Privacy in RFID-Systemen

Peter Schartner

Universität Klagenfurt
Fakultät für Technische Wissenschaften, Institut für Angewandte Informatik
Forschungsgruppe Systemsicherheit – syssec
Universitätsstraße 65–67, 9020 Klagenfurt
peter.schartner@uni-klu.ac.at

Schlagworte: Radio-Frequency Identification, RFID, Privacy, Security, Privatsphäre, Bedrohungen, Data-Privacy, Location-Privacy, Schutzmechanismen, Kennzeichnungspflicht, technische Mindeststandards

Abstract: Radio-Frequency Identification ist die kontaktlose Identifikation von Objekten. Diese Technologie schafft ohne zusätzliche Maßnahmen Bedrohungen der Privatsphäre. Dieser Beitrag beschreibt die Bedrohungen, denen Benutzer von RFID-Systemen ausgesetzt sind, listet exemplarisch bestehende organisatorische und technische Gegenmaßnahmen auf und schließt mit dem Vorschlag, technische Mindeststandards und eine Kennzeichnungspflicht für RFID-Technologie gesetzlich zu verankern.

1. Einleitung

Radio-Frequency Identification (RFID), die kontaktlose Identifikation von Objekten, wird als bestehende Massenanwendung zB im Bereich der elektronischen Artikelsicherung (= Diebstahlschutz) und als Barcode-Ersatz eingesetzt. Das Wesentliche an dieser Technologie ist, dass der so genannte RFID-Tag (auch elektronisches Etikett genannt) vom Lesegerät (auch Reader genannt) ohne Sichtverbindung und Kenntnisnahme des Benutzers aus einiger Entfernung (cm – m) ausgelesen werden kann und jeder RFID-Tag mit einer eindeutigen Nummer (ID) versehen ist. Zudem sind RFID-Tags relativ unempfindlich gegenüber Umwelteinflüssen und können angesichts ihrer Größe und Kosten relativ große Datenmengen dauerhaft (aber wiederbeschreibbar) speichern. Da sie vom Lesegerät mit Energie versorgt werden, benötigen sie keine eigene Energieversorgung und sind somit langlebige (sichere) Datenspeicher.

Diese Eigenschaften heben RFID-Tags von Barcodes ab, die nur bei Sichtverbindung ausgelesen werden können und zudem nur den Objekttyp iden-

tifizieren. Beispielsweise können zwei Packungen Milch anhand des Barcodes nicht, anhand des RFID-Tags aber sehr wohl unterschieden werden.

Die automatisierte Identifikation von Objekten birgt ohne Zweifel ein großes Optimierungspotential im Bereich der Warenlogistik, da nun große Mengen an Gütern ohne menschliches Zutun erfasst und verwaltet werden können. Allerdings bringt die unbemerkte und eindeutige Identifikation von Objekten auch Gefahren für die Privatsphäre der Betroffenen mit sich, die von unserer durch diverse Überwachungsszenarien sensibilisierten Gesellschaft (siehe [Horster, Schartner 2007]) als besonders bedrohlich wahrgenommen werden.

In diesem Beitrag werden neben den Bedrohungen auch bestehende organisatorische und technische und mögliche zukünftige rechtliche Gegenmaßnahmen diskutiert.

2. Mögliche Bedrohungen

In der Literatur werden die Bedrohungen zunächst in Bedrohungen der Betreiber und in Bedrohungen der Benutzer von RFID-Systemen unterteilt. Die erste Gruppe soll hier nicht näher betrachtet werden; eine ausführliche Abhandlung der für die Betreiber relevanten Bedrohungen kann [BSI 2004] entnommen werden. Bezüglich der Benutzer von RFID-Systemen (= Konsumenten) werden zwei wesentliche Bedrohungen unterschieden: Die Bedrohung der Data-Privacy und die Bedrohung der Location-Privacy.

2.1 Bedrohung der Data-Privacy

RFID-Tags müssen als Massenartikel zu möglichst geringen Kosten produziert werden. Es ist daher nahe liegend, dass sie in erster Linie nur jene Funktionen unterstützen, die für eine vernünftige Nutzung mindestens vorhanden sein müssen. Dieses grundlegende Nutzungsszenario ist die Bekanntgabe der eigenen Identität und eventuell zusätzlicher Daten, sobald das Lesegerät darum bittet (dh den RFID-Tag aktiviert). Werden keine zusätzlichen Mechanismen vorgesehen, so ist die Geheimhaltung der auf dem RFID-Tag gespeicherten Daten und damit die Data-Privacy bedroht.

2.2 Bedrohung der Location-Privacy

Die Eigenschaft der eindeutigen Identifizierbarkeit von RFID-Tags kann – eine ausreichende Dichte von miteinander verknüpften Lesegeräten vorausgesetzt – ohne zusätzliche Mechanismen zur Erstellung von Bewegungsprofilen genutzt werden, was die Location-Privacy (= Geheimhaltung des Aufenthaltsorts) verletzt. Hierzu wird einfach protokolliert, wo welcher Tag (bzw welche ID) wann aufgetaucht ist. Tauchen unterschiedliche IDs mehrfach zur selben Zeit am selben Ort auf, so können sie einem Träger bzw einem Profil zugeordnet werden. Kann eine dieser IDs (und damit das ganze Profil) noch dazu mit einer Person und somit anderen personenbezogenen Daten wie Geschlecht, Alter oder Wohnort in Verbindung gebracht werden, weil das zugehörige Produkt mit Kredit-, Kundenbindungs- oder Geldkarte bezahlt wurde, dann wird das Profil umso wertvoller.

Im Folgenden werden ausgewählte bestehende Gegenmaßnahmen vorgestellt, die den beiden geschilderten Bedrohungen entgegen wirken können.

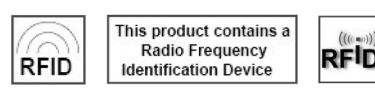
3. Gegenmaßnahmen

Die Gegenmaßnahmen, die der Bedrohung der Privatsphäre entgegengestellt werden können, unterteilen sich in organisatorische, technische und rechtliche Gegenmaßnahmen. Diese Maßnahmen sollten aber nicht isoliert von einander betrachtet und eingesetzt werden, da sie im Zusammenspiel einen wesentlich besseren Schutz der Privatsphäre bieten können, als getrennt.

3.1 Organisatorische Maßnahmen

Nach Simson Garfinkel [Garfinkel 2002] sollten Benutzer:

– Wissen, dass ein bestimmtes Produkt RFID nutzt, indem das Produkt dementsprechend gekennzeichnet ist. Hier einige vorgeschlagene Labels:



– In der Lage sein, RFID-Tags (dauerhaft) zu deaktivieren oder zu entfernen.

– Auch ohne den Tag Zugang zu den entsprechenden Services haben.
– Lese-Zugriff auf die im Tag gespeicherten Daten haben.
– Wissen, wann, wo und warum auf ihren Tag von wem zugegriffen wurde.

Betrachtet man die Umsetzbarkeit dieser Forderungen, so ist offensichtlich, dass die erste Forderung durch einen zusätzlichen Aufdruck auf dem Produkt oder dessen Verpackung leicht erfüllbar ist. Die (dauerhafte) Deaktivierung des Tags ist beim derzeitigen Stand der Technik ebenfalls problemlos umsetzbar (siehe unten). Bei der Nutzung der Services ohne den Tag wird es etwas problematischer, da die kontaktlose Identifikation meist ein zentrales Element dieser Services sein wird. Diese Forderung ist daher umstritten und kann auch entfallen, wenn die Forderungen 1, 2 und 4 vollständig umgesetzt sind. Die vierte Forderung ist umsetzbar, allerdings mit einem gewissen Aufwand und finanziellen Belastungen für den Konsumenten verbunden, der nun ein Lesegerät benötigt. Die letzte der Forderungen ist nicht zielführend, da sie einen enormen organisatorischen Mehraufwand für den Betreiber des RFID-Systems bedeutet und zudem technisch nicht-versierte Benutzer kaum von dieser Kontrollmöglichkeit Gebrauch machen werden.

3.2 Technische Maßnahmen

Es existieren zahlreiche technische Gegenmaßnahmen, um die oben genannten Bedrohungen hintan zu halten. Ein allgemeiner Überblick ist in [Juels, Pappu, Garfinkel 2005] und [Juels 2005] zu finden, aktuelle Beiträge können der Webseite von Gildas Avoine [Avoine 2007] entnommen werden. Im Folgenden werden ausgewählte technische Schutzmechanismen vorgestellt, die von der Authentifikation (= Echtheitsnachweis von Leser und Tag) bis hin zur vollständigen Deaktivierung der Tags reichen. Neben diesen Schutzmechanismen gibt es preisgünstige Geräte, die ein Auffinden von RFID-Tags und sogar das vollständige Blockieren ihrer Nutzung ermöglichen.

– **Authentifikation:** Prinzipiell ist es wichtig, dass nur Berechtigte Daten des RFID-Tags auslesen bzw manipulieren können und somit die Data-Privacy gegenüber Unberechtigten aufrechterhalten wird. Hierzu sind Authentifikationsmechanismen (und nachfolgende verschlüsselte Kommunikation) erforderlich, wobei bei gegenseitiger Authentifikation neben der Berechtigung des Lesegerätes auch die Echtheit des Tags sicher gestellt ist.

- **Anonymisierung:** Die Anonymisierung stellt sicher, dass die Location-Privacy geschützt wird. Ohne diese Schutzmechanismen sind die einzelnen Lesezugriffe verkettbar, da der RFID-Tag nun mit seiner eindeutigen ID (anstelle des Pseudonyms) antwortet. Die bei den jeweiligen Lesevorgängen verwendeten Pseudonyme können sich mit jedem Lesezugriff ändern, oder zyklisch (dh innerhalb einer begrenzten Menge) gewechselt werden. Die Verkettung einzelner Lesezugriffe wird somit entweder gänzlich verhindert, oder zumindest erschwert.
- **Passwort-geschützter Zugriff:** Die Ausführung bestimmter Kommandos kann an die Kenntnis eines Passwortes gebunden werden. Der Tag akzeptiert das Kommando nur, wenn das Lesegerät zuvor das zugehörige Passwort angegeben hat. Auf diese Weise können kritische Befehle (wie das Kill-Kommando oder das Auslesen sensitiver Informationen) geschützt werden.
- **Kill-Kommando:** Ein Mechanismus, der die Benutzerakzeptanz wesentlich erhöhen kann, ist das so genannte Kill-Kommando. Nach Erhalt dieses speziellen Kommandos deaktiviert sich der RFID-Tag dauerhaft und kann somit nicht mehr erkannt (und ausgelesen) werden.
- **physikalische Deaktivierung:** Da diese Deaktivierung aber ein rein elektronischer Vorgang ist, stellt die physikalische Deaktivierung (zB durch Entfernen der Antennen oder des Tags selbst) eine weitere Verbesserung dar: nun kann der Benutzer optisch verifizieren, dass der Tag unbrauchbar gemacht wurde.
- **Tag-Finder:** Diese Geräte ermöglichen das Auffinden von versteckten oder in das Produkt integrierten RFID-Tags. Sie funktionieren im Prinzip wie ein normales Lesegerät [Schüler, Kurz 2005], können allerdings keine Daten aus dem Tag auslesen.
- **Blocker-Tags:** Blocker-Tags [Juels, Rivest, Szydlo 2003] simulieren gegenüber einem Lesegerät alle möglichen RFID-Tags (oder eine zuvor spezifizierte Teilmenge) und verhindern somit, dass ein konkreter Tag vom Leser ausgelesen werden kann. Diese Vorgehensweise ist zwar ein sehr effizienter Schutz gegen das Auslesen, allerdings wird durch ihren Einsatz die gesamte RFID-Technologie unbrauchbar. Zudem ist eine juristische Bewertung vorzunehmen, wann und inwieweit der Einsatz von Blocker-Tags rechtlich zulässig ist.

3.3 Rechtliche Maßnahmen

Auf eine Darstellung der rechtlichen Rahmenbedingungen, die das Sammeln und Verarbeiten von Daten in RFID-Systemen regulieren, wird in diesem Beitrag bewusst verzichtet. Eine Analyse, was in welchen Grenzen erlaubt ist und was nicht, bleibt den Juristen vorbehalten. Es muss aber klar sein, dass Verbote und Regulierungen allein nicht ausreichen, um die Privatsphäre der Betroffenen zu schützen.

4. Resümee & Regulierungsvorschlag

Es ist klar, dass die bestehenden rechtlichen Rahmenbedingungen die oben beschriebenen Szenarien theoretisch verhindern, da es in den meisten Fällen verboten ist, die Tags auszulesen, oder die auf ihnen gespeicherten (personenenbezogenen) Daten zu sammeln bzw zu verarbeiten. Vom technischen Standpunkt her wäre es aber besser, diese Datensammlung durch Nicht-Berechtigte zu unterbinden.

Organisatorische und technische Maßnahmen, um dieses Ziel zu erreichen, sind vorhanden, sie müssen jedoch auch ein- und durchgesetzt werden, um die Betroffenen zu schützen.

Es ist daher auszudiskutieren, ob die oben beschriebene **Kennzeichnung von RFID-Produkten** nicht (analog zur Gentechnikkennzeichnungspflicht) gesetzlich vorgeschrieben werden sollte, damit der Konsument zumindest weiß, worauf er sich einlässt. Es ist zudem auch denkbar, noch einen Schritt weiter zu gehen und neben der Kennzeichnungspflicht (analog zu Signaturgesetz und Signaturverordnung) auch **verpflichtende technische Mindeststandards** festzulegen, die RFID-Tags, die in gewissen Bereichen verwendet werden sollen, aufweisen müssen. Solche Mindestanforderungen können zB Authentifikation, Passwort-geschütztes Auslesen oder die Unterstützung des Kill-Kommandos umfassen.

5. Literatur

Avoine 2007: Homepage von „Security and Privacy in RFID Systems“. (lasecwww.epfl.ch/~gavoine/rfid/index.html)

BSI 2004: „Risiken und Chancen des Einsatzes von RFID-Systemen“. (www.bsi.de/fachthem/rfid/studie.htm)

Horster, Schartner 2007: „Szenarien, die die Welt verändern“. In: Bammé, Böszörmenyi (Hrsg), „Information und Gesellschaft“.

Garfinkel 2002: „Adopting Fair Information Practices to Low Cost RFID Systems“, UbiComp Workshop. (www.simson.net/clips/academic/2002.Ubicomp_RFID.pdf)

Juels, Pappu, Garfinkel 2005: „RFID Privacy: An Overview of Problems and Proposed Solutions“ In IEEE Security and Privacy.

Juels 2005: „RFID Privacy: A Technical Primer for the Non-Technical Reader“. In Strandburg (edt): „Privacy and Identity“, Springer.

Juels, Rivest, Szydlo 2003: „The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy“, ACM Press.

Schüler, Kurz 2005: „Schnüffler enttarnen – Elektronik spürt RFID-Etiketten auf“. c't 2/2005, 202. (http://www.heise.de/ct/05/02/202/)