl* die Seriennummer einer RFID-Marke und verhindert damit eine Identifizierung [15]. Beim *Meta-ID*-Verfahren wird die Seriennummer durch eine Meta-ID ersetzt [18]. Die eigentliche Kennung der RFID Marke erfährt nur derjenige, der den geheimen Schlüssel kennt, mit der die Meta-ID erzeugt wurde, und diesen an die RFID-Marke sendet.

Bekanntestes Beispiel ist das *Blocker-Tag*, ein Transponder, der dem Lesegerät vorgaukelt, es wären Millionen von RFID-Marken in Reichweite und die Identifizierung der (wenigen) real existierenden Marken verhindert [19]. Das Blocker-Tag macht sich dabei die Tatsache zunutze, daß ein Lesegerät nicht mehr als eine RFID-Marke gleichzeitig auslesen kann. Antworten mehrere RFID-Marken auf die Anfrage eines Lesegerätes, so kann es zu Kollisionen kommen, die vom Lesegerät erkannt werden müssen. Verfahren, die es einem Lesegerät ermöglichen, mit jedem der detektierten RFID-Marken einzeln zu kommunizieren, werden als Antikollisionsverfahren (oder Singulationsverfahren) bezeichnet. Antikollisionsprotokolle nutzen zur Kollisionsvermeidung überwiegend „Tree-Walking“- oder ALOHA-Algorithmen.

„Tree-Walking“-Algorithmen setzen voraus, daß das Lesegerät in der Lage ist, die genaue Bitposition einer Datenkollision zu erkennen. Das Lesegerät sollte zudem

seine Suche auf bestimmte RFID-Marken eingrenzen können. Angenommen im Ansprechfeld eines Lesegerätes befinden sich zwei RFID-Marken mit den binär codierten IDs 101 und 111. Beim Auslesen der Marken erkennt das Lesegerät nun eine Datenkollision an der zweiten Bitstelle, empfängt demnach nur Bit 1 und 3 korrekt (1x1). Durch sequentielles Abfragen der beiden Transponder kann das Lesegerät die Informationen getrennt voneinander auslesen. Kommt es an mehreren Bitstellen zu Kollisionen, was bei üblichen ID-Längen von bis zu einhundert Bit häufiger auftreten kann, so fragt das Lesegerät alle möglichen Bitkombinationen ab und bedient sich dabei eines binären Suchverfahrens. Jede mögliche ID im Ansprechfeld des Lesegerätes stellt dabei ein Zweig des binären Suchbaumes dar (daher „Tree-Walking“).

Das Blocker-Tag antwortet auf jede Anfrage des Lesegerätes, die das Bit an einer bestimmten Position abfragt, gleichzeitig mit 0 und 1 und erzeugt damit eine Kollision. Dadurch wird das Lesegerät gezwungen den Suchbaum weiter „hinabzusteigen“ und das nächste Bit abzufragen. Auch auf diese Anfrage antwortet das Blocker-Tag mit 0 und 1 gleichzeitig und löst eine Kollision aus usw. Dies hat zwei Auswirkungen: (1) der Auslesevorgang dauert sehr lange und (2) das Lesegerät kann nicht unterscheiden ob eine komplette Seriennummer vom Blocker-Tag oder von einer real existierenden RFID-Marke stammt.

Alle angeführten Aktivitäten zeigen, auch wenn sie nur einen Ausschnitt aller Forschungsbestrebungen auf dem Gebiet wiedergeben, daß Bedarf an einer „sicheren“ RFID-Technologie besteht, die das Recht der informationellen Selbstbestimmung besser schützt als bestehende Systeme.

Fazit

Die RFID-Technologie wurde an den Rand der Markteinführung gebracht. Verbraucherschützer nahmen sich des Themas an, deckten Sicherheitslücken auf und fanden mit ihren Kritikpunkten ein offenes Ohr bei den Medien. Daraufhin werden nun Sicherheitslösungen nachgeliefert, die allesamt nicht mehr als das Bild eines Flickenteppichs abgeben. Ein derartiges Verfahren (wenn man mit Blick auf den Ablauf überhaupt davon sprechen mag) weckt freilich Mißtrauen in der Bevölkerung und kann zu einer Ablehnung der RFID-Technologie an sich samt ihrer (größtenteils nutzbringenden) Anwendungen führen.

Die Akzeptanzprobleme der RFID-Technologie zeigen, daß bei der Einführung neuer (Ubiquitous-Computing)-Technologien in den Massenmarkt ein anderer Ansatz bezüglich des Umgangs mit möglichen Sicherheitsrisiken gewählt werden muß: Datenschutzbelange müssen vor der Einführung einer neuen Technologie in den Massenmarkt adressiert und sich abzeichnende Probleme zufriedenstellend gelöst sein, um eine möglichst hohe Akzeptanz in der Bevölkerung zu erreichen.

Quellenverzeichnis

[1] Presse-Archiv des FoeBuD, URL: http://www.foebud.org/archiv/dp/.
[2] METRO Group Future Store Initiative, URL: http://www.future-store.org.

[3] Controlling für Wäschereien, URL: http://www.argus-electronic.de/.
[4] Heise News 3.7.2004, US-Fluggesellschaft will Gepäck mit RFID orten, URL: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48831&words=RFID%20Fluggesellschaft
[5] Heise News 21.04.2004, RFID-Umfrage: Fußball-WM 2006 soll den Durchbruch bringen, URL: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/46724&words=RFID%20Fu%DFball.
[6] Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD), URL: http://www.foebud.org.
[7] Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), URL: http://www.nocards.org/.
[8] BigBrother Awards Deutschland, URL: http://www.bigbrotherawards.de/.
[9] Finkenzeller, K., RFID-Handbuch, Carl Hanser Verlag, München 2002.
[10] Texas Instruments Tag-it HF-I Transponder Inlays – Reference Guide, Texas Instruments, Mai 2002.
[11] Philips Icode SLI Product Specification, Royal Philips Electronics, Januar 2003.
[12] Takaragi, K., Usami, M., Imura, R., Itsuki, R., Satoh, T., An Ultra Small Individual Recognition Security Chip, IEEE Micro, Band 23/6, S. 43-49, November-Dezember 2001.
[13] Hitachi Pressemitteilung, Hitachi Develops a New RFID Chip With Embedded Antenna, URL: http://www.hitachi.com/New/cnews/030902.html, September 2003.
[14] EPCglobal, URL: http://www.epcglobalinc.org.
[15] EPCglobal Konsortium, EPC Spezifikation 1.0, URL: http://www.epcglobalinc.org/standards_technology/specifications.html.
[16] Laudatio zur Verleihung des BigBrother-Awards 2003 an die METRO AG, URL: http://www.bigbrotherawards.de/2003/.cop/.
[17] Golem IT-News 19.2.2004, FoeBuD ruft zur Demonstration gegen Metro-RFID auf, URL: http://www.golem.de/0402/29853.html.
[18] Sarma, S., Weis, S., Engels, D., RFID Systems and Security and Privacy Implications, in Kaliski, B., Co, C. K., Paar, C., (Hrsg.), Cryptographic Hardware and Embedded Systems - CHES 2002, LNCS Band 2523, S. 454-469, Redwood Shores, California, USA, Springer-Verlag, August 2002.
[19] Juels, A., Rivest, R.L., Szydlo, M., The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, in V. Atluri (Hrsg.), Proc. of the 8th ACM Conference on Computer and Communications Security, S. 103-111, ACM Press, 2003.