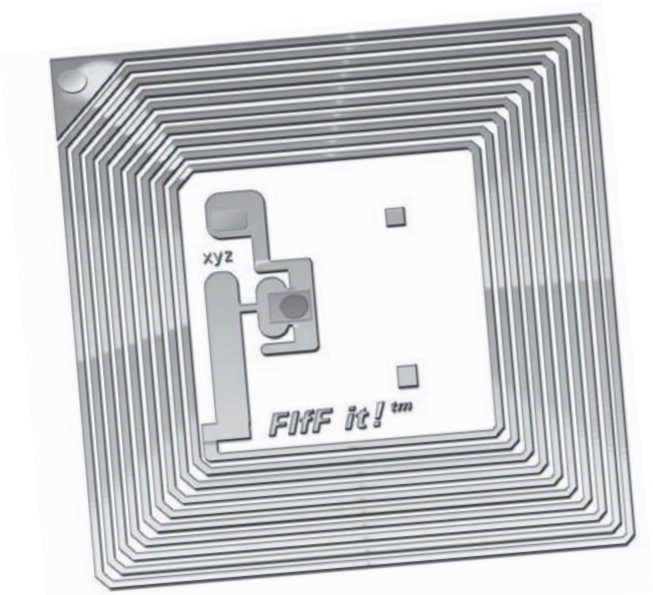
Preis: 3,50 Euro

978-3-9802468-6-6

RFID

Radio Frequency Identification



Die cleveren Dinge für überall – oder wir im Netz der Dinge?

Information | Meinungen | Kritik | Quellen

FIFF

Forum InformatikerInnen für
Frieden und gesellschaftliche Verantwortung e.V.

FIfF Radio Frequency Identification

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

Herausgeber	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.
Adresse	FIfF e.V. Goetheplatz 4 D-28203 Bremen Telefon 0421 - 33 65 92 55 Fax 0421 - 33 65 92 56 E-Mail *fiff@fiff.de*
Redaktion	Dagmar Boedicker
	namentlich gekennzeichnete Beiträge geben die Meinung ihrer Autoren wieder. Zusammenstellung und Kommentierung nicht namentlich gekennzeichneter Beiträge: Dagmar Boedicker
V.i.S.d.P.	Dagmar Boedicker, Fürstenrieder Str. 24 D-80687 München
Layout und Titelbild	Carsten Büttemeier, Paderborn
Fotos	Wir bedanken uns sehr herzlich für die Genehmigungen bei: Detlef Borchers, Baumer Ident GmbH, Egoméxico, FoeBuD e.V., Dina Kuznetsova, Schreiner LogiData GmbH & CO. KG, SOREON Research und Uwe Wissendheit
Druck	Meiners Druck, Bremen
ISBN	978-3-9802468-6-6
Nachdruck	mit Quellenangabe und Übersendung eines Belegexemplars erwünscht elektronische Fassung abrufbar unter: *http://www.fiff.de*

Die Informationen in dieser Broschüre wurden sorgfältig recherchiert und zusammengestellt. Sollten Sie trotzdem einen Fehler finden, bitten wir Sie um Verständnis und würden uns über einen Hinweis freuen.

Bremen, September 2006

Inhalt

Dagmar Boedicker

Man kauft sie mit!

Eine kurze Einführung in die Radiofrequenz-Identifikation (RFID)

Foto: Detlev Borchers

RFIDs sind zweifellos eine zukunftsweisende Technologie. Die Produkt- und Dienstleistungsbereiche, in denen sie sich einsetzen lassen, wachsen ständig. Und sie sind eine Technologie mit weltweiter Bedeutung. Die Republik Korea (Südkorea) machte im Jahr 2004 Inlandsumsätze mit RFID und hierauf bezogenen Geräten und Dienstleistungen von ca. 86,9 Mio. Euro. In Mexiko implantiert die Staatsanwaltschaft ihren Mitarbeiterinnen und Mitarbeitern einen VeriChip *für den sicheren Zugang zu einem zentralisierten neuen Datenzentrum zur Verbrechensbekämpfung. In den USA schlägt* Applied Digital *Chef Scott Silverman vor, mexikanischen Arbeitsimmigranten – selbstverständlich freiwillig – ebenfalls einen solchen Chip in den Arm zu pflanzen, wohl als probates Mittel zur Bekämpfung des Terrors und der illegalen Einwanderung. Die Münchner Stadtbibliothek stattet alle Bücher und Medien mit RFIDs aus, damit ihre Ausleiher sich in Zukunft selbst bedienen können.*

So funktioniert's

Unsere Sinne können elektromagnetische Wellen nicht wahrnehmen, wir können sie weder riechen, noch hören, sehen oder fühlen. Das mag ein Grund dafür sein, dass sich viele Menschen für die kleinen Funkchips überhaupt nicht interessieren. Ein RFID-Chip sendet Information, ein Lesegerät liest sie und wir merken nichts davon. Auf welchen Frequenzen ein RFID sendet entscheidet über seine Reichweite und damit seinen möglichen Einsatz. Es nutzt vielleicht den Radiowellenbereich, der zwischen 30 kHz und 300 MHz liegt, aber es gibt auch RFIDs im Mikrowellenbereich. Viele Systeme für die Identifikation (beispielsweise Zugangskontrolle, Zeiterfassung, elektronische Wegfahrsperren) arbeiten bei 125 kHz, sie haben zwar eine relativ geringe Lesegeschwindigkeit, sind dafür aber billig. RFID-Chips im Einzelhan-

del nutzen meist 13,56 MHz, Lösungen in der Logistik den UHF-Bereich (868MHz, 915MHz sowie 2,45GHz). Für **I**ndustrielle, wissenschaftliche (**S**cientifical) oder **M**edizinische Anwendungen gilt der ISM-Bereich 2,4 bis 5 GHz. Im Mikrowellenbereich funktionieren neben RFIDs auch Wireless LAN-Systeme (WLAN). Längere Wellen mit niedrigeren Frequenzen durchdringen viele Stoffe, brauchen also keinen Sichtkontakt, sie werden aber von Metall reflektiert. Für hohe Frequenzen kann schon Wasser ein Hindernis sein.

Weil RFIDs auf Produkte geklebt werden können, heißen sie auch Funk-Etiketten oder –Labels. Sie können mehr Information speichern als die herkömmlichen Strichcodes, und anders als diese müssen sie nicht mehr optisch gelesen werden. So lassen sich die Einzelteile etikettieren und anschließend in einen Karton verpacken, das Lesegerät *sieht* durch die Umverpackung. Für die Logistik sind sie deshalb ideal, denn ein Produkt lässt sich auf dem Transportweg verfolgen. Raffiniertere Chips können im Produktionsprozess steuern, was mit dem Bauteil passiert, auf dem sie angebracht sind.

RFIDs können also ein Objekt, ein Tier oder einen Menschen kennzeichnen, einen Prozess steuern und sie können Objekte oder Lebewesen lokalisieren. Hinter den RFID-Chips und Lesegeräten gehört dazu eine großräumige IKT-Infrastruktur für die vielen Anwendungen, Datenbanken zum Speichern der Produktcodes, ein Lokalisierungssystem wie GPS *(Global Positioning System)* zur Ortsbestimmung, Standards, Logistikverfahren oder Anwendungen im Warenwirtschafts- oder ERP-Bereich *(Enterprise Resource-Planning)*.

Wo ein Chip eingesetzt werden soll ist ausschlaggebend dafür, ob der Chip selbst eine Energiequelle in Form einer Batterie hat (aktiv) oder auf die Energie angewiesen ist, die ihm das Lesegerät übermittelt (passiv). Passive RFIDs lassen sich nur lesen und nicht beschreiben, aktive lassen sich meist auch beschreiben, sie können weiter senden und haben mehr Speicherplatz. Ihre Batterien halten mehrere Jahre lang. RFIDs können sehr unterschiedliche Speicherkapazitäten haben, und sie können mit einem eigenen Prozessor ausgestattet sein, der beispielsweise Daten verschlüsselt. Je leistungsfähiger ein Chip ist, umso teurer wird er natürlich.

Dagmar Boedicker

Dagmar Boedicker ist technische Redakteurin und Trainerin für Softwaredokumentation. Sie hat Politikwissenschaft studiert und ist stellvertretende Vorsitzende des FIfF e.V.

Mit dem internationalen *Electronic Product Code* (EPC) erhält jeder Chip eine weltweit eindeutige Identifikationsnummer. Es gibt Varianten mit 64 Bit (EPC-64), 96 Bit (EPC-96) und 256 Bit (EPC-256). Neben anderen Informationen enthält beispielsweise der EPC-96 die Seriennummer des Chips (36 Bit) und mit einer Gesamtlänge von 44 Bits sowohl eine Nummer für den Hersteller (20-40 Bits) als auch für die Produktart, die der Chip kennzeichnet, den Item- oder Objektcode (4-24 Bit).

Foto: Detlev Borchers

RFID-Chips sehen sehr unterschiedlich aus, winzig klein wie ein Stecknadelkopf oder fast so groß wie ein Taschenbuch, rund oder eckig, mit sichtbarer oder unsichtbarer Antenne, ... Sie haben verschiedene Namen: Transponder *(transmitting responder)*, Tag oder Label. RFIDs lassen sich auch abschalten, dauerhaft oder auf Zeit. IBM entwickelt zur Zeit einen Chip, dessen Antenne sich abknipsen lässt, es kann aber auch eine Kill-Funktion eingebaut sein, oder Sie können den Chip in die Mikrowelle legen.

Spektrum der Anwendungen

Es gibt sicher viele wünschenswerte Anwendungen für die Zukunft: So wäre eine Kennzeichnung von Bauteilen für elektronische Geräte beim Recycling hilfreich, RFIDs auf verschiedenen Produkten könnten sowohl die Fälschung (beispielsweise bei Arzneimitteln) als auch den Diebstahl teurer Güter (Kennzeichnung von Elektronikgeräten, Wegfahrsperre bei Fahrzeugen) erschweren. Garantie- und Rückgaberechte könnten im Chip festgeschrieben sein, Rückrufaktionen erleichtert werden. Verbesserte Logistik-Abläufe können Energie sparen, RFIDs in Fertigungsprozessen den Ressourcen-Verbrauch minimieren. Produkte können zu ihrem Ursprung zurück verfolgt werden. Werden RFIDs mit Sensoren kombiniert, erleichtern sie die Qualitätskontrolle, beispielsweise bei Produkten, die ohne Unterbrechung in der Kühlkette verarbeitet oder transportiert werden müssen. Zahlreiche Einsatzmöglichkeiten tun sich in Labors auf, beispielsweise bei Gewebeproben für die *Life Sciences*.

Zum Einsatz auf manchen dieser Gebiete sind aber noch Schwierigkeiten zu überwinden. Sie sind einerseits technischer Art, wie die Wechselwirkungen zwischen hochfrequenten Feldern, liegen aber auch in den Standards. Die Standardisierungsbemüh-ungen sind auf einem guten Weg, zumindest innerhalb der Europäischen Union. Die IT-Infrastruktur muss aber noch ausgebaut werden. Immerhin ist das Ziel, RFIDs durch Massenherstellung billiger zu machen, durch ihre zunehmende Verbreitung in den letzten Jahren deutlich näher gerückt.

Die Experten sehen auch im Gesundheitswesen ein wichtiges Einsatzgebiet, wenn beispielsweise im Krankenhaus der Zu-

gang zu den Behandlungsdaten durch einen Chip im oder am Patienten erleichtert wird. Gebrechliche könnten bei Unfällen einen automatischen Notruf auslösen oder verwirrte Menschen besser zu finden oder zu identifizieren sein. Selbstverständlich hat auch die Rüstungsindustrie die nützlichen Kleinteile im Blick. Sie sollen mit erweiterten Funktionen sogar in die Lage versetzt werden, Satelliten, Handy-Netze und WLAN-Hot-Spots anzufunken und ihren Standort mitzuteilen. Das haben sich die Militärlogistiker gewünscht. Wie viele andere Techniken wurde übrigens auch die Transponder-Technik zunächst für militärische Zwecke entwickelt und erst 1977 für den zivilen Einsatz freigegeben.

Pläne der europäischen Zentralbank, die Euro-Banknoten mit RFIDs zu versehen, scheinen sich zerschlagen zu haben. Davon hatte man sich erhofft, die Wege *schwarzen* Gelds verfolgen zu können, und die Chips sollten die Geldscheine fälschungssicherer machen.

Risiken und Chancen

Zugangskontrollen sind ein beliebter Einsatzzweck für die Chips, sowohl in Bereichen, in denen Sicherheit wichtig ist, wie Atomkraftwerken, Flughäfen oder Rechenzentren, als auch beim wenig sicherheitskritischen Benutzen des öffentlichen Nahverkehrs. Dort wird die Karte eingesetzt, um Fahrtkosten abzubuchen. Das alles spart Zeit, ist bequem und scheint sicher zu sein. Nur schade, dass der neue Reisepass so viel teurer ist als der alte. Vielleicht sparen Sie das aber wieder ein, wenn Ihr kommunales Nahverkehrssystem automatisch den für Ihre Nutzung günstigsten Tarif abrechnet? Schon jetzt ist in manchen Städten der Busfahrschein aus dem Automaten billiger als der beim Fahrer oder am Schalter gekaufte. Das lässt sich sehr wohl auch als Preisdiskriminierung derjenigen kritisieren, die keine Möglichkeit (oder nicht den Wunsch) haben, diesen Weg zum Erwerb einzuschlagen. Auch andere Dienstleistungen werden wohl billiger werden, jedenfalls für die Anbieter, wenn weniger Aufwand für eine menschliche Bearbeitung anfällt.

Unsere neuen Reisepässe enthalten bereits einen RFID-Chip, der übrigens mitsamt den Daten schon geklont werden konnte, für die Personalausweise wird darüber diskutiert. Andere Länder sind wesentlich weiter im Einsatz, so soll China zur Zeit seine Personalausweise und Führerscheine auf RFID-Technik umstellen, in den USA sollen es im ersten Jahr 67 Millionen Pässe werden, und weltweit wird ein jährliches Marktvolumen für Ausweispapiere von 125 Millionen erwartet. Hier treffen zwei, vielleicht drei gesellschaftliche Trends zusammen: Der Wunsch nach möglichst umfassender Sicherheit und der nach mehr Komfort, vielleicht auch ein Streben staatlicher Einrichtungen nach mehr Kontrolle über die Bevölkerung.

Die Kombination von berührungslos auslesbaren Ortungs- und Identifizierungsdaten, Videoüberwachung und einer Vorratsspeicherung von Kommunikationsdaten auf der einen (staatlichen), und von steigenden Komfortwünschen, Zeitersparnis und Rationalisierungsbestrebungen auf der anderen (privatwirtschaftlichen) Seite sollte die Gesellschaft beschäftigen. Diese Entwicklung bedeutet in Zukunft neue He-

rausforderungen für diejenigen, denen es wichtig ist selbst zu entscheiden, wer was über sie oder ihn erfährt. Immerhin ist das ein verfassungsrechtlich garantierter Anspruch.

Die Chancen der Rationalisierung werden von der Industrie deutlich wahrgenommen und sie sind im Sinne der Wettbewerbsfähigkeit und Ressourcen-Ersparnis sicher wichtig. Die Kehrseite jeder Rationalisierung ist aber der Verlust von Arbeitsplätzen, und es wundert doch, dass dieses Thema so gut wie gar nicht in der öffentlichen Diskussion auftaucht. Wenn doch einmal, wird beschwichtigt, dass eingespartes Personal für höher qualifizierte Tätigkeiten eingesetzt werden soll.

Wenn es um Fragen der Technik geht, die eine Entscheidung verlangen zwischen einem Implantat oder einem tragbaren Chip, fällt sicher die Abneigung vieler Menschen gegenüber einem eingepflanzten Fremdkörper ins Gewicht. Das Armband oder der Anhänger können zwar verloren gehen oder vertauscht werden, aber der Chip unter der Haut kann wandern. Wenn das flotte Implantat für den Disko-Besuch oder den Zugang zum PC unter wenig hygienischen Bedingungen injiziert wird, können hässliche Entzündungen folgen, wie bei Piercings auch.

RFID-Chips kommunizieren mit Schreib-/Lesegeräten durch elektromagnetische Wellen. Von denen sind wir ohnehin umgeben, die meisten kommen von drahtlos kommunizierenden Geräten (beispielsweise im Mobilfunk oder den Netzen rund um den PC im Büro oder Haushalt), aber auch von jedem Elektrogerät im Betrieb. Es ist noch völlig ungeklärt, wie sich eine weitere Zunahme des allgegenwärtigen Elektrosmogs auswirken wird. Dass elektromagnetische Wellen einen Einfluss auf den menschlichen Körper haben, steht außer Frage. Dabei ist nicht nur der Wärme-Effekt zu diskutieren, sondern auch gentoxische Wirkungen in den Körperzellen. Die EU-weite REFLEX-Studie hat den Zusammenhang zwischen einer Radiowellen-Exposition und der Entstehung funktioneller Störungen zwar nicht belegt, die Annahme aber plausibler gemacht. Träger von Hörgeräten und Herzschrittmachern sollten jedenfalls Abstand von Schreib-/Lesegeräten halten. Zwar gibt es auf europäischer Ebene bereits gesetzliche Regelungen zum Gesundheitsschutz für die Öffentlichkeit und am Arbeitsplatz, auf diesem Gebiet ist aber weitere Forschung nötig.

Auch sind wohl Probleme zu erwarten, wenn private Unternehmen oder der Staat auf personenbezogene Daten zugreifen wollen und können, die wir alle lieber für uns behalten möchten. Inzwischen hat es sich herumgesprochen, dass RFIDs datenschutzrechtlich alles andere als unbedenklich sind, deshalb dazu ein eigener Abschnitt:

Datenschutz-Anforderungen

Vor allem in der Fähigkeit, Personen zu lokalisieren, liegt etwas Beunruhigendes. Schließlich ist es nicht schwierig, ein Objekt mit einer Person in Verbindung zu bringen. Wer mit der Kunden- oder Geldkarte einkauft und dann ein RFID-gekennzeichnetes Objekt aus dem Laden trägt, der lässt sich womöglich auch an einem anderen Ort unbemerkt identifizieren. Bei

den Strichcodes, die Sie heute noch auf fast allen Etiketten im Einzelhandel finden, ist das nicht möglich.

Der Bundesbeauftragte für den Datenschutz, Peter Schaar, verlangt, dass der RFID-Einsatz dem Verbraucher bekannt sein muss und nicht heimlich erfolgen darf. Daten der Chips aus verschiedenen Produkten dürfen nicht zu Verhaltens-, Nutzungs- und Bewegungsprofilen zusammengeführt werden, und die Verbraucher müssen die Möglichkeit haben, den Speicherinhalt auszulesen. Die Kunden sollen die RFIDs auf Produkten und Verpackungen deaktivieren und die Lese-/Schreib-Mechanismen kontrollieren können. Im Sinne eines effektiven Datenschutzes sollten die Betroffenen möglichst früh informiert werden, also bereits auf dem Produkt und an den Verkaufsregalen, und nicht erst, wenn die Daten des Kunden durch ein Kassensystem erfasst werden. Schaar schlägt vor, dass sich Industrie und Handel über Selbstregulierung und Selbstverpflichtung zur umfassenden Gewährleistung des Datenschutzes verpflichten.

Foebud e.V., Initiator des *BigBrother-Awards,* hat in einem Positionspapier Forderungen aufgeführt, die von einer Vielzahl von Bürgerrechts-Organisationen unterstützt werden. Sie halten freiwillige Selbstverpflichtungen nicht für ausreichend und verlangen eine Technikfolgen-Abschätzung und bis zu deren Ergebnis die Einhaltung folgender Grundregeln durch die Hersteller und Anwender von RFIDs: Chips und Lesegeräte müssen deutlich und verständlich gekennzeichnet sein, auch mit ihren technischen Spezifikationen. Jeder Lesevorgang muss für die Verbraucher erkennbar sein, und die Zwecke bekanntgegeben werden, für die die Daten ausgelesen werden. Nur die notwendigen Daten für diesen jeweiligen Zweck dürfen erfasst werden. Niemand darf genötigt oder gezwungen werden, RFIDs zu akzeptieren. Die Übermittlung der Daten muss sicher und geheim sein, eine neutrale Instanz mit der Kontrolle beauftragt werden. Es muss eine verpflichtende Verantwortlichkeit der Anwender geschaffen werden, und bei öffentlichen und privatwirtschaftlichen Einrichtungen eine Instanz, an die sich die Bürgerinnen und Bürger bei Verletzungen ihrer Rechte wenden können. Menschen dürfen nicht mit Hilfe der RFIDs verfolgt werden, es sei denn, sie hätten ausdrücklich und schriftlich zugestimmt. Die Chips dürfen nicht als Mittel eingesetzt werden, das die Anonymität einer Person verringert oder unmöglich macht.

Von dieser Situation sind wir freilich noch weit entfernt, auch wenn viele Unternehmen sich darüber im Klaren sind, dass ein guter Schutz der Verbraucher der Technik den Weg ebnen kann. Der wenig verbraucherfreundliche Umgang einiger Unternehmen mit RFIDs hat schon viele Menschen misstrauisch gemacht. – Es sind noch viele Fragen offen: Werden Ihnen aus dem Deaktivieren eines RFIDs Nachteile entstehen? Können Sie das Produkt nach geltendem Verbraucherschutzrecht dann noch umtauschen oder zurückgeben? Wie ließe sich ein Chip verlässlich deaktivieren, der in ein Gerät integriert ist? Was bedeutet es, Millionen kleiner, schwer auffindbarer Chips umweltgerecht zu entsorgen? - Auf diese Fragen kann auch unsere Broschüre noch keine Antwort geben, auf viele andere aber hoffentlich doch.

Michael Riemer

Radio Frequency Identification

Wo liegen ihre Möglichkeiten und Grenzen?

Das Kürzel RFID *steht für* Radio Frequency Identification*. RFID-Systeme sind automatische Identifikationssysteme, mit denen Daten berührungslos aus* Etiketten *gelesen und bei manchen Systemen auch in sie geschrieben werden können. RFID-Etiketten besitzen Mikroprozessoren oder hochminiaturisierte Logikschaltungen, und sie arbeiten im Allgemeinen ohne eigene Energiequelle. Sie lassen sich daher unauffällig an oder in Objekten aller Art unterbringen und sogar in Mensch und Tier implantieren. Über Lesegeräte können angeschlossene Systeme Objekte und Personen weltweit eindeutig identifizieren. So ermöglicht die RFID-Technologie beispielsweise, Warenflüsse vom Erzeuger bis an die Ladentheke oder sogar bis in den Haushalt der Kunden zu verfolgen.*

Zu einem RFID-System gehören Lesegeräte und die Etiketten (auch *Tags, Labels, Transponder* genannt), die auf Anstoß des Lesegerätes Signale mit einem programmierten oder programmierbaren Informationsgehalt abgeben. Da die Tags so weit miniaturisiert sind, dass sie in Objekte oder Verpackungen eingearbeitet werden können, werden sie als intelligente Etiketten (*smart tags* oder *smart labels*), Funkchips oder kurz Tags bezeichnet. Wenn sie komplexe Signale abstrahlen können, wird auch die Bezeichnung Transponder (*transmitting responder*) verwendet. Informationen werden zwischen Lesegeräten und Tags mittels elektromagnetischer Wellen oder per Funk übertragen. Tags mit komplexerer Funktion brauchen Energie, sie wird normalerweise durch elektromagnetische Felder übertragen.

Die Lesegeräte sind ihrerseits Teile eines umfangreicheren Systems. In der Regel sind sie an größere Softwareanwendungen und Datenbanken angeschlossen, damit die Daten weiterverarbeitet werden können. So können mit RFID-Systemen beispielsweise aktueller Zustand und Standort eines Produkts schnell und genau festgestellt werden, wenn Prozesse in einem Unternehmen werksübergreifend organisiert werden müssen.

Die feld– oder funkbasierte Datenübertragung ist ein wesentlicher Vorteil der RFID-Technik gegenüber herkömmlichen Identifikationssystemen wie dem weit verbreiteten Barcode und dem von Postsendungen bekannten Datamatrix-Code, die optisch ausgelesen werden. Funk und Felder erweitern die Lesemöglichkeiten, deshalb lässt sich RFID auch überall dort einsetzen, wo Schmutz und ungünstige Objektpositionierung ein optisches Auslesen erschweren. RFID-Systeme ermöglichen die Identifikation der Tags und das Auslesen ihrer Daten innerhalb einer durch Sendeleistung und Empfangsempfindlichkeit begrenzten Reichweite. Mehrere intelligente Etiketten, beispielsweise auf Warenpaletten oder in Einkaufswagen, können in einem Vorgang angesprochen werden.

Dass RFID als Mittel zur berührungslosen Objekterkennung in den letzten Jahren rasant an Bedeutung gewinnt, ist nicht zuletzt dem technischen und technologischen Fortschritt auf diesem Gebiet zuzurechen. Die Optimierung der Fertigungstechnologie lässt Preis und Abmessungen schrumpfen. Gleichzeitig werden die in den Tags verwendeten Prozessoren leistungsstärker. Die Industrie findet immer neue Anwendungen für die Technik. Besonders in der Logistikbranche verbreitet sich RFID rasch.

Über den ökonomischen Nutzen hinaus entstehen mit zunehmender Verbreitung und Leistungsfähigkeit auch gesellschaftliche und persönliche Risiken aus der Möglichkeit, Personen und Objekte verdeckt zu identifizieren. Um sowohl die Risiken als auch die Möglichkeiten von RFID-Systemen einschätzen zu können, ist ein Einblick in ihre Technik und Leistungsmerkmale hilfreich, der aber immer nur eine Momentaufnahme sein kann. Die Technik hat die Grenzen ihrer Entwicklung noch lange nicht erreicht. Eine grobe Orientierung geben die Sende- und Empfangsentfernungen, die maßgeblich durch die verwendeten Frequenzen und die Übertragungsverfahren von Daten und Energie bestimmt werden [1].

Unterschiedliche Systeme und ihre Einsatzbereiche

Seit vielen Jahren gibt es elektronische Artikelsicherungssysteme (EAS) in Kaufhäusern. Sie haben nur eine geringe Leistungsfähigkeit, denn ihre Funktion ist darauf beschränkt, ein An-/Aus-Signal zu

Michael Riemer

Michael Riemer studierte „Electrical and Electronic Engineering“ (BEng) an der London South Bank University und beschäftigte sich in seiner Bachelorarbeit mit RFID. Er arbeitet seit vier Jahren für FIfF e.V. und ist Mitglied des Vorstands. Zur Zeit absolviert er das Diplomstudium der technischen Informatik an der Hochschule Bremen.

geben. Individuelle Objekte können mit ihnen nicht unterschieden werden.

In der Regel wird mit dem Begriff RFID jedoch mehr als nur der Diebstahlschutz assoziiert. Systeme mit *mittlerer Leistungsfähigkeit* können über Speicher von mehreren Kilobyte verfügen, die bei manchen Tag-Typen auch wiederbeschreibbar sind. Hier sind solche Systeme anzusiedeln, die zur Objekt- bzw. Produkterkennung eine längere Identifikationsnummer an ein Lesegerät übermitteln. So lassen sich, anders als bei den EAS, individuelle Objekte aus der selben Produktreihe voneinander unterscheiden, was vom Warentransport vom Produzenten zum Laden bis zur Abrechnung an der Kasse genutzt werden kann. Je nach Einsatzgebiet können die Tags über Authentifizierungs- und Verschlüsselungsfunktionen verfügen.

RFID-Systeme mit *hoher Leistungsfähigkeit* zeichnen sich dadurch aus, dass die Prozessoren auf den Tags komplexe Berechnungen für Verschlüsselung und Authentifizierung ausführen können. Sie sind teurer und kommen deswegen vorwiegend in sicherheitsrelevanten Anwendungen zum Einsatz wie der Identifikation von Personen, Bezahlvorgängen und Zugangskontrollen.

Energieversorgung

RFID-Tags sind im einfachsten Fall mit einer Logikschaltung ausgerüstet, die die für die Informationsabgabe benötigte Datenfolge produziert. Tags der komplexeren Art besitzen sogar Prozessoren und Speicherbausteine. Logikschaltungen, Prozessoren und Speicher benötigen für die Aktivierung, Programmsteuerung und Datenübertragung eine Energieversorgung. Unterschieden wird zwischen aktiven und passiven RFID-Tags.

Aktive RFID-Tags verfügen über eine eigene Spannungsversorgung, zum Beispiel eine kleine Batterie. Sie versorgt den Prozessor, der von außen durch das Feld– oder Funksignal des Lesegeräts aktiviert wird. Wegen der Batterie sind aktive RFID-Tags meist größer als passive. Deshalb, und auch aus Kostengründen, werden sie nicht in der massenhaften Artikelkennzeichnung im Handel genutzt.

Passive RFID-Tags beziehen ihre Betriebsenergie aus dem elektromagnetischen Feld oder aus der elektromagnetischen Welle des Lesegerätes. Das Lesegerät kann einen in seiner Reichweite befindlichen Tag entweder permanent oder gepulst mit Energie versorgen. In gepulsten Systemen werden die Daten vom Lesegerät simultan mit der Betriebsenergie übermittelt. Die Tags speichern die Energie in Kondensatoren, um die Versorgung in den Phasen zu sichern, in denen das Lesegerät die Energieübertragung zwecks Informationsempfang unterbricht.

Datenübertragung

Für die Datenübertragung zwischen Lesegeräten und RFID-Tags gibt es drei verschiedene Verfahren: die kapazitive Kopplung, die induktive Kopplung (Transformator-Prinzip) und das *Backscatter-Verfahren* [2].

Bei einer *kapazitiven* Verbindung müssen die Tags so nahe am Lesegerät sein, dass der Plattenkondensator-Effekt zum Tragen kommt. Zwischen den Kondensatorflächen von Lesegerät und Tag wird ein elektrisches Feld aufgebaut. Die Logik des Tags verändert seine kapazitiven Eigenschaften in zeitlicher Folge. Diese wiederum beeinflussen den Feldverlauf, der Rückwirkungen auf das Lesegerät ausübt. Über diese Veränderungen können die gewünschten Informationen ausgelesen werden. Die Versorgungsenergie kann aus einem zusätzlichen elektromagnetischen Feld nach dem Transformator-Prinzip gewonnen werden.

Induktiv gekoppelte Systeme arbeiten nach diesem Transformator-Prinzip. Das Lesegerät baut über seine Sendespule ein magnetisches Feld auf und versorgt die Tags über deren Empfangsspule mit Energie. Die Tags entziehen dem Feld Energie, beispielsweise durch eine Folge von Veränderungen des Widerstandswerts der Empfangsspule. Anhand dieser Änderungen ermittelt das Lesegerät die zu übertragenden Daten.

Beim Backscatter-Verfahren kommt ein aus der Radar-Technik bekannter Effekt zum Einsatz: Ein Objekt reflektiert elektromagnetische Wellen, wenn seine Ausdehnung mehr als die Hälfte der Wellenlänge des Signals beträgt. Dieser so genannte Rückstrahleffekt funktioniert besonders gut, wenn die Antennen der Tags Resonanz mit der Sendefrequenz des Lesegeräts herstellen, wenn also die Sendefrequenz mit der Eigenfrequenz des Objekts übereinstimmt. Bei der Eigenfrequenz eines Systems schwingt dieses nach einmaliger Anregung weiter, solange es seine Dämpfung erlaubt. Über eine Steuerung des reflektierten Signals werden die Daten ähnlich wie bei der induktiven Kopplung an das Lesegerät übermittelt.

Frequenzbereiche

Für Energie und Datenübertragung werden abhängig von den Funktionsprinzipien Felder oder Wellen in unterschiedlichen Bereichen des Radio– und Mikrowellen–Frequenzbandes [3] genutzt. RFID-Systeme für die Produktidentifizierung arbeiten meist im Langwellenbereich zwischen 100 kHz und 135 kHz oder im Kurzwellenbereich bei 13,56 MHz. Komplexere Systeme mit höheren Reichweiten arbeiten auch im Mobilfunkbereich um 900 MHz, in Nordamerika auf 915 MHz, in Europa auf 868 MHz. Auch das Mikrowellenspektrum ist mit den Frequenzen 2,45 GHz und 5,80 GHz für RFID-Systeme erschlossen.

Die unterschiedlichen Frequenzbereiche, die für die Energie– und Datenübertragung genutzt werden können, weisen je nach Anwendungsgebiet Vor- und Nachteile auf [2]. Je höher die Frequenz, desto mehr Daten können pro Zeiteinheit übertragen werden. Ist es für eine Anwendung wichtig, viele Daten in kurzer Zeit zu lesen, so würde sich eine hohe Kommunikationsfrequenz anbieten. Flüssigkeiten oder Feuchtigkeit können bei hohen Frequenzen aber zu Problemen führen, da sie die Feld– oder Wellenausbreitung erschweren. Bei niedrigen Frequenzen führen metallische Objekte zu Störungen (wenn sich beispielsweise ein RFID-Tag auf einer Blechdose befindet).

Mit Sendefrequenzen im Langwellenbereich (unterhalb 135 kHz) werden heute in der Regel Übertragungsweiten von ca. 1,5 Meter erreicht. Bei 13,56 MHz liegen diese noch bei knapp einem Meter [3]. Bei Systemen im Mobilfunk– und Mikrowellenbereich können heute auch schon auch 3 bis 7 Meter Reichweite überbrückt werden. Die effektive Reichweite hängt von den Umgebungsvariablen ab: Störeffekte wie Flüssigkeiten oder Metallteile, die bei den verschiedenen Frequenzen unterschiedlich wirken, verringern die Reichweite.

Ausblick

Eindeutige Grenzen für die maximal erzielbare Reichweite, die ein wichtiges Kriterium nicht nur für den Einsatz sondern auch für unerwünschte Nebeneffekte sind, können grundsätzlich nicht genannt werden. Abgesehen von den oben genannten Beeinträchtigungen der Feld– oder Wellenausbreitung hängt die überbrückbare Entfernung entscheidend von der Sendeenergie und der Empfangsempfindlichkeit der Übertragungsstrecke sowie von der Störungsempfindlichkeit der Signalcodierung ab.

Standardisierungsorganisationen und Gesetzgeber beschränken heute lediglich die Sendeleistung von RFID-Lesegeräten. Dahinter stehen Überlegungen zum Gesundheitsschutz von Menschen. In Europa gelten u.a. die europäischen Normen 50357 und 50364, zur „Begrenzung der Exposition von Personen gegenüber elektromagnetischen Feldern von Geräten, die im Frequenzbereich von 0 Hz bis 10 GHz betrieben und in der elektronischen Artikelüberwachung (EAS), Hochfrequenz-Identifizierung (RFID) und ähnlichen Anwendungen verwendet werden“.

Dass damit gleichzeitig die Maximalreichweite begrenzt wird, kann daraus keinesfalls abgeleitet werden. Sie ist abhängig von der Technologie der Empfangskomponenten und der Komplexität der Signalaufbereitung. In wenigen Jahren können Grenzen um Größenordnungen übersprungen werden, die aus der Sicht des gegenwärtigen Standes von Methodik und Technologie postuliert werden. Das zeigen Beispiele wie etwa die Entwicklung des Ethernet (10 MHz schienen anfangs die Obergrenze zu sein), die Steigerung der Datenraten über Telefonleitungen oder die Ausweitung der Kanalkapazität von Satellitenfunkstrecken bei immer kleineren Parabolantennen.Forschung und Entwicklung tragen mit Sicherheit weiterhin dazu bei, dass die bisherigen RFID-Konzepte ausgebaut und optimiert werden und sich damit auch weitere neue Anwendungsfelder erschließen. Der Polymer-Technik kommt dabei eine Schlüsselrolle zu. Mit ihrer Hilfe sollen Tags nur noch aus organischen Polymerstrukturen bestehen. Sollten einmal Chips auf Silizium-Basis und Antennen aus Metall entfallen, würde dies entscheidend zur Umweltverträglichkeit der RFID-Tags beitragen — ein nicht zu vernachlässigender Aspekt, wenn man an die weite Verbreitung, die hohen Stückzahlen und das zukünftige Potenzial denkt. Ein primäres Ziel der Weiterentwicklung ist es, die Produktion preisgünstiger zu machen und dadurch der Masseneinführung zu einem Schub zu verhelfen. Wenn zukünftige Tags sich noch einfacher in bestehende Produktverpackungen integrieren lassen, ist es lediglich eine Frage der Zeit, bis RFID

für die Logistik im großen Stil eingesetzt wird.

In den Diskussionen über das RFID-Thema muss auch über missbräuchliche Verwendung und über die Notwendigkeit von Sicherheitsmaßnahmen gesprochen werden. Wo Daten, die mittels Funk gelesen werden können, nur unzureichend geschützt sind, da gewinnt der Aspekt der Lesereichweite an Bedeutung und damit die Frage, wie die Datenabfrage kontrolliert werden kann. Mit leistungsstarken Prozessoren können komplexe Authentifizierungs- und Verschlüsselungsverfahren realisiert werden, es können aber auch vielfältige Daten gesammelt werden, mit denen umfangreiche Bewegungsprotokolle etc. erstellt werden können. Ob dem Einsatz solcher komplexeren und leistungsfähigeren Systeme Kostengründe entgegenstehen, ist lediglich eine Frage der Nachfrage und einer durch Produktionsmengen gesteuerten Preisentwicklung.

Die Objektidentifikation ist einerseits ein wichtiger Bestandteil vieler Prozesse in der Produktion und Logistik. Durch ihre Automatisierung können Unternehmen ihre bestehenden Abläufe optimieren und langfristig kontrollieren. Die Vorteile der RFID-Technik in der Industrie bringen andererseits auch Gefahren für die Verbraucher mit sich. Sie treten spätestens dort auf, wo individuell gekennzeichnete Produkte über die Ladentheke wandern. Wenn Objekte jederzeit automatisch erkannt werden können, dann ist der Personenbezug ebenso leicht möglich. Und hier schafft RFID ein spezielles Problem: Menschen identifizieren sich in der Regel wissentlich, zum Beispiel bei einer förmlichen Vorstellung „Guten Tag, mein Name ist ...“, oder man wird zur Identifizierung mittels Personalausweis, Reisepass oder Kundenkarte aufgefordert. RFID macht es jedoch möglich, dass Menschen auch ohne ihr Wissen und sogar gegen ihren Willen erkannt werden können: Gefährdet wird die Anonymität im Alltag. Dies ist eine neue Dimension der Bedrohung der Privatsphäre.

Bei den Verantwortlichen für Entwicklung und Anwendung muss ein Bewusstsein dafür geschaffen werden, dass RFID nicht per se nur Vorteile bringt. Es liegt (auch) in ihren Händen, dass die Systemrisiken bereits in den frühen Konzept und – Entwurfsstadien erkannt und minimiert werden. Darüber hinaus ist der Gesetzgeber in die Pflicht genommen, vorausschauend im Interesse der Bürger zu handeln. Im Moment läuft er im Rennen um die Verbraucherinteressen mit der Wirtschaft allerdings nur mäßig motiviert hinterher …

Literatur

[1]Bundesamt für Sicherheit in der Informationstechnik (2004), *Risiken und Chancen des Einsatzes von RFID-Systemen*, SecuMedia Verlags-GmbH

[2] Finkenzeller K. (2002) *RFID-Handbuch*, Hanser Fachbuchverlag, München

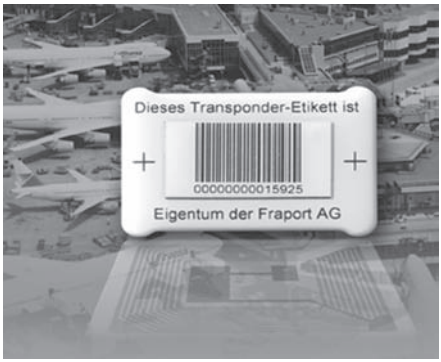
[3] Lampe M., Flörkemeier C., Haller S. (2005), *Das Internet der Dinge — Ubiquitous Computing und RFID in der Praxis*, Hrsg. Fleisch E., Mattern F., Springer Verlag, Berlin, (S. 69 – 86)

Uwe Wissendheit, Dina Kuznetsova

RFID-Anwendungen heute und morgen

In vielen Bereichen hat die RFID-Technik bereits Einzug gehalten und generell sind RFID-Systeme eine hervorragende Grundlage, um auch weitere, zukunftsorientierte Anwendungsfelder zu erschließen:

- Logistik/Supply Chain (Warenidentifikation und Verfolgung, Fluggepäckverfolgung, Paketdienste);
- Prozesskontrolle/Produktion (Werkzeugkontrolle, Produktionsverfolgung/ Fertigungshistory, Merkmal für Fälschungssicherheit (Pharmaindustrie));
- Sicherheits- und Zahlungssysteme (Zugangssysteme, Diebstahlreduktion, Ticketing, elektronische Bezahlung, Wegfahrsperre, Smart-Pass);
- Tieridentifikation (Landwirtschaft, Brieftauben, Populationsverfolgung von Insekten);
- Archivierungssysteme (Akten- und Dokumentenerfassung, Bibliotheken, Inventarisierung);
- weitere Anwendungen in Medizin/Chemie, für Menschen mit Aktivitätsbeschränkung, Gasbehälter (zur Füllstandskontrolle), Sportveranstaltungen, Implantate usw.



Quelle: www.schreiner-group.de

Anlagenverwaltung für Fraport

Die Fraport AG, Eigentümerin des Flughafens Frankfurt, betreut im Rahmen des Immobilien- und Facility-Managements rund 420 Gebäude und Anlagen. Eine zentrale Aufgabe ist die regelmäßige Instandhaltung und Kontrolle von technischen Komponenten mit gesetzlich vorgeschriebener Wartung.

Die Fraport AG nutzt RFID-Chips in Verbindung mit der Software *Mobile Asset Management* (mobile Anlagenverwaltung) von SAP, um Lüftungssysteme zu überwachen und zu warten. Mobile End-

geräte des Wartungspersonals speichern die täglichen Aufträge und erfassen die RFID-Tags an den Lüftungssystemen. Anschließend übermitteln sie die Ergebnisse der Wartungsarbeiten an das ERP-System. Die RFID-Chips gewährleisten in diesem Fall, dass jeder Abschnitt der Anlagen überprüft wird. Die per Funk übertragenen Daten bestätigen den Wartungsvorgang.

Fertigung in der Industrie

Vor allem die traditionell unter besonderem Kostendruck stehende Automobilindustrie hat in den letzten Jahrzehnten viele Produktionsschritte automatisiert, wie andere Unternehmen mit Massenfertigung auch. Allerdings müssen die Firmen heute in der Lage sein, *maßgeschneiderte* Produktvarianten herzustellen, um die gestiegenen Ansprüche der Verbraucher zu befriedigen – auch hier ist die Automobilindustrie Vorreiter. Viele Varianten eines Produkts werden auf der selben Fertigungslinie erstellt, was eine eindeutige Identifikation des zu bearbeitenden Objekts an jeder Fertigungsstation notwendig macht. Ein Steuerungssystem für die einzelnen Fertigungsstationen sorgt dann dafür, dass nur die diesem Objekt zugeordneten Schritte ausgeführt werden (im Falle der Automobilindustrie vielleicht eine Lackierung dieses speziellen Autos in Silbergrau).

RFID-Systeme reduzieren nicht nur die Kosten an den einzelnen Fertigungsstationen, sie haben viele weitere Vorteile gegenüber anderen Automatisierungskonzepten. So sind RFID-Systeme - im Gegensatz beispielsweise zu Barcodes - weitgehend unempfindlich gegenüber rauen Umgebungsbedingungen wie Schmutz, Staub oder Licht.

Elektronische Wegfahrsperre

Wegfahrsperren wurden Mitte der 1990er Jahre in Deutschland in großem Stil eingeführt, um die in den 90er Jahren sprunghaft angestiegenen Kfz-Diebstähle einzudämmen. Um das Kurzschließen des Zündschlosses (eine der verbreitetsten Diebstahlsmethoden) unmöglich zu machen, wird bei jedem Start des Motors die Echtheit des Zündschlüssels elektronisch geprüft. Dazu muss die Kommunikation zwischen Lesegerät im Fahrzeug und Tag

Quelle: www.baumerident.com

Quelle: www.foebud.org

Foto: Dina Kuznetsova

im Autoschlüssel verschlüsselt werden. Zum Einsatz kommen ausschließlich induktive Systeme, da hier keine Stützbatterie benötigt wird und die Systeme somit vollständig wartungsfrei sind.

ÖPNV

In den kommenden Jahren lässt die Verwendung von RFID-Technik im öffentlichen Personennahverkehr (ÖPNV) große Zuwächse erwarten.

Bis heute sind der klassische Fahrscheinverkauf und die zumindest stichpunktartigen Kontrollen der Fahrgäste mit hohen Kosten verbunden. RFID-Tags stellen eine billigere und zuverlässigere elektronische Variante dar, sie sind witterungsbeständig, langlebig und komfortabel (z.B. Abbuchung von der Karte, ohne sie aus dem Geldbeutel zu nehmen).

Bei Pre-paid-Systemen wird die Karte mit einem Geldbetrag geladen und vor oder nach jeder Fahrt ein entsprechender Betrag abgebucht, vergleichbar mit den Mensa-, bzw. Kantinenkarten vieler Universitäten oder Firmen (ein weiteres Beispiel für RFID-Anwendungen). Im Falle eines Abo-Systems würde bei der Einlasskontrolle überprüft, ob der Fahrgast im Besitz einer gültigen Karte ist, die wochen-, monats- oder jahresweise, aber auch in einem frei definierbaren Zeitraum gültig sein könnte. Beide Systemvarianten sind nebeneinander möglich.

Tierhaltung

In der Tierhaltung werden RFIDs schon seit längerem angewendet. So werden in *High-Tech-Kuhställen* automatisierte Fütterungsanlagen eingesetzt, bei denen der Fütterungsautomat für jedes Tier genau die vorgesehene Futtermenge ausgibt. Hat eine Kuh die vorgesehene Tagesration bereits gefressen, gibt der Fütterungsautomat einfach kein weiteres Futter aus. Umgekehrt lässt sich überwachen, ob eine Kuh zu wenig oder gar nicht frisst. Eine automatisierte Milchmengen-Statistik lässt sich in die Melkanlage integrieren.

In den letzten Jahren gibt es Bestrebungen in der Landwirtschaft, die RFID-Technologie auch zur betriebsübergreifenden Kennzeichnung der Tiere für die Seuchen- und Qualitätskontrolle sowie zur Herkunftsverfolgung einzusetzen.

RFID-Technik wird auch zur Haustieridentifizierung eingesetzt. Der *Tierpass* registriert alle durchgeführten Impfungen, und sollte ein Haustier verloren gehen, ist eine RFID-Erkennung sehr sinnvoll, da über die Registrierungsnummer der Besitzer schnell ermittelt werden kann. Darüber hinaus gibt es weitere Anwendungsmöglichkeiten, beispielsweise spezielle Katzen- oder

Hundetüren, die nur die eigene Katze oder den eigenen Hund ins Haus lassen. Eine automatische Fütterungsanlage ist auch für Kleintiere denkbar.

Tags zur Tierkennzeichnung haben teilweise nur die Größe eines Reiskorns und werden den Tieren mit einer Spritze unter die Haut injiziert.

RFID-Implantate

Ähnliche RFID-Tags in Form von kleinen Glaskapseln finden seit kurzem auch beim Menschen Anwendung. Die Tags können mittels einer Spritze unter örtlicher Betäubung innerhalb weniger Minuten unter die Haut implantiert werden. Sichere Zugangssysteme zu Computern oder Gebäuden sind bereits im Einsatz.

Aber auch in der Medizin eröffnen RFID-Implantate ein breites Anwendungsgebiet: Sie können zur Identifikation von Patienten dienen und so deren Verwechslung im Krankenhaus oder einer falschen Medikation (Art, Dosis, Zeit) vorbeugen. Von besondern Vorteil sind sie bei Patienten, die sich nicht verständlich machen können, wie Bewusstlosen oder Alzheimer-Kranken. Der Chip muss nicht implantiert werden, die beschriebene Funktionalität lässt sich auch durch einen Chip in Form eines Armbandes gewährleisten. Bei einer abnehmbaren Identifikationsquelle ist die Fehlermöglichkeit aber höher.

Die Autoren

Dipl.-Ing. Uwe Wissendheit hat an der Friedrich-Alexander-Universität (FAU) in Erlangen Elektrotechnik studiert und ist nach seiner Tätigkeit als Entwicklungsingenieur in der Abteilung für Hochfrequenztechnik am Fraunhofer Institut für Integrierte Schaltungen IIS in Erlangen jetzt wissenschaftlicher Mitarbeiter am Lehrstuhl für Informationstechnik der FAU Erlangen. Sein Promotionsthema behandelt die Lokalisierung induktiver Transponder. Mit dem Thema RFID befasst er sich seit 5-6 Jahren.

MSc. Dina Kuznetsova hat an der Staatlichen Universität Wladimir (Russland) Projektierung und Technologie der Radioelektronischen Geräte studiert und ist jetzt wissenschaftliche Mitarbeiterin am Lehrstuhl für Informationstechnik der FAU Erlangen. Ihr Promotionsthema ist die Modifikation von herkömmlichen RFID-Systemen zur Verbesserung der Eigenschaften (schnelleres Lesen/Schreiben, Erhöhung der Genauigkeit induktiver Identifikations- und Lokalisierungssysteme usw.). Mit dem Thema RFID befasst sie sich seit ca. 2,5 Jahren.

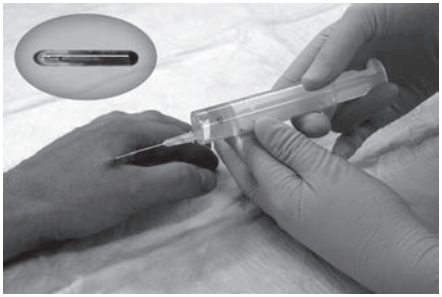


Foto: Uwe Wissendheit

RFID-Sensoren

Neben der reinen Identifikation können heutige Tags auch mit Sensoren verknüpft werden und somit einen ganz neuen Anwendungsbereich eröffnen. Sie werden hauptsächlich dort genutzt, wo man keine kabelgebundenen Sensoren einsetzen will oder kann. Dabei ist der entscheidende Vorteil von RFIDs im Vergleich zu anderen Funkübertragungsstandards wie *Bluetooth* oder *DECT*, dass der Sensor über das Feld der Datenkommunikation gleichzeitig seine Energie erhält, die Tags mit integrierten Sensoren also rein passiv sind.

Bei industriellen Anwendungen an beweglichen Teilen entfallen so die fehleranfälligen mechanischen Schleifkontakte. So lässt sich der Reifenfülldruck von Fahrzeugen messen oder die Temperatur ätzender Flüssigkeiten in der chemischen Industrie durch säurebeständige (glasgekapselte) RFID-Sensoren ermitteln.

Im Bereich der Logistik stattet man bereits Container mit Sensoren in RFID-Technik aus, um sensible Güter auf ihrem Weg zum Bestimmungsort zu überwachen. Die Messwerte wie Temperatur, Feuchtigkeit oder Erschütterungen werden meist im Tag zur späteren Auswertung gespeichert, um später beispielsweise die Einhaltung der Kühlkette bei Lebensmitteltransporten nachweisen zu können.

ePass

Der neue Reisepass mit biometrischen Verfahren ist heftig umstritten. Die biometrischen Daten werden digital kodiert auf einem RFID-Chip gespeichert, der sich in einem RFID-Inlay in der Passbuchdecke befindet. So soll es schwieriger werden, den Ausweis zu fälschen, und einfacher, bei Grenzkontrollen die Identität festzustellen. Durch die neue Technologie erhöhen sich die Kosten für den Reisepass von 26 € auf 59 €.

Das RFID-Inlay besteht aus einer Antennenspule und dem RFID-Chip, der von der Bundesdruckerei bei den Herstellern Philips (Typ SmartMX) oder Infineon (Typ 66CXLxxxP) bezogen wird und mit 72kB bzw. 64kB EEPROM zur Speicherung der biometrischen Daten ausgestattet ist. Die Chips haben einen kryptographischen Koprozessor, über den die Kommunikation zwischen Ausweis und Lesegerät verschlüsselt wird.

In der Ausbaustufe 1 enthält der ePass, der seit kurzem erhältlich ist, im RFID-Chip nur die personenbezogenen Daten und als einziges biometrisches Merkmal das Gesichtsbild, das im JPEG-Bildformat kodiert etwa 15kB des EEPROM-Speichers belegt. In der Ausbaustufe 2, die im März 2007 eingeführt werden soll, wird zusätzlich ein Fingerabdruck als biometrisches Merkmal

mit aufgenommen werden. Jedes Lesegerät muss durch das den Ausweis ausstellende Land zertifiziert werden. Dieses kann so bestimmen, welches Land welche Informationen aus dem Datenbereich des RFID-Chips auslesen darf.

Bibliothek der Zukunft

Auch für Bibliotheken wird RFID zunehmend interessanter, um die Effizienz zu steigern oder die Kosten zu reduzieren, bzw. neue Serviceleistungen für ihre Kunden anbieten zu können. Bedienung und Instandhaltung lassen sich automatisieren. Wenn Benutzer einen ganzen Bücherstapel auf eine Ablage legen und ein System automatisch sekundenschnell alle Bücher als ausgeliehen oder zurückgebracht verbucht, so steckt eine fortschrittliche Bibliothekstechnik dahinter, in der Regel in Form von RFID.

Die Unterstützung durch RFID für große und kleine Bibliotheken bietet neben einer Optimierung vor allem ein effizientes „Ressourcen-Management" zur Bewältigung der ständig steigenden Anforderungen an Beratung und Service. Mit dem BiblioChip™ System lassen sich (im Vergleich zum Barcode) bei der Ausleihe, bzw. der Rückgabe etwa 85% Arbeitszeit einsparen.

Quelle: www.schreiner-group.de

Neben einer Effizienzsteigerung geht beim Einsatz vom BiblioChips™ auch eine zentrale Mediensicherung mit den BiblioChips™ einher. Einfache Sicherungsschleusen an den Ausgängen prüfen, ob die Medien korrekt registriert wurden. Ist dies nicht der Fall, wird ein Alarmsignal ausgelöst.

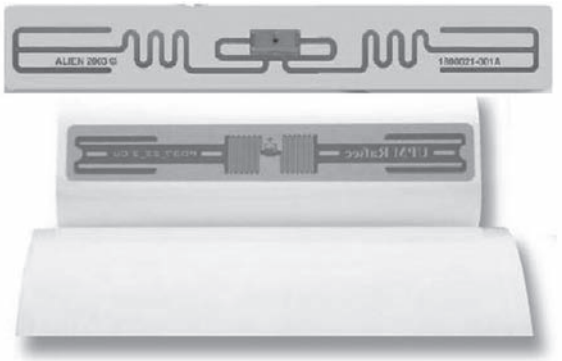
Ein weiterer großer Vorteil, der erst durch Technologien wie RFID ermöglicht wird, ist dass die Medien nicht nur lokal, sondern auch an vielen Orten in der Stadt an so genannten Rückgabeautomaten wieder abgegeben werden können.

RFID-Anwendungen morgen

Polymer-Technik

Als ICs *(Integrated Circuits)* auf Siliziumbasis ist die Herstellung von RFID-Tags zu teuer für den Einsatz bei Billigartikeln. Es bietet sich daher an, nach kostengünstigeren Herstellungsmethoden zu suchen. Ein möglicher Ansatz ist die Polymer-Technologie, die sich mit leitenden und halbleitenden Kunststoffen und deren Einsatz in der Elektronik beschäftigt. Schaltungen in Polymertechnik können mit herkömmlichen Druckverfahren produziert werden, sie halten wegen der Flexibilität der Kunststoffe hohen mechanischen Belastungen stand, sind billig und können auf nahezu beliebig geformte Oberflächen

aufgebracht werden. Zur Zeit sind die für die RFID-Tags in Polymerelektronik benötigten Technologien teilweise bereits entwickelt und es wird intensiv an der Umsetzung geforscht. Wegen der geringen Herstellungskosten sind auch Einweg-Tags vorstellbar.



Quelle: www.egomexico.com

Die Firma PolyIC aus Erlangen hat im Dezember 2005 einen komplett funktionierenden Tag (135 MHz) vorgestellt, der aus einem Chip in Polymertechnik und einer den IC umgebenden Antennenspule besteht. Anfang 2006 ist es ihnen gelungen, einen 1-Bit-Tag für 13,56 MHz zu entwickeln.

Sinnvolle Anwendungen für Polymertechnik sind auch Sensoren, Batterien und Displays. Sie lassen sich in Verpackungen integrieren, um damit relevante Informationen über ein Produkt auf einem ebenfalls integrierten Display anzuzeigen. Würde man zusätzlich einen Transponder integrieren, kann die Information auch auf einem PDA oder einem Handy dargestellt werden. Verbindungen von Polymerelektronik und RFID-Technik bieten also große Chancen in vielen Bereichen.

UHF-Transponder

Viele Firmen und Forschungseinrichtungen forschen an der Entwicklung von RFID-Systemen im UHF-Bereich um 900 MHz (Europa 865 - 870 MHz, USA 902 - 928 MHz, Japan 952 - 955 MHz). In diesem Frequenzbereich haben auch passive Tags deutlich größere Reichweiten, sie sind weniger störempfindlich, und die Datenübertragungsrate ist schneller als bei der 13,56 MHz-Technik. Es gibt aber auch einige Nachteile, die in der größeren Anfälligkeit für Reflektionen und der schlechteren Durchdringung von Medien, speziell bei Wasser, liegen.

Das Industriegremium *EPC Global* hat inzwischen die Testphase eines Standards (EPC Class1/Gen.2) für UHF-Transponder abgeschlossen, was die Interoperabilität dieser Transponder fördert.

Lokalisierung

Nahezu alle bisher am Markt angebotenen induktiven RFID-Systeme dienen der Identifizierung und Steuerung von Objekten, bzw. der Identifizierung von Lebewesen. Über die reine Identifizierung hinaus bietet eine zusätzliche Positions-, Richtungs- und Bewegungsermittlung eine erhebliche Erweiterung von RFID-Systemen, so dass damit auch völlig neue Anwendungsgebiete entstehen können. So kann damit ein Tag lokalisiert werden, der sich an einem Objekt in einer Flüssigkeit oder einem

anderen Medium befindet, das problematisch für Verfahren mit hochfrequenten elektromagnetischen Wellen ist (Backscatter-Verfahren/UHF-Tag).

Es ist allerdings nicht ganz einfach, die Lokalisierungsprinzipien praktisch umzusetzen, die Zusammenhänge magnetischer Wechselfelder und die geometrischen Beziehungen der sie erzeugenden Antennen sind komplex. Mitarbeiter am Lehrstuhl für Informationstechnik (LIKE) der Universität Erlangen-Nürnberg und am Institut für Elektrische Messtechnik und Grundlagen der Elektrotechnik (EMG) der TU Braunschweig können bereits erste erfolgreich abgeschlossene Forschungsergebnisse vorweisen.

Marktanalyse

Zum Abschluss noch eine Prognose von Soreon Research: Sie besagt, dass sich der europäische RFID-Markt im Sektor Handel und Handelslogistik von 400 Mio. Euro (2004) auf über 2,5 Mrd. Euro (2008) entwickeln wird (Abbildung 1). Laut dieser Analyse werden die RFID-Tags einen Anteil von rund 75% des gesamten RFID-Markts ausmachen. Trotz des schnellen Preisverfalls bei RFID-Tags sagt Soreon Research ein stabiles Marktwachstum über die nächsten fünf Jahre voraus und geht von einem deutlich überwiegenden Anteil an passiven Tags aus. Die Hersteller selbst prognostizieren eine Prozentverteilung von 71% zu 29% für passive Tags.

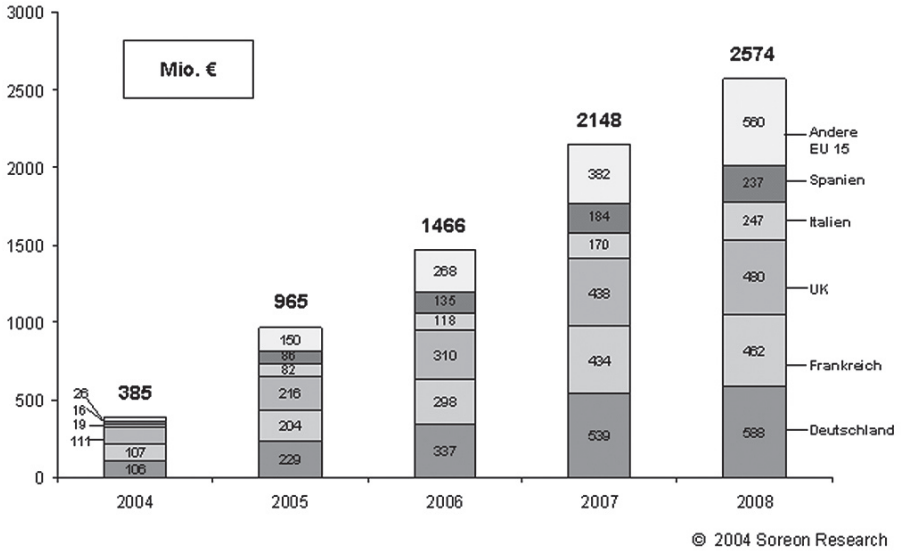


Abbildung 1: Gesamtmarkt RFID im Handel in Europa 2004-2008 (Soreon Research, http://www.soreon.de)

Literatur:

Finkenzeller, K.: RFID-Handbuch; 3. Auflage. Hanser Verlag, München, 2002.

White Paper RFID Technologie, Systeme und Anwendungen. BITKOM e.V., Berlin, August 2005.

SOREON Research GmbH: Enorme Wachstumsraten für RFID-Markt in Europa, Frankfurt a. M., Mai 2004.

Bundesamt für Sicherheit in der Informationstechnik: Digitale Sicherheitsmerkmale im ePass, Juni 2005, *http://www.bsi.bund.de/*.

Lindl, B.: RFID-Technology für die Bibliothek der Zukunft. B.I.T.online, Nr. 2-2004.

Hecker, K.: Organische Elektronik - Potential, Status, Herausforderungen. 2. Workshop RFID, Intelligente Funketiketten - Chancen und Herausforderungen, Erlangen, Juli 2006.

Wissendheit, U.; Kuznetsova, D.; Gerhäuser, H.: Lokalisierung und dynamische Antennensteuerung zur Verbesserung induktiver RFID-Systeme. 2. Workshop RFID, Intelligente Funketiketten - Chancen und Herausforderungen, Erlangen, Juli 2006.

OrganicID: White-Papers, *www.organicid.com*.

PolyIC: Printed electronics with Integrated Polymer Circuits, *www.polyic.de*.

VeriChip: Implantable RFID for the Health Industry. Juni 2005, *http://www.verichipcorp.com/*.

Siemens, Signaling and Control Systems: *http://www.siemens.com.vn/Marketplaces/Transportation/*.

Foto: Detlev Borchers

Sarah Spiekermann und Holger Ziekow

Technische Analyse RFID-bezogener Angstszenarien

Die Vorstellung einer Integration von Chips in alle uns umgebenden Objekte sowie die damit mögliche geräuschlose Kommunikation von Objekten untereinander rufen bei vielen Unbehagen hervor. So hat z.B. die Gesellschaft für Informatik eine Warnung vor der Technologie formuliert und einen Maßnahmenkatalog aufgestellt, „um die potentiellen Gefahren von Transpondern für die Bürger und die Gesellschaft auf ein Minimum zu reduzieren." *(Pohl 2004)*

Selbst industrienahe Studien belegen negative Reaktionen auf potenzielle Folgen der RFID-Technik. Dabei steht die Angst vor einem Verlust der Privatsphäre im Vordergrund und dominiert andere potenzielle Auswirkungen der Technologie auf Gesundheit und Arbeitsmarkt. Tabelle 1 fasst wesentliche wahrgenommene Ängste zusammen.

Im Folgenden werden einzelne Angriffszenarien diskutiert, die konkrete Ausprägungen der in Tabelle 1 beschriebenen Ängste darstellen.

Unautorisierte Erfassung von Besitz

Die Angst, dass Fremde unbemerkt Informationen über den eigenen Besitz erwerben könnten, ist der Furcht vor Überwachung zuzuordnen. Die fehlende Kontrolle über den Informationsfluss ist eine Einschränkung der informationellen Selbstbestimmung. Dritten wird potenziell der Besitz von Objekten wie Medikamente oder den Intimbereich betreffende Produkte bekannt.

Technisches Angriffsmodell

Für das Auslesen des auf einem Tag gespeicherten EPCs (Electronic Product Code) kann entweder der Tag direkt ausgelesen oder Kommunikation in der nachgelagerten IT-Infrastruktur abgehört werden.

Tag direkt auslesen: Für den Einsatz im Einzelhandel sind Tags der Klasse 1 vorgesehen. Diese Tags besitzen keine Mechanismen, um den Lesezugriff auf autorisierte Parteien zu beschränken. Die einzige

beim Lesen zu überwindende Hürde ist die Entfernung zum Tag. Der Frequenzbereich von 13.56 Megahertz war jahrelang ausreichend, funktioniert jedoch nur im Nahfeld des Lesegerätes (maximal 3,5 Meter). Für den praktischen Einsatz im Handel wird derzeit jedoch eine Kommunikationsfrequenz im Bereich von 865 bis 868 Megahertz vorgeschlagen, mit unter optimalen Bedingungen einer praktisch zu überwindenden Distanz von 6–8 Metern, bei der das unbemerkte Auslesen von Tags möglich wäre.

Nachgelagerte IT-Infrastruktur nutzen: In RFID Anwendungen werden Informationen von RFID Tags durch Reader ausgelesen und an nachgelagerte Anwendungen weitergeleitet, welche zum Teil über das Internet miteinander interagieren. Die dabei verwendeten Kommunikationskanäle weisen mitunter Schwachstellen auf. Beispielsweise werden EPC-Codes unverschlüsselt im Internet übermittelt, wenn der Object Name Service (ONS) zum Auffinden von objektbezogenen Informationen genutzt wird. Solche und ähnliche Schwachstellen könnten von Angreifern genutzt werden, um von Dritten ausgelesene EPC-Codes zu erfahren.

EPC interpretieren: Gelingt es einem Angreifer, die Identifikationsnummer (EPC) eines Tags auszulesen, muss er diese in-

Wahrgenommene Ängste	Beschreibung
Erfassen von Besitz	unbemerktes und ungewolltes Auslesen des persönlichen Besitzes durch Dritte
Tracking von Personen	Möglichkeit, dass Lesegeräte von Menschen unbemerkt auf Objekte zugreifen und auf diese Weise pseudonyme oder identifizierte Bewegungsprofile entstehen sowie Aufenthaltsorte von Personen kurz- und langfristig nachvollzogen werden
Erheben sozialer Netzwerke	automatisiertes Erheben von Beziehungen zwischen Menschen
unkontrollierbarer Technologie-Paternalismus	Möglichkeit, durch die Objekt-Erkennung der Technologie selbst kleinste Fehltritte systematisch und automatisch zu sanktionieren
langfristige objektbezogene Verantwortlichkeit	Angst vor einer eins-zu-eins Zuordnung von Personen zu ihren Objekten, die mit einem potenziellen Verantwortlich-Machen für den Missbrauch oder Verbleib von Objekten einhergeht

Tabelle 1: Auswahl RFID-bezogener Ängste in der öffentlichen Wahrnehmung

terpretieren können. Die Produktart (Objektklasse) ist im EPC kodiert, sein Aufbau ist öffentlich bekannt. Die Zuordnung des Nummernteils ist nicht in öffentlichen Listen gespeichert, derartige Listen könnten aber erstellt werden, indem die Nummern im Laden erhältlicher Produkte ausgelesen und gespeichert werden. Parteien mit Zugang zu im Aufbau befindlichen EPC Information Services könnten die Produktinformationen auch über diese Systeme erhalten.

Gegenmaßnahmen

Eine permanente Deaktivierung der Tags durch die vorgesehene Kill-Funktion würde die meisten Angriffszenarien unmöglich machen, weil deaktivierte Tags sich nicht auslesen lassen. Ein Nachteil der Kill-Funktion ist, dass wünschenswerte Anwendungen verhindert werden. Hier wäre vielleicht ein Passwortschutz oder ein Hash-Lock Verfahren sinnvoll, welche die volle Kontrolle über Tags in den Nutzerbereich verlagern würden. Möchten Kunden intelligente Dienste oder Heimanwendungen nutzen, oder Garantie- und Recycling-Ansprüche geltend machen, so würden sie an der Leseschnittstelle ein persönliches Passwort eingeben. Bezogen auf das Tracking könnten Kunden in Einkaufspassagen oder Läden am Eingang gefragt werden, ob sie eine Personalisierung der Leistung wünschen. Wenn ja, werden sie aufgefordert, sich zu authentifizieren und können die Leistung in Anspruch nehmen. Lehnen sie dies ab, so bleiben die eigenen Tags still.

Tracking von Personen

Tracking bezieht sich auf die Angst vor der Überwachung der eigenen Bewegung bzw. der langfristigen und unmittelbaren Nachvollziehbarkeit von Aufenthaltsorten. Allgemein kann man Tracking innerhalb eines Ladens, innerhalb einer städtischen

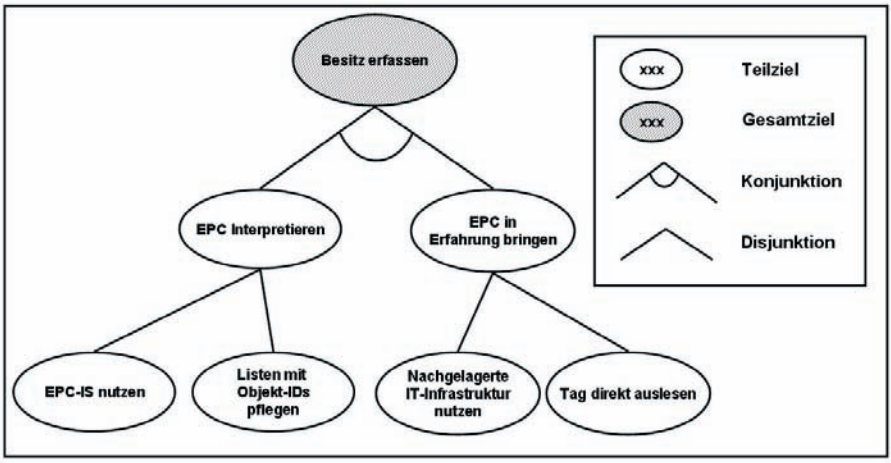
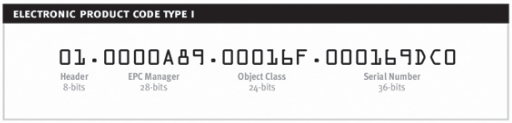


Abbildung 1: Abstrakter Attack-Tree für unautorisiertes Auslesen von RFID-Tags



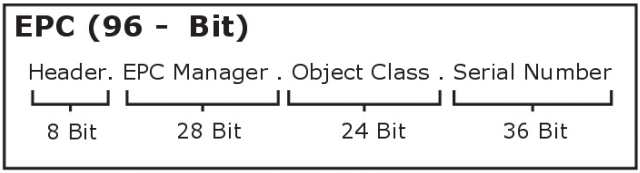


Abbildung 2: Aufbau des Electronic Product Code (Variante SGTIN-96)

Infrastruktur (z.B. einem Einkaufszentrum), in einer Region, oder überregional unterscheiden. Die räumliche Skalierung bezeichnet man als Granularität, von fein bis grob.

Technisches Angriffsmodell

Das Angriffsmodell ist in Abbildung 3 auf der nächsten Seite dargestellt.

Gegenmaßnahmen

Wenn Unternehmen über eigene Messpunkte verfügen, kann die Sammlung individueller Daten nur schwer durch technische Maßnahmen verhindert werden. Ebenso ist eine Verknüpfung mit Personendaten nur schwer einzudämmen. Alternativ zu einer freiwilligen Selbsteinschränkung könnte das Erheben von Bewegungsprofilen gesetzlich eingeschränkt werden.

Die Granularität der Readerdaten ließe sich reduzieren. Gäben die Reader (oder die dazu gehörige Middleware) standardmäßig nur zeitlich aggregierte Zeitstempel von Objekteinlesungen weiter, so würde ein Tracking zwar für logistische Zwecke noch ausreichen, ein Personen-Tracking jedoch einschränken. Ebenso möglich ist, dass Kunden ein Privacy-Profil anlegen (beispielsweise im Zusammenhang mit ihrer Kundenkarte), in dem sie bestimmen, welche Daten über sie erhoben werden dürfen. Vorschläge sind unter dem Begriff „Identitätsmanagement“ im E-Commerce Umfeld bereits häufig gemacht worden

Tracking-Vorhaben ohne eigene Messpunkte sind auf die Nutzung des EPC Netzwerks angewiesen. Durch restriktive Zugriffsrechte oder die Nichtweitergabe von lokalen Bewegungsprofilen kann die Bedrohung hier eingedämmt werden. Geht ein Objekt in den Besitz einer Privatperson über, sind auf dieses Objekt bezogene Daten stärker (vor unkontrolliertem Zugriff) zu schützen. Besitzer eines Objektes sollten darüber hinaus Einfluss auf die Festlegung der Zugriffsrechte haben.

Für die Zugriffsrechte sind Rollen, Attribute und Dienste zu definieren, für die der Zugriff eingeschränkt werden kann. Dabei ist darauf zu achten, dass Angreifer keine privilegierten Rollen erlangen können. Definiert man beispielsweise eine Rolle für in das Handelsregister eingetragene Firmen,

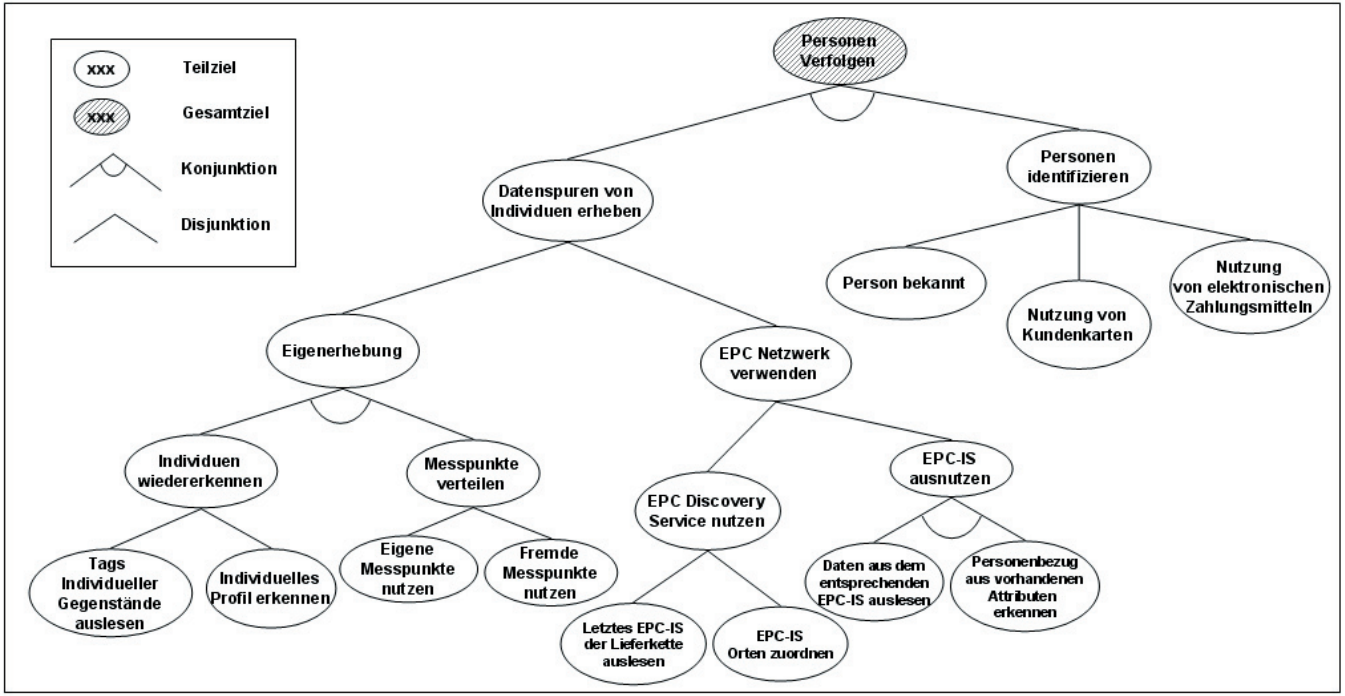


Abbildung 3: Abstrakter Attack-Tree zum Erstellen von Bewegungsprofilen

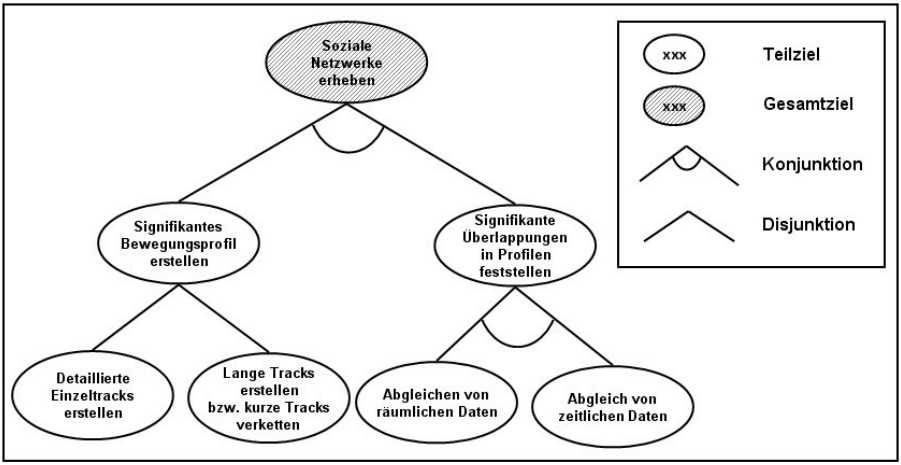


Abbildung 4: Abstrakter Attack-Tree zum Erheben sozialer Netzwerke

so ist zu bedenken, dass auch Privatpersonen mit geringem Aufwand (durch Gründung eines Gewerbes) diese Rolle einnehmen können.

Zur Eindämmung von Tracking-Ängsten muss der Zugriff auf Informationen darüber, wo sich ein Produkt wann befunden hat, beschränkt werden. Diese Informationen lassen sich aber zum Teil indirekt aus anderen Attributen gewinnen. Beispielsweise lässt sich der Zeitpunkt des Verkaufs auch durch ein Verfallsdatum oder das Herstellungsdatum eingrenzen.

Erheben sozialer Netzwerke

Hier geht es um das Szenario, dass Unbefugte oder Befugte prüfen können, wer mit wem wann und wo Kontakt hat. Dies kann insbesondere im Rahmen der Strafverfolgung oder Prävention, aber auch im Marketing oder aus persönlichen Motiven heraus von Interesse sein. Es ist nur für solche Instanzen sinnvoll, welche diese Assoziationen nicht leichter auf anderem Wege herstellen können, beispielsweise über soziale Verbindungen und direkte Beobachtungen.

Das Erheben sozialer Netzwerke fußt auf der Annahme, dass Personen, die wiederholt oder über längere Zeit gemeinsam unterwegs sind, eine soziale Verbindung zueinander haben. Dieser Angriff schließt also das Tracking ein.

Technisches Angriffsmodell

Das Modell ist der Abbildung 4 zu entnehmen.

Gegenmaßnahmen

In der Strafverfolgung oder Prävention sind die Bürger insbesondere vor Fehlern in der Erhebung sozialer Verbindungen zu schützen. Die Herausforderung besteht darin, keine falschen Schlüsse aufgrund von örtlichen Gemeinsamkeiten zu ziehen, sie könnten auch durch ähnliche Arbeitswege entstehen. Die Methode sollte in der

Strafverfolgung oder Prävention gesetzlich geregelt werden. Um ein solches Szenario generell abzuwenden, müssten objektbezogene Daten zur Erstellung von Tracks im Hinblick auf Ort, Zeit und Speicherfristen sparsam gespeichert werden.

Technologiepaternalismus

Geringfügige Fehltritte und ungewöhnliche Verhaltensweisen könnten durch Maschinen automatisiert erkannt, gemeldet oder sogar geahndet werden, wodurch ein Gefühl ständiger Kontrolle und Bevormundung entstehen könnte. Derartige Kontrollen gibt es schon jetzt, zum Beispiel Warnsignale beim unangeschnallten Autofahren. In Zukunft könnte ein Alarmsignal ertönen, falls Ware in ein falsches Regal zurückgestellt wird. Ähnlich könnte Fehlsortierung bei der Mülltrennung oder bei Veranstaltungen das unerwünschte Mitführen von Lebensmitteln überprüft werden. Einsparungen aus diesen Maßnahmen sind den Kosten gegenüberzustellen.

Technisches Angriffsmodell

Für diesen Angriff ist es notwendig, Fehlverhalten erstens automatisch festzustellen und zweitens zu ahnden. Bei gesetzlich

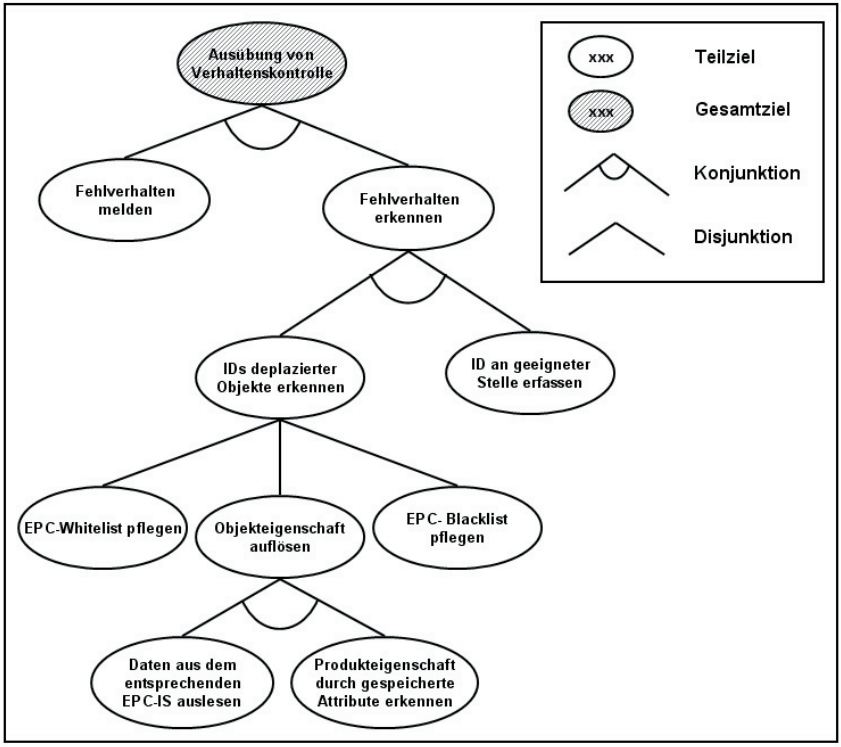


Abbildung 5: Abstrakter Attack-Tree für die Ausübung von Verhaltenskontrolle

nicht strafbarem Fehlverhalten würde die Ahndung ohne rechtliche Mittel erfolgen, beispielsweise durch Bloßstellung (Regale, die bei Fehlsortierung Warnsignale auslösen). Handelt es sich um gesetzlich erfasste Kleinstdelikte, könnten aber auch Strafzahlungen eingefordert werden.

Gegenmaßnahmen

Sind beim Angriff (zur Klassifikation von Objekten) Daten aus dem EPC Netzwerk notwendig, wären auf dieser Ebene technische Abwehrmaßnahmen denkbar. Zugriffsrechte auf objektbezogene Daten könnten stark eingeschränkt werden. Insbesondere wenn das Objekt einer Privatperson gehört, muss überlegt werden, inwieweit ein Zugriff auf diese Objektinformationen überhaupt noch rechtens ist. Zur Gewährleistung der informationellen Selbstbestimmung wäre es ferner wünschenswert, wenn diese Einschränkungen durch den Besitzer konfigurierbar wären. Derartige Beschränkungen sind jedoch ungeeignet, um staatlichen Zugriff zu verhindern. Viele Anwendungsfälle des Angriffs lassen sich über einfache Blacklists realisieren, Schutzmaßnahmen im EPC Netzwerk würden nicht greifen, weil gewisse Informationen, wie Hersteller und Objektklasse, bereits im EPC codiert sind. Die Zuordnung der Objektklassen zu realen Produkten ist zwar gegenwärtig nicht öffentlich bekannt, aber entsprechende Datenbanken befinden sich im Aufbau. Eine Alternative zur Abwehr dieser Angriffe ist, das Auslesen

Die Autoren

Sarah Spiekermann leitet das Berliner Forschungszentrum Internetökonomie an der Humboldt-Universität zu Berlin, Institut für Wirtschaftsinformatik. Sie lehrt dort zum Thema IT System Design. In ihrer Forschung beschäftigt sie sich seit vielen Jahren mit dem Thema Technikakzeptanz und insbesondere mit Fragen nach dem Erhalt von Privatsphäre im Internet.

Dipl.-Inf. Holger Ziekow promoviert aktuell am Institut für Wirtschaftsinformatik. Seine Forschungstätigkeit umfasst die Verarbeitung ubiquitärer Daten in Geschäftsanwendungen. Zuvor war er für SAP Research tätig, wo er Technologien für die SAP Smart Items Infrastruktur entwickelte.

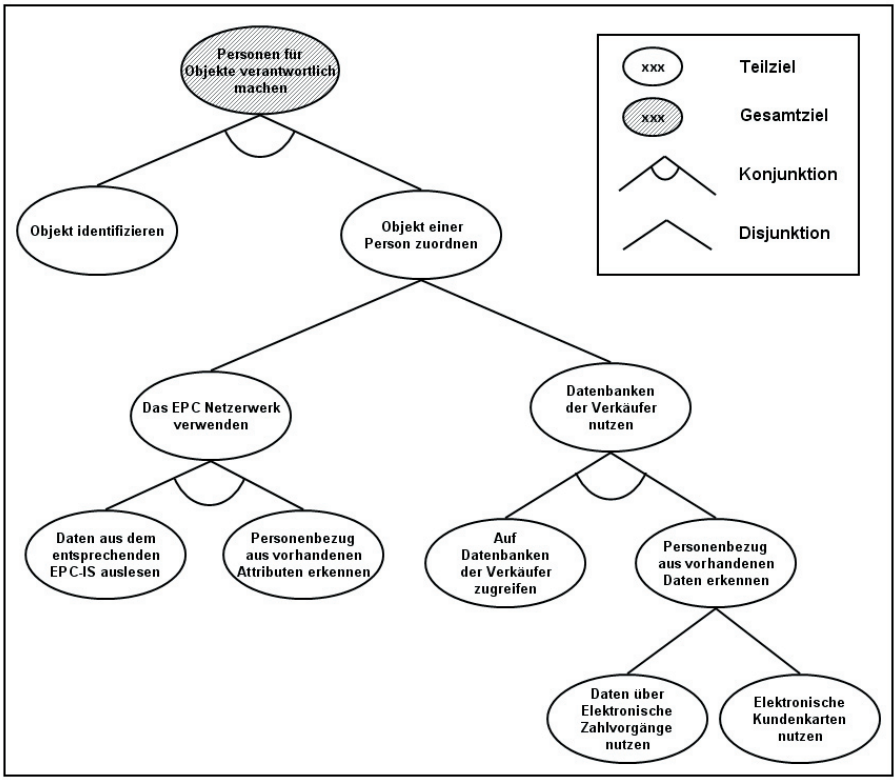


Abbildung 6: Abstrakter Attack-Tree für das Vorhaben, eine Person für ein Objekt verantwortlich zu machen

der RFID-Tags durch eine Abschirmung oder Deaktivierung zu verhindern.

Personen für Objekte verantwortlich machen

Die Möglichkeit, Objekte bestimmten Personen zuzuordnen, kann in mehreren Fällen von Interesse sein. Für den *Staat* ergeben sich über den hier diskutierten Angriff erweiterte Möglichkeiten für die Strafverfolgung oder Prävention. Werden an dem Schauplatz eines Verbrechens Gegenstände gefunden, sind damit in Verbindung zu bringende Personen grundsätzlich verdächtig oder könnten wichtige Zeugen sein.

Für *Betreiber öffentlich zugänglicher Anlagen* (Einkaufspassagen, Schwimmbädern oder Parkanlagen) entstehen Reinigungskosten für von Besuchern verursachte Verschmutzung. Um die Verantwortlichen zur Rechenschaft zu ziehen, müssten die in Abbildung 6 visualisierten Teilziele erreicht werden.

Foto: Detlef Borchers

eine Deaktivierung ohne Löschung abgewehrt werden.

Alternativ wäre der Angriff abzuwenden, indem die Verknüpfung von vollständigen EPCs mit Personendaten verhindert wird. Tritt der Staat als Angreifer auf, ist sein Zugriff möglicherweise rechtlich gesichert. Einschränkungen der Zugriffsrechte seitens der Datenbankbetreiber sind gegen diesen Angreifer somit wirkungslos. In diesem Fall können die Daten nur durch Verzicht auf die Speicherung geschützt werden. Zwar ist für die Abwicklung von Garantiefällen und Produktrückrufen eine Speicherung von Objekt-Personenbezug gewünscht, allerdings wäre zu diskutieren, wie lange und in welchem Präzisionsgrad eine Speicherung stattfinden kann und soll. Denkbar ist, dass der Seriennummernteil eines EPCs beim Verkauf eines Produktes nicht vollständig gespeichert wird.

Technisches Angriffsmodell

Das technische Angriffsmodell ist in Abbildung 6 dargestellt.

Gegenmaßnahmen

Um den Angriff abzuwehren, sind zwei Strategien denkbar. Einmal, das Auslesen von Objekt-IDs zu verhindern. Um auch mächtige Angreifer wie den Staat abzuwehren, muss dafür der Speicherinhalt auf dem Tag zerstört werden. Eine Deaktivierung des Chips mittels eines Passworts genügt nicht, da Laboratorien die Informationen dennoch auslesen könnten. Schwächere Angreifer (wie Betreiber öffentlicher Anlagen) könnten jedoch bereits durch

Anm. der Redaktion:

Dieser Beitrag ist die aktualisierte und stark gekürzte Version eines Texts, den Sarah Spiekermann und Holger Ziekow im November 2004 am Institut für Wirtschaftsinformatik, Humboldt-Universität zu Berlin, unter dem gleichen Titel publizierten. Den vollständigen Text finden Sie unter *http://interval.hu-berlin.de/rfid/*

Gabriele Spenger

RFID und Datenschutz

Kryptographische Methoden auf RFID-Systemen

Mit der zunehmenden Verbreitung von RFID-Systemen, die eine kontaktlose automatische Erfassung von Daten erlauben, wächst die Bedeutung von Datenschutz und Datensicherheit. Für sicherheitsrelevante Anwendungen können kryptographische Verfahren den Schutz der übertragenen Daten gewährleisten.
Die automatische Identifikation über Funk, die die Grundlage der RFID-Technik bildet, wurde erstmals 1940 im militärischen Bereich zur Unterscheidung eigener und feindlicher Flugzeuge eingesetzt. Harry Stockman beschrieb in seinem Paper Communications by Means of Reflected Power *[Sto48] einige Jahre später die Idee, reflektierende Energie in der Kommunikationstechnik zu nutzen. Mit der fortschreitenden Entwicklung der Mikroelektronik eröffnet die RFID-Technik heute ein weites Feld von Anwendungsszenarien. Während erste Anwendungen im zivilen Bereich bis Ende der 70er Jahre zunächst die Identifikation von Nutztieren ermöglichten, hat RFID in den letzten 35 Jahren fast unbemerkt Einzug ins tägliche Leben jedes Einzelnen gefunden.*

Die Einsatzmöglichkeiten werden einerseits von den technischen Gegebenheiten wie Speicherkapazität und Reichweite, andererseits vom damit verbundenen Kostenfaktor begrenzt. Ein Konsumgut von geringem Warenwert mit einem 20 Cent teueren Chip zu versehen, wäre beispielsweise nicht sinnvoll. In dem Paper *RFID Systems, Security and Privacy Implications* [SWE03] des MIT wurde eine Kostengrenze für Tags (auch *Transponder* genannt) von 5 Cent ermittelt, um eine Durchsetzung der RFID-Technik am Massenmarkt erreichen zu können. Voraussetzung für das Erreichen dieser geringen Stückkosten wäre jedoch die Verwendung einfachster Read-Only-Tags, modernster Technologien und Produktionsverfahren und ein sehr großes Produktionsvolumen. Die technische Möglichkeit, ein Produkt weltweit eindeutig zu identifizieren, birgt nicht nur Vorteile, sondern wirft gleichzeitig

die Frage nach Datenschutz und Datensicherheit auf. Kryptographische Verfahren bieten eine Möglichkeit zur Absicherung übertragener und gespeicherter Daten vor unbefugtem Zugriff, müssen jedoch unter Berücksichtigung der besonderen Eigenschaften von RFID-Systemen betrachtet werden.

Bedrohungsanalyse

Im Gegensatz zu anderen Systemen erfolgt bei RFID eine Identifikation ohne Berührung und ohne Sichtkontakt. Daher ist es notwendig zu analysieren, welche möglichen Angriffsarten auftreten können, um diese durch geeignete Schutzmechanismen zu verhindern.

- Abhören der Luftschnittstelle, um durch Wiedervorspielen der Daten einen echten Datenträger vorzutäuschen,
- unautorisiertes Auslesen des Datenträgers, um dessen Inhalt zu verändern oder zu duplizieren,
- Einbringen eines fremden Datenträgers in das Lesefeld, um Echtheit vorzutäuschen.

Das Ergebnis der Bedrohungsanalyse entscheidet über die Wahl eines geeigneten kryptographischen Verfahrens.

Kryptographische Verfahren

Bei RFID-Systemen ist insbesondere die Authentifizierung von Tags durch das Lesegerät und umgekehrt von Bedeutung. RFID-Systeme müssen beim Erfassen eines Tags dessen Identität überprüfen, um festzustellen, ob dieses Tag zur Teilnahme berechtigt ist. Eine weltweit eindeutige Regelung zur Vergabe der ID-Nummern (Seriennummern), wie es z. B. in Form des Electronic Product Code (EPC) vorgeschlagen wird, bietet einen gewissen Schutz vor gefälschten Tags. Damit kann das Auftauchen nicht vergebener Nummern oder von Duplikaten *(Cloning)* in manchen Anwendungsfällen erkannt werden. In den übrigen Fällen ist eine Authentifizierung notwendig

Ein einfaches Verfahren zur Authentifizierung des Lesegeräts gegenüber dem Tag ist der Passwortschutz. Das Passwort, das typischerweise eine Länge von 8, 24 oder 32 Bit besitzt, ist nur dem Lesegerät und dem Tag bekannt und wird zum Beginn der Datenübertragung an das Tag gesendet und von diesem überprüft. Stimmt es mit dem im Tag gespeicherten Passwort überein, gewährt dieses den Zugriff auf seine Daten. Dieser Zugriff kann sich bei aufwändigeren Systemen auf einzelne Speicherbereiche beziehen, so dass mittels einer Schlüsselhierarchie komplexere Sicherheitsmechanismen realisiert werden können. Da das Passwort bei jeder Authentifizierung über die Luftschnittstelle übertragen wird, kann ein Angreifer es abhören und dadurch auf die Daten des Tags zugreifen. Abhilfe schafft die Verwendung variabler Passworte, die sich nach jeder Authentifizierung ändern. Dies setzt ein beschreibbares Tag voraus. In einer Anwendung, in der nur eine beschränkte Anzahl von Zugriffen auf das Tag erforderlich ist, kann hierzu eine Liste von Einmalpasswörtern eingesetzt werden, die dem Tag und dem Lesegerät bekannt sein muss. Beispiele für solche Anwendungen mit beschränkter Zugriffszahl wären Ein-

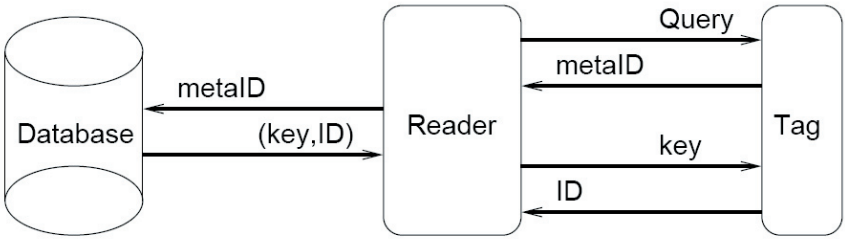


Abbildung 1: Hash-Lock-Verfahren

trittskarten zu Fußballspielen oder Konzertabonnements.

Ein Authentifizierungsverfahren, das eine größere Sicherheit gegen unautorisiertes Auslesen bietet, ist das *Hash-Lock*-Verfahren (Abb. 1). Bei diesem Verfahren werden so genannte Einwegfunktionen eingesetzt, die sich mit geringem Aufwand berechnen, jedoch nur mit sehr hohem Aufwand umkehren lassen. Vor dem erstmaligen Beschreiben des Tags wird ein Paar erzeugt und im Lesegerät gespeichert, das aus einem Schlüssel und dem dazugehörigen so genannten Hash besteht, der mittels der Einwegfunktion berechnet wird. Dieser Hash, der im Zusammenhang mit dem Hash-Lock-Verfahren auch als *metaID* bezeichnet wird, wird zusätzlich im Tag gespeichert. Bei der Authentifizierung überträgt zunächst das Tag den Hash an das Lesegerät. Dieses sucht in seiner Datenbank den dazugehörigen Schlüssel und überträgt diesen an das Tag. Das Tag berechnet mittels der Einwegfunktion einen Hashwert aus dem empfangenen Schlüssel und vergleicht ihn mit dem gespeicherten Hash. Stimmen sie überein, wird der Zugriff auf die Daten gewährt. Das Hash-Lock-Verfahren ist für viele Anwendungen als Schutz ausreichend, erfordert jedoch die Fähigkeit des Tags, die Einwegfunktion zu berechnen. Damit ist das Tag aufwändiger und teurer als ein Tag, das nur einen einfachen Passwortschutz bietet. Da außerdem der zum Hash gehörige Schlüs-

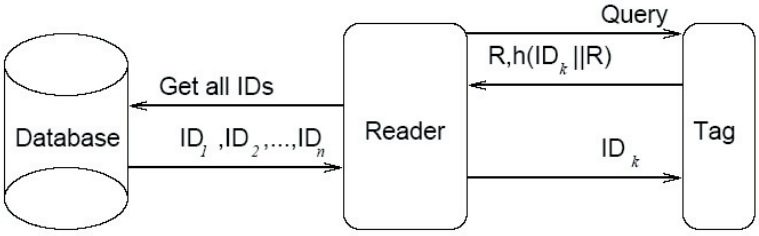


Abbildung 2: Randomized Hash-Lock-Verfahren

Abbildung 3: Challenge-Response-Verfahren

sel während der Übertragung über die Luftschnittstelle ausgespäht werden kann, kann damit später dem Tag ein autorisiertes Lesegerät vorgetäuscht werden.

Die Sicherheit lässt sich durch das *Randomized Hash-Lock*-Verfahren (Abb. 2) verbessern. Hierbei sendet das Lesegerät eine Anfrage an das Tag. Anschließend generiert das Tag eine Zufallszahl, die dann an das Lesegerät gesendet wird. Lesegerät und Tag berechnen unabhängig voneinander mittels der Einwegfunktion einen Hash aus dieser Zufallszahl. Das Lesegerät sendet den resultierenden Hash an das Tag. Stimmen die beiden Hashwerte überein, wird Zugriff auf die Daten gewährt. Dadurch, dass der Hashwert sich bei jeder Authentifizierung abhängig von der verwendeten Zufallszahl ändert, ist das Ausspähen sinnlos [BSI04]. Der Aufwand und die damit verbundenen Kosten für das Tag sind höher als beim einfachen Hash-Lock-Verfahren, da das Tag die Fähigkeit haben muss, Zufallszahlen zu berechnen.

Bei Anwendungen, die größte Sicherheit erfordern, kommen Authentifizierungsverfahren mit Verschlüsselung nach dem *Challenge-Response*-Prinzip (Abb. 3) zum Einsatz. Voraussetzung hierfür ist die Fähigkeit des Tags kryptographische Algorithmen zu berechnen. In der ISO-Norm 9798 werden verschiedene Challenge-Response-Verfahren für eine starke Authentifizierung bei kontaktbehafteten Chipkarten und RFID-Systemen definiert, darunter auch die gegenseitige Authentifizierung nach dem *Three-pass mutual authentication protocol*.

Auf ein *get_challenge* Kommando des Lesegeräts hin generiert das angesprochenen Tag eine Zufallszahl A und sendet diese an das Lesegerät. Das Lesegerät generiert ebenfalls eine Zufallszahl B und erzeugt mit dieser und der Zufallszahl A auf Basis eines Verschlüsselungsalgorithmus und eines geheimen Schlüssels K einen verschlüsselten Datenblock (Token T) und sendet ihn an das Tag. Da beide Seiten den gleichen Verschlüsselungsalgorithmus verwenden und der Schlüssel K auf dem Tag gespeichert ist, kann das Tag den Token T entschlüsseln. Stimmen die ursprüngliche und die nun entschlüsselte Zufallszahl A und A' überein, ist die Authentizität des Lesegeräts bewiesen. Die Prozedur wird nun zur Authentifizierung des Tags gegenüber dem Lesegerät wie-

derholt, indem im Tag ein zweites Token S erzeugt wird. Bei Übereinstimmung der entschlüsselten Zufallszahlen B und B' ist auch die Authentizität des Tags gegenüber dem Lesegerät bewiesen. Da bei diesem Verfahren niemals geheime Schlüssel, sondern nur verschlüsselte Zufallszahlen über die unsichere Luftschnittstelle übertragen werden, ist ein hoher Grad an Sicherheit gegenüber unauthorisiertem Zugriff gegeben. Auch durch Aufzeichnen und späteres Wiedervorspielen der Initialisierungssequenz *(Replay-Attack)* kann kein Zugriff auf das Tag oder das Lesegerät erreicht werden [BSI04].

Tags, die die Authentifizierung nach dem *Challenge-Reponse*-Prinzip ermöglichen, sind die aufwändigsten und teuersten. Neben der Berechnung von Zufallszahlen müssen sie starke Verschlüsselungsalgorithmen berechnen können. Dies ist nur mittels eines leistungsstarken Hauptprozessors oder durch die Verwendung kryptographischer Koprozessoren möglich. Dadurch wird der Preis eines einzelnen Tags in den Bereich von mehreren Euros hochgetrieben und macht damit eine Durchsetzung am Massenmarkt unmöglich. Einsatz finden solche Tags daher nicht zur Kennzeichnung von Waren, sondern beispielsweise bei Zutrittssystemen.

Datensicherheit in der Praxis

Um die Chancen von RFID zu nutzen und gleichzeitig die Bedrohung für die Persönlichkeitsphäre des Einzelnen so gering wie

Gabriele Sprenger

Nach dem Abschluss ihres Mathematikstudiums an der Friedrich-Alexander-Universität Erlangen-Nürnberg im Jahr 1998 arbeitete Gabriele Spenger einige Jahre als wissenschaftliche Mitarbeiterin in der Audioabteilung des Fraunhofer Instituts für Integrierte Schaltungen in Erlangen. Anschließend war sie 3 Jahre als Assistentin am Lehrstuhl für Informationstechnik mit dem Schwerpunkt Kommunikationselektronik der Universität Erlangen-Nürnberg tätig. Zurzeit ist sie bei Philips Semiconductors in Nürnberg beschäftigt und promoviert über das Thema *Kryptographische Verfahren auf RFID-Systemen*.

möglich zu halten, müssen Grundsätze eines zeitgemäßen Datenschutzrechts in RFID-Systemen bereits frühzeitig im Design-Prozess und in der Markteinführung umgesetzt werden [BSI04].

Mit Hilfe von kryptographischen Verfahren können Daten verschlüsselt und somit vor dem Zugriff unberechtigter Dritter geschützt werden. Trotz kryptographischer Verfahren kann eine 100 % Sicherheit nicht garantiert werden, weil die Möglichkeit von Seitenangriffen besteht, die für jedes Anwendungsfeld individuell geprüft werden muss. Unter Seitenangriffen versteht man Angriffe, die nicht auf Schwächen der kryptographischen Verfahren basieren, sondern auf Sicherheitslücken in anderen Teilen des Gesamtsystems. Beispiele hierfür sind leicht zu erratende Passwörter, oder die Übertragung der Daten nach der Entschlüsselung über einen ungesicherten Kanal. Weiterhin erfordern kryptographische Verfahren mit ansteigender Sicherheit und der damit verbundenen Komplexität gleichzeitig höhere technische Voraussetzungen. Dies führt zu einem Anstieg der Tag-Kosten. Im Zuge der Durchsetzung von RFID-Systemen auf dem Massenmarkt besteht gleichzeitig ein hoher Kostendruck. Er darf nicht dazu führen, dass die Datenschutzaspekte dieser Technologie außer Acht gelassen werden.

Literatur

[BSI04] Bundesamt für Sicherheit in der Informationstechnik; Risiken und Chancen des Einsatzes von RFID-Systemen, SecuMedia Verlags-GmbH, Bonn 2004

[Sto48] Harry Stockman; Communication by Means of Reflected Power Proceedings of the IRE, pp1196-1204, October 1948

[SWE03] Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels; RFID Systems, Security and Privacy Implications in Kaliski, B.S./Koc, C.K./Paar, C. (Eds.): Cryptographic Hardware and Embedded Systems - CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13-15. Revised Papers. Springer LNCS, Vol. 2523/2003, 454-469

Bilderverzeichnis

Abbildung 1: [Wei03] Weis, Stephen August; Security and Privacy in Radio-Frequency Identification Devices, Master Thesis at the Massachusetts Institute of Technology, May 2003

Abbildung 2: [Wei03] Weis, Stephen August; Security and Privacy in Radio-Frequency Identification Devices, Master Thesis at the Massachusetts Institute of Technology, May 2003

Abbildung 3: [FrSt04] Frey, H. und Strum, P. (Universität Trier); UBICOMP Episode 14, http://www.syssoft.uni-trier.de/systemsoftware/Download/Sommersemester_2004/Vorlesung/Ubiquitous_Computing/14%20RFID.pdf

Rena Tangens

RFID in der Kritik

Von interessierter Wirtschaftsseite wird es oft so dargestellt, dass Kritik an RFID grundsätzliche Technologiekritik wäre oder gar irrationale Angst vor neuer Technik. Diese Darstellung ist falsch – und am Beispiel des FoeBuD *lässt sich das auch gut belegen, denn Technikfeindlichkeit kann man dieser Organisation beim besten Willen nicht nachsagen. Die Aktiven im FoeBuD haben schon seit 1987 mit neuester Technik gearbeitet, kreativ ihre Grenzen ausgelotet und Technik auch aktiv mitgestaltet.*

RFID – eine Gefährdung der Privatsphäre mit neuer Qualität

Mit RFID – seinerzeit noch Transponder-Technik genannt – hatte sich der FoeBuD bereits ein paar Jahre auseinandergesetzt, bevor die Metro mit ihrem *Future Store* in Rheinberg bei Düsseldorf Furore machte. Und bei aller Technik-Faszination lagen für den FoeBuD die kritischen Punkte auf der Hand.

- Jede Ware, jedes einzelne Objekt erhält mit RFID eine weltweit eindeutige Seriennummer (anders als beim Strichcode, der nur die Warengruppe bezeichnet).
- RFID-Chips können berührungslos aus der Entfernung gelesen werden (auch ohne Sichtkontakt).
- Durch Registrierung und Tracking der RFID-Chips werden neue große Datensammlungen erzeugt.
- Die Seriennummer und die Information auf dem RFID-Chip sind nur scheinbar produktbezogen und anonym. Tatsächlich können sie an vielen Stellen mit persönlichen Daten der Besitzer/-innen verknüpft werden.

- Neue Datenbanken mit den RFID-Chip-Seriennummern und verknüpften Informationen bieten schnellen Zugang zu großen Mengen an personenbeziehbaren Daten.
- RFID-Chips und RFID-Scanner können versteckt angebracht sein.
- Ohne dass sie es bemerken, können Bürger/-innen gescannt werden, ob sie RFID-Chips mit sich führen.
- Die Leseentfernung lässt sich unter anderem vergrößern durch Erhöhung der Sendeleistung der RFID-Scanner und durch Abschalten von Sicherheitsfeatures.
- RFID ermöglichen nicht nur Konsumprofile wie Kundenkarten schon jetzt, sondern zusätzlich detaillierte Bewegungs-, Interessen- und Kontaktprofile.

Welche Folgen hat das?

- Es entsteht die Gefahr der Überwachung.
- Tracking wird möglich durch RFID in Kleidung, Ausweispapieren, Bargeld etc.
- Gezielte Manipulation wird möglich, z.B. durch Nutzen der Informationen, die durch Speicherung des Bewegungs- und Interessenprofils gewonnenen werden.
- Gezielte Diskriminierung wird möglich, z.B. Preisdiskriminierung. Das heißt: unterschiedliche Preise für unterschiedliche Menschen für dieselbe Ware im selben Supermarkt. Günstige Angebote gelten nur für profitable, wohlhabende Kunden, die außerdem per Kundenkarte bereit sind, ihre Privatsphäre preiszugeben. Das ist unsozial.

Um einige Gefahren zu verdeutlichen, muss ein wenig in die Zukunft geschaut werden - wie wir es für die Big Brother Award-Laudatio anno 2003 getan haben. (Vollständiger Text: *www.bigbrotherawards.de/2003/.cop/*). Einige der Zukunftsszenarien sind mittlerweile sehr bekannt und viel zitiert worden. Zum Beispiel dieses hier:

November 2004

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.

Dieses Szenario hat anschaulich gemacht, was eine RFID-Kennzeichnung von Einzelprodukten bewirken kann: Jedes einzelne Produkt könnte durch die Registrierung beim Einkauf einem Menschen zugeordnet werden. Und das kann weit unangenehmere Folgen als 10 Euro Bußgeld haben.

Aber auch für Arbeitnehmer/-innen könnte die Einführung von RFID zu unangenehmen Überraschungen führen:

Juni 200?

Als Supermarkt-Fachkraft Gerd J. abends nach Hause kommt, liegt dort ein Brief seiner Geschäftsleitung mit einer Abmahnung. Er sei in den vergangenen Wochen durchschnittlich 9 Mal auf der Toilette gewesen und habe dort pro Tag ca. 72 Minuten zugebracht. Das liege 27 Minuten über dem Soll und

diese Zeit werde ihm zukünftig von seinem Arbeitszeitkonto abgezogen. Entsetzt sucht er seinen Supermarkt-Kittel ab und findet einen RFID im Kragensaum.

Arbeitskleidung mit integrierten RFID-Chips und Seifenspender, die anhand des Chips kontrollieren, ob sich jemand die Hände gewaschen hat, sind in den USA bereits Realität.

Forderungen zu RFID

- Wichtigster Grundsatz: Datenvermeidung und Datensparsamkeit. Daten, die nicht notwendig sind, dürfen gar nicht erst erfasst werden. Und: Es sollen so wenig wie möglich persönliche Daten erhoben, gespeichert und verarbeitet werden.

- Transparenz. Das heißt: Sowohl RFID-Chips als auch RFID-Scanner müssen, wo immer sie sind, deutlich sichtbar mit einem Warnhinweis gekennzeichnet werden.

- Datenschutz muss Standard sein. Das bedeutet, Opt-Out-Lösungen, wo die Kundinnen erst tätig werden müssen, um ihre Privatsphäre zu schützen, sind nicht akzeptabel. So zum Beispiel der sogenannte Deaktivator im Future Store – der ist definitiv keine Lösung. Bislang müssen sich Kundinnen und Kunden noch einmal neu anstellen,

Rena Tangens

Rena Tangens ist Künstlerin, Publizistin und Netzpionierin aus Bielefeld. 1984 gründete sie gemeinsam mit padeluun das Kunstprojekt „Art d'Ameublement", 1987 den FoeBuD e.V. Seit 1987 ist sie Veranstalterin der monatlichen Kultur- und Technologie-Reihe ‚PUBLIC DOMAIN'. Ab 1989 Aufbau der elektronischen Bürgernetze Z-NETZ und /CL in Deutschland sowie des Zamir Transnational Network in Ex-Jugoslawien. Seit 2000 recherchiert und organisiert sie die jährlichen deutschen Big Brother Awards. Als Expertin für RFID und Datenschutz berät sie Verbände, Ministerien und EU-Kommission und ist unterwegs als Vortragsreisende in Sachen Kunst und Technik, Datenschutz, Bürgerrechte und Demokratie.

Kontakt: FoeBuD e.V. & Big Brother Awards Deutschland
Marktstr. 18
D-33602 Bielefeld
Tel: +49-521-175254 Fax: +49-521-61172
Mail: *mail@foebud.org*
Web: *www.foebud.org*, *www.bigbrotherawards.de*, *www.stoprfid.de*

nachdem sie die Kasse passiert haben, und jedes einzelne Produkt auf den Deaktivator stellen, um den auf dem RFID-Chip gespeicherten Nummerncode mit Nullen zu überschreiben. Solche Opt-Out-Lösungen haben lediglich Alibifunktion. Außerdem bleibt bei diesem Verfahren die weltweit einmalige Seriennummer jedes Artikels erhalten und kann weiter verarbeitet werden.

- Das Tracking von Personen ist völlig abzulehnen, sowohl direkt als auch indirekt. Die RFID-Industrie argumentiert oft, dass die Nummern auf den RFID-Chips „nicht personenbezogen" seien, sondern nur Informationen zum Produkt enthalten würden. Dies stimmt aber nur auf den ersten Blick. Sobald nämlich auch nur an *einer einzigen* Stelle – z.B. durch das Zahlen mit Kredit- oder EC-Karte oder das Registrieren-Lassen einer Kundenkarte – die Verbindung von einem dieser RFID-Chips zu einer Person hergestellt werden kann, können auch die Informationen aller anderen RFID-Chips, die diese Person trägt, mit ihren persönlichen Daten verknüpft werden. Mit anderen Worten: Die Daten auf den RFID-Chips sind *personenbeziehbar*. Wenn RFID-Chips auf Einzelprodukt-Ebene eingeführt würden, trügen Bürgerinnen und Bürger aus der Ferne identifizierbare Dinge bei sich und könnten niemals sicher sein, ob nicht doch eine Verknüpfung dieser Produktdaten mit ihren persönlichen Daten geschieht und damit z.B. Bewegungs- und Interessenprofile von ihnen erstellt werden können.

- Keine RFID-Chips auf Einzelprodukten (*item level*).

- Keine RFID-Chips auf Produkten in auch von Kund-innen genutzten Räumen, also zum Beispiel in den Verkaufsräumen. Wenn RFID-Technik in der Logistik bis hin zu den Lagerräumen zum Einsatz kommt, ist das zunächst kein Problem für die Verbraucherinnen und Verbraucher (möglicherweise aber für die Arbeitnehmer/-innen!).

- Keine RFID-Chips in Bargeld. Es muss auch in Zukunft möglich sein etwas zu bezahlen, ohne eine Datenspur zu hinterlassen.

- Keine RFID-Chips in Reisepässen, Personalausweisen oder sonstigen Ausweisdokumenten. Wenn Bürger nicht sicher sein können, ob sie ohne ihr Wissen jederzeit und überall identifiziert werden können, werden sie in Zukunft möglicherweise zögern, ihr Recht auf freie Meinungsäußerung

oder Versammlungsfreiheit wahrzunehmen. So stirbt Demokratie, sagte schon das Bundesverfassungsgericht in seinem Volkszählungsurteil *(http://www.foebud.org/video/volkszaehlungsurteil*).

Fazit

Wir brauchen datenschutzfreundliche Technik (Privacy Enhancing Technologies)

Wenn eine technische Infrastruktur erst einmal in einer bestimmten Form allgemein installiert ist, kann sie kaum noch geändert werden. Wenn die Technik nicht von vornherein so gestaltet ist, dass sie Missbrauch schwer oder unmöglich macht, wird er früher oder später passieren – legal oder illegal. Mit der RFID-Technik kann auch etwas anderes passieren: Wenn die Verbraucher/-innen die möglichen negativen Konsequenzen der Technik erst einmal kennen und merken, dass ihre Interessen ignoriert und ihre Besorgnis nicht ernstgenommen wird, dann werden sie die RFID-Technik nicht annehmen, sondern boykottieren. Späteres Nachbessern an der Technik wird teuer und kann den Schaden kaum wieder gutmachen.

Wir brauchen Gesetze, die den neuen Gefährdungen wirksam begegnen

Die RFID-Industrie und ihre Lobbyverbände bemühen sich intensiv, eine gesetzliche Regulierung von RFID abzuwehren, indem sie sogenannte *Selbstverpflichtungserklärungen* propagieren. Diese sollten jedoch zutreffender *unverbindliche Absichtserklärungen* genannt werden. Es leuchtet nicht ein, warum Firmen, die stets beteuern, nichts Böses mit den gewonnenen Daten machen zu wollen, Angst vor einer gesetzlichen Regulierung haben. Denn eine gesetzliche Regulierung würde die *good guys* schützen, also die Firmen, die die Privatsphäre der Bürger tatsächlich achten, – und zwar sowohl vor der böswilligen Konkurrenz als auch vor ihren eigenen Aktionären.

Wenn einige Firmen meinen, sie könnten die RFID-Einführung wie geplant durchziehen und müssten nun – angesichts der wachsenden Abneigung der Öffentlichkeit gegen eine Allgegenwart von Schnüffelchips – lediglich etwas mehr in Lobbyarbeit, Marketing und Public Relations investieren, um kritische Stimmen platt zu machen – dann unterliegen sie einem gefährlichen Irrtum. Wir haben zur Zeit die einmalige Chance, bei der RFID-Technologie die Richtung mit zu bestimmen. Wir müssen uns entscheiden, ob wir z8i für eine Kontrollgesellschaft oder für eine lebenswerte Welt arbeiten.

L. Humbert, J. Koubek, A. Pasternak, H. Puhlmann

Informatische Allgemeinbildung und RFID

Der Institution Schule wird in modernen Industriegesellschaften eine Verantwortung für gesellschaftliche Entwicklungen zugewiesen. Soll das Subsystem Schule dieser Anforderung gerecht werden, braucht es einen Informatikunterricht, der Aspekte des gesellschaftlich wirksamen Einsatzes von Informatiksystemen auf einer fachlichen Grundlage thematisiert - ein Pflichtfach Informatik in allen Schulstufen und Schulformen. Der Beitrag versteht sich als Plädoyer für das Pflichtfach Informatik und für eine Durchführung des Informatikunterrichts, die gesellschaftlich virulente Inhalte einbezieht. Damit werden andere Fächer nicht aus ihrer Verantwortung entlassen – im Gegenteil: sie müssen sich auf die durch das Pflichtfach Informatik aufgebaute Fach- und Sachkompetenz der Schülerinnen als Grundlage für ihre fachbezogenen Betrachtungsweisen verlassen können.
In diesem Beitrag wird für geschlechtsbezogene Bezeichnungen das generische Femininum verwendet. Männer mögen sich auch angesprochen fühlen.

Informatische Allgemeinbildung

In diesem Beitrag geht es uns darum, wie Informatische Allgemeinbildung so gestaltet werden kann, dass sie sich mit bekannten Instrumenten qualitativ und vor allem auch quantitativ analysieren lässt.

Um die erfolgreiche Bewältigung fachlich orientierter Fragestellungen aus der Informatik zu zeigen (und zu evaluieren), lassen sich drei Dimensionen in Form von Kompetenzklassen ausweisen (Abbildung 1, Kompetenzklassen). Bekannte und verbreitete Konzepte des Informatikunterrichts verweisen in ihrer Präambel immer auf die Entscheidungskompetenz, empfehlen dann aber einen Unterricht, der auf der Anwendung oder bestenfalls auf rudimentären Anteilen von Gestaltung gründet. Um Entscheidungskompetenz einzulösen, ist für alle Schülerinnen ein Informatikunterricht einzufordern, der zwar die Anwendung nicht außer Acht lässt, aber einen deutlichen Schwerpunkt bei der Gestaltung setzt, um damit die notwendi-

1. **Anwendung** – Anwenden von Informatiksystemen
2. **Gestaltung** – Gestalten von Informatiksystemen; verweist auf die Informatische Modellierung – verstanden als Prozess und Kenntnis der Möglichkeiten, diesen Prozess umzusetzen – umfasst neben der Analyse auch die konkrete Implementierung und Test
3. **Entscheidung** – Entscheiden über den verantwortungsvollen Einsatz und die Entwicklung von Informatiksystemen

Abbildung 1: Kompetenzklassen [Puhlmann2003, S. 148]

gen Voraussetzungen auf einer fachlich ausgewiesenen Basis zu schaffen.

Daher wird seit einigen Jahren an Standards für die Informatische Allgemeinbildung gearbeitet. In Tabelle 1 sind zeilenweise Inhaltsbereiche des Informatikunterrichts ausgewiesen, die sich für Standards als tragfähig herausgebildet haben. Die Bezeichnung der prozessorientierten Zieldimensionen werden noch diskutiert, wir beschäftigen uns im Folgenden mit den Inhalten.

Informatische Phänomene

Wir verwenden den Begriff *Informatische Literalität* als Entsprechung für den angelsächsischen Begriff *Literacy*. Bildungsbemühungen im Schulfach Informatik sollten aus unserer Sicht informatische Literalität als ausweisbaren Baustein der Informatischen Allgemeinbildung verankern. Ein Strukturierungsmittel dazu sind die oben vorgestellten Kompetenzklassen, aber wir können auch die Sichtweise von OECD/PISA einnehmen: Die Kompetenzen müssen für die individuelle Welterklärung und

	Prozess					
Inhalt (Band)	Informatisches Problemlösen	Begründen Bewerten	Kommunizieren Kooperieren	Zusammenhänge herstellen	Darstellen Interpretieren	
Information und Daten						
Algorithmen						
Sprachen und Automaten						
Aufbau und Funktion von Informatiksystemen						
Informatik und Gesellschaft						

Tabelle 1: Informatikstandards, Inhalts- und prozessbezogene Kompetenzen

das Leben als mündige Bürgerin geeignet sein. Darüber hinaus müssen diese Kompetenzen anschlussfähig für die weitere (Aus-) Bildung sein. Dabei geht es um den Umgang mit informatischen Phänomenen wie: „Man muss an der Kasse seine Waren nicht mehr einzeln vorführen". Die intensive Beschäftigung mit diesen Phänomenen soll zu einer begründeten Position zu gesellschaftlich relevanten Fragen führen. Für die Phänomenerklärung wie für eine begründete Position braucht es Fachkenntnisse. Das bringt *Informatik und Gesellschaft* zusammen mit informatischen Fachinhalten.

RFID - erste Unterrichtsideen

Meine Katze

Ohne weitere zielführende Fragen kann der in Abbildung 2 dargestellte Stimulus als *stiller Impuls* eingesetzt werden, um eine Unterrichtseinheit/-reihe zu RFID, zu den Folgen des Einsatzes, zu Möglichkeiten und zum Einsatz von Informatiksystemen in Verbindung mit RFID zu motivieren. Die Schülerinnen werden nach diesem Stimulus Fragen aufwerfen. Folgende Aspekte können Schülerinnen nach einer solchen Auseinandersetzung bearbeiten:

- Gib an, warum Haustiere diesen Chip erhalten.
- Nenne weitere Bereiche, Gegenstände, in denen solche Chips zur Kennzeichnung eingesetzt werden.
- Warum werden Menschen nicht mit diesem Chip *geimpft*?
- Gib die Unterschiede zwischen einer sichtbaren Kennzeichnung, wie sie durch einen Barcode (z. B. European Article Number (EAN)) vorgenommen wird und der Kennzeichnung durch einen RFID-Chip an.
- Welche Vorteile bietet der Einsatz in Kleidungsstücken?

Der Tierarzt hat unserer Katze an der linken Halsseite eine Spritze gegeben. Es war aber keine Impfung. Damit - so hat der Tierarzt mir erklärt - erhält die Katze eine eindeutige Nummer. Diese befindet sich in einem Bauteil (Chip), das mit der Katze verwächst und von außen nicht gesehen werden kann. Der Chip ist ungefähr so groß wie ein Reiskorn.

Abbildung 2: Stimulusmaterial Meine Katze

Am Türsteher vorbei - dank RFID

Die obercoole Masche: Barcelona: lass Dir einen Chip einsetzen und Du musst Dich nie mehr vom Türsteher dumm ansehen lassen.

Der Vorteil: Bei Besuchen des Etablissements brauchen die Chipträger künftig weder ihren Ausweis einzustecken, noch ihr Portemonnaie mitzunehmen. Auf dem Mikrochip werden nicht nur relevante Personendaten gespeichert:

Die Träger können Geld einzahlen und auf ihrem *VeriChip* gutschreiben lassen. Im Baja Beach Club ist endlich Schluss mit biergetränkten Euroscheinen und Cocktail-klebrigem Wechselgeld. Wer sich in dem Club an Barcelonas Strandpromenade künftig einen Mai Thai bestellt, dem bucht das Barteam den Rechnungsbetrag gleich vom Oberarm ab. [Neuber2004]

Sabrina liest viel

Dann woll'n wir doch mal schauen, wie lange Sabrina in welchen Heften in der Zeitschriftenabteilung eines Kaufhauses blättert. Exemplarische Umsetzung einer Überwachung, die mit RFID möglich ist.

Inhaltsbereiche

Bei den Beispielen stellt sich die Frage, wie die abstrakte Idee Persönlichkeitsschutz für den Unterricht so umgesetzt werden kann, dass Schülerinnen handelnd Lerngelegenheiten erhalten. Einer der Autoren setzt seit vielen Jahren das *Planspiel Datenschutz* [Hammer und Prodesch 1987] im Unterricht ein. Alle Daten werden von Hand aufgenommen. Mit den entstehenden Listen werden anschließend sogenannte *Vorfälle* händisch ausgewertet. Diese Reihe hat eine hohe Akzeptanz und bietet grundlegende Einsichten in vernetzte Systeme, ohne dass Informatiksysteme zum Einsatz kommen.

Die Autoren

Studiendirektor Dipl.-Inform. Dr. rer. nat. Ludger Humbert arbeitet als Informatiklehrer an der Willy-Brandt-Gesamtschule in Bergkamen und als Ausbilder für Informatiklehrerinnen an den Studienseminaren für Lehrämter an Schulen Hamm und Arnsberg. (*http://humbert.in.hagen.de/*)

Dipl.-Math. Dr. phil. Jochen Koubek arbeitet als wissenschaftlicher Assistent am Institut für Informatik der Humboldt-Universität zu Berlin in der Fachdidaktik der Informatik. (*http://waste.informatik.hu-berlin.de/koubek*)

Oberstudienrat Dipl.-Math. Arno Pasternak arbeitet als Informatik-, Mathematik- und Physiklehrer an der Fritz-Steinhoff-Gesamtschule Hagen. (*http://pasternak.in.hagen.de/*)

Studienrat Dipl.-Inform. Dipl.-Math. Dr. rer. nat. Hermann Puhlmann, M.Sc. (Univ. of London) arbeitet als Informatik- und Mathematiklehrer am Leibniz-Gymnasium Altdorf und als Ausbilder für Mathematiklehrerinnen und -lehrer am dortigen Studienseminar.

Technische Ausstattung?

Je nach Rahmenbedingungen im Unterricht kann es nützlich sein, ein RFID-Lese-/Schreibgerät zu beschaffen. Solche Geräte sind zur Zeit für ca. 200 Euro erhältlich. Unter der GNU General Public License (GPL) steht Software bereit, um RFID auszulesen und zu beschreiben: *http://www.rf-dump.org/*

So ist es möglich, die Schülerinnen aufzufordern, vor Beginn der Unterrichtsreihe einige *RFID-verdächtige* Dinge mit in den Unterricht zu bringen. Diese werden dann in der Schule geprüft, es lässt sich feststellen, welche Daten sich auf den RFIDs befinden. Anschließend können - je nach Ziel der Unterrichtsreihe - bestimmte Fragestellungen differenziert beleuchtet werden.

Ausblick - weitere Arbeit

In der Lehrerbildung lassen sich Umsetzungen der Standards am Beispiel RFID evaluieren. Die Ergebnisse sollten breit kommuniziert und diskutiert werden. Beispielhafte Umsetzungen sollten in Materialien für Lehrerinnen eingehen, die regelmäßig aktualisiert werden. Solche Materialien sollten modular aufgebaut sein und dabei Module mit unterschiedlichem Zeitaufwand kombinieren. Wenn die Standards so praktisch mit Inhalten und prozessorientierten Hinweisen verbunden sind, liefern sie Anreize, den eigenen Unterricht qualifiziert vorzubereiten und mit aktuellen Entwicklungen anzureichern.

Literatur

[Hammer und Prodesch 1987] HAMMER, Volker; PRODESCH, Ulrich: Planspiel Datenschutz in vernetzten Informationssystemen. Verlag Die Schulpraxis. Mai 1987. - *http://www.medienzentrum-kassel.de/fortbildung/download/datenschutz/planspiel.zip* (Stand: 16. Juni 2006)

[Humbert und Puhlmann 2005] HUMBERT, Ludger; PUHLMANN, Hermann: Essential Ingredients of Literacy in Informatics. In: 8th IFIP World Conference on Computers in Education, 4-7th July 2005, University of Stellenbosch. Cape Town, South Africa: Document Transformation Technologies cc, July 2005. Documents/445.pdf. - ISBN 1-920-01711-9

[Neuber 2004] NEUBER, Harald: Das Konto im Oberarm - Eine Diskothek in Barcelona bietet ihren Stammgästen Microchipimplantate an - 25. Juni 2004. In: Telepolis (2004), Juni. - *http://www.heise.de/tp/r4/artikel/17/17707/1.html* (Stand: 9. Mai 2006)

[Puhlmann 2003] PUHLMANN, Hermann: Informatische Literalität nach dem PISA-Muster. In: HUBWIESER, Peter (Hrsg.): Informatik und Schule - Informatische Fachkonzepte im Unterricht INFOS 2003 - 10. GI-Fachtagung 17.-19. September 2003, München. Bonn: Gesellschaft für Informatik, Köllen Druck + Verlag GmbH, September 2003 (GI-Edition - Lecture Notes in Informatics - Proceedings P 32). - *http://bscw.schule.de/pub/nj_bscw.cgi/S444a5148/d182025/Informatische_Literalitaet_PISA_Puhlmann_INFOS03.pdf* (Stand: 22. April 2006) - ISBN 3-88579-361-X, S. 145-154

Link-Liste

Interessante Webseiten mit Kurzkommentar

Die Webseiten (URLs) in den folgenden Tabellen wenden sich naturgemäß an unterschiedliche Adressatinnen und Adressaten, weshalb wir versucht haben, Ihnen mit einer Einstufung nach den hilfreichen Vorkenntnissen eine Orientierung zu geben. Dabei bedeutet 1, dass Sie für die Webseite auf dem jeweiligen Gebiet keine Vorkenntnisse brauchen, während Sie sich bei 5 schon recht gut mit dem Thema auskennen sollten. Die Zahl kann fehlen, wenn es sich um die Seiten einer Einrichtung handelt, die das Thema in sehr verschiedenen Beiträgen darstellt.

Leider kann eine solche Auflistung nie vollständig und die Einstufung – weil subjektiv – für Sie auch ganz unzutreffend sein. Wenn Sie das Thema interessant finden, gucken Sie sich die URL doch trotzdem an, auch wenn die Zahl auf umfassende Vorkenntnisse hinweist! Und wenn Sie außerhalb dieser Liste eine Webseite finden, von der Sie annehmen, dass sie im Zusammenhang mit RFIDs von allgemeinem Interesse ist, freuen wir uns über eine Mitteilung von Ihnen. Die Kontaktinformation finden Sie auf der ersten Seite dieser Broschüre.

Allgemeine Information

Auf dem Heise-Newsticker finden Sie immer interessante Informationen und es lässt sich gut nach Stichwörtern suchen, ein Ausgangspunkt für weitere Recherche

http://www.heise.de/newsticker/ (Stand: 25.8.06)

GS1 Germany ist das Dienstleistungs- und Kompetenzzentrum für unternehmensübergreifende Geschäftsabläufe in der deutschen Konsumgüterwirtschaft und ihren angrenzenden Wirtschaftsbereichen. Sie ist Gründungsmitglied der internationalen EAN-Organisation, deren Standards heute in 129 Ländern eingesetzt werden. GS1 Germany ist kartellrechtlich anerkannter Rationalisierungsverband und Trägerin des Normenausschusses Daten- und Warenverkehr in der Konsumgüterwirtschaft (NDWK) im DIN.

http://www.gs1-germany.de (Stand: 18.8.06)

AIM Deutschland e.V. ist der nationale Industrieverband für Automatische Identifikation, Datenerfassungssysteme und Mobilität und Mitglied von AIM Global, eine Non-Profit Organisation. AIM Mitglieder mit Sitz oder Niederlassung im deutschsprachigen Raum sind Hersteller, Lieferanten, Systemintegratoren und Nutzer von Technologien zur automatischen Erfassung, mobilen Datenkommunikation und Bereitstellung von Daten zur Verarbeitung in Managementsystemen.

http://aimgermany.aimglobal.org/ (Stand: 18.8.06)

„Risikoabschätzung zur RFID-Technik", Cornelia Brandt, Referentin für Innovations- und Technologiepolitik in der ver.di-Bundesverwaltung Berlin

http://www.verdi-innotec.de/news.php3 (Stand: 8.6.06, Vorkenntnisse: 2)

Studie über Risiken und Chancen des Einsatzes von RFID-Systemen (veröffentlicht 2004) des Bundesamts für Sicherheit in der Informationstechnik (BSI)

http://www.bsi.de/fachthem/rfid/studie.htm (Stand: 23.5.06, Vorkenntnisse: 4)

Privates Projekt des Interessenkreises biometrische Ausweise: Der Interessenkreis besteht aus einer Pastorin, zwei Lehrern, einer Lehrerin, einem kaufmännischen Angestellten und einem Webdesigner. Informative Zusammenstellung von vielen Beiträgen aus unterschiedlichen Quellen zu elektronischen Pässen in Deutschland und anderswo sowie andere Information in diesem Zusammenhang.

http://www.neuer-reisepass.de/rfid.htm (Stand: 17.8.06, Vorkenntnisse: 1)

RFID Informationen ist ein Projekt von Mirko Kulpa; es enthält Nachrichten zu RFID, ein Archiv, erklärt die Grundlagen der Technik, enthält ein RFID Lexikon und Information zu Datenschutz und Datensicherheit, berichtet, wo Radio Frequency Identification eingesetzt wird, und bringt Testberichte zu Hard- und Software.

http://rfid-informationen.de/misc/sitemap.html (Stand: 17.8.06, Vorkenntnisse: 2-3)

---

nützliches Glossar für Begriffe rund um die RFID-Technologie

http://www.epc-forum.de/glossar/index/ (Stand:25.8.06, Vorkenntnisse: 2)

---

nützliches Glossar für Begriffe rund um die RFID-Technologie

http://www.rfid-ready.de/252-0-rfid-glossar.html (Stand: 25.8.06, Vorkenntnisse: 2)

---

nützliche Erklärungen rund um die RFID-Technologie

http://de.wikipedia.org/wiki/Rfid (Stand: 25.8.06, Vorkenntnisse: 2 - 3)

Zukünftige Anwendungen, Wirtschaftsinformationen

„Funketiketten in Korea (Rep.) zunehmend verbreitet“, Bundesagentur für Außenwirtschaft

http://www.bfai.de/fdb-SE,MKT20060803103332,Google.html

(Stand: 17.8.06, Vorkenntnisse: 1)

„US-Armee plant globale Überwachung per RFID“ (24. Nov 2005)

http://www.netzeitung.de/internet/369583.html (Stand: 17.8.06, Vorkenntnisse: 1)

„Memory Spot Chip - HP stellt neuen Mini-Speicher vor“, W. Janssen

http://www.at-mix.de/news/1705.html (Stand: 17.8.06, Vorkenntnisse: 1)

Gesundheit

„RFID und Gesundheitsschutz“ Management-Information von GS1 und AIM; enthält im Anhang ein Verzeichnis von Richtlinien, Direktiven, Standards und Studien

http://www.logistik-inside.de/fm/2239/RFID_gesundheit.pdf

(Stand: 17.8.06, Vorkenntnisse: 2 - 3)

„Siemens to pilot RFID bracelets for health care. Others seek to implant data under the skin“, Ephraim Schwartz

http://www.infoworld.com/article/04/07/23/HNrfidimplants_1.html

(Stand: 8.6.06, Vorkenntnisse: 2)

„RFID Implants Could Chip Away At Your Health, Identity Microchips Not Approved By FDA“, Jennifer Brady

http://www.10news.com/technology/7968362/detail.html

(Stand: 8.6.06, Vorkenntnisse: 2)

„RFID in R&D: Biospecimen Tracking“, Eric Newmark, senior research analyst for Health Industry Insights

http://www.bio-itworld.com/columns/insights--outlook/copy5_of_insights-outlook
(Stand: 8.6.06, Vorkenntnisse: 2)

„Implementation of new technologies to better protect our drug supply", Food and Drug Administration (FDA), USA

http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html

(Stand: 8.6.06, Vorkenntnisse: 2)

Datenschutz

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. ist eine Vereinigung Technikinteressierter sowie von Menschen, die sich in den Bereichen Politik, Umwelt oder Menschenrechte engagieren. Bekannt wurde FoeBuD vor allem durch die BigBrotherAwards, die er (zusammen mit anderen Organisationen) seit sechs Jahren an die *größten Datenkraken* verleiht. Zum Thema RFID finden Sie Publikationen und die Dokumentation verschiedener Aktionen.

http://foebud.org/ (Stand: 25.8.06, Vorkenntnisse: 2)

Homepage der EICAR RFID-Taskforce zum Thema Datenschutz, hauptsächlich in englischer Sprache, mit einem deutschen Datenschutz-Leitfaden unter *http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf*

http://www.eicar.org/rfid/ (Stand: 17.8.06)

Virtuelles Datenschutzbüro, ein gemeinsamer Service der Datenschutzorganisationen, mit einem gut verständlichen Dossier zu RFIDs unter *http://www.datenschutz.de/feature/detail/?featid=2*, das viele weitere Quellen enthält

http://www.datenschutz.de/ (Stand: 8.6.06, Vorkenntnisse: 1)

Metalink - die Linkliste von Datenschutz.de

http://www.datenschutz.de/themen/ (Stand: 9.5.06)

Startseite Datenschutz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

http://www.bfdi.bund.de/cln_030/nn_672634/DE/Home/homepage__node.html__nnn=true (Stand: 25.8.06, Vorkenntnisse: 1)

Homepage des Projekts *RFID Viruses and Worms* des Department of Computer Science der Vrije Universiteit Amsterdam, dort finden Sie in englischer Sprache ein preisgekröntes Dokument über die Sicherheit von RFID-Chips angesichts von Viren und anderen Schädlingen

http://www.rfidvirus.org/ (Stand: 25.8.06, Vorkenntnisse: 2)

Hier wird (in englischer Sprache) der Prototyp eines *RFID-Guardian* vorgestellt. Der RFID-Guardian ist ein in Personal Digital Assistants (PDAs) oder Mobiltelefone integrierbares Gerät, das als Lesegerät oder RFID-Chip agieren kann und das Sicherheitsmanagement gegenüber den Chips und Lesegeräten in der Umgebung eines Menschen übernimmt

http://www.rfidguardian.org/index.html (Stand: 25.8.06, Vorkenntnisse: 3)

„Injecting RFID into the Immigration Mess, Literally", Evan Schuman, Ziff Davis Internet

http://www.eweek.com/article2/0,1895,1965110,00.asp

(Stand: 8.6.06, Vorkenntnisse: 2)

Kontrolle der Mitarbeiter (Zeiterfassung + Zugangskontrolle)

http://zeiterfassung.3sdesign.de/ (Stand: 18.8.06, Vorkenntnisse: 2)

CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) – eine Verbraucherschutz-Organisation, die sich ganz gezielt mit RFIDs befasst, gegründet 1999. Katherine Albrecht und Liz McIntyre sind mit ihren Publikationen und Aktionen sehr bekannt geworden.

http://spychips.com/rfid_overview.htm (Stand: 9.5.06, Vorkenntnise: 2)

Datenschutz und RFID-Technik, Jan Suhr, Malwina Prokopczyk, Frank Reimann Präsentation zum Gutachten, Technische Universität Berlin, Arbeitsbereich Informatik und Gesellschaft, Februar 2004

http://www.opensourcejahrbuch.de/lehre/w2003/ir1/uebref/SuhrEtAl-Gutachten-Vortrag-G4-022004.pdf/publication_view (Stand: 18.8.06, Vorkenntnisse: 2)

Bauanleitung für ein eigenes Lesegerät für 13,56-MHz-RFIDs

http://www.heise.de/ct/05/02/202/default.shtml#literatur

(Stand: 18.8.06, Vorkenntnisse: 4)

unterhaltsame österreichische Seite, leichte Lektüre mit einem interessanten Glossar zur Informationssicherheit und (u.a.) einer plakativen, nicht sonderlich geschmackvollen Karikatur zu RFIDs

http://sicherheitskultur.at/RFID_privacy.htm (Stand: 18.8.06, Vorkenntnisse: 1)

Dagmar Boedicker

Glossar und Abkürzungsverzeichnis

Es enthält die gebräuchlichsten Begriffe um RFIDs (und benachbarte Themen), denen Sie begegnen werden, wenn Sie diese Broschüre lesen oder ein wenig im Internet stöbern.

(R&TTE)
European **R**adio and **T**elecommunications **T**erminal **E**quipment

1999/5/EG Richtlinie
EG Richtlinie 1999/5/EG des Europäischen Parlaments und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung ihrer Konformität (R&TTE-Richtlinie). Diese europäische Richtlinie enthält Grenzwerte zum Schutz vor Schädigungen durch elektromagnetische Felder und ist mit den Werten der → ICNIRP vergleichbar

AIM
AIM Deutschland e.V., nationaler Industrieverband für **A**utomatische **I**dentifikation, Datenerfassungssysteme und **M**obilität, Mitglied von AIM Global, eine Non-Profit Organisation. AIM Mitglieder mit Sitz oder Niederlassung im deutschsprachigen Raum sind Hersteller, Lieferanten, Systemintegratoren und Nutzer von Technologien zur automatischen Erfassung, mobilen Datenkommunikation und Bereitstellung von Daten zur Verarbeitung in Managementsystemen.

aktiver RFID-Chip
Chip mit eigener Energieversorgung, der eine höhere Reichweite hat als ein passiver RFID-Chip

Aloha-Protokoll
Protokoll zum Auslesen von Informationen aus RFID-Transpondern. Das Lesegerät fordert damit alle Transponder in seiner Reichweite auf, nach einer Zufallszeit zu antworten. Kommt es dabei zu Kollisionen, wird der Vorgang so lange wiederholt, bis die Information aller Transponder gelesen wurde.

Antikollisions-Protokoll
Verfahrensregeln für die Kommunikation zwischen RFIDs und Lesegerät, die dafür sorgen, dass das Lesegerät mehrere RFIDs in seiner Reichweite nacheinander ausliest

Authentifizierung
elektronische Identitätsprüfung

Authentisierung
in einem IT-System der Nachweis einer behaupteten Identität, insbesondere die Funktion, mit der dieser Nachweis bei der →Authentifizierung erbracht wird

Auto-ID Center
1999 am Massachusetts Institute of Technology (MIT) gegründet, sollte die Vision des „Internets der Dinge" implementieren, Vorläufer von → EPCglobal

Backscatter-Verfahren
modulierter Rückstrahlquerschnitt: Verfahren zur kontaktlosen Energie- und Datenübertragung auf der Basis von RADAR-Technik (Radio Detection and Ranging, bekannt aus der Luftfahrt)

Blacklist
Ausschlussliste, Gegenteil einer Whitelist. Hier sind Objekte aufgeführt, für die ein bestimmtes Kriterium *nicht* zutrifft: Eine Berechtigung wurde *nicht* erteilt, sie gehören *nicht* zu einer bestimmten Kategorie oder ähnliches.

Blocker-Tag
→ RFID-Chip, der das Lesegerät behindert oder lahmlegt, indem er gegenüber dem Lesegerät eine große Zahl adressierbarer RFID-Chips simuliert

Deaktivator
Gerät zur → Deaktivierung von RFID-Chips

Deaktivierung
Vorgang, durch den verhindert wird, dass ein RFID-Chip auf die Abfrage eines Lesegeräts antwortet

DoS-Angriff
Denial-of-Service-Angriff; bei diesem Angriff wird das RFID-System so gestört, dass es nicht mehr oder nur noch eingeschränkt funktioniert

EAN·UCC
Europäische **A**rtikel**n**ummer, weltweit eindeutige Produktkennzeichnung für Handelsartikel der EAN International, und Uniform Product Code (UPC), vom **U**niform **C**ode **C**ouncil (UCC) betreut. Beide Standardisierungsorganisationen sind heute integriert und haben einen RFID-Standard vorgelegt, den → EPC

EICAR
European **I**nstitute for **C**omputer **A**nti-Virus **R**esearch. Als eingetragener Verein wurde es 1991 in Deutschland gegründet. Das Institut versteht sich als Plattform für den Informationsaustausch für alle Sicherheitsexperten, die in den Bereichen Forschung und Entwicklung, Implementierung sowie Management tätig sind. Ziel des Instituts ist es, Lösungen und Präventivmaßnahmen gegenüber allen Arten der Computerkriminalität zu entwickeln.

EAS
Electronic **A**rticle **S**urveillance, Diebstahlsicherung durch RFID

EPC

Electronic **P**roduct **C**ode, eindeutige Identifikationsnummer eines RFID-Chips. Es gibt Varianten mit 64 Bit (EPC-64), 96 Bit (EPC-96) und 256 Bit (EPC-256). Neben anderen Informationen enthält der EPC-96 die Seriennummer des Chips (36 Bit) und mit einer Gesamtlänge von 44 Bits eine Nummer für den Hersteller (20-40 Bits) und für die Produktart, die der Chip kennzeichnet, den Item- oder Objektcode (4-24 Bit).

EPCglobal (Inc.)

internationale Entwicklungsplattform, Non-profit Organisation, die wirtschaftliche und technische Standards für das Electronic Product Code (→ EPC)TM-Netzwerk entwickelt und einführt, 2003 von EAN International und dem Uniform Code Council, Inc. (heute → GS1 und GS1 US) gegründet; Ziel ist es, das EPCTM-Netzwerk aufzubauen und die Verbreitung standardisierter, RFID-unterstützter Prozesse voranzutreiben.

EPCTM-Netzwerk

RFID/EPCglobal-Netzwerk, basiert auf Forschungs- und Entwicklungsarbeiten zunächst des Auto-ID Center des Massachusetts Institute of Technology (MIT), später EPCglobal

ERP

Effective **R**adiated **P**ower, effektive abgestrahlte Leistung in der Hauptstrahlungsrichtung einer Antenne

GPL

GNU General **P**ublic **L**icense

Granularität

räumliche Skalierung beim → Tracking, von fein (beispielsweise innerhalb eines Raums oder Ladens) bis zu grob (beispielsweise innerhalb eines Staats)

GS1

GS1 Germany (vormals CCG, Centrale für Coorganisation GmbH), Dienstleistungs- und Kompetenzzentrum für unternehmensübergreifende Geschäftsabläufe in der deutschen Konsumgüterwirtschaft und ihren angrenzenden Wirtschaftsbereichen, Gründungsmitglied der internationalen EAN-Organisation, deren Standards heute in 129 Ländern eingesetzt werden. GS1 Germany ist kartellrechtlich anerkannter Rationalisierungsverband und Trägerin des Normenausschusses Daten- und Warenverkehr in der Konsumgüterwirtschaft (NDWK) im DIN.

Hash-Lock Verfahren

Verfahren, bei dem eine schwer umkehrbare Funktion einen Schlüssel zu einem gespeicherten Schlüssel erzeugt, der dann vom Lesegerät benutzt wird, um auf die Daten im Chip zuzugreifen

ICNIRP

International **C**ommission on **N**on-**i**onizing **R**adiation **P**rotection

Identifizierung

Feststellung der Identität

IKT

Informations- und Kommunikationstechnik

induktive Kopplung
Ein Lesegerät generiert ein magnetisches Wechselfeld, das über seine Induktionswirkung im Antennenkreis des RFID-Chips eine Spannung induziert. Diese elektrische Spannung versorgt die auf dem RFID-Chip vorhandene → Steuerlogik mit Energie.

Interoperabilität
Fähigkeit eines Gerätes, in einem Netz mit anderen Geräten desselben Standards zu kommunizieren, auch wenn die Geräte von verschiedenen Herstellern stammen

ISM (-Frequenzen)
Frequenzbereiche für **I**ndustrielle, wissenschaftliche (**S**cientifical) oder **M**edizinische Anwendungen

Kill-Funktion
RFID-Chips der 2. Generation erhalten (jedenfalls bei Einsatz in Geschäften der *Metro Group*) eine Kill-Funktion und ein Passwort, das Unbefugten den Zugriff auf diese Funktion versagen soll. Das Passwort wird in einer Datenbank hinterlegt und bei der Deaktivierung dem Lesegerät zur Verfügung gestellt. Die Deaktivierungs-Anwendung übermittelt das Passwort und den Kill-Befehl über das Sende-/Empfangsprotokoll an das Lesegerät, das dann den RFID-Chip abschaltet. Nach Angaben von Metro ist die Deaktivierung unwiderruflich. Sie lässt sich aber abhören.

Kollisionsbehandlung
Vorgehen, das nötig wird, wenn mehrere RFIDs im Lesebereich eines Lesegeräts gleichzeitig auf seine Abfrage reagieren → Antikollisions-Protokoll

Kryptographie
Verschlüsselung

Label → RFID-Chip

Lesegerät
Gerät zum Lesen eines RFIDs, das ein Signal mit definierter Frequenz und Signalstärke sendet. Dieses Signal versorgt den (passiven) RFID-Chip mit Energie, der dann die Amplitude des Signals moduliert und dadurch seine gespeicherte Information überträgt. Lesegeräte sind meist an Softwareanwendungen und Datenbanken angeschlossen, von wo sie Information erhalten, beispielsweise den Code einer → Objektklasse, und an die sie Daten weitergeben.

Nahfeld
Bereich, innerhalb dessen eine induktive Kopplung zwischen Lesegerät und Transponder möglich ist. Er ist durch die verwendete Frequenz festgelegt, mit steigender Frequenz verkürzt sich die Wellenlänge. Bei einer Frequenz von 13,56 MHz beträgt die Wellenlänge etwa 22 Meter, und das Nahfeld hat einen Radius von 3,5 Metern.

Objektklasse
Produktart (im → EPC codiert)

OECD
Organisation for **E**conomic **C**ooperation and **D**evelopment

ONS
Object **N**ame **S**ervice, Verzeichnis zur Umwandlung eines → EPC in eine → URL. Mit Hilfe der URL wird dann eine IP-Adresse gefunden, dort liegen die detaillierten Informationen über das Objekt (Palette, Verpackung oder Produkt)

passiver RFID-Chip
Chip ohne eigene Energieversorgung mit geringerer Reichweite als ein aktiver RFID-Chip

Pervasive Computing
„durchdringende Computertechnik" → ubiquitous computing

PML
Product-**M**arkup-**L**anguage

pseudonym
nicht auf eine Person beziehbar

Normen
ISO 11784 und ISO 11785 (Niederfrequenz 125-148,5 kHz), ISO 14443 und ISO 15693 (Hochfrequenz 13,56 MHz), ISO 18000 (Ultra-Hochfrequenz 400 MHz – 1 GHz)

RF-Chip → RFID-Chip

RFID
Radio **F**requency **Id**entification

RFID-Chip
Chip für die *Radio Frequency Identification,* der auf Abfrage eines Lesegeräts seine gespeicherten Daten über elektromagnetische Wellen an das Lesegerät sendet. Der Chip hat eine Antenne, er kann einen Prozessor und eine Batterie haben.

RFID-Label → RFID-Chip

RFID-System
besteht aus einem RFID-Chip, der die zu speichernden und bei Bedarf zu übermittelnden Informationen enthält, einem Schreibgerät zur Programmierung und dem Schreiben von Identifikationsdaten auf den RFID-Chip sowie einem Lesegerät, das die im RFID-Chip enthaltenen Informationen ausliest

RFID-Tag → RFID-Chip

Rolle
Definition von Personen, Gruppen und ihren Aufgaben bei der Vergabe von Zugriffsrechten auf (personenbezogene u.a.) Daten

Scanner → Lesegerät

Spezifikation
schriftliche Festlegung von Anforderungen an und nötigen Arbeiten für ein Verfahren, System, Gerät oder Programm

Steuerlogik
Die Steuerlogik eines RFID-Chips kann eine einfache Logik sein (Zustandsautomat Ja/Nein) oder eine leistungsfähige Prozessoreinheit mit Co-Prozessoren für Spezialaufgaben wie das Berechnen elektronischer Signaturen

Tag → RFID-Chip

Tag-Finder
Sucht Systeme im 13,56 MHz-Bereich (ISO14443). Antwortet ein Tag nicht auf den Tag-Finder, ist es defekt.

Tracking
Verfolgen einer Person, in unserem Zusammenhang durch einen RFID-Chip ermöglicht, der von verschiedenen Lesegeräten immer wieder lokalisiert wird und dadurch die Ortung der Person möglich macht

Träger
Signal mit definierter Frequenz und Signalstärke, das vom Lesegerät erzeugt wird. Es dient einerseits der Energieversorgung des RFID-Chips und andererseits, durch Amplitudenmodulation des Signals, der Informationsübertragung in den Seitenbändern.

Transponder
transmitting responder → RFID-Chip

ubiquitous computing
„allgegenwärtige Computertechnik", auch *pervasive computing,* beschreibt die Möglichkeit, dass IKT alle Lebensbereiche, privat, beruflich, öffentlich, im Nah- und Fernbereich durchdringt

UHF-Transponder
RFID-Chip, dessen Frequenz im UKW-Bereich liegt und der deshalb eine höhere Reichweite hat als Chips mit niedrigerer Frequenz

URL
Universal **R**esource **L**ocator, symbolische Adresse eines Rechners im Internet

Vertraulichkeit
Daten sind nur einer definierten und legitimierten Gruppe von Benutzern verfügbar

Whitelist
Gegenteil einer → Blacklist. Hier sind Objekte aufgeführt, für die ein bestimmtes Kriterium zutrifft.

Das Forum InformatikerInnen und Informatiker für Frieden und gesellschaftliche Verantwortung (FIfF) e.V.

Wir sind

... rund 700 engagierte Frauen und Männer aus Lehre, Forschung, Entwicklung und Anwendung der Informatik und Informationstechnik, die bei ihrer Arbeit auch über deren Konsequenzen nachdenken, die dafür eintreten, dass nicht alles Machbare gemacht wird, die überzeugt sind, dass nicht alle unsere Probleme mit Technik zu lösen sind. Allen, die sich mit Informatik und Informationstechnik beschäftigen – in der Ausbildung, im Beruf oder danach – wollen wir ein Forum für eine kritische und lebendige Auseinandersetzung bieten – offen für alle, die mitarbeiten möchten oder auch einfach nur informiert bleiben wollen.

Wir arbeiten

... bundesweit und in Regionalgruppen. Unterstützt wird das FIfF durch einen Beirat, in den anerkannte Expertinnen und Experten aus Wissenschaft und Praxis berufen werden. Das FIfF gibt, zum Teil in Zusammenarbeit mit anderen Verlagen, regelmäßig Publikationen heraus, darunter Reader, Tagungsbände, Broschüren sowie die Vierteljahres-Zeitschrift FIfF-Kommunikation. Das FIfF kooperiert mit zahlreichen Initiativen und Organisationen im In- und Ausland.

Wir wollen

... dass Informationstechnik im Dienst einer lebenswerten Welt steht.

Deshalb

- warnen wir die Öffentlichkeit vor Entwicklungen in unserem Fachgebiet, die wir für schädlich halten;
- setzen wir möglichen Gefahren eigene Vorstellungen entgegen;
- kämpfen wir gegen den Einsatz der Informationstechnik zur Kontrolle und Überwachung;
- engagieren wir uns für eine Abrüstung der Informatik in militärischen Anwendungen;
- unterstützen wir die menschengerechte Gestaltung von Arbeitsprozessen;
- setzen wir uns bei Gestaltung und Nutzung der Informationstechnik für die Gleichberechtigung von Menschen mit Behinderungen ein;
- arbeiten wir gegen die Benachteiligung von Frauen in der Informatik;
- wehren wir uns gegen jede rassistische und sexistische oder andere diskriminierende Nutzung der Informationstechnik;
- setzen wir der Vorherrschaft der Ökonomie eine humane und ökologische Orientierung entgegen.

Wir veröffentlichen vierteljährlich unsere Zeitschrift zu Informatik und Gesellschaft, die FIfF-Kommunikation. Auf ca. 60 Seiten behandeln Expertinnen und Experten aktuelle Themen, damit ist die FIfF-Kommunikation eine Quelle für fachliche Information und ein Medium für den kritischen Meinungsaustausch.

RFIDs sind weder technisch noch sozial und politisch ein triviales Thema, womöglich werden sie uns in Zukunft sogar mit ökologischen oder gesundheitlichen Problemen konfrontieren. Das ist die eine Seite, die andere präsentiert ein spannendes Spektrum immens nützlicher Anwendungen. Und weil die reichhaltige Information aus dem Web, teils von interessierter Seite, nach einem kompakten Überblick zu rufen schien, haben wir als engagiertes Forum für Informatiker und andere uns wieder an die Arbeit gemacht, wie schon bei der elektronischen Gesundheitskarte im letzten Jahr.

Wenn Sie also etwas zu den vielfältigen Aspekten dieses Themas wissen möchten, sollte diese Broschüre eine geeignete Lektüre sein. Sie müssen dazu keine umfassenden Vorkenntnisse haben, ein wenig technisches und auch politisches Interesse sind aber hilfreich. - Wir haben die Veröffentlichungen zu diesem Thema gesichtet und namhafte Autorinnen und Autoren aus verschiedenen Fachgebieten und Institutionen um Beiträge gebeten. Auch FIfF-Mitglieder beschäftigen sich mit dem Thema und haben etwas zu dieser Broschüre beigetragen.

Wenn Sie und andere sich für diese Broschüre interessieren, werden wir sie 2007 aktualisieren, denn wie Sie der Roadmap der Europäischen Kommission entnehmen können, wird es neue Entwicklungen geben, die eine 2. Auflage lohnen. Gibt es etwas, was Sie gern wüssten und nicht gefunden haben? Dann teilen Sie es uns bitte mit. Auf der ersten Seite finden Sie die Kontaktmöglichkeiten zu uns.