Die Kontroverse um RFID

Stéphane Beer

ETH Zürich

Zusammenfassung Spätestens seit WalMart im Juni 2003 angekündigt hat, dass ab 2005 jeder Zulieferer seine Palletten mit einem RFID Tag ausrüsten muss, hat sich die RFID Technologie durchgesetzt. Die wichtigsten Anwendungen dieser zukunftsträchtigen Technologie finden sich jedoch nicht nur in Produktionsketten, sondern in diversen Bereichen des täglichen Lebens. Obwohl RFID viele Bereiche in unserem täglichen Leben vereinfachen wird, sind viele Probleme mit der Anwendung dieser Technologie verbunden. Insbesondere der Begriff Privacy wird in diesem Zusammenhang immer wieder erwähnt.

1 Einführung

1.1 Radio Frequency Identification - RFID

Radio Frequency Identification, oder RFID, ist eine Technologie, die es ermöglicht, ein Objekt zu erkennen, ohne dass direkter Sichtkontakt besteht. Dabei wird an einem Objekt ein sogenannter RFID Tag angebracht (Abbildung 1) und dieser übermittelt mittels Radiowellen einem Lesegerät eine eindeutige Identifikationsnummer. Die wichtigste Eigenschaft der RFID Technologie besteht darin, dass zwischen dem Tag und dem Lesegerät kein Sichtkontakt bestehen muss. Die Wurzeln dieser Technologie reichen bis in den zweiten Weltkrieg. In England konnte man durch das Radar Flugzeuge zwar bereits erkennen, jedoch nicht identifizieren. Um diesen Missstand zu korrigieren, brachte man Transponder an den Flugzeugen an, welche die Flugzeuge als Freund oder Feind identifizierten.

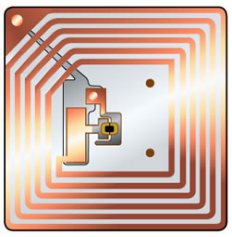

Abbildung 1. RFID Tag [6]

1.2 Der elektronische Produktcode - EPC

Der elektronische Produktcode (Abbildung 2), kurz EPC, ermöglicht eine weltweit eindeutige Identifikation von Produkten. Dazu enthält er eine Nummer, die einem Hersteller eindeutig zugeordnet ist. Ein so genannter Object Name Service (ONS) ordnet der EPC-Seriennummer eine Internet-Adresse in Form einer URL zu, die auf eine Objektbeschreibung des Herstellers verweist. Somit können Informationen über getagte Produkte jederzeit über das Internet abgerufen werden. Die Entwicklung erfolgt durch die Organisation EPCglobal in Massachusetts, USA.

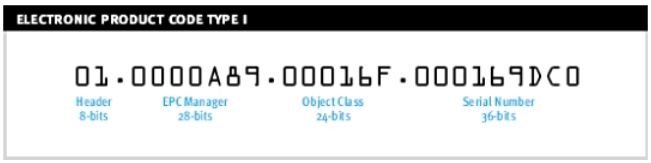

Abbildung 2. Elektronischer Produktcode [7]

2 Gegenwärtige und zukünftige Anwendungsgebiete von RFID

WalMart verkündete im Juni 2003, dass seine 100 wichtigsten Lieferanten ab Januar 2005 ihre für drei ausgewählte Distributionszentren bestimmten Kisten und Paletten mittels RFID-Etiketten kenntlich machen müssen. Diese Ankündigung hatte zur Folge, dass die Nachfrage nach RFID Tags in die Höhe schnellte, wurde doch erwartet, dass alleine die hundert grössten Lieferanten jährlich etwa 1 Million Tags benötigen würden. Ausserdem brachte diese Ankündigung der RFID Technologie zwei weitere Vorteile. Auf der einen Seite war der Weg für einen Standard geebnet und zum anderen konnten die Herstellungskosten durch die riesige Nachfrage drastisch gesenkt werden. Kostete ein Tag bis anhin etwa 25-50 Cents, würde ein solcher in Zukunft etwa 5-10 Cents kosten. WalMart erhoffte sich durch dieses RFID Tagging Einsparungen von bis zu 407 Millionen Dollar pro Jahr. Dies sollte durch den Rückgang von Diebstählen in der Produktionskette, Steigerung der Verkaufseinnahmen durch Verminderung von ausverkauften Gütern und exakteren Voraussagen über den Nachfüllbedarf gewisser Bestände erreicht werden.

2.1 Item-level Tagging

Dass WalMart Kisten und Palletten durch Tags eindeutig identifizierbar machen will, soll nur der Anfang sein. Der Grosskonzern erhofft sich in Zukunft durch das Anbringen von RFID Tags an jedem einzelnen Produkt Einsparungen von bis zu

7.6 Milliarden Dollar pro Jahr. Der RFID Tag enthält dabei einen elektronischen Produktcode, der es ermöglicht, über einen Object-Name-Server Anfragen über die Grösse, das Gewicht, Ablaufdatum, Herstellungsort, Versanddetails usw. zu machen. Der Hauptgrund für dieses Vorhaben besteht jedoch wiederum darin, die Lagerbestände besser kontrollieren zu können. Dadurch lassen sich die Warenbestände nicht mehr nur im Lager ermitteln, sondern direkt in den Regalen der Geschäfte. Regale, welche mit RFID Lesegeräten ausgerüstet sind, werden dann die volle Kontrolle über die Artikel haben, welche sich in denselben befinden. Der Nutzen der Tags bleibt jedoch nicht nur auf die Produktionskette beschränkt, denn der Kunde kommt beim Kauf eines Gegenstandes ebenfalls in den Besitz des Tags. So wäre es beispielsweise möglich, dass ein Kunde eine Tiefkühlpizza kauft, welche mit einem RFID Tag versehen ist und diese bei sich zu Hause im Ofen backen kann, wobei sich der Ofen anhand der Daten auf dem RFID Chip selber einschaltet. Ein Lesegerät im Ofen identifiziert die Pizza beim Einlegen und stellt automatisch die richtige Temperatur und Backzeit ein. Wirtschaftsexperten vermuten jedoch, dass Item-level Tagging noch mindestens ein Jahrzehnt enfernt ist. [1]

2.2 Human Implants

Im Dezember 2001 führte Applied Digital Solutions (ADS) den VeriChip (Abbildung 3) ein. Dieser Chip, eingehüllt in einem kleinen Glasbehälter der Grösse eines Reiskorns, wird üblicherweise oberhalb des Trizeps unter die Haut des rechten Armes eingepflanzt und erlaubt es, eine Person zu identifizieren und somit auf persönliche Daten zuzugreifen. ADS verkaufte 2004 etwa 7000 VeriChips. Der Baja Beach Club in Barcelona und die Bar Soba in Glasgow offerieren ihren Stammkunden eine VIP Mietgliedschaft, wenn sich diese bereit erklären, einen VeriChip zu implantieren. Auch die United States Food and Drug Administration (FDA) hat den Einsatz von VeriChips gutgeheissen, um schnell und effizient auf die Krankengeschichte eines Patienten zugreifen zu können. In den USA verfügen bereits über 60 Krankenhäuser über die nötige Infrastruktur, um mittels VeriChips auf die Krankengeschichte ihrer Patienten zugreifen zu können. VeriChip hebt drei Vorteile bei der Benützung ihrer Technologie besonders hervor:

- Die Chips stellen eine gesicherte, manipulationsgeschütze Mikrochiptechnologie dar, die eine unmittelbare Identifikation und Abfrage von persönlichen Informationen erlaubt.
- Der Zugang zu den persönlichen Informationen erfolgt gesichert und passwortgeschützt.
- Betreuung und Unterstützung durch eine ständig wachsende Anzahl von Partnergesellschaften im Bereich Finanzen und Sicherheit und einer Anzahl an anderen Gesellschaften

In Portugal hat die Regierung angeordnet, dass alle Hunde (etwa zwei Millionen) des Landes mit einem VeriChip ausgerüstet und in einer nationalen Datenbank

erfasst werden sollen, um so die Tollwut zu bekämpfen. In den USA haben im Jahr 2003 pro Monat schätzungsweise 6000 Hundebesitzer durch den Einsatz von RFID Chips ihre vermissten Tiere wiedergefunden.

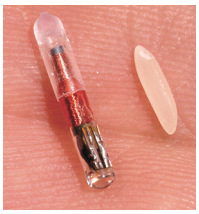

Abbildung 3. VeriChip [8]

2.3 RFID-chipped Passports or National ID Cards

Als Folge der Anschläge vom 11. September in New York City, hat die US-amerikanische Regierung Anstrengungen unternommen, Ausweise zu kreieren, die einerseits sicher und andererseits schwierig zu fälschen sein sollten. Sie kam zum Schluss, dass die einzige Möglichkeit, dies zu erreichen, der Einbau von RFID Tags sei. Die Ausweise basieren auf einem Standard, welcher von der Civil Aviation Organization (ICAO) entwickelt wurde und der verlangt, dass der Ausweis mit einem Chip ausgestattet wird, welcher alle Daten enthält, die auch auf dem Ausweis gedruckt sind, und zusätzlich ein digitales Lichtbild und mindestens eine biometrische Kennung.

3 Bedrohungen und Probleme aktueller und künftiger RFID-Technologien

3.1 Item-level Tagging

Obwohl die Zeit, in der jedes einzelne Produkt mit einem RFID Tag versehen ist, noch mindestens ein Jahrzehnt entfernt wird, gilt es als sicher, dass diese aufgrund der sinkenden Preise der entsprechenden Infrastruktur und der Tags kommen wird. Dies würde nach sich ziehen, dass die Tags nicht mehr nur in der Produktionskette eines Artikels zum Einsatz kommen, sondern dass diese auch tatsächlich in den Besitz eines Kunden kommen. Geschäfte könnten dann, auch als Massnahme zum Schutz vor Diebstahl, an jedem Ein- und Ausgang RFID Reader anbringen. Damit wäre es möglich jegliche Tags, die eine Person, welche das Geschäft betritt oder verlässt, auf sich trägt, zu lesen. Gegenstände wie Schuhe, die von einer Person täglich getragen werden und mit einem Tag versehen wären, könnten durch Geschäfte als persönliche Kennung genutzt werden und erlaubten eine gezielte Auflistung von Geschäften, welche die entsprechende

Person betritt. Falls Geschäfter zusätzlich bei einem Kauf eines Artikels Zahlungsinformationen mit den Informationen der Artikel verknüpfen, erlaubt dies nicht mehr nur die Verfolgung einer anonymen Person, sondern die Einkaufsgewohnheiten, Aufenthaltsorte und Aktionen eines bestimmten Individuums zu erfassen.
Abbildung 4 zeigt die verschiedenen Bereiche, in denen RFID Tags in Zusammenhang mit EPC zum Einsatz kommen:

- Innerhalb der Produktionskette (supply chain). Dies Umfasst die Fabrik, in welcher die Waren hergestellt werden, die Transportsysteme sowie die Lagerhallen der einzelnen Geschäfte.
- Die Übergangszone, also der Bereich wo der Arktiel seinen Besitzer wechselt. Dieser umfasst die Zone zwischen dem Regal, auf welchem der Gegenstand präsentiert wird, bis zur Kasse, wo der Artikel bezahlt wird.
- Ausserhalb der Produktionskette. Diese Zone umfasst alle Bereiche ausserhalb der Produktionskette bis einschliesslich des Zuhauses des Kunden.

Bedrohungen können weiter aufgeteilt werden in solche, die hauptsächlich Firmen und andere Organisationen betreffen und solche, die vor allem einzelne Personen betreffen.

Bedrohungen für Firmen und Organisationen Corporate Espionage Threat: Objekte, welche mit Tags versehen sind, können von der Konkurrenz auf sehr einfache Art und Weise ausgelesen werden, um so Informationen über die Produktionskette zu erlangen.
Competitive Marketing Threat: Durch mit Tags versehene Objekte lassen sich einfach Informationen über Einkaufsgewohnheiten einzelner Personen sammeln. Damit lassen sich exakte Marketingstrategien entwickeln.
Infrastructure Threat: Geschäfte, welche sogenannte Smart-Shelves einsetzen, sind sehr empfindlich auf Denial-of-Service attacks.
Trust perimeter Threat: Während Geschäfte immer grössere Mengen an Daten miteinander austauschen, werden diese immer empfindlicher auf Angriffe auf eben diese Daten.

Bedrohungen für einzelne Personen Action Threat: Werden zum Beispiel Gegenstände in einem Geschäft angehoben, wäre ein mögliches Szenario, dass eine Kamera auf den Kunden gerichtet wird, die beobachtet, wie der Kunde mit diesem Gegenstand interagiert.
Association Threat: Beim Kauf eines Gegenstandes wird ohne das Wissen des Kunden die Information des Objekts mit den Informationen der Person verknüpft. Dies kann beispielsweise durch die Zahlungsinformationen geschehen.
Location Threat: Durch Tags an Objekten kann wie im einleitenden Abschnitt bereits erwähnt eine Person verfolgt werden und der momentane Aufenthaltsort bestimmt werden.
Preference Threat: Ebenfalls bereits im einleitenden Abschnitt erwähnt, ist es durch Item-level Tagging möglich, Einkaufsgewohnheiten und Vorlieben einer

einzelnen Person zu erfassen.
Constellation Threat: Selbst wenn keine persönlichen Daten mit einem Objekt verknüpft werden, ist es möglich, eine Person ohne genaueres Wissen über diese zu Verfolgen.
Transaction Threat: Wenn ein Objekt den Besitzer wechselt, ist es möglich durch die Informationen zu ermitteln, was für eine Transaktion zwischen den beiden Parteien stattgefunden hat.
Breadcrumb Threat: Objekte, die weggeworfen werden, sind möglicherweise immer noch mit den Informationen einer bestimmten Person verknüpft. Bei einem Verbrechen könnten diese am Tatort gefundenen Objekte möglicherweise Hinweise auf einen falschen Täter liefern, nämlich auf diejenige Person, welche zuletzt im Besitz dieses Objektes war.

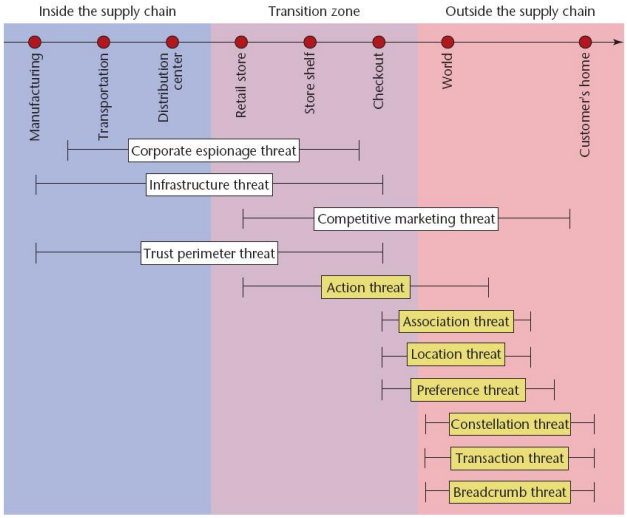

Abbildung 4. Item-level Tagging Bedrohungen. Gelb markierte Bedrohungen bezeichnen Gefahren für die Privatsphäre, während weisse Bedrohungen auf Gefahren für geheime Firmendaten hinweisen [2]

3.2 Human Implants

ADS behauptet, dass die Informationen in ihrem System sicher und passwortgeschützt sind und dass diese nur durch ihre eigenen Geräte ausgelesen werden können. Die Vergangenheit hat jedoch oft gezeigt, dass Behauptungen dieser Art widerlegt wurden. Der Justizminister von Mexiko befürwortete den Einsatz von VeriChips als Waffe gegen die steigende Anzahl von Entführungen. Allerdings sind VeriChips passive Chips und senden somit keine Informationen, solange

sie nicht von einem Lesegerät gescannt werden. Solange also keine flächendeckenden Netze von Lesegeräten zur Verfügung stehen, kann diese Technologie Entführungsopfer erst dann identifizieren, wenn diese bereits gefunden worden sind. Als Reaktion auf diesen Vorwurf hat ADS einen Personal Security Chip entwickelt, welcher eine GPS Einheit enthält, die ihre Position durch das Mobiltelefon des Trägers übermittelt. Weil die Existenz dieser Chips auch einem Entführer nicht unbekannt ist und diese immer an der selben Stelle eingepflanzt werden, wäre es jedoch ein Leichtes, diese Chips zu entfernen. Dieses Szenario deckt nicht nur die Untauglichkeit dieser Chips gegen mögliche Entführungen auf, sondern auch gegen die eindeutige Identifizierung einer Person, da entfernte Chips leicht einer anderen Person eingepflanzt werden könnten. Es ist nicht anzunehmen, dass sich Stammgäste des Baja Beach Clubs Chips aus diesem Grund entfernen lassen würden, aber sollten Banken wie auch staatliche Organisationen Chips als Zugangskontrolle zu Sicherheitsbereichen einsetzen, würden diese Chips sehr viel wertvoller und solche Szenarien wären durchaus denkbar.
Nebst den Nachteilen in der Anwendung dieser VeriChips, äussert die Food and Drug Administration [4] auch medizinische Bedenken. Bei Tierversuchen hat sich herausgestellt, dass die Wahrscheinlichkeit des Auftretens eines Tumors bei Tieren mit einem VeriChip um ein Vielfaches höher ist, als bei Tieren, welche keinen VeriChip in sich tragen. Ausserdem konnten bei Patienten mit einem VeriChip keine Kernspintomografien mehr durchgeführt werden.
Wie schwierig es ist, sich einen VeriChip wieder entfernen zu lassen, musste die CNN-Reporterin Robyn Curnow am eigenen Leib erfahren. Im Zuge einer Reportage liess sie sich im Baja Beach Club in Barcelona einen VeriChip in ihren rechten Oberarm einfügen. Zurück in London war es erst durch einen Spezialisten möglich, den Chip wieder zu entfernen. Dieser hatte sich vom ursprünglichen Punkt verschoben und war, obwohl durch ein Röntgengerät sichtbar, nicht ganz einfach aufzufinden. Erst durch den Einsatz eines speziellen Röntgengerätes und zwei Monitoren konnte der Chip unter einer Teilnarkose des rechten Oberarmes wieder entfernt werden.[5]

3.3 RFID-chipped Passports or National ID Cards

Während Item-level Tagging und Human Implants noch mindestens ein Jahrzehnt entfernt ist, sind mit RFID Chips ausgerüstete Ausweise bereits in Verwendung und dementsprechend sind auch die Probleme und Bedrohungen dadurch allgegenwärtig. Das Problem, dass die Daten eines Ausweises ohne das Wissen des Besitzers ausgelesen werden können, könnte zu einer ernsthaften Bedrohung werden. Der Name einer Person, die exakte Adresse sowie ihr Geburtsort wie auch Datum könnten ohne weiters ermittelt werden und als falsche Identität gebraucht werden. Weitaus bedrohlicher ist die Tatsache, dass auch die Nationalität ermittelt werden kann. Diese Information wäre beispielsweise wertvoll für Taschendiebe, Entführer und Terroristen bei Reisen in fremde Länder. An einem belebten Ort wäre es kein Problem, ein Lesegerät nahe genug an einen Chip zu bringen, um diesen auszulesen. Sobald die Identität einer Person ermittelt ist,

Abbildung 5. VeriChip Gegner [9]

kann ihr Wert für eine entsprechende Aktion abgeschätzt werden. Zudem wäre es sehr einfach Reisende, die einen Pass mit sich tragen, zu verfolgen.

4 Mögliche Lösungsansätze und Richtlinien

4.1 Technische Lösungen

Aluminium-Folie Die einfachste und auch billigste Lösung, um zu verhindern, dass ein RFID Chip ausgelesen wird, ist diesen mit einer Aluminium Folie zu umgeben. Dies wird aufgrund ihrer Einfachheit mittelfristig mit Sicherheit die am weitesten verbreitete Lösung sein. Ausweise sowie Pässe und Identitätskarten sowie zukünftig mit RFID Tags versehene Banknoten lassen sich damit vor ungewolltem Zugriff schützen. Human Implants sowie Kleidung und andere Gegenstände, welche sich nicht einfach mit einer Folie umschliessen lassen, werden jedoch immer noch verwundbar bleiben.

Tag Killing Im Bereich von Item-level Tagging gilt Tag Killing als die Lösung aller Privacy Probleme. Die meisten RFID Tags haben eine Kill Funktion, die es erlaubt, dass der Tag nicht mehr weiter funktionsfähig ist. Falls Tags auf Objekten demnach beim Kauf funktionslos gemacht würden, wäre die Privatsphäre durch tote Tags in keiner Weise mehr bedroht. Gegen diese Lösung spricht, dass immer noch festgestellt werden kann, wer die jeweiligen Gegenstände gekauft hat und dass tracking innerhalb eines Geschäfts immer noch möglich ist. Ein weiterer Grund, der dagegen spricht, ist dass ein Objekt somit nach dem Kauf nicht mehr identifizierbar ist und somit auch die damit einhergehenden Vorteile

nicht mehr genutzt werden können. Ein Kunde, der sich beispielsweise eine Tiefkühlpizza kauft, könnte nicht mehr vom Vorteil profiteren, dass andere Geräte, wie zum Beispiel der Backofen zu Hause, diese identifizieren kann.

Blocker Tag Aufgrund der Annahme, dass viele Leute die Tags an gekauften Gegenständen nicht deaktivieren würden, haben RSA Laboratorien Blocker Tags entwickelt, eine alternative Methode, um die Privatsphäre einer einzelnen Person zu schützen. Ein solcher Tag ist in der Lage, die Funktion eines Lesegerätes ausser Betrieb zu setzen, indem dieser jeden möglichen RFID Code übermittelt und es somit dem Lesegerät verunmöglicht, den wahren Code von irgendwelchen Daten zu unterscheiden. Diese Lösung scheint ein guter Mittelweg zwischen der Aluminium-Folie und dem Tag Killing zu sein, schafft sie doch im Umkreis von etwa 1.5 m eine Zone, in der die Privatsphäre einer Person gewahrt bleibt, weil in dieser kein Tag gelesen werden kann. Ausserdem kann jeder Tag durch Entfernen dieses Blocker Tags gelesen werden. Leider sind trotzdem einige Nachteile mit dieser Lösung verbunden. Es ist durchaus vorstellbar, dass an gewissen Orten diese Blocker Tags verboten werden. Falls ein Sicherheitssystem eines Geschäftes auf RFID basiert, liegt es im Interesse dieses Geschäfts, dass Blocker Tags in demselben verboten sind. Auch an Flughäfen würden solche Tags höchstwahrscheinlich verboten, würden sie doch die Identifizierung von Reisenden mittels ihrer mit RFID Tags versehenen Ausweisen ausser Gefecht setzen.

Tag Pseudonyms RFID Tags könnten ihre Serienummer periodisch ändern. Man könnte einem Tag also verschiedene Pseudonyme $p_1, p_2, \ldots p_k$ vergeben und diese abwechselnd durch Lesegeräte auslesen lassen, jedesmal wenn der Tag gelesen wird. Unbefugtes Verfolgen eines Tags wäre so um einiges komplizierter, dürfte es doch schwierig sein, herauszufinden welche Tags zu welchem Objekt gehören.

Encryption Eine weitere Alternative wäre, die Daten auf RFID Tags zu verschlüsseln. Dies führt aber zwei grundlegende Probleme mit sich. Zum einen stellt sich die Frage nach dem sogenannten Key Management. Wie würden die Schlüssel, die zur Entschlüsselung notwendig sind, gehandhabt und verteilt? Auf der anderen Seite löst eine Verschlüsselung das Tracking-Problem nicht. Auch eine verschlüsselte Information ist eine eindeutige Kennung und erlaubt somit eine Verfolgung und Ansammlung von Daten einer bestimmten Person.

4.2 Politische / Rechtliche Lösungen

Nebst den im vorigen Abschnitt präsentierten technischen Lösungen insbesondere zur Wahrung der Privatsphäre gibt es auch Ansätze, die Nachteile der RFID Technologie durch politische sowie rechtliche Richtlinien und Gesetze zu minimieren.

The RFID Bill of Rights RFID und Privacy Experte Simson Garfinkle stellte 2002 die sogenannte RFID Bill of Rights zusammen. Diese sollten als Richtlinien von Unternehmen auf freiwilliger Basis befolgt werden, um die Privatsphäre von Konsumenten zu schützen. Die fünf wichtigsten Grundrechte eines Konsumenten lauten demnach:

- Das Recht zu wissen, ob ein Produkt einen RFID Tag enthält oder nicht
- Das Recht RFID Tags von Gegenständen beim Kauf zu entfernen oder ausser Funktion zu setzen
- Das Recht Dienstleistungen auf RFID Basis ohne RFID Tags in Anspruch zu nehmen
- Das Recht auf Daten zuzugreifen, welche in RFID Tags gespeichert sind
- Das Recht zu wissen, wann, wo und warum ein RFID Tag ausgelesen wird

Fair information practices Die Grundsätze der Fair Information Practices (FIPs) sind die Eckpfeiler der Datenschutzgesetze auf der ganzen Welt. Als solche haben viele Organisationen sich an diesen orientiert um Applikationen auf Basis der RFID Technologie zu entwickeln. Demnach gibt es drei wichtige Grundsätze in der Sammlung von Daten. Diese drei Grundprinzipien umfassen die bewusste, authorisierte und kontrollierte Verwaltung von persönlichen Daten. In Bezug auf RFID besagen diese Grundprinzipien, dass alle Tags und Lesegeräte sichtbar gekennzeichnet sein müssen, die Teilnahme an einem RFID System, welches Daten sammelt soll freiwillig sein und alle Konsumenten sollen das Recht haben, RFID Tags kostenlos zu entfernen oder auszuschalten und dass alle Konsumenten das Recht haben zu verhindern, dass persönliche Daten mit Daten eines Objekts verknüpft werden. Nebst diesen drei Grundprinzipien gibt es weitere Prinzipien, welche befolgt werden sollen:

- Entwicklungen, Verfahren sowie Richtlinien sollen öffentlich zugänglich sein
- Nutzer müssen den Grund für den Einsatz von RFID Tags offen legen
- Persönliche Daten müssen stets vor unbefugtem Zugriff, Verlust, Zerstörung und Missbrauch geschützt werden

5 Schlussfolgerung

Obwohl einige Lösungen technischer Natur vorhanden wären, ist keine davon gut genug, um wirklich vollumfänglich überzeugen zu können. Es ist anzunehmen, dass an gewissen Orten beispielsweise ein Blocker Tag einen guten Schutz der Privatsphäre darstellt, während an anderen Orten, wie zum Beispiel an einem Flughafen, diese Lösung wiederum nicht brauchbar ist. Die einzige Möglichkeit, welche das Problem vollumfänglich löst, wird ein Mittelweg zwischen Gesetzen und Richtlinien, gepaart mit jeweiligen technischen Lösungen sein. Diese müssen jedoch stark genug sein und auch konsequent umgesetzt werden, damit Vertrauen in die RFID Technologie gewonnen werden kann. Sollte dies wirklich erreicht werden, steht dem endgültigen Durchbruch von RFID nichts mehr im Weg.

Literatur

1. Vance Lockton and Richard S. Rosenberg: RFID: The next serious threat to privacy (2005)
2. Simson L. Garfinkel, Ari Juels, Ravi Pappu: RFID Privacy: An Overview of Problems and Proposed Solutions (2005)
3. Ari Juels: RFID Security and Privacy: A Research Survey (2006)
4. Donna-Bea Tillman: FDA's VeriChip Letter RFID Security and Privacy: A Research Survey (2004)
5. http://edition.cnn.com/2004/TECH/10/05/spark.bajabeach/, gelesen am 25. April 2008
6. http://glossary.ippaper.com/default.asp?req=knowledge/article/489
7. http://rfid.home.att.net/epc.htm
8. http://billkosloskymd.typepad.com/wirelessdoc/2007/09/verichip-corpor.html
9. http://www.antichips.com/