Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info 11. Jahrgang, Heft 2, Juni 2011

Schwerpunkt:

Location Based Services

fokus: Datenschutz in ortsbasierten Diensten
fokus: Location Privacy in RFID-Systemen
report: Offene Deklaration von Web Analytics

Schulthess §

inhalt

fokus

Schwerpunkt:
Location Based Services

Datenschutz in ortsbasierten Diensten

Ortsbasierte Dienste ermöglichen eine Nutzung von Mobiltelefonen als persönliche Informationsquelle und helfen dabei, die für eine Person relevante Information aus der Datenflut des Internets herauszufiltern. Der Autor erklärt die Probleme von ortsbasierten Diensten und erläutert mögliche Lösungsansätze.

Datenschutzgerechte ortsbasierte Dienste

Bei vielen ortsbasierten Diensten besteht die Gefahr, dass die Diensteanbieter exzessiven Zugang zu den personenbezogenen Daten über die Nutzer erhalten. Wie können ortsbasierte Dienste rechts- und datenschutzkonform gestaltet werden?

Location Privacy in RFID-Systemen

RFID-Systeme ermöglichen die automatische drahtlose Identifikation von Objekten und stellen eine allgegenwärtige Technologie mit zahlreichen Anwendungsmöglichkeiten dar. Welches sind die Sicherheits- und Datenschutzanforderungen an solche Anwendungen?

Schutz von Lieferketten mit RFID-Tags

Das Einschleusen von Fälschungen stellt heute eine grosse Gefahr für Warenlieferketten dar. Das System «Tracker» setzt einfache RFID-Tags als Ersatz für herkömmliche Barcodes ein, um Lieferketten gegen eingeschleuste Fälschungen abzusichern und ausserdem neugierige Mitbewerber davon abzuhalten, die eigene Warenlieferkette auszuspähen.

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 131.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Offene Deklaration von Web Analytics

Website-Betreiber sammeln und analysieren eine Fülle an Daten, ohne dies offen zu deklarieren. Datenschutz-Gütesiegel wie EuroPriSe erhöhen die Transparenz beim Einsatz von Web Analytics.

Häusliche Gewalt

StPO und OHG regelten die Mitteilung von Name und Adresse von Opfern an eine Beratungsstelle abschliessend und damit bleibe für kantonales Recht kein Raum, kritisieren Kettiger/Schwander einen in digma 2010.4 erschienenen Artikel von Glockengiesser/Stämpfli. Stimmt nicht ganz, wenden die beiden Autorinnen des ersten Beitrages ein, und weisen darauf hin, dass in Fällen von häuslicher Gewalt ausserhalb des Geltungsbereichs der StPO durchaus kantonaler Regelungsspielraum und -bedarf besteht.

Raserei auf der Strasse

Wer mit seinem Auto auf der Strasse zu schnell unterwegs ist, riskiert, geblitzt zu werden. Höchste Zeit, dass das Strassenverkehrsgesetz geändert und die Höchstgeschwindigkeit abgeschafft werden. Eine abwegige Argumentation? Mitnichten, wenn man die Reaktion auf ein Bundesverwaltungsgerichtsurteil zu einer anderen «Raserei auf der Strasse» hört …

Location Privacy in RFID-Systemen

Neben vielen Vorteilen bringen RFID-Systeme Risiken hinsichtlich Sicherheit und Datenschutz mit sich

Christian Wachsmann, Dipl.-Ing., Technische Universität Darmstadt/ Center for Advanced Security Research Darmstadt (CASED), Darmstadt, Deutschland christian.wachsmann @trust.cased.de

Ahmad-Reza Sadeghi, Prof. Dr.-Ing., Technische Universität Darmstadt/ Center for Advanced Security Research Darmstadt (CASED) und Fraunhofer SIT Darmstadt, Darmstadt, Deutschland ahmad.sadeghi@ trust.cased.de

RFID-Technologie wird heute in vielen Anwendungen verwendet. Ohne «Security & Privacy by Design» kann der Einsatz jedoch zu gravierenden Sicherheits- und Datenschutzproblemen führen.

Radio Frequency Identification (RFID) ist eine weit verbreitete Technologie, die es ermöglicht, Objekte automatisch und drahtlos zu identifizieren. Ursprünglich wurde RFID hauptsächlich für die elektronische Kennzeichnung von Paletten, Kartons und Produkten verwendet, um eine lückenlose Überwachung von Lieferketten zu ermöglichen. Heute werden RFID-Systeme auch in zahlreichen anderen Anwendungen eingesetzt, z.B. zur Kennzeichnung von Nutz- und Haustieren, im Bibliotheksmanagement, zur Zugangskontrolle, in elektronischen Pässen und Ausweisen und sogar in (medizinischen) Implantaten für Menschen.

Ein typisches RFID-System besteht aus einer Vielzahl von RFID-Tags und Lesegeräten (siehe Abbildung 1). Ein Tag kombiniert eine integrierte Schaltung mit einer Antenne und ist üblicherweise in eine Plastikkarte oder einen Aufkleber integriert. Es gibt passive und aktive RFID-Tags mit unterschiedlichen Reichweiten zwischen 10 cm und mehreren hundert Metern (siehe Tabelle 1). Passive Tags werden durch das elektromagnetische Feld des Lesegerätes mit Energie versorgt und besitzen daher meist nur sehr eingeschränkte Rechen- und Speicherressourcen sowie eine deutlich geringere Reichweite als aktive Tags, welche über eine eigene Energieversorgung verfügen. Für die meisten praktischen Anwendungen (z.B. elektronische Bezahl- und Ticket-Systeme) sind aktive Tags aufgrund ihrer Grösse und/oder Kosten jedoch nur bedingt geeignet.

Funktionale Anforderungen

Kommerzielle RFID-Systeme, wie elektronische Ticket-Systeme, erfordern eine hohe Skalierbarkeit, da sie oft aus einer sehr grossen Anzahl von Tags bestehen. Zudem wird eine schnelle Ausführungszeit der zugrunde liegenden Protokolle benötigt, um beispielsweise in Logistikanwendungen die Anzahl der in einem bestimmten Zeitraum erfassbaren Tags zu maximieren oder die Wartezeiten in RFID-basierten Zugriffskontrollsystemen so gering wie möglich zu halten.

Sicherheits- und Datenschutzanforderungen

RFID-Systeme verarbeiten und kommunizieren in vielen Fällen sicherheits- und datenschutzkritische Informationen. Daher stellen Tracing-Angriffe, bei denen sensitive anwenderspezifische Informationen, wie z.B. die Identität oder indirekt der Aufenthaltsort eines Tags, unbemerkt über die drahtlose Schnittstelle der Tags gesammelt werden, eine besondere Bedrohung für RFID-Systeme dar. Diese Informationen ermöglichen oftmals

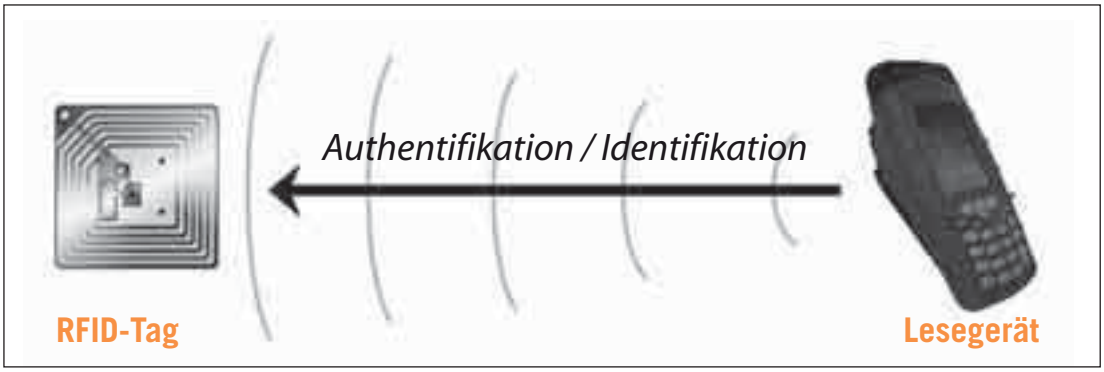

Abbildung 1: Typisches RFID-System

Tabelle 1: RFID-Tags und deren Fähigkeiten

Klasse	Low-End	Mittelklasse	High-End
Typische Anwendung	■ Tier- und Produktkennzeichnung ■ Diebstahlsicherungssysteme	■ Elektronische Ticket- und Bezahlsysteme ■ Zugangskontrollsysteme	■ Elektronische Ausweisdokumente
Funktionalität	■ Lediglich drahtlos auslesbarer Speicher ■ Keine Kryptografie	■ Starre Programmierung ■ Symmetrische Kryptografie	■ Flexible Programmierung ■ Hardwarebeschleunigte symmetrische und Public-Key-Kryptografie
Speicherkapazität	≤ 1 kByte	≤ 64 kBytes	≤ 128 kBytes
Typen	LF, HF, UHF	LF, HF,UHF	HF, Aktive Tags
Reichweite	≤ 1,5 m (LF) ≤ 0,3 m (HF) ≤ 3,0 m (UHF)	≤ 1,5 m (LF) ≤ 0,3 m (HF) ≤ 3,0 m (UHF)	≤ 0,3 m (HF) > 10 m (aktiv)
Preis	≤ 0,05 €	≤ 1 €	< 20 €

Rückschlüsse auf die persönlichen Gewohnheiten, Interessen und Vorlieben der Tag-Nutzer. Meist können die gesammelten Informationen mit der Identität des Tag-Nutzers verknüpft werden, z.B. wenn eine identifizierende Bezahlmethode, wie eine Kreditkarte, beim Erwerb eines RFID-basierten elektronischen Tickets verwendet wird.

In manchen Anwendungen, wie elektronischen Ausweisdokumenten, werden RFID-Tags sogar explizit zur eindeutigen Identifikation von Personen verwendet. Dies kann bei unsachgemässem Einsatz von RFID zu einem vollständigen Verlust der Location Privacy der Anwender führen und sämtliche Bewegungen der Nutzer verfolgbar machen. Während der Betreiber eines RFID-Systems durch gesetzliche Regelungen und regelmässige Kontrollen zum verantwortungsbewussten und vertraulichen Umgang mit den gesammelten Daten gezwungen werden kann, wie es z.B. für Kreditkartenanbieter der Fall ist, ist die Verfolgbarkeit durch unbekannte, nicht vom Nutzer autorisierte Parteien als besonders kritisch einzustufen.

Eine wichtige Anforderung an RFID-Systeme ist daher die Wahrung von Location Privacy durch

- das Verhindern von unberechtigtem Zugriff auf anwenderbezogene Daten (Geheimhaltung),
- die unberechtigte Identifikation von Tags (Anonymität) und
- das unberechtigte Verfolgen von Tags durch das Verlinken von deren Kommunikation (Unverkettbarkeit).

Neben Datenschutzrisiken müssen auch die klassischen Bedrohungen gegen Authentifikations- und Identifikationssysteme berücksichtigt werden. So müssen Angriffe unterbunden werden, bei denen ein Angreifer versucht, ein legitimes Tag zu impersonieren (Authentifikation) oder zu kopieren (Unklonbarkeit). Zudem müssen Bedrohungen wie Denial-of-Service-Angriffe (DoS-Angriffe) in die Beurteilung einbezogen werden. Hierbei nutzt ein Angreifer Schwachstellen in den zugrunde liegenden Protokollen aus, um legitime RFID-Tags dauerhaft zu deaktivieren. Neben unmittelbaren finanziellen Einbussen kann ein solcher Angriff die Reputation des Betreibers des RFID-Systems ernsthaft schädigen. Daher sollten derartige Angriffe ebenfalls verhindert werden (Verfügbarkeit).

Bei den Sicherheitsmodellen werden meist zu schwache Angreifermodelle verwendet, welche die Fähigkeiten eines praktischen Angreifers nicht angemessen abbilden.

RFID-Protokolle müssen sorgfältig entworfen werden, um die Anforderungen der zugrunde liegenden Anwendungsszenarien zu erfüllen («Se-

Kurz&bündig

RFID-Systeme ermöglichen die automatische drahtlose Identifikation von Objekten und stellen eine allgegenwärtige Technologie mit zahlreichen Anwendungsmöglichkeiten dar. Neben ihren Vorteilen bringen RFID-Systeme auch viele herausfordernde Risiken mit sich, insbesondere hinsichtlich des Daten- und Privatsphäreschutzes ihrer Nutzer. Der unsachgemässe Einsatz von RFID kann sensitive Informationen über Anwender und deren Aufenthaltsort preisgeben und die Erstellung von detaillierten Nutzerprofilen ermöglichen. Für den praktischen Einsatz von RFID ist es daher unerlässlich, Sicherheits- und Datenschutzanforderungen zu ermitteln und durchzusetzen. Dieser Artikel diskutiert Sicherheits- und Datenschutzanforderungen in RFID-Anwendungen, betrachtet die technischen Fortschritte im Kontext von RFID-Systemen, zeigt die Sicherheits- und Datenschutzdefizite bestehender Lösungen auf und stellt neuartige Lösungsansätze vor.

curity & Privacy by Design»). Dabei ist es jedoch möglich, dass eine praktische Realisierung nicht alle Anforderungen der Anwendung erfüllen kann. Insbesondere die funktionalen und die Sicherheitsanforderungen können im Widerspruch zu den Datenschutzanforderungen stehen.

Einen umfassenden Überblick über die wissenschaftliche Literatur zu Sicherheit und Datenschutz in RFID-Systemen bietet die RFID Security & Privacy Lounge[1].

RFID-Sicherheitsmodelle

Um die Sicherheit von RFID-Protokollen in der Praxis zu gewährleisten, ist es notwendig, die Protokolle formal zu analysieren. Dies erfordert eine sorgfältige Formalisierung der in den vorhergehenden Abschnitten diskutierten Sicherheits- und Datenschutzanforderungen. In der Literatur finden sich zahlreiche Sicherheitsmodelle für RFID-Systeme, die jedoch alle verschiedenen Einschränkungen hinsichtlich der Modellierung der Datenschutzaspekte unterliegen. Meist werden zu schwache Angreifermodelle verwendet, welche die Fähigkeiten eines praktischen Angreifers nicht angemessen abbilden: Man nimmt an, der Angreifer hätte keinen physischen Zugriff auf die Geheimnisse der Tags, keine Möglichkeit, Seitenkanalangriffe durchzuführen, und keinen Zugriff auf Zusatzinformationen wie die Information, ob die Authentifikation eines Tags erfolgreich war oder nicht.

RFID-Tags mit der Fähigkeit, Public-Key-Kryptografie auszuführen, werden nur in sicherheitskritischen Anwendungen wie elektronischen Pässen verwendet.

In der Praxis sind nur wenige, sehr teure RFID-Tags mit Hardwareschutzmechanismen ausgestattet. Diese werden typischerweise nur in sicherheitskritischen Anwendungen wie elektronischen Ausweisdokumenten eingesetzt. Die meisten in kommerziellen Anwendungen (z.B. in elektronischen Bezahl- und Ticket-Systemen) verwendeten Tags bieten aufgrund ihrer eingeschränkten Ressourcen und/oder aus Kostengründen keine derartigen Schutzmassnahmen. Daher sind Hardware- und Seitenkanalangriffe in der Praxis durchaus eine ernstzunehmende Bedrohung. Ein prominentes Beispiel hierfür sind die Angriffe, die zum vollständigen Brechen der Sicherheitsfunktionen der MiFare Classic RFID-Tags führten[2], die auch heute noch in vielen elektronischen Bezahl- und Ticket-Systemen verwendet werden.

Daten- und Privatsphäre schützende RFID-Protokolle

Die heute in kommerziellen Anwendungen eingesetzten RFID-Tags unterstützen bestenfalls die Erzeugung von kryptografisch sicheren Zufallszahlen und symmetrische kryptografische Verfahren. RFID-Tags mit der Fähigkeit, Public-Key-Kryptografie auszuführen, sind immer noch sehr teuer und werden daher nur in sicherheitskritischen Anwendungen wie elektronischen Pässen verwendet. Für die meisten kommerziellen Anwendungen sind diese Tags aufgrund ihrer hohen Kosten und oft langsamen Ausführungsgeschwindigkeit bei Public-Key-basierten Protokollen ungeeignet. Daher wurden zahlreiche Verfahren vorgeschlagen, welche nur minimale Anforderungen an die Fähigkeiten der RFID-Tags stellen.

Verfahren für einfache RFID-Tags

Sehr einfache RFID-Tags, die z.B. zur Warenkennzeichnung (Electronic Product Code, EPC)[3] eingesetzt werden, implementieren meist nur einen drahtlos auslesbaren Speicher und verfügen über keinerlei Rechenressourcen. Für derartig eingeschränkte Tags wurden verschiedene Ansätze zum Schutz der Daten und Privatsphäre vorgeschlagen. EPC-Tags unterstützen ein tagspezifisches Passwort (Kill Command), welches während der Produktion des Tags festgelegt wird und später dazu verwendet werden kann, das Tag permanent zu deaktivieren, so dass dieses nicht mehr auslesbar ist.

Andere Ansätze basieren auf der Störung der Kommunikation zwischen Tags und Lesegeräten. Eine einfache Lösung besteht darin, Tags in metallischen Hüllen zu transportieren, welche wie faradaysche Käfige wirken und für die RFID-Funkfrequenzen undurchlässig sind. Derartige Hüllen werden bereits in Brieftaschen integriert oder als separate Schutzhüllen, z.B. für elektronische Reisepässe, angeboten[4]. Alternativ wurde vorgeschlagen, dass Nutzer einen aktiven Störsender (z.B. ein Blocker Tag) mit sich führen, der die Kommunikation zwischen Tags und Lesegeräten in der Nähe des Anwenders verhindert.

Alle diese Ansätze wirken den Vorteilen der RFID-Technologie entgegen, indem sie eine Interaktion des Benutzers oder die permanente Deaktivierung von Tags erfordern.

Es wurden auch kryptografische Ansätze zur Daten- und Privatsphäre schützenden Authentifikation von einfachen RFID-Tags vorgeschlagen. Diese Verfahren können jedoch keine Authentifikation und Unklonbarkeit gewährleisten und sind somit für praktische Anwendungen nicht geeignet. Ein Angreifer kann immer alle auf diesen einfachen Tags gespeicherten Daten auslesen und diese Tags damit impersonieren und kopieren,

z.B. indem er die Daten auf ein anderes, leeres Tag kopiert.

Anonyme Authentifikation

In einem idealen RFID-System sollten selbst die Lesegeräte keinerlei Informationen über die Nutzer in Erfahrung bringen können, ausser dass diese ein gültiges Tag besitzen. Das liesse sich durch anonyme Credential-Systeme realisieren. Diese basieren jedoch auf rechenintensiven kryptografischen Primitiven mit hohem Kommunikationsaufwand und sind daher aufgrund der hohen Anforderungen an die Tag-Hardware und der langsamen Protokollausführungszeit von mehreren Sekunden für den Einsatz in kommerziellen RFID-Systemen (z.B. Ticket-Systemen) im Allgemeinen nicht geeignet[5].

Auf symmetrischer Kryptografie basierende Verfahren

Die derzeit in elektronischen Bezahl- und Ticket-Systemen verwendeten RFID-Tags unterstützen meist nur symmetrische kryptografische Verfahren. Die darauf aufbauenden in der Praxis eingesetzten Systeme berücksichtigen aber nur selten Aspekte des Daten- und Privatsphäreschutzes.

Ein generelles Problem hinsichtlich der Daten und Privatsphäre schützenden Authentifikation von RFID-Tags basierend auf symmetrischer Kryptografie besteht darin, dem Lesegerät mitzuteilen, welchen Schlüssel es zur Authentifikation des Tags verwenden muss. Ein Tag kann die Identität des Schlüssels, und damit seine eigene Identität, nicht preisgeben, bevor sich das Lesegerät gegenüber dem Tag authentifiziert hat, da dies sowohl die Anonymität als auch Unverkettbarkeit verletzen würde. Das Lesegerät kann sich jedoch nicht gegenüber dem Tag authentifizieren, ohne die Identität (d.h. den Schlüssel) des Tags zu kennen.

In der Literatur gibt es eine Vielzahl von Vorschlägen, dieses Problem zu lösen. Die meisten davon haben jedoch Schwächen hinsichtlich ihrer Praktikabilität. So ist für viele Protokolle der zur Authentifikation eines Tags benötigte Rechenaufwand des Lesegerätes sehr gross und abhängig von der Anzahl aller im System vorhandenen Tags. Dies ist für Systeme mit einer sehr grossen Anzahl von Tags, wie elektronische Ticket-Systeme, inakzeptabel. Andere Protokolle erfordern eine permanente Datenverbindung zwischen dem Lesegerät und einer Datenbank, was für Systeme mit mobilen Lesegeräten, wie z.B. zur mobilen Kontrolle von elektronischen Tickets, ungeeignet ist.

Als kosteneffiziente Alternative zu existierenden Hardwareschutzmassnahmen sind insbesondere Physically Unclonable Functions (PUFs) von besonderem Interesse.

Zusammenfassend kann man sagen, dass bestehende Ansätze zur Daten- und Privatsphäre schützenden Authentifikation von RFID-Tags für den praktischen Einsatz nur bedingt geeignet sind, da sie entweder keine Location Privacy bieten, anfällig für Impersonierungs-Angriffe sind oder die Verifikation der Tags durch das Lesegerät ineffizient ist.

Anonymizer-basierte Protokolle

Einen neuartigen Ansatz bieten Anonymizer-basierte Protokolle. Diese verwenden ein externes Zusatzgerät (Anonymizer), welches in regelmässigen Abständen mit dem Tag kommuniziert und dessen Anonymität und Unverkettbarkeit in der Kommunikation mit dem Lesegerät sicherstellt (siehe Abbildung 2). Hierbei entlastet der Anonymizer das Tag, indem er die rechenintensiven Operationen des Authentifikationsprotokolls für das Tag teilweise vorberechnet. Dieser Ansatz eignet sich besonders für Anwendungen, die eine grosse Anzahl von kostengünstigen RFID-Tags mit eingeschränkten Ressourcen verwenden müssen.

Anonymizer können auf zwei unterschiedliche Arten realisiert werden: öffentliche und private Anonymizer. Öffentliche Anonymizer können an öffentlichen Plätzen platziert werden und von allen Nutzern in der Nähe verwendet werden, während private Anonymizer vom Nutzer selbst

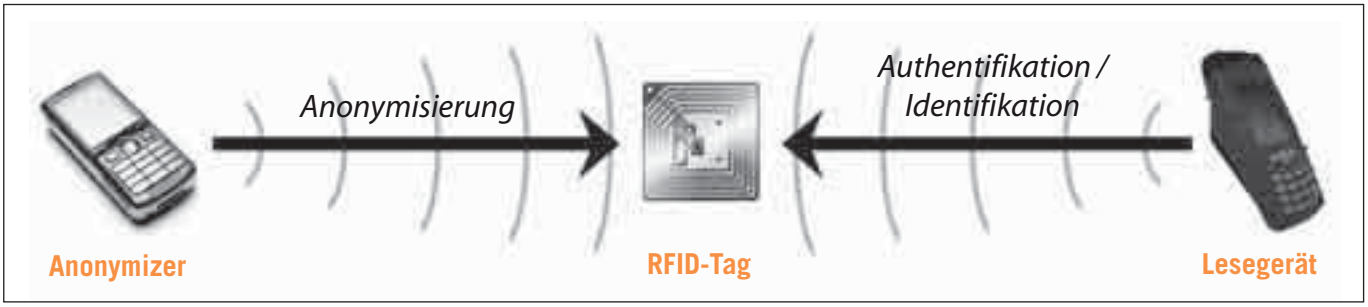

Abbildung 2: RFID-System mit Anonymizer

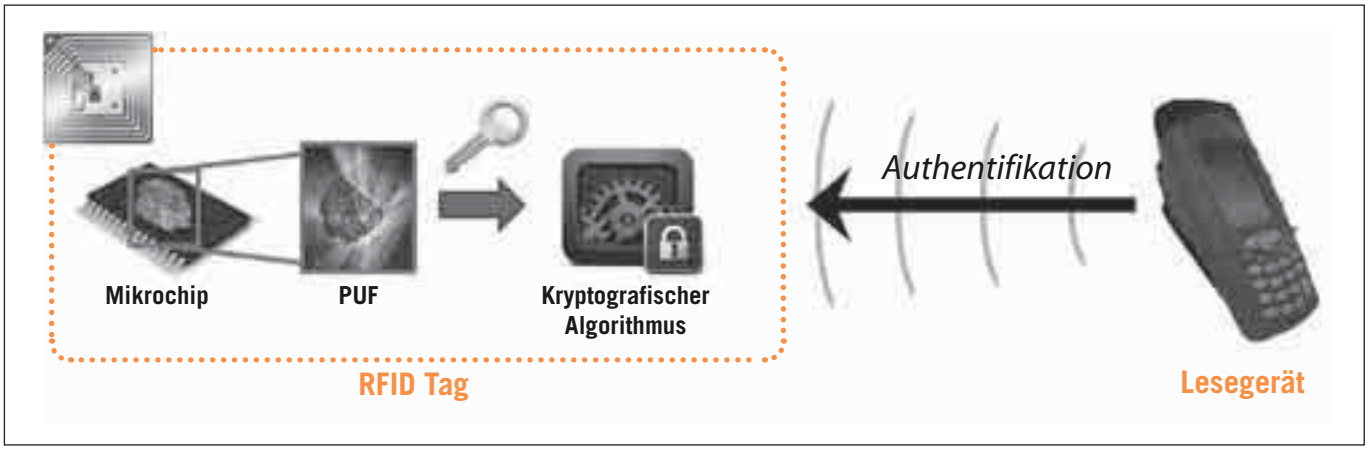

Abbildung 3: Integration von PUFs in kryptografische Algorithmen und Protokolle

verwaltet und nur für dessen Tags verwendet werden können. Private Anonymizer könnten als Anwendung (Anonymizer-App) auf dem Mobiltelefon des Tag-Nutzers realisiert werden[6].

Anonymizer ermöglichen eine kosteneffiziente Realisierung von Daten- und Privatsphäre schützenden RFID-Systemen, da die Anforderungen an die zugrunde liegenden RFID-Tags mit denen bestehender kommerzieller RFID-Systeme vergleichbar sind und der Anwender die Anonymizer-Hardware (d.h. das Mobiltelefon) in der Regel bereits besitzt. Alternativ könnte der Systembetreiber dem Anwender ein spezielles Anonymizer-Gerät gegen Pfand aushändigen.

Ein Nachteil dieses Ansatzes besteht darin, dass während eines Ausfalls des Anonymizers (z.B. bei leeren Batterien) die Unverkettbarkeit der Tags temporär verloren geht. Jedoch bleibt in diesem Fall die Verfügbarkeit gewährleistet, da sich ein Tag auch in Abwesenheit des Anonymizers gegenüber den Lesegeräten authentifizieren kann.

Physically Unclonable Functions (PUFs) gegen Hardware-Angriffe

Um die Unklonbarkeit eines RFID-Tags zu gewährleisten, müssen sowohl Softwareangriffe gegen die verwendeten Protokolle als auch Hardwareangriffe gegen Tags verhindert werden. Insbesondere kostengünstige RFID-Tags bieten in der Praxis oftmals keinen ausreichenden Schutz vor physikalischen Angriffen. In diesem Zusammenhang sind Physically Unclonable Functions (PUFs) als kosteneffiziente Alternative zu existierenden Hardwareschutzmassnahmen von besonderem Interesse. PUFs basieren auf den bei Herstellungsprozessen von Geräten unvermeidlichen zufälligen Variationen, welche zwar mit geringem Aufwand gemessen, jedoch praktisch nicht reproduziert werden können. Diese sind für jedes Gerät einzigartig und können daher als Identifikationsmerkmal verwendet werden, sozusagen als physikalischer Fingerabdruck des Gerätes. PUFs ermöglichen zudem die Bindung von Soft- und Hardwarekomponenten an Geräte, die Realisierung sicheren Speichers (z.B. für kryptografische Schlüssel) und können direkt in kryptografische Algorithmen und Protokolle integriert werden (siehe Abbildung 3).

In der Literatur gibt es bereits eine Vielzahl von PUF-basierten Authentifikationsprotokollen, darunter auch einige Daten- und Privatsphäre schützende Ansätze. Obwohl bereits kommerzielle Produkte basierend auf PUF-Technologie existieren, darunter auch RFID-Tags mit integrierter PUF[7], gibt es beim praktischen Einsatz von PUFs noch einige offene Probleme, insbesondere hinsichtlich der Effizienz und Skalierbarkeit von PUF-basierten Sicherheitslösungen sowie der Sicherheitsanalyse von PUF-Implementierungen. So basieren viele bestehende PUF-basierte Authentifikationsprotokolle auf der Annahme, dass zur Verifikation der PUF-Ausgaben eine Datenbank mit Referenzwerten zur Verfügung steht. Diese Datenbank kann in Anwendungen mit einer Vielzahl von mit PUFs ausgestatteten Geräten (z.B. RFID-Tags) sehr gross werden, insbesondere da jeder Referenzwert nur für eine einzige Authentifikation verwendet werden darf, da sonst Replay-Angriffe möglich sind. Zudem basiert die Sicherheit von PUF-basierten Protokollen meist auf physikalischen Annahmen, die für reale PUF-Implementierungen bisher noch nicht hinreichend untersucht wurden.

Fazit

Die Entwicklung und das Design von in der Praxis anwendbaren Daten- und Privatsphäre schützenden RFID-Protokollen sind sehr herausfordernd. Tatsächlich ist die Frage nach der Existenz eines nicht auf Public-Key-Kryptografie basierenden und damit für kommerzielle Systeme geeigneten RFID-Protokolls, welches den Schutz von Location Privacy gewährleistet, derzeit ein offenes Problem.

Eine weitere Herausforderung besteht in der Vielzahl von verschiedenen Sicherheitsmodellen für RFID-Systeme, welche oftmals nicht miteinander vergleichbar oder gar inkompatibel sind. So existieren RFID-Protokolle, die zwar in einem bestimmten Sicherheitsmodell formal als sicher bewiesen werden können, in einem anderen jedoch angreifbar sind. Um verlässliche Aussagen über die Sicherheit von RFID-Protokollen in der Praxis treffen zu können, ist es daher unabdingbar, ein einheitliches und praxisnahes Sicherheitsmodell zur Evaluation von RFID-Protokollen zu etablieren.

Neben den technischen Herausforderungen gibt es auch andere Probleme, wie z.B. das oft nicht vorhandene Sicherheitsbewusstsein der Anwender, insbesondere hinsichtlich des Daten- und Privatsphärenschutzes. Zudem zwingen kurze Produktzyklen Firmen oft dazu, Datenschutzaspekte in ihren Produkten nicht zu berücksichtigen, wenn diese nicht durch gesetzliche Regelungen oder Verbraucherschutzorganisationen erzwungen werden. ■

Literatur

- Ari Juels, RFID Security and Privacy: A Research Survey, in: IEEE Journal on Selected Areas in Communications, 24(2), 381–394, Februar 2006.
- Marc Langheinrich, A Survey of RFID Privacy Approaches, in: Journal of Personal and Ubiquitous Computing, 13(6), 413–421, August 2009.
- Ahmad-Reza Sadeghi/Ivan Visconti/Christian Wachsmann, Location Privacy in RFID Applications, in: Privacy in Location-Based Applications: Research Issues and Emerging Trends, Springer Verlag, Vol. 5599, LNCS, 127–150, August 2009.
- Ahmad-Reza Sadeghi/Ivan Visconti/Christian Wachsmann, Anonymizer-Enabled Security and Privacy for RFID, in: 8th International Conference on Cryptology and Network Security (CANS), Dezember 2009.
- Ahmad-Reza Sadeghi/Ivan Visconti/Christian Wachsmann, Enhancing RFID Security and Privacy by Physically Unclonable Functions, In: Towards Hardware-Intrinsic Security: Foundations and Practice, Springer Verlag, September 2010.

Fussnoten

1 Gildas Avoine, RFID Security & Privacy Lounge, April 2011; <http://www.avoine.net/rfid/>.

2 Nicolas T. Courtois, The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime, in: RFIDSec'09, July 2009; <http://eprint.iacr.org/2009/137.pdf>.

3 EPC Global Inc. (<www.epcglobalinc.org/>).

4 z.B. DIFRwear (<http://difrwear.com/>) oder Epiguard (<http://www.epiguard.ch/>).

5 Patrik Bichsel/Jan Camenisch/Thomas Gross/Victor Shoup, Anonymous Credentials on a Standard Java Card, in: Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09), ACM, New York, NY, USA, 600–610, 2009.

6 Einige existierende Mobiltelefone und viele Smartphones der neuesten Generation besitzen eine Near-Field-Communication-Schnittstelle (NFC-Schnittstelle), welche die Kommunikation zwischen Telefon und RFID-Tags ermöglicht.

7 Verayo: Unclonable RFIDs (<http://www.verayo.com/product/pufrfid.html>).

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 131.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §