RFID-Systeme – Sicher genug für den Einsatz im medizinischen Umfeld?

B. Schütze[1], M. Kroll[2], M. Kämmerer[3]
1 HI Consulting, Düsseldorf, Deutschland
2 Michael Kroll Consulting & Solutions, Mülheim, Deutschland
3 Gesellschaft für Sicherheit, Informationstechnologie und Telemedizin mbH (GeSIT), Mainz, Deutschland

Einleitung: **RFID ermöglicht eine berührungslose Datenübertragung. Der Einsatz von RFID-Systemen wird in der Medizin und Pharmazie immer stärker diskutiert. Die US-amerikanische Food and Drug Administration (FDA) empfiehlt den Einsatz von RFID-Transpondern zur eindeutigen Identifizierung von Medikamenten zu oder Medizingeräte, in Deutschland wird beim RFID-Einsatz in der Medizin häufiger an die Möglichkeiten der Prozessoptimierung gedacht. Allerdings wird RFID auch in der Patientenversorgung und der Forschung verstärkt eingesetzt.**
Material und Methode: **In dieser Arbeit wird basierend auf einer Literaturrecherche überprüft, ob der Einsatz von RFID-Systemen hinsichtlich der Sicherheit der medizinischen Daten unbedenklich ist oder ob zum Schutz der Daten gegen unbefugtes Ausspähen oder Abändern zusätzliche Maßnahmen getroffen werden müssen.**
Ergebnisse: **Das Grundkonzept von RFID-Systemen basiert auf einer Kopplung (induktiv oder durch elektromagnetische Wellen) zwischen zwei Spulen (resp. Antennen), eine im Lesegerät, eine im Transponder. Die wichtigsten Unterscheidungsmerkmale für RFID-Systeme sind die Betriebsfrequenz des Lesegerätes, das physikalische Kopplungsverfahren und die Reichweite des Systems. Grundsätzlich kann ein Angriff auf den Transponder, das Lesegerät oder auf die Kommunikation zwischen beiden erfolgen. Denkbare Angriffszenarios auf RFID-Systeme bestehen im unberechtigten Auslesen der Daten, dem Verändern bzw. Fälschen der Daten, dem Verhindern, das die Daten berechtigt ausgelesen werden können und dem Zerstören der Daten.**
Diskussion: **Die Verwendung von RFID-Systemen wird in Zukunft zunehmen, neue Einsatzmöglichkeiten entwickelt und neue Anwendungsfelder erschlossen werden. Werden RFID-Systeme in sicherheitsrelevanten Umgebungen eingesetzt, muss mit potenziellen Angriffsversuchen gerechnet werden und entsprechende Schutzvorkehrungen getroffen werden, die RFID-Systeme bieten von sich aus nicht hinreichend Schutz vor Datenmanipulation.**

Einleitung

Genau wie beim Strich- oder Barcode ermöglicht RFID (**R**adio **F**requency **Id**entification) eine berührungslose Datenübertragung. Beim RFID können Informationen über unterschiedliche Entfernungen hinweg ausgetauscht werden. Die Bezeichnung RFID ist ein Synonym für die Radiofrequenztechnik, die zu Identifikationszwecken eingesetzt wird, kurz: RFID = Identifikation per Funk.

In der Medizin und Pharmazie ist RFID ein beliebtes Thema. Das RFID-Anwendungsspektrum erstreckt sich von der Kontrolle von Blutkonserven bis hin zur Medikamentensicherheit. Die US-amerikanische Food and Drug Administration (FDA) empfiehlt den Einsatz von RFID-Transpondern unter anderem, um Produktfälschungen von Medikamenten zu verhindern oder Medizingeräte eindeutig zuordnen zu können [14, 15]. In Deutschland wird häufiger an die Möglichkeiten der Prozessoptimierung gedacht.

RFID kann zum Zwecke der zeitnahen Erfassung von Mengen und Positionsangaben eingesetzt werden. Ob die Kontrolle von Zutrittsrechten (beispielsweise zu Säuglingsstationen, Intensivstationen oder OP-Sälen), die automatisierte Erfassung des Lagerbestandes (z. B. in der Apotheke) oder die Überwachung von mobilen medizinischen Geräten und Betten in Echtzeit: Viele Anwendungsmöglichkeiten zur optimierten Prozesssteuerung und –überwachung im medizinischen Umfeld sind denkbar. Die kontaktlose Datenübertragung der RFID-Systeme kommt zudem den Hygienestandards entgegen.

Auch die Patientenversorgung ist im Blickfeld der RFID-Entwicklung: Siemens hat zusätzlich eine RFID-Uhr entwickelt, die Herzfrequenz und den Standort des Trägers übermittelt [13]. Ein spezieller Sensor an der Brust misst die Herzwerte und sendet sie an die Uhr, die die Daten wiederum an den Arzt funkt. Um die Position des Trägers auf zwei Meter genau ermitteln zu können, befinden sich auf dem Klinikareal mehrere Antennen. Wenn sich der Zustand des Patienten verschlechtert, können sich die Mediziner sofort an dessen Aufenthaltsort begeben und eingreifen. Woanders werden RFID-Systeme zur Positionsbestimmung von Endotrachealtuben bei der Beatmung von Patienten auf der Intensivstation eingesetzt [16]. Im OP werden RFID-Systeme eingesetzt, um zu überprüfen, ob alle Tücher, Schwämme usw. den Patienten wieder verlassen haben [17]. Im Inselspital Bern kommt die die RFID-Technologie in der Bettenwirtschaft zum Einsatz [18].

Aber auch in der Forschung wird der Einsatz von RFID-Systemen immer stärker diskutiert. Ein passiver Transponder besitzt keine eigene Spannungsversorgung und wird daher nur aktiv, wenn sich ein

Autoren: B. Schütze, M. Kroll, M. Kämmerer
Titel: RFID-Systeme – Sicher genug für den Einsatz im medizinischen Umfeld?
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 251-257

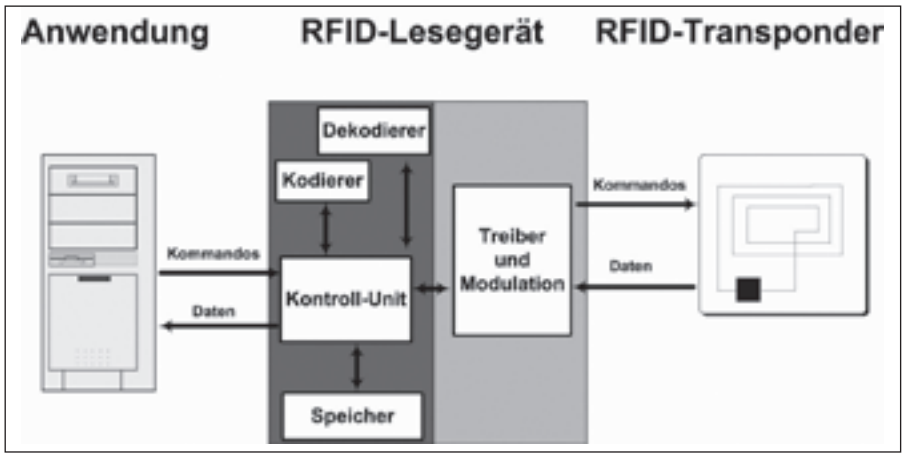

Abbildung 1: *RFID-Lesegerät und -Transponder in Verbindung mit der Anwendungsumgebung*

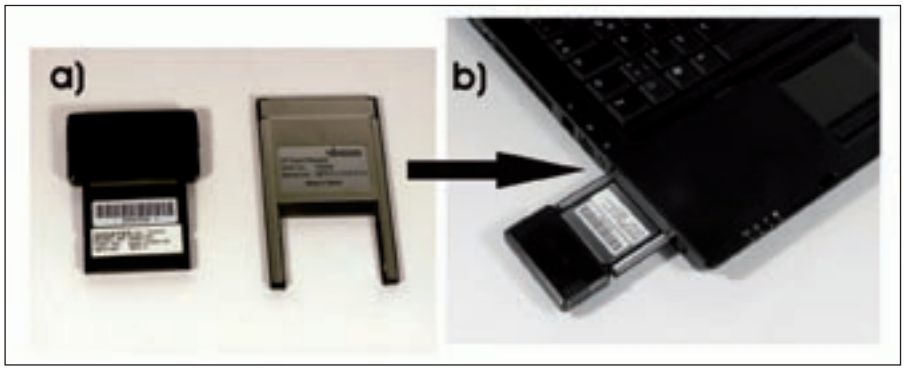

Abbildung 2: *RFID-Lesegerät für mobile Geräte*

dementsprechendes Lesegerät in der Nähe befindet, von dem er seinen Spannungsbedarf durch Induktion bezieht. Die somit erreichte Strahlungsarmut ermöglicht die Nutzung dieser Transponder auf Langzeit am Patienten. Mit dem Transponder gekoppelte Sensoren senden hierbei Daten an diesen, sobald er aktiviert wird, um von dort medizinische Werte an das Lesegerät zurückzusenden. Hierbei kann man sich Glastranspondern in Form von 12-32mm langen Glasröhrchen bedienen. Diese werden unter der Haut des Patienten eingesetzt. Auf diese Weise lassen sich beispielsweise Langzeituntersuchungen am Menschen realisieren.

Material und Methode

In dieser Arbeit soll überprüft werden, ob der Einsatz von RFID-Systemen hinsichtlich der Sicherheit der medizinischen Daten unbedenklich ist oder ob zum Schutz der Daten gegen unbefugtes Ausspähen oder Abändern zusätzliche Maßnahmen getroffen werden müssen.

Hierzu wurde im ersten Schritt eine Literaturrecherche über die medizinische Datenbank „Medline“ zu diesem Thema durchgeführt. Des weiteren erfolgte eine Recherche mittels des Internets über diese Thematik. Basierend auf den Ergebnissen dieser Recherchen wird das Risikopotential bzgl. der Datensicherheit beim Einsatz von RFID-Systemen aufgezeigt.

Ergebnisse

Um die Sicherheitsrisiken des RFID-Einsatzes darstellen zu können, muss zunächst die zugrunde liegende Technik übersichtsartig dargestellt werden.

RFID-Technik

Grundlagen

Ein RFID-System besteht immer aus zwei Komponenten:

- dem Transponder, der an dem zu identifizierenden Objekt angebracht wird
- dem Erfassungs- oder Lesegerät, welches je nach Ausführung und eingesetzter Technologie als reines Lesegerät oder als Schreib-/Lese-Einheit erhältlich ist.

Das Grundkonzept von RFID-Systemen basiert auf einer Kopplung (induktiv oder durch elektromagnetische Wellen) zwischen zwei Spulen (Antennen), eine im Lesegerät, eine im Transponder [8]. Die Spule des Lesegerätes erzeugt ein Magnetfeld, welches als Energieträger für die Spule des Transponders dient, der hierdurch mit Energie versorgt wird. Ebenso fungiert das Magnetfeld als Träger der Information (siehe Abbildung 1).

Lesegerät

Ein Lesegerät beinhaltet typischerweise ein Hochfrequenzmodul (= Sender und Empfänger), eine Kontrolleinheit sowie ein Koppelelement zum Transponder. Zusätzlich sind viele Lesegeräte mit einer Schnittstelle (RS232, IEEE 1284, IEEE 1394, USB usw.) ausgestattet, um die Datenweitergabe an einen Computer zu ermöglichen.

Lesegeräte existieren in den verschiedensten Formen, z. B. für mobile Geräte wie Handhelds (Abbildung 2a), die mit einem Adapter auch in Notebooks eingesetzt werden können (Abbildung 2b).

Andere Lesegeräte sind mittels USB-Schnittstelle an jedem handelsüblichen Computer anschließbar (Abbildung 3b). Spezielle Geräte bieten über die USB-Schnittstelle sogar Debug-Möglichkeiten, so dass durch den Einsatz geeigneter Software die gesamte RFID-Kommunikation am Computer verfolgt werden kann (Abbildung 3a).

Transponder

Ein Transponder ist ein drahtloses Kommunikations-, Anzeige- oder Kontrollgerät, welches eingehende Signale aufnimmt und automatisch darauf antwortet. Der Begriff Transponder ist zusammengesetzt aus den begriffen Transmitter und Responder. Es existieren passive und aktive Transponder.

Der Transponder besteht aus einem Koppelelement (in der Regel eine Spule) sowie einem Mikrochip, die in einem Gehäuse zwecks besserer Transportabili-

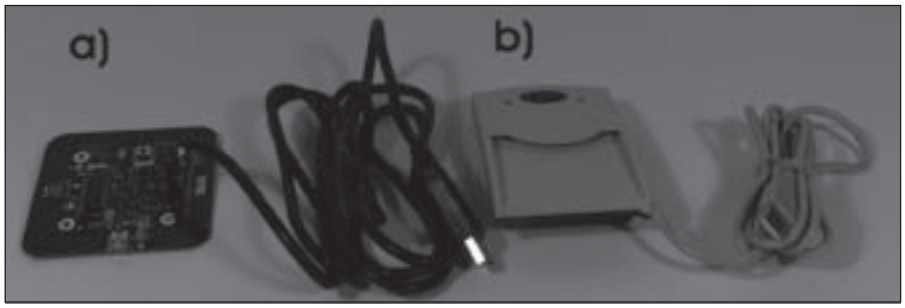

Abbildung 3: *RFID-Lesegerät mit USB-Schnittstelle*

tät sowie dem Schutz vor physikalischen Beschädigungen untergebracht werden (Abbildung 4). Außerhalb des Ansprechbereiches eines Lesegerätes verhält sich der Transponder vollkommen passiv. Erst innerhalb eines Lesegerätes wird der Transponder aktiviert. Die zum Betrieb des Transponders benötigte Energie wird durch die Koppeleinheit durch die elektromagnetischen Wechselfelder als Übertragungsmedium vom Lesegerät zum Transponder übertragen.

Die Datenmenge von RFID-Transpondern reicht üblicherweise von wenigen Bytes bis zu mehreren KBytes. Eine Ausnahme stellen die sogenannten 1-bit-Transponder dar. Eine Datenmenge von 1 Bit ermöglicht dem Lesegerät die Erkennung von 2 Zuständen: „Transponder im Feld“ oder „kein Transponder im Feld“ [8]. Für einfache Überwachungs- bzw. Sicherungsaufgaben (z. B. Diebstahlschutz im Kaufhaus) ist diese Funktionalität jedoch völlig ausreichend. Beim Verlassen des Kaufhauses mit unbezahlter Ware erkennt das am Ausgang installierte Lesegerät (Beispiel siehe Abbildung 5) dann den Zustand „Transponder im Feld“ und löst einen entsprechenden Alarm aus. Bei der ordnungsgemäß bezahlten Ware wird der 1-bit-Transponder an der Kasse entfernt oder deaktiviert.

Fast alle 13,56 MHz-Transponder erhalten bei der Herstellung eine weltweit einmalig vergebene Identifikations-Nummer (UID) [1, 2]. Die Länge der UID legt ISO15693 mit 64 bit fest. Die UID bleibt stets unverändert gespeichert und dient als Seriennummer für den Transponder.

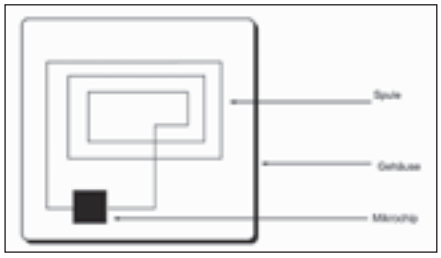

Abbildung 4: *Aufbau eines Transponders*

Da Transponder in Form und Größe häufig dem Aussehen eines Etikett oder einer Plakette (engl. „Tag“) entsprechen, wird hier häufig auch von einem RFID-Tag oder Smart-Tag gesprochen.

Ein Aussehen eines RFID-Tag kann nahezu beliebig angepasst werden (rund, eckig, massiv, flach, usw.) und werden je nach Verwendungszweck in verschiedene Bauformen realisiert oder auf entsprechende Trägermaterialien angebracht. Damit können RFID-Tags an verschiedenste Umgebungen und Anforderungen angepasst werden und können zudem – je nach Bauform – extrem robust und langlebig sein.

Standardmäßig sind RFID-Tags verfügbar als:

- Etiketten,
- (Chip-) Karte,
- Scheiben,
- Armbänder,
- Schlüsselanhänger.

Transponder können aktiv oder passiv sein. Aktive Transponder sind batteriebetrieben und können in der Regel sowohl gelesen als auch beschrieben werden. Dabei kann der interne Speicher - je nach Transponder - über 1 MByte aufnehmen. Aktive Tags befinden sich normalerweise im Ruhezustand und senden ihre Informationen nur aus, wenn sie ein spezielles Aktivierungssignal empfangen. Aktive Transponder sind im Vergleich zu passiven meist größer, besitzen eine höhere Sendereichweite, eine geringere Lebensdauer und sind deutlich teurer.

Passive Transponder beziehen ihre Energie zur Informationsübermittlung ausschließlich aus den empfangenen Funkwellen. Passive Transponder können wesentlich weniger Daten speichern als aktive Transponder. Zudem können die gespeicherten Daten in der Regel nur gelesen werden.

Unterscheidungsmerkmale von RFID-Systemen

Die wichtigsten Unterscheidungsmerkmale für RFID-Systeme sind die Betriebsfrequenz des Lesegerätes, das physikalische Kopplungsverfahren und die Reichweite des Systems.

Frequenz

Der niedrigste Frequenzbereich für RFID liegt im Langwellenbereich bei 100 kHz bis 135 kHz, diese Frequenzen werden überwiegend in Nord- und Südamerika sowie in Japan genutzt. Da die Übertragungsrate bei diesen Frequenzen relativ gering ist und außerdem die Antenne äußerst lang, benutzt man bei RFID zunehmend HF-Frequenzen und Mikrowellen.

Der nächsthöhere Frequenzbereich liegt zwischen 6,765 MHz und 6,795 MHz und ist international als ISM-Band ausgewiesen und wird in Deutschland nicht für RFID genutzt.

Der darauf folgende HF-Bereich liegt im Kurzwellenbereich bei 13,56 MHz, ein

Abbildung 5: *Lesegerät für 1-bit-Transponder zum Diebstahlschutz in einem Kaufhaus*

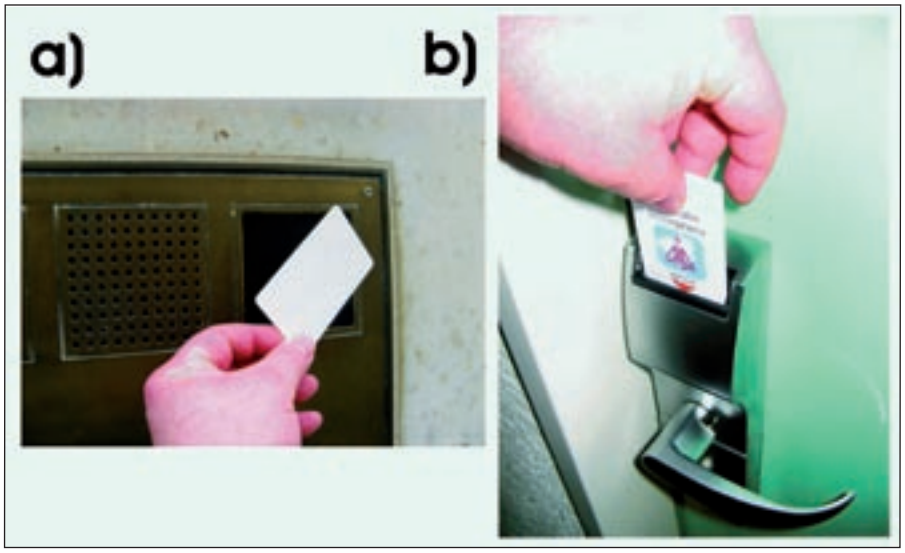

Abbildung 6: *RFID-Chipkarten-Applikation als elekronischer Türöffner; a) kontaktlos, b) kontaktgebunden*

weiterer RFID-HF-Frequenzbereich im CB-Band bei 27,125 MHz.

433,920 MHz ist das unterste Frequenzband im UHF-Bereich, weitere liegen bei 869 MHz, 889 MHz und 915 MHz. Die beiden letztgenannten Frequenzbereiche werden international nicht einheitlich genutzt.

Mit 2,45 GHz und 5,8 GHZ werden wiederum ISM-Bänder im SHF-Band für RFID genutzt. RFID-Tags in diesem Frequenzbereich werden als Mikrowellen-Tags bezeichnet.

Die EPCglobal, eine internationale Organisation für die Weiterentwicklung des Electronic Product Codes (EPC), hat die Sendefrequenz für RFID-Tags auf 866 MHz bis 956 MHz spezifiziert.

Die unterschiedlichen Frequenzbereiche unterscheiden sich in ihren Eigenschaften hinsichtlich der überbrückbaren Entfernung zwischen RFID-Tag und Lesegerät, der Penetration der Waren und dem Einfluss von elektromagnetischen Störungen.

Reichweite und Kopplung

RFID-Systeme mit sehr kleinen Reichweiten im Bereich bis zu 1 cm werden als „Close-coupling-Systeme“ bezeichnet. Die Transponder müssen zum Betrieb entweder in ein Lesegerät eingesteckt oder auf einer dafür vorgesehenen Oberfläche positioniert werden. Close-coupling-Systeme verwenden sowohl elektrische wie auch magnetische Felder zur Kopplung. Close-coupling-Systeme werden vor allem in Applikationen eingesetzt, an die große Sicherheitsanforderungen gestellt werden, die jedoch keine großen Reichweiten erfordern wie z. B. elektronische Türschließanlagen (siehe Abbildung 6a) kontaktlos oder 6b) kontaktgebunden) oder kontaktlose Chipkartensysteme mit Zahlungsfunktion.

RFID-Systeme mit Schreib- und Lesereichweiten bis zu einem Meter werden als Remote-coupling-Systeme bezeichnet. Etwa 10 % dieser Systeme nutzen eine kapazitive Kopplung, dementsprechend verwenden etwa 90 % der Systeme eine induktive Kopplung, weshalb sie mitunter auch als induktive Funkanlage bezeichnet werden. Als Sendefrequenzen werden Frequenzen unter 135 kHz oder 13,56 MHz verwendet.

RFID-Systeme mit Reichweiten von über 1 Meter werden als Long-range-Systeme oder Backscatter-Geräte bezeichnet. Alle Long-Range-Systeme arbeiten mit elektromagnetischen Wellen im UHF- (868 MHz in Europa, 915 MHz in den USA) und Mikrowellenbereich (2,5 und 5,8 GHz). Mit passiven Transpondern können Reichweiten von 3 Metern realisiert werden, mit aktiven Transpondern können Reichweiten von über 15 Metern realisiert werden.

Datenintegrität

Bei einer kontaktlosen Datenübertragung können leicht Störungen auftreten, welche die übertragenen Daten verändern, woraus eine fehlerhafte Übertragung resultiert. Durch Prüfsummenverfahren können Übertragungsfehler erkannt und Korrekturmaßnahmen ergriffen werden. Die gebräuchlichsten Prüfsummenverfahren sind:

- Paritätsprüfung (parity check)
- XOR-Summe oder LRC (longitudinal redundancy check = Längssummenprüfung)
- CRC (cyclic redundancy check)

Alle drei Verfahren haben sich bewährt und werden bei RFID-Anwendungen eingesetzt [8].

Beim Betrieb eines RFID-Systems arbeitet häufig ein Lesegerät mit einer Vielzahl von Transpondern. Dabei sind zwei Übertragungswege möglich:

a) Daten werden von dem einen Lesegerät an alle in Reichweite befindlichen Transponder übertragen („broadcast-message“)
b) Daten werden von den in Reichweite befindlichen Transpondern an das Lesegerät übertragen.

	Induktive Kopplung	Elektromagnetische Kopplung
Frequenzen	125 / 135 kHz 13,56 MHz	862 bis 956 MHz 2,45 GHz
Antennen	(Großflächige) Spulen	Dipole, Monopole
Reichweite	Bis ca. 1,5 m	> 15 m
Einsetzbarkeit	Gut in nasser Umgebung, schlecht in metallischer Umgebung	Schlecht in nasser Umgubung, gut in metallischer Umgebung

Tabelle 1: *Parameter bzgl. der Auswahl eines geeigneten RFID-Systems*

Jeder Kommunikationskanal verfügt über eine definierte Kanalkapazität, welche durch die maximale Datenrate des Kommunikationskanals sowie die Zeitspanne seiner Verfügbarkeit bestimmt wird. Die vorhandene Kanalkapazität muss den einzelnen Transpondern so zugeteilt werden, dass eine Übertragung der Daten von mehreren Transpondern an ein einzelnes Lesegerät ohne gegenseitige Störung (= Kollision) stattfinden kann.

Bei RFID-Transpondern existieren nur kurze Phasen der Aktivität mit ungleich längeren Ruhepausen, weshalb die aus der Funktechnik bekannten Antikollisionsverfahren zur Kollisionsvermeidung nicht 1:1 eingesetzt werden können. Aus Wettbewerbsgründen sind RFID-Systemhersteller in der Regel nicht bereit, die von ihnen eingesetzten Antikollisionsverfahren zu veröffentlichen. Bekannt sind die folgenden Verfahren:

- ALOHA-Verfahren
- Slotted ALOHA-Verfahren
- Binary-Search-Algorithmus

In der Praxis haben sich die beiden Letztgenannten durchgesetzt.

Systemübersicht

Typische industrielle Einsatzgebiete für RFID-Tags sind:

- Kfz-Wegfahrsperren
  125 kHz, Transponderchip im Schlüsselknauf
- Tier- und Menschidentifikation
  125 kHz, „Einspritzen“ des Tags unter die Haut
- Warenmarkierungen
  13,56 MHz, „Smart Label“ unter Preisschildern
- Zutrittskontrollen
  125 kHz/13,56 MHz, Plastikkarten mit integriertem Chip
- Diebstahlsicherungen
  versteckter Einbau des RFID-Tags im Objekt
- Logistik und industrieller Warenfluss
  RFID-Labels an Fahrzeugkomponenten
- Forstwirtschaft
  RFID-„Einschlagnägel“ zum Markieren von Bäumen

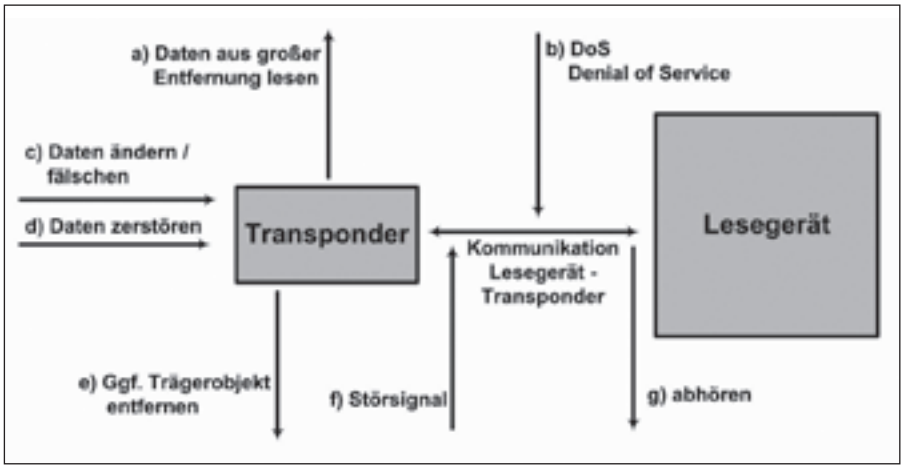

Abbildung 7: *Mögliche Angriffszenarien auf ein RFID-System*

RFID-Sicherheit

Grundsätzlich kann ein Angriff auf den Transponder, das Lesegerät oder auf die Kommunikation zwischen beiden erfolgen. Abbildung 7 zeigt verschiedene denkbare Angriffsszenarien auf ein RFID-System:

- Unberechtigtes Auslesen der Daten
  Die Daten können direkt vom Transponder ausgelesen werden (Abbildung 7a) oder während der Kommunikation zwischen Lesegerät und Transponder „mitgehört“ werden (Abbildung 7g) werden.
- Verändern/fälschen der Daten
  Die Daten können auf dem Transponder geändert (Abbildung 7c) oder zerstört (Abbildung 7d) werden. Je nach Anwendungsszenario können die Daten auch kopiert und auf einen neuen Transponder eingelesen werden, z. B. beim Kopieren einer Chipkarte für ein elektronisches Türschloss.
- Verhindern des Auslesens der Daten
  Die Kommunikation zwischen Lesegerät und Transponder kann durch ein Störsignal (Abbildung 7f) verhindert werden oder durch einen Denial-of-Service-Angriff (Abbildung 7b) blockiert werden. Das entfernen eines evtl. vorhandenen Trägerobjektes (Abbildung 7e) verhindert, dass der Transponder in Reichweite des Lesegerätes gebracht werden kann.

Ausspähen der Daten aus größerer Entfernung

Durch die Vergrößerung der Lesereichweite kann ein Transponder aus sicherer Entfernung ausgelesen werden.

Lauschen mittels induktiver Kopplung

Soll die Reichweite eines RFID-Lesegerätes vergrößert werden, muss die Energiereichweite des Lesegerätes vergrößert werden. Hierzu wird der Durchmesser der Leseantenne sowie der Strom in der Sendeantenne erhöht.

Durch die Vergrößerung des Antennendurchmessers der Leseantenne nimmt jedoch die Gegeninduktivität und damit der Pegel des Lastmodulationssignals am Lesegerät ab. Zusätzlich wird das am Sender erzeugte Rauschen im Frequenzbereich der Lastmodulationsbänder durch die zunehmende Sendeleistung erhöht.

Daher kann die Reichweite eines Lesegerätes, welches 13,56 MHz Transponder aus 10 cm ausliest, selbst unter Optimierung aller Parameter nicht über mehr als 40 cm ausgelesen werden.

Abhören bei Backscatter-Kopplung

Bei den heute verbreiteten Backscatter-Systemen ist zunächst einmal die für den Betrieb des Transponders benötigte Energie für die Reichweite des Systems ausschlaggebend. Zur Erhöhung der Reichweite ist daher die Energie der Sendeleistung des Lesegerätes zu erhöhen.

Um jedoch die Reichweite zu verdoppeln und dabei zugleich die vom Transponder zurückkommende Energie der

Datenübermittlung konstant zu halten, muss die Sendeleistung des Gerätes um den Faktor 16 erhöht werden.

Die Verwendung einer Langyagi-Antenne statt der herkömmlichen Dipolantenne kann die Reichweite um das sieben- bis Achtfache erhöhen [6]. Mit vertretbarem Aufwand kann aus heutiger Sicht die Reichweite auf das 20fache des Ursprungswertes gesteigert werden.

Abhören der Kommunikation

RFID-Systeme kommunizieren mittels (elektro-) magnetischen Wellen, daher ist das Abhören der Systeme grundsätzlich möglich. Die für RFID-Systeme angegeben Reichweiten von wenigen Zentimetern (13,56 MHz, ISO/IEC 14443) bis hin zu mehreren Metern (868 MHz, ISO/IEC 18000-6) gelten für die aktive Kommunikation, bei welcher der Transponder mit Energie versorgt werden muss. Das passive Abhören der Kommunikation hingegen ist auf eine größere Umgebung möglich [5].

Kopieren eines Transponders / Ändern der Transponder-Daten

Im einfachsten Fall des Read-only-Transponders verfügt der Transponder lediglich über seine Seriennummer, die der Transponder periodisch ausstrahlt, sobald er in ein ausreichend starkes Feld eines Lesegerätes gelangt. Der Kanadier Jonathan Westhues beschreibt auf seiner Internetseite den Aufbau einer Schaltung zum Auslesen und Kopieren von RFID-Transpondern [4]. Durch den Ersatz des PROM, welches die Seriennummer erhält, durch ein mehrfach programmierbares EEPROM ist das „RFID-Cloning“ relativ leicht zu bewerkstelligen.

Bei den beschreibbaren RFID-Transpondern können die Speicherbereiche völlig nach belieben gelesen und beschrieben werden. Neben dem Kopieren eines Transponders können hier natürlich auch die Daten nach belieben geändert oder auch gelöscht werden.

Verhindern des Auslesens des Transponders

Im einfachsten Fall reicht es, einen Transponder in eine metallische Folie (z. B. Alu-Haushaltsfolie“ zu wickeln, denn bei induktiv gekoppelten Transpondern wird der Antennenschwingkreis des Transponders durch eine Metalloberfläche verändert [12]. Zusätzlich wird das magnetische Feld des Lesegerätes durch Wirbelstromverluste in der Metallfolie gedämpft. Auf diesem Prinzip basiert auch die RFID-Pass-Schutzhülle des Vereins zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V. [3].

Antennen von UHF-Transpondern werden durch das Auf- und Einbringen in ein Dielektrikum (z. B. Glas oder Kunststoff) verstimmt und so nach dem obengenannten Prinzip die Kommunikation verhindert.

Der Vorteil liegt darin, dass ein Transponder nur zeitweise außer Betrieb gesetzt wird, z. B. um das unberechtigte Ausspähen der enthaltenen Daten zu verhindern.

Denial of Service, Slotted-ALOHA-Verfahren

Beim Slotted-ALOHA-Verfahren folgt dem Antikollisionskommando eines Lesegerätes eine vorher definierte Anzahl von Zeitintervallen („Slots“), in welchen die in der Reichweite des Lesegerätes Transponder ihre Daten an das Lesegerät senden. Die Transponder wählen dabei den von ihnen verwendeten Slot zufällig aus.

Versuchen zwei oder mehr Transponder ihre Daten im selben Slot zu übertragen, so können wegen der auftretenden Kollisionen keine Daten richtig gelesen werden.

Um das Slotted-ALOHA-Verfahren muss ein Stör-Transponder („Blocker-Tag“) nur in jedem der zur Verfügung stehenden Slots Daten senden, idealerweise ein ungültiges Datenpaket, z. B. ein Datenpaket mit falscher Prüfsumme. Für das Lesegerät ist es so unmöglich, mit einem anderen Transponder in Reichweite zu kommunizieren.

Denial of Service, Binary-Search-Tree-Algorithmus

Bei Verwendung des binären Suchbaums wird ein rekursiver Algorithmus eingesetzt, be idem bei jeder auftretenden Kollision an einer Bitstelle der empfangenen Seriennummer eine Verzweigung im binären Baum ausgewählt wird, indem das entsprechende Bit auf “0”oder “1”gesetzt wird.

Das Blocker-Tag simuliert an jeder Bitposition der Seriennummer eine Kollision, indem es gleichzeitig eine „0“ und eine „1“ sendet [7]. Das Lesegerät muss daher den gesamten binären Suchbaum durchlaufen.

Dabei täuscht das Blocker-Tag einem Lesegerät vor, es befinden sich 2^k Transponder in dessen Reichweite, wobei k die Anzahl der Bits der Seriennummer darstellt. Das Abfragen einer derart großen Anzahl blockiert das Lesegerät vollständig.

Ein Blocker-Tag, welches den vollständigen Suchbaum eines Lesegerätes blockiert, wird auch als „Full-Blocker“ oder als „Universal-Blocker“ bezeichnet [7].

Störsender

Um das starke Trägersignal eines Lesegerätes zu überdecken und so die Kommunikation zwischen Lesegerät und Transponder stören zu können, müssen Abstand, Sendeleistung und Antennengewinn (bzw. Antennendurchmesser bei induktiver Kopplung) mindestens dem eingesetzten Lesegerät entsprechen.

Der Transponder hat jedoch nur ein deutlich schwächeres Antwortsignal, sodass hier eine Störung zwischen Lesegerät und Transponder mit deutlich weniger Aufwand erzielbar ist. Ein Störsender auf den Frequenzen der Modulationsseitenbänder des Transponders kann bei gleichem Abstand zum Transponder und Lesegerät mit einer Sendeleistung von wenigen mW die Kommunikation deutlich stören.

Lösen des Tags vom Trägerobjekt

Ein Angreifer kann das Tag vom Trägerobjekt lösen. Dadurch kann der Transport bzw. Bewegungen des ursprünglichen Objektes nicht mehr verfolgt werden. Zugleich besteht die Möglichkeit, ein anderes Objekt gegenüber der RFID-Leseeinheit als das ursprüngliche Trägerobjekt auszugeben.

Zerstören des Transponders

In der Regel ist der Transponder für einen Angreifer am leichtesten zugänglich und dessen Zerstörung fällt relativ leicht. Bei der Diebstahlsicherung im Kaufhaus reicht hier beispielsweise die Zerstörung der Antenne, z. B. durch Durchtrennung oder Durchbrechen.

Auch das Einbringen in ein System mit entsprechend starker Feldeinwirkung zerstört einen Transponder. Für die gebräuchlichsten induktiv gekoppelten 13,56 MHz Transponder ist nach ISO/IEC 1443 bzw.

ISO/IEC 15693 eine maximale Feldstärke von 12 A/m spezifiziert. Das Einbringen eines derartigen Transponders in die Mikrowelle oder ein MRT führt zu einer thermischen Zerstörung.

Diskussion

Die Verwendung von RFID-Systemen wird in Zukunft zunehmen, neue Einsatzmöglichkeiten entwickelt und neue Anwendungsfelder erschlossen werden.

Werden RFID-Systeme in sicherheitsrelevanten Umgebungen eingesetzt, muss mit potenziellen Angriffsversuchen gerechnet werden und entsprechende Schutzvorkehrungen getroffen werden,

Kryptographische Funktionen bieten sich zum Schutz der Daten vor unberechtigtem Auslesen an. Die Verwendung kryptographischer Funktionen verhindert jedoch die Nutzung billigerer Transponder, da vergleichsweise mehr Daten auf den Transpondern geschrieben werden müssen. Einige High-end RFID-Systeme ermöglichen die Authentifizierung zwischen Lesegerät und Transponder sowie die Daten-Verschlüsselung mit proprietären Protokollen, sodass die Anwendung hinter dem Lesegerät sich nicht um die Verschlüsselung kümmern muss [8]. Allerdings fordert eine proprietäre Lösung interessierte Anwender zum sogenannten „hacken“ heraus, sodass speziell an den Entschlüsselung der RFID-Verschlüsselungs-Systeme schon gearbeitet wird und die Sicherheit dieser Systeme für die nähere Zukunft schlecht eingeschätzt werden kann [9]. Letztlich sollte sich also doch die Anwendung um die entsprechende kryptographische Absicherung kümmern.

Kryptographie kann heute jedoch das Kopieren eines Transponders noch nicht verhindern, obwohl hier interessante Ansätze vorhanden sind [10, 11]. Zum Schutz dieser potenziellen Schwachstelle müssen ebenso wie zur Verhinderung der Störung der Kommunikation zwischen Lesegerät und Transponder zusätzlich organisatorische Schutzmaßnahmen ergriffen werden [12].

Literatur

1 Vollmer A. (2003) RFID im Überblick. elektronik industrie. 03(2003): 32 – 33

2 tecChannel. (2006) RFID - Die technischen Gundlagen. [Online, zitiert 2007-08-23]; Verfügbar unter http://www.tecchannel.de/test_technik/grundlagen/431196/index5.html

3 Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V . (2007) RFID-Pass-Schutzhülle [Online, zitiert 2007-08-23]; Verfügbar unter https://shop.foebud.org/product_info.php?pName=rfidpassschutzhuelle-p-130

4 Westhues J. (2003) Proximity Cards [Online, zitiert 2007-08-23]; Verfügbar unter http://cq.cx/prox.pl

5 Bundesamt für Sicherheit in der Informationstechnik – BSI (2004) Risiken und Chancen des RFID-Einsatzes. [Online, zitiert 2007-08-23]; Verfügbar unter http://www.bsi.bund.de/fachthem/rfid/RIKCHA_barrierefrei.pdf

6 Finkenzeller K. (2006) RFID-Handbuch [Online, zitiert 2007-08-23]; Verfügbar unter http://www.deutsches-fachbuch.de/info/detail.php?isbn=3446403981&part=4&words=zulssige+Ausmitte+bei+einachsiger+biegung&PHPSESSID=spa95ea6cf01

7 Juels A (2003) RSA Security Designs RFID Blocker [Online, zitiert 2007-08-23]; Verfügbar unter http://www.rfidjournal.com/article/articleview/549/1/1/

8 Knospe H, Pohl H. (2004) RFID Security. Information Security Technical Report. 9(4): 30 – 41

9 Chaos Computer Club e.V. (2007) CCC Camp: Practical RFID Attacks. [Online, zitiert 2007-08-23]; Verfügbar unter http http://www.mitternachtshacking.de/blog/217-217-ccc-camp-practical-rfid-attacks

10 Lemieux S, Tang A. (2007) Clone Resistant Mutual Authentication for Low-Cost RFID and Contactless Credit Cards. Cryptology ePrint Archive, Report 2007/170 [Online, zitiert 2007-08-23]; Verfügbar unter http://eprint.iacr.org/2007/170.pdf

11 Zhang X, King B. (2007) An Anti-Counterfeiting RFID Privacy Protection Protocol. Journal of Computer Science and Technology. 22(3): 438 – 448

12 Peris-Lopez, P Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A. (2006) RFID Systems: A Survey on Security Threats and Proposed Solutions. Lecture Notes in Computer Science. 4217: 159—170

13 Schulzki-Haddouti C. (2006) ‘Schöne neue Welt’: Der elektronisch bewachte Kranke. [Online, zitiert 2007-08-23]; Verfügbar unter http://www.sicherheit-heute.de/technik/medizin,186,Schoene_neue_Welt_Der_elektronisch_bewachte_Kranke,news.htm

14 Food and Drug Administration - FDA (2006) Task 4 White Paper - Automatic Identification of Medical Devices - Final Version. [Online, zitiert 2007-08-23]; Verfügbar unter http://www.fda.gov/cdrh/ocd/ecritask4.html#32

15 Food and Drug Administration - FDA (2007) Presentation: FDA Automatic Identification Initiatives for Drugs and Medical Devices. [Online, zitiert 2007-08-23]; Verfügbar unter http://www.fda.gov/cdrh/ocd/udi/presentations/Ferriter.html

16 Reicher J, Reicher D, Reicher M. (2007) Use of Radio Frequency Identification (RFID) Tags in bedside monitoring of endotracheal Tube position. Journal of Clinical Monitoring and Computing 21:155–158

17 Rogers A, Jones E, Oleyniko D. (2007) Radio frequency identification (RFID) applied to surgical sponges. Surg Endosc. 21(7): 1235-1237

18 Hotz G, Calame A (2007) RFID-Einsatz in der Medizin. Mdi 9(1): 21 – 23

19 Kelter H. (2005) Radio Frequency Identification – Bedrohungslage aktueller Technologie. KES. 1: 38 – 42

Kontakt
Dr. Bernd Schütze
HI Consulting, Düsseldorf
Tel.: +49 (0) 1 73 / 2 77 11 14
Fax: +49 (0) 2 11 / 7 94 88 97
schuetze@medizin-informatik.org