Datenschutzgerechte RFID-Technologie

Oliver Berthold

Informatik/Datenbanken und Informationssysteme
Humboldt-Universität zu Berlin
berthold@informatik.hu-berlin.de

Abstract: Radio-Frequency-Identification (RFID) steht für eine Technologie, die in naher Zukunft Wirtschaft und Gesellschaft wesentlich gestalten wird. Durch die angestrebte global eindeutige und unbemerkt auslesbare Kennzeichnung nahezu jedes physischen Objektes entstehen erhebliche Privacy-Gefahren. Technische Lösungen zur Vermeidung unkontrollierter Datenweitergabe sind notwendig. Der Artikel vergleicht verschiedene Privacy-Ansätze für RFID-Tags bezüglich Ihrer Sicherheit und Praktikabilität. Ein praktikabler eigener Ansatzes wird vorgestellt und durch Kombination mit einem anderen Ansatz optimiert.

1 Einleitung

Heutzutage wird RFID hauptsächlich in der Warenlogistik auf Palettenebene eingesetzt. Dies ermöglicht z.B. die automatische Erfassung von Wareneingängen. Mittelfristig geplant ist das „tagging“ von Einzelprodukten, um automatische Supermarkt-Kassen, Recycling-Anwendungen, Garantieverwaltung, Produktverfolgung und „smarte“ Heimelektronik wie die intelligente Mikrowelle zu ermöglichen.

Ein RFID-Tag, ein kleiner Chip mit Antenne zur Energieversorgung und Datenaustausch (Reichweite ca. 2-10 Meter), speichert i.d.R. nur eine einzige Nummer, den so genannten Electronic Product Code (EPC), welcher den bisher genutzten Barcode und zusätzlich eine Seriennummer enthält [A-ID03]. Die Auswertung der Daten des EPC erfolgt per Internet über das momentan im Standardisierungsprozess befindliche EPC Netzwerk [GCI03]. Kyptofunktionalität kann aus Kostengründen nur sehr eingeschränkt integriert werden.

Privacy-Bedenken richten sich gegen die jederzeit durch jedermann mögliche unbemerkte Auslesbarkeit der RFID-Tags. Dies ermöglicht das „Durchleuchten“ von Menschen bezüglich mitgeführter Produkte, die Identifizierung von Personen z.B. durch Nutzung der Informationen des EPC-Netzwerkes und das Aufzeichnen von Bewegungsspuren. Eine wirksame technische Lösung zum Schutz des Konsumenten muss daher beim RFID-Tag selbst ansetzen. Es muss vermieden werden, dass ein im Besitz eines Konsumenten befindlicher RFID-Tag gegenüber jedem RFID-Tag-Lesegerät seinen EPC oder andere eineindeutige bzw. identifizierende Daten offenbart.

2 Privacy Enhancing Funktionalität für RFID-Tags

Alle EPC-Standards für RFID-Tags [EPC03] enthalten eine **Kill-Funktion**, welche passwortgeschützt die endgültige Zerstörung des RFID-Tags ermöglicht. Logistisch aufwendig sind die mangels Verschlüsselung notwendigen individuellen Passwörter, die bereits bei der Produktion festgelegt werden und zur Deaktivierung, welche im Supermarkt an der Kasse erfolgen sollen, zur Verfügung stehen müssen. Der Einsatz dieser Funktion verhindert jedoch jede Nutzung der Tags „nach dem Kauf".

Blocker-Tags [JuRiS03] wie auch die Funk-Abschirmung von RFID-Tags stellen Ansätze dar, die Datenübertragung zwischen Lesegerät und Tag zu stören. Jedoch wird durch diese Ansätze nur Selbstschutz gegen eine „schlechte" Technologie ermöglicht.

Eine Reihe weiterer Verfahren wie **Hash-Lock** [Weis03] und **Private ID** [Inoue04] sperren den Zugriff auf den EPC und ersetzt diesen durch einen zufällig gewählten Wert *h*. Dadurch wird verhindert, dass Unbefugte die ausgelesenen Daten in Beziehung zu Produkten setzen oder die Identität einer Person direkt ermitteln können. Der Besitzer des Tags muss nun aber eine Datenbank führen, welche die EPC-Zuordnung und ggf. die Tag-Reaktivierungsschlüssel speichert. Das Hash-Lock-Verfahren setzt zum Schutz vor unberechtigter Reaktivierung eine Hashfunktion auf den Tags ein, wobei zum Sperren des Tags h=hash(k) und zum Reaktivieren die Zufallszahl k gesendet wird. In [Weis03] wird gezeigt, dass ausreichend sichere Hashfunktionen u.U. preiswert auf RFID-Tags realisiert werden können. Nachteil dieser Lösungen ist, dass der Wert h über lange Zeiträume konstant bleibt und daher zur Wiedererkennung und dem Aufzeichnen von Bewegungsspuren verwendet werden kann.

Diesen Nachteil versucht die Weiterentwicklung **Randomized Hash-Lock** [Weis03] zu vermeiden. Statt einen festen Wert auszusenden generiert der RFID-Tag bei jeder Anfrage eines Lesegerätes einen neuen Hashwert, indem er über einen integrierten Zufallsgenerator einen Zufallswert r bildet und $<r$, hash(EPC|r)$>$ sendet. Der Besitzer führt eine Datenbank mit allen bekannten EPC. Da die Rückrechnung eines Hashwertes nicht effizient möglich ist, muss die Berechnung mit allen EPC der Datenbank nachvollzogen werden. Dieser quadratische Aufwand schränkt die Einsatzmöglichkeiten stark ein. Keinesfalls lassen sich auf diese Weise die Produkte eines Supermarktes schützen, so dass ebenso wie bei Private-ID und Blocker-Tags zusätzliche Verfahren für den Schutz der Tags vor Missbrauch wie unerlaubter Sperrung oder Störung der Funkverbindung in Supermarkt und Logistikkette vorgesehen werden müssen.

Ein vom Autor vorgeschlagenes **Passwort-Verfahren** [SpBe04] modifiziert die im EPC-Standard vorgesehene Kill-Funktion zu einer Aktivierungs-/Deaktivierungs-funktion, welche ebenfalls passwortgeschützt realisiert ist. Bis zur Supermarktkasse kann daher die bisherige RFID-Infrastruktur beibehalten werden. Die Kasse deaktiviert die Tags statt diese zu killen mit Hilfe der in der Warenbestandsdatenbank gespeicherten bzw. über das EPC-Netzwerk ermittelten Passwörter. Damit der Kunde später seine Tags reaktivieren kann, müssen die Passwörter weitergegeben werden, beispielsweise durch Ausdruck auf den Kassenbon oder Übergabe an ein Gerät im Besitz des Kunden. Da ein deaktivierter RFID-Tag keinerlei Daten ausgibt, ist die Auswahl des richtigen

Passwortes ein Problem. Als einfache Lösung schlagen wir die Verwendung von gemeinsamen (Gruppen-) Passwörtern für alle Tags eines Besitzers bzw. dessen Haushalt vor. Die Nutzung jedes Tags wäre dann einfach durch Senden des gemeinsamen Passwortes möglich. Das Neusetzen der verschiedenen Passwörter der Tags sollte zeitlich nah nach dem Einkaufzeitpunkt geschehen, z.B. gleich im Supermarkt, an einer zertifizierten Station. Problematisch ist die Abhörbarkeit des im Vertrauensbereich ausgesendeten gemeinsamen Passwortes. Eine Massenüberwachung ermöglicht dies hingegen nicht: Real kann nur eine sehr begrenzte Anzahl von Passwörtern pro Passant durchprobiert werden, da deaktivierte Tags ja keine identifizierenden Daten aussenden.

Das Abhör-Problem lässt sich lösen, wenn die Tags Hashfunktion und Zufallsgenerator enthalten: Statt das Passwort unverschlüsselt auszusenden beweist das Lesegerät dessen Kenntnis, indem eine vom Tag empfangene Zufallszahl *r* mit *h*=hash(*Passwort*|*r*) beantwortet wird. Der Tag überprüft das Ergebnis anhand des gespeicherten Passwortes und führt das Kommando nur bei Übereinstimmung aus. Die Übermittlung eines neuen Passwortes kann durch bitweise Addition (XOR, Vernam-Chiffre [Shann49]) mit dem alten Passwort erfolgen, so dass ein Außenstehender, der das alte Passwort nicht kennt, auch bei dieser Operation keine Informationen ermitteln kann. Neben dem Schutz der Privatsphäre wäre im Falle des Vorhandenseins von Hashfunktion und Zufallsgenerator zusätzlicher Nutzen vorstellbar: Der Besitzer kann gegenüber jedem (z.B. einem Käufer) beweisen, dass ein Tag und damit ein bestimmtes Produkt ihm gehört/ rechtmäßig erworben wurde. Ebenso wäre die Erkennung von Produktfälschungen leicht überprüfbar, wenn die Hersteller einen zusätzlichen Code im RFID-Tag speichern, dessen Kenntnis der (aktivierte) Tag gegenüber einem Authentikationsdienst des Herstellers nach obigem Verfahren beweisen kann.

Einen ganz ähnlichen Ansatz verfolgt Engberg et. al. [EnHJ04]. Ebenso wie bei dem Passwort-Modell wird ein Gruppenschlüssel (gemeinsames Passwort) für verschiedene Tags eines Bereiches vorgeschlagen. Allerdings verwendet Engberg ein komplexeres Authentikationsprotokoll: Ein Lesegerät sendet folgende Nachricht:

$$<t, r \text{ XOR } \text{hash}(t \text{ XOR } key), \text{hash}(r \text{ XOR } key)>$$

wobei *t* ein Zeitstempel, *r* eine Zufallszahl und *key* der Gruppenschlüssel ist. Der RFID-Tag kann diese Berechnung nachvollziehen und somit verifizieren, dass das Lesegerät den Gruppenschlüssel kennt. Der letzte akzeptierte Zeitstempel muss jedoch gespeichert werden, um Wiederholungsangriffe zu verhindern. Zudem müssen alle Lesegeräte synchronisiert werden. Der Vorteil dieser Methode ist einerseits der Verzicht auf die Notwendigkeit eines Zufallsgenerators im RFID-Tag andererseits steht der Wert *r* für die Verschlüsselung eines Kommandos oder einer Antwort des Tags zur Verfügung, da ein Abhörer *r* nicht ermitteln kann. Eine unverschlüsselte Übertragung des EPC kann so vermieden werden. Zusätzlich propagiert Engberg die Löschung des EPC und die Ersetzung durch einen zufälligen Wert, ähnlich wie bei „Private ID“. Der Vorteil soll Schutz vor physischen Angriffen auf die RFID-Tags, durch Verzicht auf jegliche identifizierende Daten, sein. Neben der dadurch notwendigen Datenbank im Nutzerbereich ist der wesentliche Nachteil die fehlende Mehrseitige Sicherheit:

Ein einmal gesperrter Tag kann niemals wieder „entsperrt“ werden, da der EPC ja gelöscht wurde. Es müsste diesbezüglich dem bisherigen Besitzer völlig vertraut werden. Bearbeitung von Garantiefällen beispielsweise wäre dann auf Basis der RFID-Tags nicht möglich. Zudem ist fraglich ob ein Schutz des EPC gegen diese relativ theoretischen Angriffe sinnvoll ist, zumal der Angreifer noch immer den Gruppenschlüssel extrahieren und somit alle Tags dieser Gruppe kontrollieren könnte.

3 Zusammenfassung

Falls es ökonomisch nicht möglich ist, Hashfunktionen in RFID-Tags für Konsum-Produkte zu integrieren, dann ist das einfache Passwort-Verfahren die vom Autor favorisierte Privacytechnik.

Schutz gegen das Auslesen des EPC bieten alle Verfahren. Schutz gegen das Erheben von Bewegungsprofilen bieten das Kill-Verfahren, die Blogger-Tags, Randomized Hash Lock, das Passwort-Verfahren und das Verfahren von Engberg. Nur die beiden letzteren Verfahren sind praktikabel und ohne Einschränkung der Nutzbarkeit der Tags einsetzbar. Sind Hashfunktionen ökonomisch realisierbar, dann sollte eine Kombination beider Verfahren eingesetzt werden: Das Passwort-Verfahren mit dem Authentikationsmechanismus von Engberg. Dies vereinigt die Vorteile der Ansätze, wie den Schutz vor Abhörern, Mehrseitige Sicherheit, den Verzicht auf eine Datenbank im Bereich des Nutzers und Integrierbarkeit in geplante oder existierende Infrastrukturen.

4 Literaturverzeichnis

[JuRiS03] A. Juels, R. Rivest, M. Szydlo: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. 2003. http://theory.lcs.mit.edu/~rivest/.

[A-ID03] Auto-ID Center: EPC-256: The 256-bit Electronic Product Code Representation. 2003, Massachusetts Institute of Technology, MIT: Cambridge, USA. http://archive.epcglobalinc.org/aboutthetech_research.asp.

[EnHJ04] Engberg, Stephan j.,Harning, Morton B.,Jensen, Christian Damsgaard: Zero-Knowledge Device Authentication. Proc. PST 2004 – Second Annual Conference on Privacy, Security and Trust, Okt. 2004, http://dev.hil.unb.ca/Texts/PST/.

[EPC03] EPC-Global: Radio Frequency (RF) Identification Tag Specification. 2003. http://www.epcglobalinc.org/standards_technology/specifications.html.

[GCI03] GCI, Global Commerce Initiative: Global Commerce Initiative EPC Roadmap. 2003.

[Inoue04] Inoue, Yasuura: RFID Privacy Using User-controllable Uniqueness. RFID Privacy Workshop, 2004, Massachusetts Institute of Technology, Cambridge, MA, USA. www.rfidprivacy.org.

[Shann49] Shannon, C. E.: Communication Theory of Secrecy Systems. In: The Bell System Technical Journal, (1949). 28/4: p. 656-715.

[SpBe04] Spiekermann, Sarah, Berthold, Oliver: Maintaining privacy in RFID enabled environments - Proposal for a disable-model. In: Privacy, Security and Trust within the Context of Pervasive Computing, Robinson, et.al. Editors. April, 2004, Springer Verlag: Vienna, Austria.

[Weis03] Weis, S.: Security and Privacy in Radio-Frequency Identification Devices. Disseration at Massachusetts Institute of Technology (MIT).