

Datensicherheitskonzept

Informationen im Sinne von digitalen Daten nehmen für Staat, Unternehmen und Privatpersonen einen nicht unterschätzbaren Stellenwert in unserer Gesellschaft ein. Ob es sich um Bürgerdienste, Geschäftsabläufe oder Privatkorrespondenz handelt: stets müssen Verfügbarkeit, Vertraulichkeit sowie Integrität der gespeicherten Daten gewährleistet sein. Dies gilt um so mehr in Zeiten der allgegenwärtigen und umfassend vernetzten informationstechnischen Systeme. Die RFID-Technik steht paradigmatisch für diese Durchdringung in nahezu alle Lebensbereiche. Die Bundesrepublik Deutschland setzt sie in ihren Ausweisdokumenten ein, Unternehmen verwenden RFID-Transponder für ihre Logistik und Privatpersonen können beispielsweise ihre Autos ganz ohne Schlüssel besteigen und starten.

Für ein Datensicherheitskonzept muss zuerst untersucht werden, welche Daten wo anfallen und wer darauf Zugriff haben soll. Im zweiten Schritt wird die Frage geklärt werden müssen, wie Verfügbarkeit, Vertraulichkeit und Integrität der gesammelten Daten technisch sichergestellt werden können.

Daten von RFID-Systemen

Ein RFID-System besteht aus der Trias Transponder, Lesegerät und einem im Hintergrund arbeitenden IT-System. Jeder Transponder besitzt eine (potentiell weltweit) eindeutige Identifikationsnummer, die von einem Lesegerät erfasst und von Computersystemen weiterverarbeitet werden kann. Das Lesegerät erfasst bei jedem Vorgang, neben der ID, die ungefähre Position des Tags samt Trägerobjekt und die genaue Uhrzeit. Das im Hintergrund arbeitende IT-System kann darüber hinaus auch die Daten aller angeschlossenen Lesegeräte miteinander verknüpfen und somit weitere Aussagen, wie Bewegungen und Aufenthaltsdauer, treffen.

Die Aussagekraft der Daten hängt damit in einem hohen Maße davon ab, wie gut die modellierten Daten mit Aspekten der (analogen) Wirklichkeit übereinstimmen und davon, dass diese Daten vor Veränderungen entsprechend geschützt sind.

Fehler- und Angriffsclassen

Schon bei der Datenerfassung können Fehler passieren, etwa wenn IDs falsch oder gar nicht eingelesen werden. Fehlerhafte Daten können durch Prüfsummenverfahren erkannt und in bestimmten Fällen auch korrigiert werden. Kleine Datenmengen, typischerweise bis zu einer Größe von 32 Bytes, werden einer Längssummenprüfung (engl.: longitudinal redundancy check, LRC) unterzogen, für größere Daten bietet sich das noch aus Diskettenlaufwerkszeiten stammende CRC-Verfahren an (cyclic redundancy check). In beiden Verfahren werden durch rekursive Kontravalenz („entweder-oder-Verknüpfung“) Übertragungsfehler erkannt.

Zudem befinden sich in der Praxis im Regelfall mehrere Transponder in Reichweite des Lesegeräts, das jedoch stets nur einen Transponder gleichzeitig erfassen kann. Da auf der anderen Seite alle passiven Transponder in Reichweite mit Strom versorgt werden und somit funken, werden sogenannte Kollisionen erzogen, denen mit gängigen Antikollisionsalgorithmen inzwischen gut begegnet werden kann.

Es muss weiterhin sichergestellt werden, dass die Verbindung Transponder-Trägerobjekt korrekt erfasst worden ist (mechanische Verbindung versus logischer Verbindung), also ob ein gesendetes und gelesenes Ident tatsächlich zu dem gekennzeichneten Objekt gehört. Die Verbindung ist einerseits physischer Natur, meist klebt das mit einem passiven RFID-Transponder ausgestattete Etikett auf dem Objekt. Andererseits muss diese Verknüpfung auch im dazugehörigen Datenbanksystem eingetragen sein, also logisch vorgenommen werden.

Darüber hinaus muss die Luftschnittstelle so abgesichert sein, dass nur berechtigte Lesegeräte die auf dem Chip gespeicherte eindeutige ID auslesen können. Aus all dem Genannten ergibt sich eine Klassifikation der Angriffe auf ein RFID-System. Daten können

1. unberechtigterweise ausgelesen werden, sie können
2. gefälscht sein oder bei Überlastung des Systems
3. nicht verfügbar sein (Denial of Service).

Angreifer können aber auch schlicht ihre Privatsphäre aktiv schützen wollen, zumal in den meisten Fällen die Aufklärung des Einsatzes von RFID-Technik zu kurz kommt. Ein passiver RFID-Tag bezieht seine Energie vom elektromagnetischen Feld des Lesegeräts, das dann automatisch die Präsenz registriert. Das kann in manchen Fällen auch unerwünscht sein, daher sehen die Spezifikationen dieser Funktechnik vor, dass es einen sogenannten »kill-Befehl« geben muss, der das Tag deaktiviert. De facto wird jedoch nicht dieser Weg der logischen Deaktivierung gewählt, sondern den der physischen. Setzt man einen RFID-Transponder einem zu intensiven Feld aus, überlastet der von der Antenne erzeugte Strom den Chip, so dass er regelrecht durchbrennt.

Die Datenschutzproblematik von RFID-Technik ist an anderer Stelle ausführlicher beschrieben worden.¹

	Ausspähen	Täuschen	Denial of Service	Schutz der Privatsphäre
Inhalt fälschen				
Identität fälschen (Tag)				
Deaktivieren				
Ablösen				
Abhören				
Blocken				
Stören				
Identität fälschen (Leser)				

Tabelle 1: Angriffsklassen nach Zweck, zit. nach [BSI2004].

Doch zurück zu den drei oben angesprochenen Angriffsmöglichkeiten Ausspähen, Täuschen und DoS.

Das unberechtigte Auslesen von Daten kann durch ein Lesegerät erfolgen oder durch das Ausspähen der Kommunikation zwischen Transponder und (berechtigtem) Lesegerät. Der Angreifer muss im ersten Fall in der Lage sein, sich die Identität des Lesegeräts anzueignen, im zweiten Fall

darf er nicht entdeckt werden. In beiden Fällen kann der Einsatz von Kryptographie einem deutlich verbesserten Schutz dienen, allerdings muss man sich vor Augen führen, dass die Ressourcen eines RFID-Transponders stark begrenzt sind. Daher können hoch-kryptographische, gegenseitige Authentifizierungen, wenn überhaupt, nur mit Hilfe von aktiven Transpondern geschehen, die über genügend Rechenleistung verfügen.

Das Fälschen von Inhalten kann direkt auf dem Tag vorgenommen werden, etwa wenn dort Daten gespeichert sind, die über die reine ID hinaus gehen; in den meisten Fällen wird aber die Seriennummer direkt gefälscht werden. Die Autoren der Studie „Chancen und Risiken der RFID-Technik“ fügen zudem noch eine simple Methode der Identitätsfälschung an: einfach durch Umkleben des Etiketts.² Im Falle des Einsatzes von RFID zur Diebstahlsicherung kann eine Deaktivierung des Tags auch eine Täuschung darstellen; man gibt vor, nicht im (unberechtigten) Besitz eines bestimmten Objektes zu sein. Wo die Zerstörung des Transponders nicht möglich ist, kann das gesendete Funksignal erheblich gestört oder gar geblockt werden, so dass die Tags in Reichweite dennoch nicht von den Lesegeräten erkannt werden.

Die Beeinträchtigung des korrekten Betriebs eines RFID-Systems (Denial of Service) kann ebenfalls durch Stören des elektromagnetischen Feldes, beispielsweise durch den Einsatz von metallischen Folien, geschehen oder durch das (temporäre wie dauerhafte) Deaktivieren der Tags. Eine etwas weiter entwickelte Technik ist der Einsatz eines Blockierungs-Chips, der in Systemen mit Kollisionskontrolle sich stets in den Vordergrund „drängelt“ und quasi

1 Marc Langheinrich: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie. In: Elgar Fleisch, Friedemann Mattern (Hrsg.): Das Internet der Dinge. Ubiquitous Computing und RFID in der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen. Springer Verlag, Berlin Heidelberg, 2005.

2 Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Risiken und Chancen des Einsatzes von RFID-Systemen. Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit. Secumedia Verlags-GmbH, Ingelheim, 2004.

am „lautesten“ seine ID bekanntgibt, so dass Lesegeräte nicht die eigentlichen Objekte erfassen, sondern stets nur dieses eine Tag. Auch könnten die Batterien aktiver Transponder durch wiederholte Anfragen verbraucht werden.

Schutzmaßnahmen

Das berechnete Auslesen von Daten setzt voraus, dass man entsprechende Zugriffsrechte vergeben und diese auch überprüfen kann. Das gegenseitige Authentifizieren ist, es wurde bereits angesprochen, ressourcenaufwändig und daher erfolgt meist lediglich eine Überprüfung der Identität des RFID-Tags durch das Lesegerät. Das RFID-System muss in der Lage sein, zu entscheiden, ob eine bestimmte Seriennummer den Tag berechtigt, dem System beizutreten. Die Überprüfung bestimmter Nummernbereiche kann um ein sogenanntes Challenge-Response-Verfahren ergänzt werden, bei dem das Lesegerät eine Zufallszahl an den Transponder schickt (Challenge) und dieser wiederum eine Antwort sendet, die mit einem geheimen Schlüssel kodiert wurde (Response). Soll eine gegenseitige Authentifizierung erfolgen, muss der RFID-Chip in der Lage sein, ebenfalls eine Challenge zu generieren. Für eine detaillierte Beschreibung dieser „Three Pass Mutual Authentication“ nach ISO/IEC 9798-2 wird auf das Kapitel 8.2.1 des RFID-Handbuchs von Klaus Finkenzeller verwiesen.³

Möchte man verhindern, dass die Luftschnittstelle abgehört wird oder dass die gesendeten Daten durch einen Angreifer manipuliert werden, bietet sich der Einsatz von Verschlüsselung zur Übertragung der Daten an. Bei RFID-Systemen kommen aufgrund der Ressourcenknappheit bislang nur symmetrische Verfahren zum Einsatz, die mit Hilfe eines gemeinsam bekannten Schlüssels den Datenverkehr sowohl ver- als auch entschlüsseln können. An der Geheimhaltung des Schlüssels hängt demzufolge die Abhörsicherheit.

Durch Pseudonymisierung können das Auslesen der Daten und ein Stück weit auch die Ortsbestimmung durch Unberechtigte verhindert werden, weil in diesem Szenario nur das Lesegerät die wahre Identität des Tags kennt. Der Transponder selbst sendet bei jedem Aufruf eine andere „Meta-ID“ an das Lesegerät, die aus einer Zufallszahl

Angriff	Kosten	Gegenmaßnahmen	Kosten
Abhören der Kommunikation zwischen Tag und Lesegerät	hoch	Verlagerung ins Backend Abschirmung Verschlüsselung	mittel
Unautorisiertes Auslesen der Daten	mittel bis hoch	Detektoren Authentifizierung	mittel
Unautorisiertes Verändern der Daten	mittel bis hoch	Read-only-Tags Detektoren Authentifizierung	gering bis mittel
Cloning und Emulation	mittel	Erkennung von Duplikaten Authentifizierung	mittel
Ablösen des Tags vom Trägerobjekt	gering	Mechanische Verbindung Alarmfunktion (aktive Tags) Zusatzmerkmale	gering bis mittel
Mechanische oder chemische Zerstörung	gering	Mechanische Verbindung	gering bis mittel
Zerstörung durch Feldeinwirkung	mittel	selbst heilende Sicherung (nur begrenzt wirksam)	in Serie gering
Zerstörung durch Missbrauch eines Kill-Befehls	mittel	Authentifizierung	mittel
Entladen der Batterie (nur aktive Tags)	mittel	Schlafmodus	in Serie gering
Blocker-Tag	gering	Verbot in AGB (nur begrenzt wirksam)	gering
Störsender	mittel bis hoch	Messungen Frequenzsprungverfahren	mittel bis hoch
Feldauslöschung	gering (jedoch schwierig)	keine	-
Feldverstimmung	sehr gering	aktive Frequenznachführung	mittel bis hoch
Abschirmung	sehr gering	verbesserte Lesestationen (nur begrenzt wirksam)	mittel

Tabelle 2: Kosten der Gegenmaßnahmen, zit. nach [BSI2004].

und der wahren ID des Tags generiert wird und lediglich einen Hash-Wert darstellt. Dem Lesegerät (oder dem im Hintergrund arbeitenden IT-System) müssen dazu allerdings die wahren IDs bekannt sein.

Als beste Gegenmaßnahme empfiehlt es sich zusammenfassend gesagt, die Daten (bis auf die ID) komplett in das Backend zu verlagern und jede Datenübertragung zu verschlüsseln. Dabei spielen die Kosten sicherlich eine erhebliche Rolle, wie nicht nur Bruce Schneier treffend feststellt: „Information security isn't a technological problem. It's an economics problem. And the way to improve information technology is to fix the economics problem. Do that, and everything else will follow.“⁴

Eine Gegenüberstellung der Kosten für Angriffe und Gegenmaßnahmen kann der Tabelle 2 entnommen werden.

3 Klaus Finkenzeller: RFID Handbuch. Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC. Hanser-Verlag, 5. Auflage, München, 2008, Seite 257f.

4 Bruce Schneier: The Problem Is Information Insecurity, <http://www.schneier.com/essay-233.html>, August 2008, letzter Zugriff am 5. März 2010.