Forschungsinstitut für Rationalisierung e.V. an der RWTH Aachen

UdZ 3/2007

Unternehmen der Zukunft

FIR-Zeitschrift für Betriebsorganisation und Unternehmensentwicklung

Schwerpunkt:

Informationsmanagement

Foto: © 2007 RACC, España

www.fir.rwth-aachen.de

ISSN 1439-2585

Datensicherheit bei RFID auf Artikelebene

Gefährdungspotenziale, Sicherheitsmaßnahmen und ein Maßnahmenpaket

Projektinfo
Trusted-RFID

Projekt-/ Forschungsträger
AiF – Arbeitsgemeinschaft industrieller Forschungsvereinigungen „Otto von Guericke" e.V., Bundesministerium für Wirtschaft und Technologie (BMWi)

Fördernummer
14912N

Laufzeit
01.08.2006 – 31.01.2008

Projektpartner
AIM Deutschland e.V., Ebcot GmbH, EURO I.D. Identifikationssysteme GmbH & Co. KG, Fraunhofer Institut für Mikroeletronische Schaltungen und Systeme, Kaufhof Warenhaus AG, TÜV Informationstechnik GmbH, MUL Services GmbH, X-ident GmbH

Kontakt
Dipl.-Ing. Dipl.-Wirt. Ing. Mirko Auerbach

Web
www.trusted-rfid.de

RFID-Anwendungen auf Artikelebene finden eine zunehmende Verbreitung, wobei Datensicherheitsaspekte an Bedeutung gewinnen. Das FIR hat eine Studie zur „Datensicherheit beim Item-Tagging im Bekleidungshandel" durchgeführt und ein Maßnahmenpaket entwickelt. Die diesbezügliche Forschungsarbeit basiert auf einem hybriden Ansatz, wobei zuerst „top-down" das theoretische Gefahrenpotenzial bei RFID auf Artikelebene und die Notwendigkeit zur Datensicherheit analysiert wurden. Auf dieser Grundlage wurde anschließend „bottom-up" eine empirische Studie im Bekleidungseinzelhandel durchgeführt [10], um die Schlüsselherausforderungen der Datensicherheit zu eruieren. Die hierbei gewonnenen Erkenntnisse stellten die Basis zur Entwicklung eines Maßnahmepakets dar, welches den herausgearbeiteten Schlüsselherausforderungen der Datensicherheit beim RFID-Item-Tagging begegnet.

Grundlagen der RFID-Technologie

RFID ist die Identifikation mit Radiofrequenzen bzw. -wellen und gehört zur Gruppe der automatischen Identifikationssysteme. Bei RFID-Systemen werden Daten auf einen elektronischen Datenträger (Transponder, Tag) gespeichert, ohne Sichtkontakt durch ein entsprechendes Lesegerät ausgelesen und über eine Software dem Anwender zur Verfügung gestellt. Gegenwärtig wird die Identifikation mittels RFID vor allem in der Logistik angewandt; auf Produktebene werden insbesondere in der Bekleidungsindustrie [1] [2] Pilotprojekte durchgeführt.

Notwendigkeit der Datensicherheit

In den letzten Jahren hat RFID in vielen Branchen starken Anklang gefunden, und in absehbarer Zukunft werden die Transponder auch auf einzelnen Produkten zu finden sein. Die Eigenschaften der RFID-Technologie können auch missbraucht werden. Das Auslesen, Missbrauchen, Fälschen und Zerstören der Daten ist ohne geeignete Sicherheitsmaßnahmen prinzipiell möglich. Da bei RFID-Systemen viele Komponenten für die Verarbeitung der entstehenden Daten zusammenspielen, muss die Datensicherheit bei jeder relevanten Komponente und bei deren Kommunikationsbeziehungen in allen Prozessschritten gewährleistet werden (siehe Bild 1). Im Rahmen des Projekts Trusted-RFID wurde durch einen „top-down"-Ansatz das theoretische Gefahrenpotenzial analysiert. Die Beziehungen und deren Aufgaben im Front-End-Bereich des Systems sind folgende:

1. Das Verhältnis zwischen den Transponderdaten und dem Transponder für die eindeutige Identifizierung des Transponders durch Daten.
2. Das Verhältnis zwischen Transponder und dem Trägerobjekt, das durch den Transponder eindeutig identifiziert wird.
3. Das Verhältnis zwischen dem Transponder und dem Lesegerät, das auf die Transponderdaten legalen und autorisierten Zugang haben muss.

Im Back-End-Bereich des RFID-Systems existieren größere Sicherheitsrisiken als im Front-End-Bereich, diese sind jedoch nicht RFID-spezifisch. Durch gewöhnliche, dynamisch und aufwandsminimal anpassbare IT-Maßnahmen (Firewall,

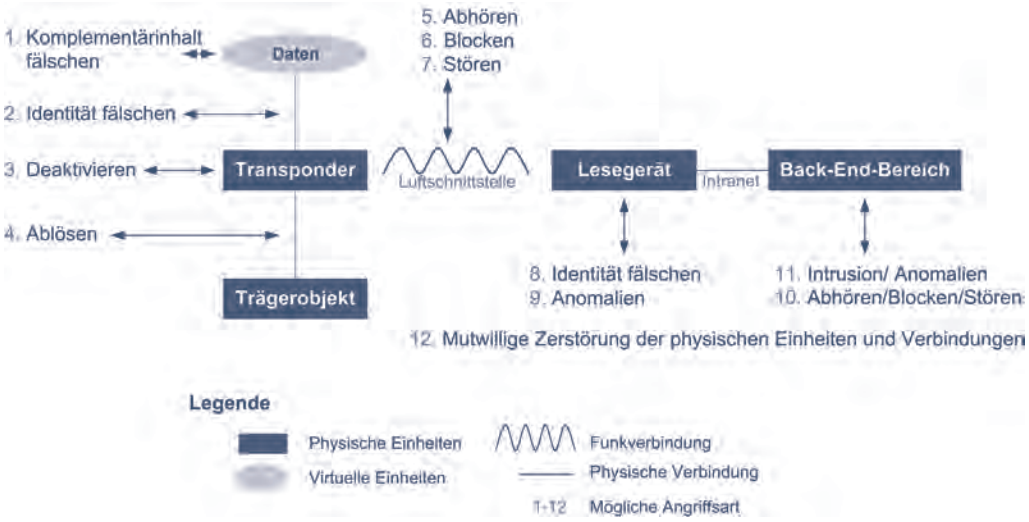

Bild 1
Mögliche Angriffsarten in einem RFID-System in Anlehnung an [3]

Täter	Motiv(e)	Angriff	geschädigte Partei	Angriffsort *
Konkurrenten	finanzielles Motiv, Schädigung, Privatsphärenschutz	1-12	Systembetreiber	SC, ES, AS
Staatliche Behörden	Sicherheitsmotiv	5, 8	Alle	SC, ES, AS
Systembetreiber	finanzielles Motiv	5, 8	Verbraucher, Angestellte	ES
Cyberterroristen	Schädigung, Profilierung, Spaß	1-12	Systembetreiber (Alle)	SC, ES, AS
Angestellte	Sicherheit (Anonymität), Betrug	1-7	Systembetreiber, (staatl. Behörden)	SC, AS
Verbraucher	Betrug, Sicherheit (Anonymität)	1-7	Systembetreiber, (staatl. Behörden)	SC, AS

* SC = Supply Chain ES = Einkaufsstätte AS = After Sales

Tabelle 1
Die Täter, deren Motive und Angriffsarten, die geschädigte Partei und der Angriffsort in einem RFID-System aus Sicht des Systembetreibers in Anlehnung an [4]

Antivirus-Software, Kryptologie, etc.) können Angriffe auf das Back-End abgewiesen werden. Ebenfalls aufgeführt sind verschiedene Angriffsarten auf ein RFID-System, die dann in Tabelle 1 ausführlich dargestellt werden. Im Weiteren werden die Angriffsarten auf den RFID-spezifischen Front-End-Bereich berücksichtigt.

Als Angriffsorte kommen dabei die Supply Chain, der Endkundenkontaktpunkt (z.B. Point of Sale) und der After Sales in Frage. Die folgende Tabelle gibt eine Übersicht über mögliche Täter, deren Motive und Angriffsarten, die dabei zu Schaden kommende Partei und den Angriffsort bei einem Angriff auf ein RFID-System. Die Verhinderung der dargestellten Angriffsarten ist das Ziel von Sicherheitsmaßnahmen, die im Folgenden kurz zusammengefasst werden.

Übersicht über bestehende Sicherungsmaßnahmen

Auf Basis einer ausführlichen Literaturstudie wurden die in Tabelle 2 dargestellten Maßnahmen zur Gewährleistung der Sicherheit in einem RFID-System ermittelt. Diese können, wie verdeutlicht, acht Maßnahmengruppen zugeordnet werden. Die Maßnahmen können generell auf den Standard-Sicherheitsmaßnahmen des Bundesamtes für Sicherheit in der Informationstechnik [5] aufsetzen. Auf eine detaillierte Beschreibung der Sicherheitsmaßnahmen wird an dieser Stelle verzichtet und auf die Projektwebseite verwiesen.

Maßnahmenpaket 4PPS

Die einzelnen in der Tabelle 2 aufgelisteten Maßnahmen haben bei ausschließlicher Implementierung entscheidende Nachteile. Die Anwendung einer bestimmten Maßnahme ist entweder zu aufwändig (z. B. Assymmetrische Verschlüsselung, Chained-Hash-Lock-Verfahren), zu umständlich (z. B. Blocker-Tags), nicht zweckmäßig (z.B. Kill-Funktion) oder nicht ausreichend (z.B. Einhaltung von Grundsätzen). Daher wurde ein vier Punkte umfassendes Maßnahmenpaket entwickelt (siehe Bild 2), um diese Nachteile bestmöglich zu

Nr.	Maßnahme	Nr.	Maßnahme
A	**Maßnahmengruppe Authentifizierung**	7	Recoding
1	Symmetrische Authentifizierung	**D**	**Maßnahmengruppe Deaktivierung**
2	Gegenseitige zufallszahlenbasierte Authentifizierung	1	Kill-Funktion (dauerhafte Deaktivierung)
3	Vorprogrammierte Authentifizierung	2	Passwort-Modell (temporäre Deaktivierung)
4	Two-Message Authentication Protocol (T2MAP)	**E**	**Maßnahmengruppe Datenintegrität**
5	Authentifizierung mit abgeleiteten Schlüsseln	1	Antikollisionsverfahren
6	Authentifizierung ausschließlich des Lesegerätes	2	Prüfsummenverfahren
7	Nachgelagerte Authentifizierung	**F**	**Maßnahmengruppe physische Verfahren**
B	**Maßnahmengruppe Verschlüsselung**	1	Verkürzen des Funkradius
1	Symmetrische Verschlüsselung	2	Abschirmung
2	Stromverschlüsselung	3	Blocker-Tags
3	Asymmetrische Verschlüsselung	4	Datenschutzagenten
4	Hybride Verschlüsselung	**G**	**Maßnahmengruppe Selbstverpflichtung**
C	**Maßnahmengruppe MetaID**	1	Hinweisschilder
1	Hash-Lock-Verfahren	2	Einhaltung von Grundsätzen
2	Randomized-Hash-Lock-Verfahren	**H**	**Maßnahmengruppe Sonstiges**
3	Chained-Hash-Lock-Verfahren	1	Erkennung doppelter EPC-Nummern
4	Hash-basierte ID-Variation	2	Zoning
5	Private ID	3	Veränderung der Funkfrequenz
6	Minimalistische Kryptographie	4	Analyse der Antennenenergie

Tabelle 2
Die wichtigsten RFID-spezifischen Sicherheitsmaßnahmen [4]

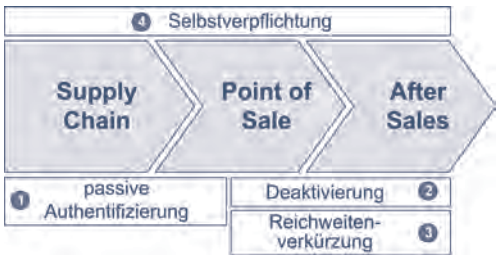

Bild 2
Das vorgeschlagene 4PPS Maßnahmenpaket

beheben und einen ganzheitlichen Schutz zu gewährleisten. 4PPS steht sowohl für „For Public Privacy and Security" als auch für „4-Punkte-Paket-für-Sicherheit". Das Maßnahmenpaket beinhaltet sowohl virtuelle als auch physische Maßnahmen die kurz dargestellt werden.

Maßnahmenpunkt 1: Hash-basierte Authentifizierung

Die Authentifizierung erfolgt als erster Schritt. Wenn ein Lesegerät die Transponderdaten auslesen möchte, muss dieser zuerst das richtige Passwort mit Hilfe einer mathematischen Funktion übersenden [6]. Das Lesegerät sendet dem Transponder das gehashte Passwort, welches der Transponder mit seinem gehashten Passwort vergleicht. Bei Übereinstimmung kann der Transponder seinen Dateninhalt (z.B. EPC) verschlüsselt an das Lesegerät übertragen. Dieser Maßnahmenpunkt zielt auf die Sicherung der Supply Chain und des Point of Sale ab.

Maßnahmenpunkt 2: Temporäre Deaktivierung

Beim Verkauf am Point of Sale sollten die Transponder ohne eine aktive Forderung der Kunden in den gesicherten Modus übergehen. Hierbei sollte die Deaktivierung temporär gültig sein [7]. Das zuvor für die Authentifizierung verwendete Passwort kann mit einem neuen überschrieben und dem Kunden übergeben werden. Alternativ kann im Transponder auch die Seriennummer des EPC verschlüsselt werden, was einer Quasi-Deaktivierung gleichkommt. Beim Auslesen würde der Transponder dann den EPC ohne Seriennummer übertragen. Dadurch kann das Objekt zwar ausgelesen, aber nicht seriell identifiziert und einer bestimmten Person zugeordnet werden (analog zum Barcode). Auf Wunsch des Kunden können die Tags durch einen Kill-Befehl, der auch im EPC vorgesehen ist, endgültig deaktiviert werden. Die dauerhafte Deaktivierung ist jedoch nicht anzustreben, da dann alle After Sales Angebote, die RFID möglich macht, nicht genutzt werden können.

Maßnahmenpunkt 3: Verkürzung der Funkreichweite

An der Kasse sollte dem Kunden die Möglichkeit gegeben werden, die Antenne abzutrennen. Voraussetzung ist eine entsprechende Bauweise der Transponder, die es zulässt, dass die Antenne entfernt wird [8]. Diese Maßnahme hat den positiven Effekt, dass die Verbraucher bei Ungewissheit über die Deaktivierung durch das manuelle Abreißen der Antenne Sicherheit und Kontrolle erhalten. Somit können die Ängste der Verbraucher vor Verfolgung weitestgehend beseitigt werden, da die Transponder sich bei einem späteren Ausleseversuch nicht mehr melden. Gleichzeitig bleiben die Transponderdaten sicher erhalten.

Maßnahmenpunkt 4: Selbstverpflichtung

Alle Prozessstufen sollten mit selbstverpflichtenden Maßnahmen verknüpft werden. Am Point of Sale sollten Hinweisschilder angebracht werden. Eine ganzheitliche Einhaltung von Grundsätzen kann beispielsweise durch ein Vertrauenssiegel sichergestellt werden, wie es im Projekt Trusted-RFID entwickelt wird [9]. Einzelhändler, die die Sicherheitskriterien und die Datenschutzgesetze nachweislich erfüllen, erhalten dann ein Zertifikat für den sicheren Umgang mit Daten wodurch das Vertrauen der Verbraucher gestärkt wird.

Fazit

Durch das Maßnahmenpaket wird das Abhören der Luftschnittstelle unterbunden. Angreifer die die Übertragung abhören, können nicht auf die eigentlichen Daten zurückschließen. Da das Maßnahmenpaket die Verwendung des EPC unterstützt, können Plagiate durch Replay-Attacken o.ä. nach dem EPC-Verfahren entdeckt werden. Auch wird eine Verfolgbarkeit bzw. Tracking sowohl in der Supply Chain, als auch im After Sales abgewehrt, denn der Transponder verweigert nicht authentifizierten Lesegeräten die Antwort. Das Überschreiben oder Löschen von Transponderdaten ist somit auch nicht möglich, da das systemfremde Lesegerät keinen Zugang auf die Transponderdaten hat. Im After Sales kann durch die Deaktivierung oder Verkürzung der Funkreichweite die Überwachung der Verbraucher verhindert werden. Letztere können den Funkradius ganz oder bis auf einige Millimeter minimieren. Somit kann auch die unautorisierte Verwendung der Daten der Kunden (z.B. Kundenlaufstudien, Kundenprofile) auf den Transpondern vermieden werden.

Das Maßnahmenpaket kann in der Supply Chain und am Point of Sale lediglich die Verhinderung des Blockens und des Störens, die Zerstörung des

Transponders und das Ablösen des Transponders vom Trägerobjekt nicht einhalten. Im als besonders gefährdet angesehenen After Sales können durch die Deaktivierung oder Antennenabtrennung das Blocken und Stören jedoch eingehalten und diese Angriffe abgewehrt werden. Das Zerstören und Ablösen des Transponders kann durch die Integration der Transponder in die Produkte (z.B. Einweben) auch in den anderen Prozessstufen abgewendet werden, so dass das vorgeschlagene Maßnahmenpaket 4PPS allen Sicherheitsanforderungen gerecht wird.

Dipl.-Ing. Dipl.-Wirt. Ing. Mirko Auerbach
Wissenschaftlicher Mitarbeiter am FIR
im Bereich Informationsmanagement
Tel.: +49 241 47705-504
E-Mail: Mirko.Auerbach@fir.rwth-aachen.de

Yilmaz Uygun, MSc
Lehrstuhl für Fabrikorganisation
Tel.: +49 231 755-5779
E-Mail: uygun@lfo.uni-dortmund.de

Literatur

[1] Fraunhofer Institut für Mikroelektronische Schaltungen: IMS-Teilnahme am Pilotprojekt Kaufhof – Gerry Weber zur Vorbereitung der RFID-Einführung in der Textillogistik. Duisburg. (2005).
[2] C. Tellkamp, U. Quiede: Einsatz von RFID in der Bekleidungsindustrie – Ergebnisse eines Pilotprojekts von Kaufhof und Gerry Weber. In: Das Internet der Dinge. Fleisch, E. und Mattern, F. (Hrsg.). Berlin, Heidelberg: Springer. (2005). S. 143–160.
[3] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Risiken und Chancen des Einsatzes von RFID-Systemen. Bonn. (2005).
[4] Y. Uygun: Datensicherheit bei RFID-Anwendungen auf Item-Level im Bekleidungseinzelhandel. Masterarbeit. Duisburg / Aachen. (2006).
[5] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge. Bonn (2005).
[6] M. Langheinrich: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. Institut für Pervasive Computing, ETH Zürich. Zürich. (2004).
[7] O. Berthold: Datenschutzgerechte RFID-Technologie. Berlin. (2005).
[8] K. N. Rindle: Datenschutz im Handumdrehen. Clipped Tags – transparente Deaktivierung von RFID-Tags durch Enthaupten. In: RFID im Blick.
[9] M. Auerbach, A. Sommer, U. Quiede: Trusted-RFID. Förderung der Akzeptanz von RFID-Anwendungen im Endkundengeschäft durch geprüftes Informationsmanagement. In: Unternehmen der Zukunft 03/2005. S. 3–4.
[10] M. Auerbach, Y. Uygun: Sicherheitsanforderungen des Bekleidungseinzelhandels an RFID-Systeme im Endkundengeschäft. Ergebnisse einer deutschlandweiten Studie. In: Unternehmen der Zukunft 03-04/2006. S. 9–10.

Die Projektpartner

Impressum

UdZ – Unternehmen der Zukunft
FIR-Zeitschrift für Betriebsorganisation
und Unternehmensentwicklung
8. Jg., Heft 3/2007, ISSN 1439-2585
„UdZ – Unternehmen der Zukunft" informiert mit Unterstützung des Landes Nordrhein-Westfalen vierteljährlich über die wissenschaftlichen Aktivitäten des FIR

Herausgeber
Forschungsinstitut für Rationalisierung e.V.
an der RWTH Aachen
Pontdriesch 14/16, D-52062 Aachen
Tel.: +49 241 47705-0
Fax: +49 241 47705-199
E-Mail: info@fir.rwth-aachen.de
Web: www.fir.rwth-aachen.de
Bankverbindung: Sparkasse Aachen
BLZ 390 500 00, Konto-Nr. 000 300 1500

Direktor
Univ.-Prof. Dr.-Ing. Dipl.-Wirt. Ing. Günther Schuh

Geschäftsführer
Dr.-Ing. Volker Stich

Bereichsleiter
Dipl.-Ing. Gerhard Gudergan (Dienstleistungsmanagement)
Dipl.-Ing. Dipl.-Wirt. Ing. Peter Laing (Informationsmanagement)
Dipl.-Ing. Carsten Schmidt (Produktionsmanagement)

Redaktion, Satz, Layout und Database Publishing
Olaf Konstantin Krueger, M.A. (Informationsmanagement)
Tel.: +49 241 47705-150
E-Mail: OlafKonstantin.Krueger@fir.rwth-aachen.de,
redaktion-udz@fir.rwth-aachen.de
School of Communication, Information and New Media
University of South Australia, Adelaide SA 5001 Australia
Ph.: +61 8 8302 4656, E-mail: office@m-publishing.com

Design und Bildbearbeitung, Satz und Layout
Birgit Kreitz, FIR, Tel.: +49 241 47705-153

Bildnachweis
Soweit nicht anders angegeben, FIR-Archiv

Anzeigenpreisliste
Es gilt Tarif Nr. 4 vom 01.02.2007

Druck
Kuper-Druck GmbH
Eduard-Mörike-Straße 36, D-52249 Eschweiler

Weitere Literatur im Web
www.fir.rwth-aachen.de/service