Universität Karlsruhe (TH)

Fakultät für Informatik
Institut für Programmstrukturen und Datenorganisation (IPD)

Seminararbeit

Wireless Location Privacy: Angriffspotential durch RFID und Gegenmaßnahmen

Im Rahmen des Seminar
Aktuelle Herausforderungen von Datenschutz und Datensicherheit
in modernen Informationssystemen

Autor: Markus Korte

Betreuer: Dipl.Inform. Thorben Burghardt

im Sommersemester 2007

Inhaltsverzeichnis

1 Einleitung

"Es ist wieder soweit! Eine technische Neuerung bahnt sich ihren Weg in den Alltag. Ihr Ziel - Zeit und Kosten sparen und für ein bequemeres Leben sorgen. Bei Erzeuger wie bei Verbraucher."
"Jetzt werden dem Verbraucher auch seine letzten noch gebliebenen Geheimnisse entlockt. Der vollkommene gläserne Mensch."
So oder so ähnlich könnten zwei Überschriften lauten, wenn von RFID (Radio Frequency Identification) die Rede ist. Sie fallen in die Kategorie "Fluch oder Segen?". Ganz so einfach wie diese beiden fiktiven Zeitungsüberschriften ist der Sachverhalt jedoch nicht. Denn auf der einen Seite möchte der Verbraucher Komfort, wodurch seine Privatsphäre gefährdet ist und auf der anderen Seite möchte er seine Privatsphäre wahren, wodurch potentieller Komfort verloren geht. Es stellt sich die grundsätzliche Frage, ob es möglich ist beides zu bekommen, Komfort und Privatsphäre. Diese Frage stellt sich auch in einem Alltag, dem der große Durchbruch von RFID noch bevorsteht. Beim bargeldlosen Einkauf sind es die Kontodaten, beim Kauf eines Handys sind es die Daten aus dem Personalausweis, die anzugeben sind. Zu recht darf sich der Verbraucher daher dazu entscheiden auf telefonische Erreichbarkeit zu verzichten, dafür aber mit dem guten Gewissen zu leben, seine Personalausweisnummer nicht an eine wenig vertrauenserweckende Person weiterzugeben.
Diese Arbeit wird zeigen, dass der Benutzer durch RFID Technik die Option "ich verzichte auf Komfort zu Gunsten meiner Privatsphäre" verlieren könnte. Im Anschluss an die Vorstellung möglicher Angriffe auf die Privatsphäre durch RFID folgt daher die Erläuterung zweier Verfahren, die dem Verbraucher diese Option zurückgeben soll. Im Allgemeinen geht es dabei darum, unbemerktes Auslesen durch Dritte zu verhindern und im Besonderen darum, festzulegen welche Information an geeigneter Stelle zu Gunsten des Komfort freigegeben wird. Die perfekte Lösung gibt es noch nicht, doch sollen die beiden Beispiele zeigen was getan werden kann, um sich in Richtung "Segen" zu bewegen.

2 Einführung in RFID

Die Abkürzung RFID steht für Radio Frequency Identification - Identifizierung über Radiowellen. Es ist ein Verfahren zur automatischen Identifizierung von Gegenständen und Lebewesen. Korrekterweise sollte man statt von RFID von einem RFID-System sprechen. Dazu gehört der Transponder, das Schreibe-/Lesegerät - auch RFID Reader genannt, und eine Middleware, die z.B. Schnittstellen zu Datenbanken zu Verfügung stellt. Auf unterster Ebene befindet sich der Tag. Er markiert das Objekt und wird mit Hilfe des RFID Reader ausgelesen. Die ID kann z.B. eine Nummer sein, durch die das Objekt in einer Datenbank repräsentiert wird.

2.1 Entstehungsgeschichte

Hinter der Abkürzung RFID steht eine Technik, deren Ursprung in die Zeit des zweiten Weltkrieges zu setzen ist [1,2]. Bereits zuvor - im Jahr 1935 - erfindet Alexander Watson-Watt das Radar. Seine Erfindung lokalisiert physikalische Objekte mit Hilfe von Radiowellen. Im zweiten Weltkrieg kommt das Radar zum Einsatz, um Flugzeuge zu entdecken. Jedoch ist es nicht möglich die feindlichen Flugzeuge von den Eigenen zu unterscheiden. Großbritannien entwickelte deshalb das IFF-System. "Identification Friend or Foe" (Erkennung Freund oder Feind) benutzt Transponder, die im Flugzeug mitgeführt werden und das Signal des Bodenradars aktiv anpassen. Ein Freund würde sich also von einem Feind an Hand des angepassten Echos über das Radar erkennen lassen. Parallel zu der Technik aus Großbritannien veröffentlichte Harry Stockmann von der US Air Force mit "Communications by Means of Reflected Power" die erste öffentliche Beschreibung der RFID-Technologie.

2.2 Technische Betrachtung

Transponder können sich in ihrer Ausstattung erheblich unterscheiden. Generell ist eine Antenne, ein Schaltkreis zum Senden und Empfangen sowie ein permanenter Speicher zu finden [3]. Variationen gibt es u.a. bei der Größe und der Wiederbeschreibbarkeit des Speichers, der benutzten Funkfrequenz und Zusatzfunktionen wie Kryptographie. Welcher Tag letztendlich gewählt wird, ist von der Anwendung abhängig. Generell gibt es zwei verschiedene Arten von Transpondern, die in einem RFID System zum Einsatz kommen können, nämlich aktive und passive. Während aktive Transponder zur Energieversorgung eine eigene Batterie mitführen, sind passive Transponder auf die Energieversorung durch das RFID Lesegerät angewiesen. Hier macht man sich die Radiowelle als Energieträger zu nutze, indem die Antenne als Spule dient und durch Induktion einen Kondensator auflädt, der dann den Tag mit Energie versorgt. Aufgrund der mitgeführten Batterie sind aktive Tags größer und teurer als passive Tags. Dafür können sie aus einer Entfernung von 20m bis zu 100m ausgelesen werden [4]. Bei passiven Tags liegt die Reichweite zwischen wenigen Zentimetern bis hin zu 10m, je nach benutzter Frequenz. Es ist zu beachten, dass frequenzabhängig der Einfluss von Feuchtigkeit und Metall geringer oder stärker ausfällt - was sich auf die Lesereichweite auswirkt.

2.3 Anwendungsbeispiele

Man unterscheidet "personenbezogen" und "objektbezogene" Anwendungen [5]. Bei der personenbezogenen Anwendung geht es darum den Schreib- bzw. Lesevorgang so sicher wie möglich zu gestalten - der Transponder wird bei dieser Anwendung auch als "kontaktlose Smartcard" bezeichnet. Wie der Name "personenbezogen" schon sagt, werden Smartcards in vielen Fällen verwendet, um personenbezogene Daten zu speichern. Entsprechend groß muss daher der Speicher sein. Um die sensitiven Daten zu schützen muss die Datenübertragung

verschlüsselt stattfinden. Dazu verfügen Smartcards über eine Kryptoeinheit. Weiterhin zeichnen sie sich durch eine hohe Übertragungsrate von bis zu mehreren 100kbit/s aus. Um die Sicherheit weiter zu erhöhen sind Smartcards nur aus direkter Nähe (bis 10cm) lesbar. Momentan sind Smartcards wegen ihrer speziellen Anforderungen noch zu teuer in der Herstellung, als das sie neben Spezialanwendungen, wie dem "elektronischen Reisepass" oder der "Zugangskontrollkarte" für Gebäude, eine weite Verbreitung finden.
Bei der objektbezogenen Anwendung wird der Transponder wie ein Etikett auf dem Objekt befestigt. Weil das Objekt dadurch markiert ist, wird der Transponder bei dieser Anwendung landläufig mit RFID-Tag bezeichnet. Der Schwerpunkt dieser Seminararbeit liegt auf dem RFID-Tag, da seine Herstellungskosten bei etwa 1 Eurocent pro Stück liegen, und RFID-Tags daher schon bald den heute üblichen Strichcode ablösen können, der sich auf praktisch allen Konsumgütern befindet. Schon heute wird RFID neben dem populären "elektronischen Reisepass" in unterschiedlichsten Bereichen eingesetzt.
An oberster Stelle steht hier die Logistik. "Tracking und Tracing", also das Wissen wo sich die Ladung befindet und welchen Weg sie gegangen ist, lässt sich mit RFID stark automatisieren. Daher ist RFID auch für das "Supply Chain Management" von hohem Interesse. Der amerikanische Verbraucher kommt bereits heute im öffentlichen Straßenverkehr durch "SmarTrip" mit RFID Transpondern in Kontakt. Und als Autofahrer verlässt er sich auf die mit RFID realisierte Wegfahrsperre und spart Zeit durch das Mitführen eines "E-ZPass", der die Mautabrechnung während der Fahrt im Hintergrund ohne zutun des Fahrers vornimmt. Und muss er doch einmal zum Tanken anhalten, dann bezahlt er möglicherweise mit American Express' "expressway", die ihrerseits einen RFID Transponder mitführt. Zum Großereignis "Fußball WM2006" in Deutschland wurde RFID eingesetzt, um die Eintrittskarten fälschungssicher zu machen. Eine Anwendung, die auch für Eurogeldscheine in Erwägung gezogen wird. Das Beispiel des Kettensägenherstellers "Stihl" in [6] zeigt, dass es sich um eine potentielle Anwendung handelt. Während der Tierfreund bisher nur sein Haustier "tagt", damit es keine Impfung verpasst und bei Orientierungslosigkeit nach Hause gebracht werden kann, gibt es erste Fälle, in denen sich Herrchen selbst einen RFID Transponder implantieren lässt [7], um das Problem des nicht auffindbaren Schlüssels ein für alle Mal zu lösen. Auch im Haushalt finden sich Einsatzgebiete. In Zukunft wird die Waschmaschine Alarm schlagen, wenn die rote Socke zusammen mit dem weißen T-Shirt in der Trommel liegt, und das auch noch bei 60°. Der Kühlschrank wird uns unterstützend über die Haltbarkeit des Inhalts aufklären. Und im Kaufhaus wird die Auswahl der passenden Kleidung durch profilangepasste Vorschläge untersützt [8]. Es lassen sich viele weitere Anwendungsgebiete vorstellen. Darunter auch Möglichkeiten, die sich durch die Ablösung des Strichcodes ergeben. Erste Jeanshosen der Marke Levis werden bereits mit RFID Tags ausgeliefert [1].

[1] www.heise.de/newsticker/meldung/72511

3 Angriffe auf die Privacy

Während der Strichcode nur innerhalb eines Produktes eindeutig ist - gemeint ist z.B. der Strichcode einer bestimmten Sorte Schokolade, ist der auf RFID Tags gespeicherte EPC (Electronic Product Code) für jeden Artikel dieses Produkts eindeutig. D.h. man könnte auch die Tafeln einer bestimmten Sorte Schokolade unterscheiden. Abbildung 1 zeigt die Aufteilung der 96bit EPC-Nummer nach dem Standardgeber EPCglobal. Außer der EPC Nummer wird auf dem RFID Tag nichts gespeichert. Sie dient als Schlüssel in eine Datenbank und kann so hinterlegte Informationen zu dem Tag liefern. Während sich durch die Verwendung des EPC völlig neue Möglichkeiten im Bereich der Logistik und des Bestandsmanagements (z.B. unsere Bibliothek) auftun, entstehen auch Gefahren. Welche das sind haben Sarah Spiekermann und Holger Ziekow [10] dargelegt.

	Header	General Manager Number	Object Class	Serial Number
GID-96	8	28	24	36
	0011 0101 (Binary value)	268,435,456 (Decimal capacity)	16,777,216 (Decimal capacity)	68,719,476,736 (Decimal capacity)

Abbildung 1. Die Struktur der EPC Nummer [9]

3.1 Unbemerktes Auslesen durch Dritte

RFID Tags können berührungslos und ohne Sichtkontakt ausgelesen werden. Bei den lowcost Tags, auf die hier der Schwerpunkt gelegt wird, kann sich das Lesegerät in bis zu 10m Entfernung befinden. Die Tags können von jeder Person, die über ein Lesegerät verfügt, ausgelesen werden. Und das unbemerkt! Der Angreifer kann also ohne größeren Aufwand in den Besitz der EPC Nummer gelangen. Um herauszufinden, welches Objekt sich hinter einer EPC Nummer verbirgt, benötigt der Angreifer Zugriff auf die Objektdatenbank. Nutzen könnte er dazu in der Zukunft einen EPC Informationsservice (EPC-ID), wie ihn das "Auto-ID Center"[2] (Object Name Service) oder "Verisign"[3] (EPC Discovery Service) plant. Mit der gewonnenen Information kann ein Profil der Person erstellt werden, um gezielte Werbung zukommen zu lassen. Ein Dieb erhält die Möglichkeit, seine Opfer auf lohnende Beute zu durchsuchen.

[2] http://www.autoidcenter.org
[3] http://www.verisign.com.sg/epc/registry.shtml

3.2 Verfolgbarkeit von Personen durch ihre Objekte

Wie heißt es doch so schön in einer Werbung von IBM: "RFID Radio Tags on the Cargo [...] helps track shipment". Das ist für den Logistiker gleichsam dem "Heiligen Gral". Zu recht stellt man sich die Frage, ob das nur für Objekte funktioniert oder auch für Menschen. Besinnt man sich auf die Tatsache, dass ein Mensch durch das Mitführen von Tags, die sich z.B. in den Turnschuhen befinden könnten, technologisch betrachtet nichts anderes als ein gelabeltes Objekt ist, liegt die Antwort auf der Hand. Die Tatsache, dass Objekte eindeutig nummeriert sind und von beliebigen Lesegeräten ausgelesen werden können, ermöglicht das Verfolgen von Personen. Sogar ohne zu wissen, wer die Person ist. Sie wird schließlich durch die mitgeührten Tags identifizierbar. Um die Person zu verfolgen, müssen die gelesenen IDs vieler Lesegeräte auf gemeinsame IDs, sprich übereinstimmende RFID Tags, durchsucht werden. Je mehr Lesegeräte im Umlauf sind, desto genauer kann die Spur verfolgt werden. Durch RFID kann also "Location Privacy" verloren gehen.

3.3 Auffinden sozialer Netzwerke

Es besteht die Möglichkeit aufgrund der Gewohnheiten einzelner Menschen, Gruppen von Personen zu bestimmen, die auf eine soziale Weise miteinander in Kontakt stehen. Dazu benötigt man Aufzeichnungen, zu welchen Zeitpunkten sich eine Person an welchen Orten aufhält. Eine feingranulare Analyse der Daten könnte auf diese Weise Personen finden, die sich auffällig häufig zu den selben Zeiten an den gleichen Orten befinden. Das kann das Ehepaar sein, dass jeden Sonntag morgen mit dem Hund in den Park geht oder Arbeitskollegen, die in der gleichen Straßenbahn fahren und gemeinsam zum Kaffeeladen gehen, ehe sie zusammen in einem Bürogebäude verschwinden. Diese Information könnte von Datamining Experten ausgenutzt werden, um gezielte Werbung zu verschicken, unter der Annahme, dass innerhalb einer Gruppe ähnliche Interessen bei den einzelnen Personen zu finden sind. Deutlich unangenehmer wird es, wenn eine kriminelle Person bei der Polizei auffällig geworden ist, und man unter Verdacht steht, weil man sich mit dieser Person innerhalb eines sozialen Netzwerkes befindet.

3.4 Verantwortlichkeit für Objekte

In [11] ist diese Bedrohung unter dem Namen Brotkrümmel zu finden. Durch die verbreitete Benutzung von Treuepunkte-Karten kann ein Indiviuum durch den Einkauf von RFID gelabelten Produkten eindeutig mit diesen Objekten in Verbindung gebracht werden. So würde der Electronic Product Code zusammen mit der ID-Nummer des Einkäufers in der Datenbank des Händlers gespeichert werden. Irgendwann wird sich der Besitzer von den eingekauften Objekten trennen, sei es weil die gekaufte Kettensäge nach Ablauf der Garantie nicht mehr funktioniert, es sich um ein Geschenk handelt, sie geklaut wird oder verloren geht. In der Datenbank gibt es weiterhin eine Verbindung zwischen der Kunden-ID

und dem Objekt. So wird mit der Zeit eine beträchtliche Spur an Brotkrümmeln gelegt, die alle zu einer Person führen. Und das ist der ursprüngliche Käufer des Objekts. Es könnte die unangenehme Situation entstehen, dass ein Objekt für eine Straftat benutzt wird, dass sich nicht mehr im Besitz des Käufers befindet. Jedoch führt das getagte Objekt zunächst einmal zum ehemaligen Besitzer, wodurch er fälschlicherweise unter Verdacht gerät.

3.5 Bevormundung durch Technik

RFID kann benutzt werden, um ein falsches Verhalten des Benutzers festzustellen und ihn darauf hinzuweisen. Beim Ersten hinschauen mag das sinnvoll und sogar vernünftig sein. Schließlich ist es gut, wenn der Kunde beim Einkauf im Supermarkt gewarnt wird, dass das ausgewählte Produkt eine Zutat enthält, auf die er allergisch reagiert. Und natürlich ist es zu begrüßen, wenn der Kühlschrank vor abgelaufenen Lebensmitteln warnt.
Doch was passiert, wenn ein Krankenhausbesucher das Gebäude nicht verlassen darf, weil der an der Tür angebrachte RFID Reader erkennt, dass man ihm Spaziergänge an der frischen Luft noch nicht erlaubt hat. Das mag sinnvoll und auch vernünftig sein. Und doch bleibt die Frage, ob die betroffene Person nicht selbst am Besten einschätzen kann, was für sie gut ist. Es ist nicht nur die mögliche Falschentscheidung, die hier ein Problem darstellt, sondern auch das Gefühl, dass beim Benutzer ausgelöst. Das Gefühl ein Kleinkind zu sein, dem die Mutter sagt, was falsch und was richtig ist. Regen sich bereits jetzt die meisten Computerbenutzer über eine freudestrahlend aufspringende Büroklammer auf, ist es sehr bedenklich, wie sie wohl reagieren, wenn sie nicht nur im Kaufhaus von Bildschirmen, zu Hause von Kühlschrank und Waschmaschine angesprochen werden und zu guter letzt beim Ausparken auch noch darauf hingewiesen werden, dass sie nicht angeschnallt sind.

4 Gegenmaßnahmen

In Abschnitt 3 wurde gezeigt, dass durch den Einsatz von RFID Technologie als Tag ein Verlust der Informationellen Selbstbestimmung droht, die in Deutschland 1983 vom Bundesverfassungsgericht im so genannten Volkszählungsurteil als Grundrecht anerkannt wurde und deren Ausgangspunkt das Allgemeine Persönlichkeitsrecht (Grundgesetzartikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1) ist. Diese Problematik hat auch die Politik erkannt und versucht sie zu lösen [12]. In diesem Abschnitt soll es nicht darum gehen wie Gesetze die Privatsphäre des Verbrauchers schützen können. Stattdessen soll anhand ausgewählter Verfahren vorgestellt werden, wie einer Beantwortung der Frage "Wie kann sich der Verbraucher gegen Angriffe auf seine Privatspähre schützen?" mittels einer technischen Lösung näher gekommen werden kann. Bei genauerer Betrachtung zeigt sich, dass jedes der Verfahren Vorteile wie Nachteile hat. Auch diese werden im folgenden aufgezeigt. Da die Integration von Schutzmaßnahmen auf dem Tag (on-Tag) momentan noch zu teuer sind, werden hier nur Möglichkeiten betrachtet, die außerhalb des Tag (off-Tag) realisierbar sind.

4.1 Manuelle Schutzmaßnahmen

Man hätte diesen Abschnitt auch mit "physikalische Lösung" bezeichnen können. Jedoch deutet der Begriff "händisch" bereits an, dass eine Aktivität des Benutzers gefordert wird, um seine Privatsphäre zu schützen.

Clipped Tag. Hierbei handelt es sich um einen speziellen Tag, der von IBM [13] entwickelt wurde. Hinter dem Verfahren steht die Idee, den maximalen Leseabstand - und somit auch den Abstand eines Angreifers - zu verringern. Und zwar auf wenige Zentimeter. Das engl. Wort clipped (zu deutsch kürzen) deutet an, wie das erreicht wird. Entlang einer Perforation kann der Benutzer einen Teil der Antenne entfernen.

Vorteile. Der Tag wird durch das Kürzen der Antenne nicht zerstört, sondern bleibt auslesbar. Es bleibt dem Verbraucher also überlassen ob, und wenn ja, zu welchem Zeitpunkt er die Lesereichweite des Tag verringern möchte. Das Vorgehen ist unkompliziert und sollte den Verbraucher vor keine Hürde stellen.

Nachteile. Der Clipped Tag ist nur soweit praktikabel, wie die Größe des Tags ein manuelles Eingreifen zulässt. Während das Preisschild an Kleidungsstücken im Kaufhaus ein attraktives Anwendungsgebiet ist, wird man die Antenne eines Tags in der Größe von einem Reiskorn nicht ernsthaft für dieses Verfahren in Erwägung ziehen. Kritik könnte auch daran geübt werden, ob der gekürzte Tag nicht doch aus der Ferne auslesbar ist, wenn ein leistungsfähiges und zielgerichtetes Lesegerät verwendet wird.

Faradaysche Käfig. Ein unbemerktes Auslesen lässt sich durch das physikalische Prinzip des Faradayschen Käfig verhindern. Aluminiumfolie ist z.B. ein Material, dass vor Radiowellen schützt. Für Smartcards, z.B. Zugangskontrollkarten oder Kreditkarten, gibt es bereits entsprechende Schutzhüllen zu kaufen [4]. Die mit Aluminiumfolie ausgestattete Geldbörse gibt es ebenfalls auf dem Markt [5].

Vorteile. Ein unbemerkte Auslesen des Tags wird zuverlässig verhindert. Die Radiowellen können das den Tag schützende Material nicht durchdringen.

Nachteile. In Zukunft können sehr viele Produkte mit RFID Tags bestückt sein. Bei vorgeschlagener Lösung wird sich der Verbraucher als mit Aluminium eingewickelte Mumie im Spiegel wiedererkennen.

[4] http://foebud.org
[5] http://www.thinkgeek.com RFID Blocking Wallet

4.2 Automatisierte Schutzmaßnahmen

Bei den oben vorgestellten händischen Lösungen wurde stillschweigend davon ausgegangen, dass man von der Anwesenheit des Tag weiß. Wegen der zunehmenden Miniaturisierung der Chips wäre diese Grundannahme jedoch ein Fehler. So hat Hitachi angekündigt Funkchips in der Größe von 0.15 mm x 0.15 mm herzustellen [14]. Während die beiden oben genannten händischen Maßnahmen zum Schutz der Privatheit im Speziellen eine gute Lösung darstellen mögen, sind für eine massentaugliche Lösung weitergehende Gedankengänge nötig.

Das Blocker Tag. Das Blocker Tag Verfahren [15] nutzt die Tatsache aus, dass ein RFID Lesegerät zu jedem Zeitpunkt nur mit einem RFID Tag kommunizieren kann. Sollte mehr als ein Tag auf die Anfrage eines Lesegerätes antworten, dann kommt es zur Kollision. Um diese auflösen zu können wird ein Protokoll benötigt, so dass das Lesegerät nacheinander mit den Tags kommunizieren kann. Diese Art von Protokoll nennt man "Singulation Protokoll". Ein solches ist auch das "tree-walking Protokoll", auf das sich die hier vorgestellte Lösung stützt. Es kommt vor allem bei RFID Systemen zum Einsatz, die mit einer Frequenz von 915Mhz arbeiten. Dazu gehören die low-cost Tags, die in Zukunft den Strichcode ersetzen werden.
Wie bereits in Abschnitt 3 erläutert, speichert diese simpelste Bauform nur die 96bit stellige EPC Nummer. Und eben diese möchte das Lesegerät vom RFID Transponder gesendet bekommen, um dann z.B. den Preis aus einer Datenbank auszulesen. Es wäre ein Fehler die gesamte EPC Nummer abzufragen, denn dann würden sich bei einem Einkaufswagen voll mit Artikeln alle Transponder zu Wort melden. Mit der Antwort könnte das Lesegerät nichts anfangen. Stattdessen fragt es gemäß dem "tree walking Protokoll" ein Bit nach dem anderen ab. In der Praxis beginnt man mit der Abfrage der höchstwertigsten Bits, weil diese die Herstellernummer repräsentieren und somit stark diskriminieren. Damit können bereits eine Menge Tags ausgeschlossen werden. Anhand eines kleinen Beispiels soll die Arbeitsweise des Protokolls erläutert werden. Abbildung 2 zeigt den Binärbaum, der abgesucht werden muss, wenn eine 3-bit Identifikationsnummer benutzt wird. Weil jedes Bit den Wert 1 oder 0 annehmen kann, gibt es gemäß des mathematischen Ausdrucks 2^3 acht mögliche Tags. In der Wurzel des Binärbaumes beginnend, werden durch Tiefensuche die tatsächlich vorhandenen Tags bestimmt. Dazu fordert das Lesegerät von allen Tags ihr höchstwertigstes Bit an. Ist die Antwort für alle Tags 1 oder für alle Tags 0, gibt es kein Problem. Es kann mit der Abfrage des nächsten Bit fortgefahren werden. Sollten bei einer Anfrage jedoch sowohl 0 als auch 1 als Antwort gegeben werden, kommt es zum Konflikt. Das Lesegerät muss sich merken an welcher Stelle der Konflikt aufgetreten ist. Es wird dann die Anfrage entweder im linken oder rechten Teilbaum des Knotens, in dem der Konflikt aufgetreten ist, fortsetzen und zu einem späteren Zeitpunkt die Anfrage im anderen Teilbaum weiterführen. Im Beispiel kommt es bereits in der Wurzel zur Kollision (optisch durch den rot markierten Knoten hervorgehoben). In diesem Beispiel soll davon ausgegangen werden, dass zunächst im linken Teilbaum weitergesucht wird. Das erste Bit auf dem Weg zu

einem Tag (Blatt im Baum) hat also den Wert 0. Bei Anfrage des nächsten Bit kommt es wieder zur Kollision. Wieder suchen wir im linken Teilbaum weiter. D.h. es ist 00 gelesen. Bei Anfrage des nächsten Bit wird 1 zurückgeliefert. Eine weitere Abfrage ist nicht möglich, weil 3 Bits abgefragt wurden. Das erste gefundene Tag hat also die ID 001. Die letzte Kollision trat beim Lesen des zweiten Bit auf. Daher setzen wir unsere Anfrage bei 01 fort und lesen das dritte Bit. Auch diese Anfrage ist eindeutig. Das zweite Tag trägt die Nummer 011. Gemäß der Tiefensuche wird man schließlich noch das letzte Tag mit der Nummer 111 finden.

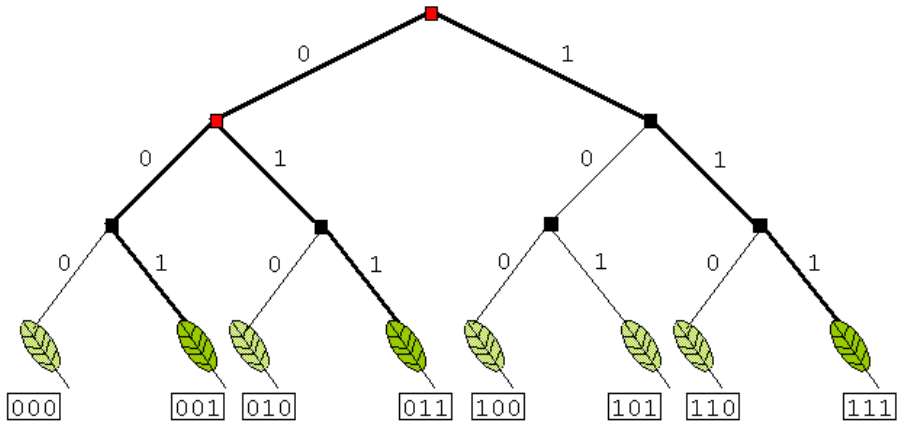

Abbildung 2. Tree-walking

Man wird bereits erahnen wie das Blocker Tag funktioniert. Bei jeder Anfrage des Lesegerätes liefert es eine 0 und eine 1 zurück, unabhängig davon ob sich entsprechende Tags in der Umgebung befinden oder nicht. Dazu ist es mit zwei Antennen ausgerüstet. Auf diese Weise repräsentiert das Blocker-Tag alle möglichen Tags. Bei Verwendung des EPC sind das 2^{96} Tags. Das Lesegerät ist daher gezwungen den gesamten Binärbaum abzusuchen. Da dies zu aufwändig ist, wird es zu einem timeout kommen und die Anfrage wird abgebrochen. Die Autoren des Papers sprechen von einem "Full Blocker", wenn der Blocker Tag die gesamte Mengen der Seriennummern simuliert.
Es könnte wünschenswert sein, nicht alle Tags vor dem Auslesen zu schützen. Damit z.B. nur die Tags eines bestimmten Hersteller vor Auslesen geschützt werden. Etwa den Hersteller von Schmuck, damit Diebe keine Möglichkeit haben, lohnende Opfer ausfindig zu machen. Umgekehrt formuliert könnte es sinnvoll sein bestimmte Tags nicht zu blockieren, weil sie gebraucht werden, um eine Dienstleistung einzufordern. Ein Beispiel ist die Fahrkarte für öffentliche Verkehrsmittel. Ein Blocker Tag, der nur eine Untermenge der möglichen Tags si-

muliert wird in [15] als "Selective Blocker" bezeichnet. Es gibt also bestimmte Zonen im Binärbaum, die blockiert sind, während der Rest des Baumes nicht blockiert wird. Beispielsweise könnten alle IDs die mit einer 0 beginnen blockiert werden, während alle IDs die mit einer 1 beginnen nicht blockiert werden. Theoretisch ist das sehr schön, aber praktisch gibt es noch ein Problem. Nach dem oben gezeigten Verfahren fängt das Lesegerät im linken Teilbaum der Wurzel an zu suchen. Da dieser im konkreten Beispiel vom Blocker Tag simuliert wird, hat das Lesegerät immer noch 2^{96-1} simulierte Tags abzufragen, ehe es die Zone verlässt und den nicht simulierten rechten Unterbaum der Wurzel abfragt. Die Abfrage von 2^{95} Tags dauert immer noch zu lange. Das Lesegerät wird also erneut blockiert.

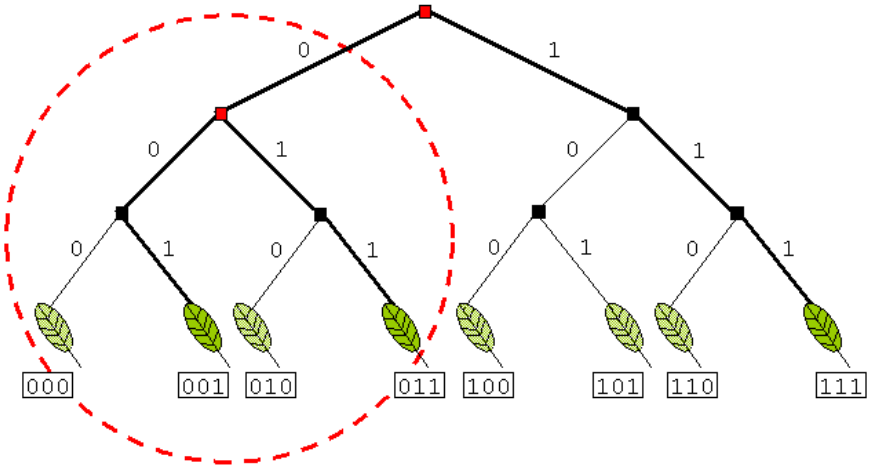

Abbildung 3. Blockieren von Zonen

Um dieses unerwünschte Verhalten zu verhindern, muss das Lesegerät wissen, wann ein Unterbaum blockiert wird. Dazu könnte das Protokoll um eine Funktion erweitert werden, die es dem Lesegerät erlaubt vor der eigentlichen Anfrage die Frage "ist der Unterbaum dieses Knoten blockiert?" zu stellen. Wenn die Antwort "Nein" ist, kann mit der Anfrage des nächsten Bit begonnen werden. Andernfalls wird an anderer Stelle fortgesetzt. Jules spricht bei dieser Lösung von "polite blocking", weil der Blocker Tag so freundlich ist zu sagen, welcher Teilbaum blockiert wird.
Zu recht stellt sich die Frage, ob durch die Anwendung eines Blocker Tags in einer alltäglichen Situation, wie dem Einkauf im Supermarkt, nicht auch Probleme entstehen. Gehen wir davon aus, dass in Zukunft das Bezahlen des Einkaufs im Supermarkt vollautomatisch über RFID Tags und Kreditkarte abgewickelt wird. Durch den Einsatz eines "Selective Blocker" könnte das Auslesen je nach gesetz-

ter Zone verhindert werden. Das muss nicht der eigene Blocker sein, sondern kann auch der des Nachbarn sein. Das Problem kann gelöst werden, indem ein Bit des 96 Bit langen EPC als "Privacy Bit" festgelegt wird. Das kann z.B. das höherwertigste Bit des "Object Manager" Codes sein. Der Blocker Tag würde dann nur diejenigen Tags blockieren, deren "Privacy Bit" auf 1 gesetzt ist. Das Privacy Bit der Produkte, die der Supermarkt verkauft, wäre bis zum Verkauf auf 0 gesetzt, so dass es zu keiner Blockierung durch einen Blocker kommt. Beim Kassiervorgang könnte das Privacy Bit dann automatisch auf 1 gesetzt werden, so dass ein Auslesen verhindert wird. Das Lesegerät seinerseits wird nicht versuchen Tags mit gesetztem Privacy Bit zu lesen, um nicht blockiert zu werden. Im Übrigen gleicht das dem Prinzip des heutigen Diebstahlschutzes in Kaufhäusern. An teurer Bekleidung findet sich hier häufig eine Diebstahlsicherung, die dann an der Kasse entfernt wird. Nur geht es jetzt darum ein Bit zu setzen, das darüber entscheidet, ob der EPC gelesen werden kann oder nicht.

Vorteile. Der Benutzer kann sich vor unbemerktem Auslösen schützen. Dazu muss er noch nicht einmal wissen, dass er im Besitz eines Tags ist. Die Herstellung eines primitiven Blocker Tags ist billig. Der Benutzer wird nicht mit der Verwaltung von Passwörter belastet, wie es bei On-Tag Verfahren der Fall wäre.

Nachteil. Durch den Einsatz eines Blocker Tags könnten die Tags einer anderen Person unbeabsichtig gestört werden. Das "Privacy Bit" löst dieses Problem. Der absichtliche Missbrauch eines "Full Blocker" als Denial of Service Attacke kann jedoch nicht verhindert werden. Ein Ladendieb hätte so in Zukunft leichtes Spiel. Zumindest könnte der Einsatz eines "Full Blockers" erkannt werden. Erkennt ein Lesegerät im Supermarkt mehr als 1000 Tags im Einkaufswagen, dann ist es wahrscheinlich, dass das Lesegerät blockiert wird. Der Backscatter eines jeden Tags ist charakteristisch. Durch genaues hinsehen könnte die Antwort des Blocker Tag gefiltert werden.

Der RFID Guardian. Der RFID Guardian ist die Idee eines portablen Geräts, das z.B. in das Handy integriert werden könnte, und eine Reihe von Aufgaben erledigen soll, um den Benutzer gefahrlos durch eine mit RFID Tags gespickte Welt zu begleiten [16,17]. Diese Aufgaben sind:

- Auditierung (engl. Auditing)
- Schlüsselverwaltung (engl. Key Management)
- Zugriffskontroll (engl. Access Control)
- Authentifizierung (engl. Authentication)

Auditing. Im Kontext von RFID bedeutet Auditierung zweierlei:

1. Das Prüfen auf RFID Aktivität in der Umgebung. Dazu nutzt der RFID Guardian seine Fähigkeit einen Tag zu emulieren, und zeichnet gleichzeitig alle Anfragen auf, die das Lesegerät stellt, um so zu einem späteren Zeitpunkt gegen illegale Benutzung von RFID Anfragen - z.B. weil der Besitzer des Gerätes nicht darauf hinweist, dass er ein Lesegerät benutzt - vorzugehen.

2. Das periodische Prüfen auf neue Tags in der Umgebung durch den RFID Guardian mit der Funktionalität als Lesegerät. Dies verhindert, dass Tags unbemerkt mitgeführt werden. Damit "Falsch Positiv" (engl. false positive) Meldungen verhindert werden, wird gefordert, dass die Tags über einen gewissen Zeitraum konstant auftauchen. Dadurch wird verhindert, dass der Guardian z.B. beim Einkauf im Supermarkt alle neuen Tags in der Umgebung meldet, die aber gar nicht zur Person gehören.

Schlüsselverwaltung. On-Tag Sicherheitsmechanismen wie Kill-Funktionen, Verschlüsselung, Sleep/Wake-Operationen, die dem Benutzer die Kontrolle über seine Tags geben sollen, fordern vom Benutzer eine Authentifizierung. Das kann ein Passwort sein oder auch ein Schlüssel. Im Moment kommen diese On-Tag Lösungen noch nicht vermehrt zum Einsatz, weil sie die Herstellungskosten in die Höhe treiben. In Zukunft wird sich das aber ändern, so dass der Benutzer leicht den Überblick verlieren kann, welcher Schlüssel zu welchem Tag gehört. Der RFID Guardian soll den Benutzer von der lästigen Schlüsselverwaltung befreien und diese Aufgabe automatisch im Hintergrund übernehmen. Als Lesegerät kann er dann auf Wunsch Tags mit Hilfe der Schlüssel sperren/entsperren. Das heißt der Benutzer braucht für diese Aufgabe keine zusätzliche Hardware.

Zugriffskontrolle. "Zugriffskontrolle" regelt, welche RFID Lesegeräte auf welche Tags zugreifen dürfen und unter welchen Umständen. Dazu muss sich das Lesegerät beim RFID Guardian auszeichnen. Dieser wird dann den Zugriff entsprechend der festgelegten Strategie steuern. Abbildung 4 zeigt, wie eine Zugangskontrolliste (ACL) aussehen könnte. Das Lesegerät von Wal-Mart darf beispielsweise jeden Tag lesen, der zu der Gruppe "MYTAGS" gehört. Schreiben darf er einen solchen Tag nicht, denn es findet sich zum Target "MYTAGS" keine Regel, in der als Source "Wal-Mart" steht, und ein schreiben erlaubt wird.

Authentifizierung. Damit die ACL funktioniert, muss der Guardian feststellen, welches Lesegerät in der Umgebung die Anfrage stellt.

Durch das Verwenden von "Zugriffskontrolle" in Verbindung mit "Schlüsselverwaltung" und "Authentifizierung" können Tags mit on-Tag Funktionen wie sleep/wake durch den RFID Guardian nach einer Strategie automatisch schlafen gelegt bzw. aktiviert werden. Während die Klamotten sich während des Stadtbummels ruhig verhalten sollen, ist es hilfreich, wenn die Waschmaschine den Benutzer rechtzeitig warnt, bevor das weiße T-Shirt durch die rote Socke rosa gefärbt wird. Auch RFID Tags ohne integrierte Schutzfunktionen kann der RFID Guardian schützen. Hat er entsprechend der ACL festgestellt, dass ein Lesegerät nicht berechtigt ist einen Tag auszulesen verhindert er dessen Antwort durch "Selective Jamming". Ein zufällig moduliertes Störsignal wird ausgesendet. Zufällig deshalb, weil ein konstantes Störsignal von dem Lesegerät erkannt und ausgefiltert werden könnte.

Action	Source	Target	Command	Comment
block	*	MYTAGS	*	Suppress all queries targeting user's tags
allow	Home	MYTAGS	*	Home system can query user's tags
allow	Wal-Mart	MYTAGS	Read data block	Wal-Mart can read (not write) data from user's tags
allow	*	*	*	All queries to other RFID tags are OK

Abbildung 4. Beispiel Access Control List

Vorteile. Mit Hilfe des RFID Guardian können individuelle Strategien zum Schutz vor unbemerkten Auslesen festgelegt werden. Als Schlüsselverwalter findet er sein Einsatzgebiet nicht nur bei lowcost RFID Tags, sondern auch bei RFID Tags mit Zusatzfunktionen wie sleep/wake, welche passwortgeschützt sind.

Nachteil. Der RFID Guardian selbst stellt ein lohnendes Angriffsziel dar. Das Einsetzen eines Störsignals, um nicht authorisiertes Auslesen zu verhindern, könnte je nach Land illegal sein. Durch gezielte Ausrichtung der Antenne könnten RFID Lesegeräte weiterhin auf Tags zugreifen. Der RFID Guardian ist auf eine aktive Stromversorgung angewiesen. Integriert im Handy würde der Schutz vor unbemerktem Auslesen nur so lange anhalten, wie der Akku Energie liefert.

5 Abschließende Worte

In der RFID Technik steckt zweifellos ein gewaltiges Potential. Dessen Gefahr ist es jedoch eine Technik in den Alltag des Menschen zu bringen, bei deren Entwicklung dem Schutz der Privatsphäre bisher zu wenig Beachtung gewidmet wurde. Diese Seminararbeit hat versucht die Problematik aufzuzeigen, die durch den Missbrauch der Technik entstehen kann. Sie hat auch gezeigt, dass es noch keine hundertprozentige Lösung gibt.
Daher liegt es jetzt auch in der Hand des Verbrauchers gegenzusteuern. Er muss Druck auf die Industrie ausüben, aber auch auf die Politik, die in Zeiten des Terrorismus für die Popularität des Schlagwortes "Überwachungsstaats" verantwortlich ist. Es wird also höchste Zeit, dass sich der Bürger daran erinnert, dass er Macht hat. So konnte er im Jahr 1984 die Volkszählung verhindern. Nach [18] legt er Wert auf seine Privatsphäre. Nun muss er sich noch an die Frage erinnern, die durch einen von Technik durchzogenen Alltag in Vergessenheit geraten ist. Sie lautet "'Was ist das für ein neumodischer Kram?!"'

Literatur

1. Melanie R. Rieback and Bruno Crispo and Andrew S. Tanenbaum: The evolution of RFID security (IEEE Pervasive Computing, Vol. 5, No. 1, 2006, pages 62-69)
2. J. Landt: The history of RFID (IEEE Potentials, Vol. 24, No. 4, 2005, pages 8-11)
3. http://de.wikipedia.org/wiki/Radio_Frequency_Identification
4. Ron Weinstein: RFID - A Technical Overview and Its Application to the Enterprise (IT Professional, Vol. 7, No. 3, 2005, pages 27-33)
5. Mit Funk-Chips in die Zukunft (elektor 9/2006)
6. Die Spur der Säge (Der Spiegel, No. 2, 08.01.07, pages 46-50)
7. A. Graafstra: Hands On (IEEE Spectrum, Vol. 44, No. 3, pages 18-23)
8. RFID Schwemme (http://www.network-secure.de, 01.05.2007)
9. EPCglobal: EPC Tag Data Standards Version 1.1 Rev.1.24 (Standard Specification 01.April 2004)
10. Sarah Spiekermann and Holger Ziekow: RFID - A Systematic Analysis of Privacy Threats & A 7-point Plan to Adress Them
11. Simson L. Garfinkel and Ari Juels and Ravi Pappu: RFID Privacy - An Overview of Problems and Proposed Solutions (IEEE Security and Privacy vol.3 no.3 2005 pages 34-43)
12. Funkfrequenzkennzeichnung (RFID) in Europa - Schritte zu einer ordnungspolitischen Rahmen (SEC(2007)312)
13. IBM White Paper: Privacy-Enhancing Radio Frequency Identification Tag - Implementation of the Clipped Tag
14. http://www.heise.de/newsticker/meldung/8432)
15. Jules, Rivest, Szydlo: The blocker tag - selective blocking of RFID tags for consumer privacy (CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, pages 103-111)
16. Rieback, Crispo, Tanenbaum: Keep on Blockin' in the Free World - Personal Access Control for Low-Cost RFID Tags (Proc. 13th International Workshop on Security Protocols 4/2005)
17. Rieback, Crispo, Tanenbaum: RFID Guardian - A Battery-Powered Mobile Device for Privacy Management (ACIDP 2005, pages 184-194)
18. Spiekermann, Grossklags, Berendt: E-privacy in 2nd generation E-commerce - privacy preferences versus actual behavior (EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce, 2001, pages 38-47)