Bewertung des Sicherheitsniveaus einiger Mechanismen zur Vertraulichkeit, Verfügbarkeit und Pseudonymität[1] von Transpondern (RFID)[2, 3]

Prof. Dr. Hartmut Pohl, Informationssicherheit, Fachbereich Informatik, Fachhochschule Bonn–Rhein–Sieg
Prof. Dr. Norbert Jung, Embedded Systems, Fachbereich Informatik, Fachhochschule Bonn-Rhein-Sieg
Dipl.-Inf. Torsten Roth, Evidian GmbH, Consultant IT-Security, Köln

Kurzfassung

Sicherheitsanforderungen an Transponder steigen mit zunehmendem Einsatz – in der Produktion, Logistik und Handel - insbesondere beim Endverbraucher bei der stationären und mobilen Nutzung. Standards und derzeit gebräuchliche RFID-Protokolle [1] beinhalten bisher nur wenige Sicherheitsmechanismen und in proprietären Protokollen wird nur ein Teil davon genutzt [23]. Insbesondere im Bereich der Low-Cost-Transponder werden nur einfache Sicherheitsfunktionen implementiert, die einen geringen Widerstandswert zu besitzen scheinen [14].
Mit Verschlüsselungs-, Challenge-Response-Verfahren und digitalen Signaturen stehen allerdings Mechanismen zur Verfügung, mit denen ein hoher Widerstandswert erreicht werden kann. Diese Mechanismen werden jedoch bisher nur teilweise und bei hochpreisigen Transpondern verwendet.
Hier werden einige zur Erreichung der Sachziele der Informationssicherheit bei RFID-Transpondern eingesetzte und einsetzbare Mechanismen dargestellt und hinsichtlich ihrer Anwendbarkeit und Angreifbarkeit bewertet. Die Ergebnisse zeigen, dass Verfahren zur Erreichung eines mittleren bis hohen Sicherheitsniveaus (Widerstandswert gegen Angriffe) vorhanden sind.
Im Beitrag wird je ein relevanter Mechanismus zur Erreichung der drei Sachziele der Informationssicherheit Verfügbarkeit, Vertraulichkeit und Pseudonymität [22] bewertet:

- Verfügbarkeit: Widerstandswert gegen Strahlenbelastung bei medizinischen Anwendungen.
- Vertraulichkeit: Dazu wurde der Widerstandswert des Passwortschutzes von Transpondern mit Hilfe eines Brute-Force-Angriffs untersucht.
- Pseudonymität: Anwendbarkeit von Meta-ID-Verfahren.

1 Technik

RFID-Systeme bestehen aus mindestens einem Transponder (tag) und einem Schreib-/Lesegerät. Zwischen ihnen werden Informationen mit modulierten magnetischen oder elektromagnetischen Feldern ausgetauscht. Sie bestehen aus einem Mikrochip und einer Antenne mit Bauformen in der Größe von wenigen Zentimetern. Es wird zwischen aktiven Transpondern mit eigener Energieversorgung sowie passiven Transpondern unterschieden, die von einem Schreib-/Lesegerät ausgesandte Energie benötigen. Genutzt werden Transponder bisher überwiegend zur Identifizierung und Authentifizierung sowie auch zur Lokalisierung physischer Objekte und zur Zustandsüberwachung und Notifikation.
RFID-Systeme nutzen verschiedene Frequenzen in den Frequenzbändern LF bis SHF. In Europa ist die Sendeleistung der Systeme je nach genutzter Frequenz auf 25 bis 500 mW beschränkt [14].
Transponder sind mit (meist sehr kleinem) nur lesbarem, mit lesbarem und (wiederbe-)schreibbarem Speicher sowie mit Mikroprozessoren und auch mit Krypto-Prozessoren erhältlich. Als Speicher kommen Electrically Erasable Programmable Read-Only Memory (EEPROM), FLASH-Speicher, Ferroelectric Random Access Memory (FRAM) für die persistente Speicherung sowie Static Random Access Memory (SRAM) für die flüchtige Speicherung zum Einsatz. Das Lesen und Schreiben auf dem Speicher wird durch ein internes Schaltwerk realisiert. Dies kann (im einfachsten Fall) ein Zustandsautomat aus einer relativ kleinen Anzahl von Logikgattern oder (aufwändiger) ein Mikroprozessor mit Betriebssystem sein [5].
Hinsichtlich der Reichweite von RFID-Systemen werden drei Distanzgruppen close coupling (< 1 cm), proximity coupling (< 10 cm) und vicinity coupling (< 100 cm) unterschieden [14]. Die prak-

Erschienen in: Hollstein, T.; Wernle, M.E.; Wissendheit, U.: 2. Workshop RFID:
Intelligente Funketiketten – Chancen und Herausforderungen. Erlangen 4./5. Juli 2006 VDE/ITG Erlangen 2006

tisch erreichbare Reichweite ist u.a. durch Abschirmung z.B. durch Wasser und Metalle [1] meist geringer als ausgewiesen.
Einige Systeme ermöglichen eine Erfassungsrate von 35 Transpondern pro Sekunde, eine Datenrate von 50 kBit/s und ein Lesen bei bis zu 0,5 m/s Bewegungsgeschwindigkeit. Jüngere Generationen wie ItemTag oder StackTag ermöglichen ein Auslesen bei 4 m/s, Datenraten von bis zu 848 kBit/s und Erfassungsraten von bis zu 500 Transpondern pro Sekunde [12].
Antikollisions-Protokolle ermöglichen ein fehlerfreies Lesen auch dann, wenn sich mehrere Transponder in Reichweite eines Schreib-/Lesegeräts befinden. Damit wird sichergestellt, dass sich die Transponder nicht gegenseitig stören [5].
Hier werden die EPC-Protokolle UHF Class 0, UHF Class 1 und HF Class 1 [4, 7], sowie einige ISO-Protokolle für Chipkarten [5], auf vorhandene Sicherheitsmechanismen untersucht. Die in den Standards genannten Sicherheitsmechanismen sind größtenteils auf einfache CRC-Integritätsprüfungen, Frequency-Hopping, Sperren von Speicherbereichen gegen Überschreibung und eine Implementierung des Kill-Befehls beschränkt. Der so erreichte Widerstandswert ist für viele wirtschaftlich und für Leib und Leben (z.B. medizinische Anwendungen) bedeutsame Anwendungen zu gering.
Nur ein sehr kleiner Teil der zur Verfügung stehenden Sicherheitsmechanismen ist in die Protokolle integriert. Dies führt dazu, dass Transponder mit höheren Sicherheitsanforderungen auf ein proprietäres Protokoll zurückgreifen müssen oder einen der Standards lediglich als reines Übertragungsprotokoll nutzen, in deren Datenblocks die Daten in einem - widerstandsfähigere Sicherheitsmechanismen bereitstellenden - anderen Protokoll eingebettet sind (tunnel).

2 Sachziele und Sicherheitsmechanismen

2.1 Verfügbarkeit

An Transponder werden in allen Anwendungsbereichen hohe Verfügbarkeitsanforderungen gestellt; dies gilt herausgehoben für eine Reihe medizinischer Anwendungen [31], für die sie bedeutende Vorteile bieten: Zum einen kann mit ihnen ein Interface für die kontaklose Kommunikation der Patientenkarte realisiert werden. Zum anderen können für eine Behandlung unmittelbar wichtige Daten direkt am Patienten gespeichert werden, indem ein Transponder z.B. subkutan appliziert wird (VeriChip Corporation): Auch bei eingeschränkter Kommunikationsfähigkeit eines Patienten, z.B. im Zusammenhang mit einer Operation, sind die Daten verfügbar.
Allerdings wäre ein Transponder den gleichen Einwirkungen ausgesetzt wie die Patienten. Insbesondere die Wirkungen der bei einigen Diagnoseverfahren eingesetzten Strahlung wie in der Radiographie, der Computer Tomographie und der Nuklear-Medizin sind hier zu beachten. Hier hat die Zuverlässigkeit der Funktion des Transponders eine besondere Bedeutung.

2.1.1 Reichweite

Die erreichbaren Sende-/Empfangsreichweiten hängen ab von der Sendeleistung und der Antennenform und –größe sowie vom verwendeten Schreib-/Lesegerät ab. Transponder wie I-Code oder Hitag werden vom Hersteller mit einer Reichweite von bis zu 1,5 m angegeben [25].
Bei anderen RFID-Systemen sind diese jedoch nur mit 14 bzw. 7 cm Reichweite angegeben [33]; dies liegt hauptsächlich an der Reichweite des Schreib-/Lesegeräts. Im durchgeführten Praxistest mit dem Tagtracer-RFID-System konnten nur Maximalwerte von vier bis sechs Zentimetern gemessen werden [23].

2.1.2 Geschwindigkeit

Auch die Geschwindigkeit von 0,5 m/s mit der sich ein Transponder am Schreib-/Lesegerät vorbei bewegen darf [12], wird in einem einfachen Praxistest nicht erreicht. Eine Erkennung erfolgt nur bis ca. 0,3 m/s [23].

2.1.3 Störungen

Blocker-Tags [13] antworten auf jede Anfrage eines Schreib-/Lesegeräts und führen so Kollisionen herbei, die eine Kommunikation mit anderen Transpondern in ihrer Umgebung verhindern. Zur Reichweite von Blocker-Tags gilt dasselbe wie zu Transpondern (s. 2.1.1).

2.1.4 Kill-Befehl

Ein Transponder, der den Kill-Befehl ausgeführt hat, soll auf keine weiteren (auch andere) Befehle (mehr) reagieren. Damit ist der Transponder nicht mehr verfügbar. Eine konkrete Implementierung ist nicht vorgegeben. Aus Kostengründen wird dies bisher in Software realisiert. Eine Reaktivierung eines Transponders (z.B. durch physischen Kontakt) kann somit nicht ausgeschlossen werden [15].

2.1.5 Klassisch-materielle Aspekte

Transponder und Schreib-/Lesegeräte können materiell beschädigt und zerstört werden. An Transponder können allerdings schadlos hohe elektrische Spannungen angelegt werden, da sie mit einer Isolation ummantelt sind. Die Schaltkreise von Transponder können durch hinreichend energiereiche Strahlung mit verschiedenen physikalischen Me-

chanismen zerstört werden: Bei relativ niedrigen Frequenzen als direkte Sendeleistung in Abhängigkeit von der Sendefrequenz und der Antennenqualität.

Bei hochfrequenter elektromagnetischer Strahlung auf einen RFID-Chip sind die beiden Dimensionen Strahlungsqualität und Strahlungsmenge zu unterscheiden. Bei dieser Betrachtung müssen die Gesetzmäßigkeiten der Quantenphysik berücksichtigt werden [8]. Die Strahlungsqualität macht eine Aussage über die Energie der einzelnen Photonen, aus denen sich die Strahlung zusammensetzt. Die Strahlungsmenge beschreibt entsprechend die Anzahl der einwirkenden Photonen in der betrachteten Beobachtungszeit.

Allerdings tritt nur ein Teil der Photonen in Wechselwirkung mit dem bestrahlten Material (Target). Wie hoch dieser Anteil ist, hängt vom Targetmaterial, seiner Dicke und der Strahlqualität ab. Wechselwirkung meint hier im wesentlichen, welcher Anteil der Energie einer Strahlung im Target verbleibt und damit dort Veränderungen hervorrufen kann.

Bei gegebener Strahlqualität ist ein möglicher Schaden für ein gegebenes Targetmaterial umso höher, je größer die Wechselwirkung ist. Letztlich entscheidend ist die wirksame Energiedosis durch die Strahlungseinwirkung.

Bei gegebenen Strahlungsparametern wird die schädliche Wirkung auf einen Chip umso kleiner sein, je dünner er aufgebaut ist, da die Wechselwirkung mit der Dicke ansteigt. Die Silicon-on-Insulator-Technologie zum Beispiel kommt mit einer sehr dünnen aktiven Halbleiterschicht aus und weist damit - sozusagen als Nebeneffekt - eine hohe inhärente Strahlungstoleranz auf [21].

Andererseits könnte der eigentliche Chip des Transponders von der Strahlung abgeschirmt werden z.B. durch eine Ummantelung. Aus physikalischen Gründen geeignet hierzu sind schwere Elemente. Der Einsatz von Blei käme wegen einer ungünstigen Bauform und der Giftigkeit allerdings nicht in Frage. So wird schon seit langem z.B. Molybdän für die Elektroden auf den Chips eingesetzt und damit die Strahlungstoleranz erhöht.

Das verwendete Halbleitermaterial hat ebenfalls entscheidenden Einfluss auf die Strahlungstoleranz. So wird bei starker Strahlung üblicherweise nicht das für Chips hauptsächlich verwendete Silizium eingesetzt sondern z.B. das wesentlich teurere Gallium-Arsenid. Die Kostenvorteile der RFID-Technologie wären dann allerdings in Frage gestellt. Für die genauere Beschreibung der Wirkung der Strahlung auf biologische Gewebe wurden zusätzlich sogenannte Qualitätsfaktoren definiert [8]: 'Dosisäquivalent'. Es ist zu beachten, dass solche Dosisäquivalente für die Wirkung auf einen Chip nur eine sehr eingeschränkt gültige Aussage liefern. Um eine Vergleichbarkeit zwischen Chip-Belastung und medizinischer Dosis zu erreichen, wird im Folgenden der Dosisäquivalentwert aber auch für nichtbiologische Wirkungen angegeben. Zur Abschätzung möglicher Strahlungsschäden auf einen Chip muss die Wirkung genauer untersucht werden. Abhängig von der Strahlungsqualität wird ionisierende und nicht-ionisierende Wirkung des absorbierten Strahlungsanteils unterschieden [18]. Ionisierende Strahlung erzeugt freie Ladungsträger im Halbleiterkristall und führt primär zu transienten Veränderungen im Chip. Da die Datenspeicherung im Chip häufig auf der Basis von elektrischen Ladungen arbeitet, kann z.B. der Datenwert in einer Speicherzelle verändert werden und daraus ein Fehler resultieren.

Ein auf diese Weise verfälschter Wert ist jedoch nicht durch einen bleibenden Defekt verursacht und kann durch nachfolgendendes Überschreiben der Speicherzelle wieder verändert werden. Beim Einsatz der üblichen fehlererkennenden und fehlerkorrigierenden Maßnahmen kann der Fehler sogar wirkungslos bleiben.

Ionisierende Strahlung kann auch zu bleibenden Veränderungen führen, wenn die eingebrachte Ladung in einer Isolatorstruktur innerhalb des Chips deponiert wird und damit im Betrieb des Chips nicht wieder entfernt werden kann.

Nicht-ionisierende Effekte können Kristallgitterfehler bewirken und damit eine bleibende Veränderung der Materialstruktur. Deshalb führt vor allem die nicht-ionisierende Wirkung zu einer dauerhaften Veränderung der Eigenschaften des betroffenen Halbleiters und kann damit mehr oder weniger gravierende Fehlfunktionen bewirken. Allerdings werden diese bleibenden Wirkungen durch die in der Medizin eingesetzte Strahlung eher selten bewirkt, da diese nur bei hohen Photonen-Energien jenseits 1 MeV hinreichend wahrscheinlich werden.

Allgemein wird in der Literatur von einem Schwellwert für die nachweisbare Wirkung der Strahlung auf einen Halbleiterchip ausgegangen. Oberhalb der Schwelle geht man von einer linearen Skalierung mit der Dosis aus.

Die meisten Untersuchungen machen eine Aussage über die Lebensdauer eines Chips bei sehr hoher Strahlenbelastung während des aktiven Betriebes oder der funktionslosen Lagerung, wie sie z.B. bei einer mehrjährigen Verwendung im Weltraum auftritt. Hierzu wird eine extrem hohe Energiedosis entsprechend einem Dosisäquivalent im Bereich kSv (1000 Sievert) auf den Chip appliziert (z.B. [16]).

Für eine Aussage zur Anwendung im medizini-

schen Umfeld sind diese Untersuchungen aber weniger relevant, da davon ausgegangen werden kann, dass neben dem Transponder auch eine Person der gleichen Strahlung ausgesetzt ist. Die hier auftretenden Dosisäquivalente liegen für eine Untersuchung bei etwa 10 mSv, also etwa 100.000 mal niedriger [9]. Auch bei häufigen Untersuchungen eines Patienten bleiben die akkumulierte Dosisäquivalente während der Nutzungsdauer eines Transponders also sehr weit unter den üblichen Testwerten der Chip-Hersteller. Weiterhin kann davon ausgegangen werden, dass ein für medizinische Aufgaben benutzter Transponder während der Bestrahlung nicht in Betrieb ist. Veränderungen betreffen daher i.w. die gespeicherten Daten oder bleibende Schäden am Chip. Letztere würden zwar einen Datenverlust bedeuten, könnten jedoch in einem entsprechenden Selbsttest bei der erneuten Aktivierung festgestellt werden. Schon Maßnahmen zur Funktionsfehlererkennung im Prozessor und ein geeignetes redunantes Speicherverfahren würde vor Datenverlust schützen. Allerdings bewirken diese bekanntlich einen erheblichen Zusatzaufwand, der im Low-Cost-Bereich und im Massenmarkt entscheidend sein kann.

2.2 Vertraulichkeit

2.2.1 Back-Office-Verschlüsselung

Daten können grundsätzlich schon auf dem Back-Office-System ver- und entschlüsselt und dann auf einem Transponder gespeichert und wieder gelesen werden. Nachteilig ist, dass die Nutzdaten zwar verschlüsselt übertragen werden, nicht aber die Steuerbefehle. So können z.B. Login-Befehle zusammen mit einem Schreibzugriff erlaubenden Passwort abgehört werden.

2.2.2 Verschlüsselung

Symmetrische Verschlüsselung mit dem Data Encryption Standard (DES) oder Triple-DES ist die am häufigsten verwendete Verschlüsselung im RFID-Bereich [3]. Ein vertrauenswürdiges Schlüsselmanagement ist aufwändig.
Für die asymmetrische Verschlüsselung werden Rivest-Shamir-Adleman (RSA) Verfahren und wird Elliptic Curve Cryptography (ECC) verwendet. Mit geringerer Schlüssellänge benötigen Angriffe weniger Ressourcen wie z.B. Rechenzeit.

2.2.3 Silent Tree Walking

Werden die in Transpondern bei der Herstellung gespeicherten Identifikationsnummern (ID) mit Hilfe des Binary-Tree-Algorithmus vom Schreib-/Lesegerät selektiert, ist es einem Angreifer möglich den Lesekanal auch auf größere Entfernung abzuhören und dann ebenfalls die IDs von Transpondern auszulesen. Silent Tree Walking kann dies verhindern [32] und auf den weniger weit reichenden und nur mit erheblichem Aufwand abhörbaren Rückkanal begrenzen [1].

2.2.4 Schutz gegen Abhören

Lesesysteme könnten Transponder mit langen Antwortzeiten oder ungewöhnlichen Signalstärken zurückweisen und generell unberechtigte Zugriffe protokollieren. Ein Wechsel der Frequenz während der Übertragung (Frequency-Hopping) erschwert ein Abhören der Kommunikation.
Zur Vermeidung oder wenigstens Erschweren des Abhörens ist beim Austausch eines Passworts im Klartext die Richtung des Austauschs vom Transponder zum Lesegerät zu wählen, da wegen der geringeren Signalstärke die Reichweite geringer ist, in der ein Angreifer das Signal noch auffangen kann.
Abhören der Kommunikation kann auch durch das Senden von irreführenden Informationen, sogenanntem Chaff, erschwert werden [32]. D.h. nur ein kleiner Teil der gesendeten Befehle und Daten wird vom empfangenden Transponder über einen Filter tatsächlich verarbeitet. Der Rest (Chaff) dient der Verwirrung eines Abhörers. Dadurch erhöht sich das Datenvolumen und die Nutzdaten-Übertragungsrate wird eingeschränkt.

2.3 Integrität

Bei der Übertragung von Daten zwischen Transponder und Schreib-/Lesegerät kann es zu Störungen kommen. Zur Erkennung werden Prüfsummenverfahren wie Paritätsprüfung, Längssummenprüfung und CRC-Prüfung eingesetzt, die sich auf eine Fehlererkennung beschränken und eine erneute Übertragung des fehlerhaften Blocks auslösen. Fehlerkorrigierende Verfahren werden bei RFID-Systemen bisher nicht eingesetzt, da sie die Leistungsfähigkeit der zur Verfügung stehenden Ressourcen übersteigen .
Ein Angreifer kann die Prüfsumme für einen veränderten Datenblock neu berechnen. Ein höheres Sicherheitsniveau kann mit digitalen Signaturen erreicht werden.
Auch gespeicherte Daten sollten auf Integrität überprüft werden.

2.4 Pseudonymität

Ein Aufzeichnen empfangener IDs von RFID-Transpondern oder sogar eine Verknüpfung mit dem Aufenthaltsort und der Aufenthaltszeit des Endverbrauchers (Kunden) ist oftmals unerwünscht. Daher wurden einige Ansätze für Low-Cost-Transponder entwickelt [15], die ein unberechtigtes Verfolgen von Transpondern und das Auslesen von Nutzdaten bzw. das Auslesen der ID verhindern.

2.4.1 Meta-IDs

Durch Anwendung einer mathematischen Funktion - meist eine Hash-Funktion (Einwegfunktion) - auf die ID eines Transponder kann eine Meta-ID gebildet werden. Statt der tatsächlichen ID sendet ein Transponder die Meta-ID. Wechselt diese Meta-ID in kurzen Abständen (bei jedem Leseversuch), so ist ein Verfolgen des Transponders nur eingeschränkt möglich. Bisher existieren nur theoretische Überlegungen zu RFID-Meta-ID-Verfahren.
Ohne die Kenntnis der ID sind Transponder für ein unautorisiertes Lesegerät nicht ansprechbar. Das Lesegerät ist nur in der Lage aus einer Meta-ID, die tatsächliche ID zu gewinnen, wenn es die Funktionen kennt, die vom Transponder zur Erzeugung der Meta-ID benutzt wurden und in der Datenbank des Lesesystems die tatsächliche ID des Transponders gespeichert ist.

2.4.2 Re-Encryption

Um mit einem häufigen, erneuten Verschlüsseln ein unautorisiertes digitales Verfolgen eines Transponders zu verhindern, müssen sowohl ID wie auch alle weiteren ohne Passwort auslesbaren Daten erneut verschlüsselt werden.

2.5 Authentifizierung

Identifizierungs- und Nutzdaten können gefälscht werden. So können Daten gelesen und auf einen beschreibbaren Transponder kopiert werden, der dann den Original-Transponder vortäuscht. Auch von Schreib-/Lesegeräten können Transponder simuliert werden.

2.5.1 Passwörter

Bei Zugriffskontrollsystemen mit Passwort-Verfahren kann ein Schreib-/Lesegerät erst nach der Übermittlung und Überprüfung des Passworts durch den Transponder zugreifen und lesen oder schreiben. Die Länge der Paßworte liegt zwischen 4 Bytes (Hitag) und 6 Bytes (Mifare).
Transponder können sich durch ein zusätzliches Passwort gegenüber Schreib-/Lesegeräten authentifizieren. Brute-Force-Attacken sind genauso möglich wie das Abhören von im Klartext übertragenen Passwörtern.

2.5.2 Challenge-Response-Verfahren zur Authentifizierung

Challenge-Response wird eingesetzt – z.B. bei Digital Signature Transpondern (DST) [29].

2.5.3 Distanzbasierte Zugriffskontrolle

In Abhängigkeit von der Entfernung zwischen Transponder und Schreib-/Lesegerät werden unterschiedlich viele Informationen preisgegeben [6]. Jedoch sind die bisher zur Verfügung stehenden Verfahren zur Distanzermittlung aufwändig und ungenau. Der Widerstandswert dieser Zugriffskontrolle ist als gering einzustufen, wenn ein Angreifer hinreichend nahe an den Transponder herankommen kann.

3 Bewertung des Sicherheitsniveaus

Sicherheitsmechanismen in den Standards sind größtenteils auf einfache CRC-Integritätsprüfungen, Frequency-Hopping, Sperren von Speicherbereichen gegen Überschreibung und eine Implementierung des Kill-Befehls beschränkt. Der so erreichte Widerstandswert ist für viele Anwendungen zu gering. Nur ein Teil der bekannten Sicherheitsmechanismen ist in Protokolle integriert. Daher muß bei höheren Sicherheitsanforderungen auf ein proprietäres Protokoll zurückgegriffen werden oder es muß ein Standard als Übertragungsprotokoll genutzt werden, der von einem – einen widerstandsfähigeren Sicherheitsmechanismus bereitstellenden - anderen Protokoll getunnelt wird.
Im folgenden wird zur Erreichung der Sachziele der Informationssicherheit Vertraulichkeit und Pseudonymität [22] je ein relevanter Mechanismus untersucht und die Verfügbarkeit bewertet.

3.1 Bewertung der Verfügbarkeit

In einer experimentellen Untersuchung wurden mehrere Transponder mehrfach mit exemplarischen Testmustern beschrieben und wiederholt aus einer medizinischen Röntgenquelle bestrahlt. Dabei wurden die Targets direkt in den Strahlenfluss gelegt. Dies führt zu einer Worst-Case-Situation und ist in der realen Anwendung nur im Ausnahmefall zu erwarten. Allerdings bewirkt die durch den Körper bedingte normale Streustrahlung während einer Untersuchung unter Umständen vergleichbar hohe Dosisäquivalente abseits der Direktstrahlung, so dass die Anordnung durchaus realitätsnahe Werte liefert [10]. Die Dosisäquivalente und Strahlqualitäten entsprachen mit einer maximalen Photonen-Energie von 150 keV und einem Dosisäquivalent von jeweils bis zu 10 mSv (vgl. Tabelle 1) den in der Diagnostik üblichen Werten [17]. Als weitere Worst-Case-Annahme wurde auf die übliche Strahlfilterung verzichtet. Dadurch gelangen auch die für die Bremsstrahlung [8] charakteristischen Photonen mit sehr niedriger Energie auf den Chip. Diese haben üblicherweise ein hohes Potenzial für eine ionisierende Wechselwirkung.
Für viele Diagnostik-Anwendungen der Nuklear-Medizin, wie z.B. Positron-Emissions-Tomography (PET) oder Single Photon Emission Computed Tomography (SPECT) ergeben sich in etwa vergleichbare Dosiswerte, die Strahlqualitäten sind allerdings etwas verschieden; sie bleiben aber üblicherweise immer unter 1 MeV. Die sinngemäße Gültigkeit der

Aussage der Untersuchung kann hier also auch angenommen werden.

Bestrahlungs-versuch	Dosisäquivalent
1	1mSv
2	3 x 1mSv = 3mSv
3	5 mSv
4	3 x 5mSv = 15mSv
5	10mSv
6	3 x 10mSv = 30mSv

Tabelle 1: Bei der Bestrahlung von Transpondern eingesetzte Dosisäquivalente

Als Ergebnis der experimentellen Untersuchung zeigte sich, dass alle Transponder auch nach wiederholten Bestrahlungen noch fehlerfrei arbeiteten. Es traten auch keine Fehler bei den gespeicherten Daten auf. Damit kann eine unbemerkte und gezielte Manipulation eines Transponders mittels Röntgenstrahlung praktisch ausgeschlossen werden. Extrem hohe Dosiswerte könnten zwar zur Zerstörung führen. Aber solche Dosiswerte wären bedingt durch die begrenzte Leistung der Generatoren auch nur über einen längeren Zeitraum verabreichbar.

3.2 Simulation des Passwortmechanismus

Brute-Force-Angriffe wurden unter Einsatz einer proprietären Funktionsbibliothek für Schreib-/Lesegeräte [33] simuliert. Ausgewählt wurde der Transponder Hitag2 [2], der ein max. 4 Bytes langes Passwort besitzt und mit 52 ms eine vergleichsweise kurze Antwortzeit zur Verifizierung eines erfolgreichen Logins; damit sind ca. 19,2 Logins pro Sekunde möglich.

Der Brute-Force-Angriff wurde in drei verschiedenen Versionen simuliert:

1. Lexikonattacke,
2. Angriff mit allen Zeichenkombinationen eines eingeschränkten Alphabets,
3. Angriff mit allen möglichen Kombinationen.

Der Angriff mit allen möglichen Kombinationen führt jedenfalls zum Erfolg – allerdings wg. der Transponder-Antwortzeit erst nach langer Zeit. Unter der Einschränkung auf Zeichen des deutschen Alphabets und Ziffern wird der Suchbereich erheblich eingeschränkt und die Suchzeit begrenzt; dies gilt erst recht für die Lexikonattacke.

Für die Lexikonattacke wurden geeignete Wörterbuchlisten eingesetzt: Eine aus häufigen Wörtern, Namen und Passwörtern aus insgesamt acht Zeichen aufgebaute englische Wortliste [20], aus der alle mehr als vier Zeichen langen Wörter herausgefiltert wurden [11] und es wurden dieselben Wörter mit großen Buchstaben, sowie kleinen Buchstaben aber mit großem Anfangsbuchstaben ergänzt. Um die Trefferwahrscheinlichkeit für im deutschsprachigen Raum eingesetzten Transponder zu erhöhen, wurde die Liste um einen deutschen Anteil mit Hilfe einer Wortliste aus den 10.000 am häufigsten gebrauchten deutschen Wörtern erweitert [30]. Eine analoge Bearbeitung wie bei der englischen Liste beschrieben, führt zu einer deutschen Wortliste, die der Gesamtliste hinzugefügt wird. Insgesamt umfaßte die erstellte Liste 21.587 Wörter.

Im Simulationsprogramm wurden neben der Lexikonattacke Angriffe mit eingeschränktem Alphabet und Angriffe mit allen Zeichenkombinationen implementiert. Die Alphabete bestanden aus Groß- und Kleinbuchstaben sowie Ziffern.

In Abhängigkeit vom benutzten Alphabet und der Paßwortlänge ergeben sich die in der Tabelle 2 genannten Gesamtzeiten für Brute-Force-Angriffe auf das vierstellige Passwort eines Hitag2-Transponders. Die benötigten Zugriffszeiten liegen um etwa 27 % über den errechneten Werten wegen des Programm-Overheads im Schreib-/Lesegerät und Transponder.

Test	Errechnete Zeit	Benötigte Zeit[1]
Wortliste	18,4 Min.	25,4 Min.
Großbuchstaben	6,6 Stdn.	8,5 Stdn.
Buchstaben	4,4 Tage	5,6 Tage
Buchstaben und Zahlen	8,9 Tage	11,4 Tage
Alle Zeichen	7,1 Jahre	9,1 Jahre

Tabelle 2: Zeitaufwand für Brute-Force-Angriffe auf vier Zeichen lange Passwörter

Die Tests zeigen, dass 4-Bytes lange Passworte bei derzeit üblichen Antwortzeiten von Transpondern unsicher sein können. So sind Lexikonattacken in 25 Minuten möglich.

3.3 Anwendbarkeit von Meta-ID-Pseudymisierungsverfahren

Eine Simulation ist auf derzeit erhältlichen Transpondern nicht möglich, da die Funktion der Antwort auf einen Request-Befehl nicht veränderbar ist und daher immer mit der ID beantwortet wird. Das Simulationsprogramm wurde in Java erstellt, da das - für die zu Simulation gut geeignete - Prinzip von Klassenobjekten gut unterstützt wird.

Für die Simulation von Meta-ID-Verfahren wurden zwei einfache Verfahren eingesetzt - das Randomized-Hash-Lock-Verfahren [32] und das Chained-Hashes-Verfahren [19]. Die eingesetzten Hash-

[1] Auf der Grundlage von Messungen hochgerechnete Werte.

Funktionen zur Erzeugung der Meta-ID sind einfach und damit für Ressourcen-begrenzte Transponder im Low-Cost-Bereich geeignet - können daher allerdings auch nicht kryptographische Robustheit, Repräsentativität und Kollisionsfreiheit in einem hohen Grade garantieren.
Die erstellten Simulationen bestehen jeweils aus den drei Klassen Transponder, Reader und Graphical User Interface (GUI). In den Klassen Transponder und Reader werden Methoden bereitgestellt, die die Funktionen der Transponder und Schreib-/Lesegeräte simulieren.
Ein Engpass kann die Anzahl der in einer Datenbank gespeicherten Transponder-IDs sein, weil durch das Errechnen der ID keine Verzögerungen entstehen sollen; bei einer Erfassungsgeschwindigkeit von 35 Transponder pro Sekunde sollte die ID in maximal 28 ms berechnet werden [26]. Wie man durch die in Tabelle 3 dargestellten Messungen erkennen kann, läge bei der Randomized-Hash-Locks-Simulation mit dem verwendeten System die maximale Anzahl der Datensätze in einer ID-Datenbank, mit denen ein Betrieb ohne Verzögerung möglich ist, bei etwa 1500 IDs.

Anzahl IDs	Zeit in ms
500	1
750	2
1000	8
1500	23
2000	32
3000	57

Tabelle 3: Benötigte Zeit für eine ID-Berechnung in Abhängigkeit von der Anzahl der Transponder in einer Datenbank

Schnellere als das für die Verwaltung der Datenbank verwendete Rechensystem[2] und optimierte Algorithmen können die Anzahl verarbeiteter IDs um ein Vielfaches nach oben verschieben. Auch schneller erfassbare Transponder, z.B. die I-Code EPC (200 erfasste Transponder pro Sek.) [24], ermöglichen eine größere Anzahl.
Je kürzer die Erkennungszeit für einen Transponder, desto weniger Zeit steht auch zur Zuordnung zur Verfügung; dies führt zu einer geringeren maximal möglichen Anzahl von IDs in der Datenbank: Die Anzahl der in Echtzeit zuordenbaren IDs sinkt mit schnelleren Transpondern.
Für das Chained-Hashes-Verfahren sind beim ersten Request-Befehl aufgrund der vergleichbaren Komplexität der Berechnungen ähnliche Werte zu erwarten. Bei weiteren Request-Befehlen steigt die Laufzeit linear mit der Anzahl der bereits erfolgten Request-Befehle an.
Bei jeder neuen Meta-ID-Bildung wird die Hash-Funktion auf die alte Meta-ID angewendet. So müssen mehrfache (verkettete) Rechnungen ausgeführt werden.

[2] AMD Athlon XP 2000+ CPU, 512 MB RAM (266 MHz)

4 Zusammenfassende Bewertung

4.1 Bewertung der Verfügbarkeit

Eine unbemerkte und gezielte Manipulation eines Transponders mittels Röntgenstrahlung kann praktisch ausgeschlossen werden. Real auftretende Strahlenbelastungen in medizinischen Anwendungen bergen nur eine sehr geringe Wahrscheinlichkeit von Daten- und Funktionsfehlern.

4.2 Widerstandswert des Passwortschutzes

Die durchgeführten Tests haben gezeigt, dass 4 Byte lange Passworte bei derzeit üblichen Antwortzeiten von Transpondern unsicher sein können. Erst die nicht sinntragende Kombination von Zeichen des gesamten Alphabets (große und kleine Buchstaben, Ziffern und Sonderzeichen) führt zu einem Sicherheitsniveau mit einem Widerstandswert von mehreren Tagen.
Es ist zu erwarten, dass zukünftige Transponder über kürzere Antwortzeiten verfügen, so dass sich die Zeiten für einen erfolgreichen Angriff linear reduzieren werden. Die kürzeren Antwortzeiten verringern den Widerstandswert jedoch nur leicht. Die Passwortlänge beeinflusst den Widerstandswert dagegen stark (exponentiell).
Zur Widerstandswerterhöhung können Transponder so modifiziert werden, dass nur eine geringe Anzahl an Logins pro Zeiteinheit zugelassen wird. Dazu müßte auf dem Transponder ein Timer installiert werden – dies würde allerdings zu einem erhöhten Energieverbrauch führen. Für Transponder mit max. 4 Byte langen Passwörtern könnte die Benutzeroberfläche zur Passworteingabe kurze bzw. unsichere Passwörter ablehnen.

4.3 Meta-ID-Pseudonymisierung

Die Simulationen zeigen, wie eine konkrete Implementierung der Modelle aussehen kann und dass die theoretischen Modelle in der Praxis funktionieren. Zusätzlich haben die Messungen gezeigt, von welcher Größenordnung der Anzahl von Transpondern bei einem System ausgegangen werden kann. Das Ergebnis zeigt, dass auf Hash-Funktionen basierende Meta-ID-Verfahren nur in einem System mit beschränkter Anzahl bekannter IDs praktikabel sind. Ist die Zahl der bekannten IDs zu groß, dauert

die Erfassung der Transponder zu lange.
Auf Hash-Funktionen basierende Meta-ID-Verfahren können nur in einem System mit beschränkter Anzahl bekannter IDs bearbeitet werden können: Die Werte in Tabelle 3 zeigen, dass bei angenommenen 28 ms Erfassungszeit die Anzahl unter den in Kap. 3.3. genannten Voraussetzungen bei etwa 1500 liegt. So hat jedes RFID-System je nach Erkennungsgeschwindigkeit, Rechenleistung und verwendetem Meta-ID-Verfahren eine spezifische maximale Anzahl von IDs, mit denen noch eine Zuordnung möglich ist.
Beispielsweise würde die Erfassung der Waren eines großen Supermarktes (mit mehr als 1500 Waren) per RFID an der Kasse zu lange dauern.
Als mögliches Einsatzgebiet kommt eher der Privatbereich in Betracht. Hier kann davon ausgegangen werden, dass wenige Transponder-bestückte Artikel vorhanden sind. Die Transponder könnten z.B. so produziert werden, dass der Verbraucher sie nach dem Kauf auf Meta-ID-Modus umschalten kann und somit nur noch seinem eigenen RFID-System ermöglicht, auf diese zuzugreifen.

5 Zukünftige Untersuchungen

Die hier vorgestellten Messungen zur Verfügbarkeit sollen vertieft werden. Verschiedene Transpondertypen sollen mit verschiedenen Schreib-/Lesegeräten hinsichtlich der Reichweite und Erkennungssicherheit getestet werden. Zu untersuchen ist dabei auch die Abhängigkeit der Lage eines Transponders zum Empfänger und die Störempfindlichkeit auf Objekte im Übertragungsweg (elektromagnetische Störungen). Sobald Blockertags verfügbar sind, sollen sie bewertet werden.
Implementierungen des Kill-Befehls sind bisher dem Hersteller überlassen. Hier sind Untersuchungen zum Widerstandwert der Implementierungen wünschenswert: Wie aufwändig ist eine Kommando-gesteuerte oder physische Manipulation, um den Transponder wieder funktionsbereit zu machen.
Weiterhin sollen die Sicherheitsfunktionen in jüngster Zeit veröffentlichter Protokolle bewertet werden und es soll das Sicherheitsniveau vorgeschlagener Verschlüsselungsalgorithmen für Ressourcen-begrenzte Transponder bewertet werden.

6 Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (Ed.): Risiken und Chancen des Einsatzes von RFID-Systemen, Bonn 2004 http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf

[2] Electronic Hardware AG (ed.): EHAG 125 kHz Multitag Reader Module ME-H10101xx, 4.9.04, Oetwil 2004 http://www.ehag.ch/prod/rfidicrongines/ata_flyer/EHAG-Multitag125V12b.pdf

[3] Engberg, S. J.: Towards Trustworty RFID Security and Privacy by design. In: EU (Ed.): RFID Consultation. Workshop on RFID Security, Data Protection & Privacy, Health and Safety Issues. Brussels 2006 http://www. rfidconsultation.eu/ cs/ficheiros/Stephan_J_Engberg.pdf

[4] EPCglobal Inc. (Ed.): Electronic Product Code (EPC) Version 1.0 Specifications. Lawrenceville 2002 – 2004 http://www.epcglobalinc.org/ tandards_technology/ specifications.html

[5] Finkenzeller, K.: RFID-Handbuch. München 2002

[6] Fishkin K.P., Roy, S.: Enhancing RFID Privacy via Antenna Energy Analysis, Boston 2003 http://www.rfidprivacy.org/papers/fishkin.pdf

[7] Flörkemeier, C.: Die Technologiestandards des Auto-ID Centers, Zürich 2004 http://www.vs.inf.ethz.ch/publ/ papers/floerkem-autoid-2004.pdf

[8] Gerthsen, C.; Meschede, D.: Physik. Berlin 2003

[9] Hänscheid, H.; Scheubeck, M.; Laßmann, M.; Seybold, S.; Reiners, C.: Kursus der Nuklearmedizin. Würzburg 1997http://www.uni-wuerzburg.de/nuklearmedizin/ kursus/Kursus.htm

[10] Hsieh, J.: Computed Tomography: Principles, Design, Artifacts, and Recent Advances. New York 2003

[11] IDM Computer Solutions (ed.): UltraEdit-32 9 Hamilton 2006 http://www.ultraedit.com

[12] Infineon Technologies (ed.): New RFID Chips from Infineon Read 500 Smart Labels Simultaneously, München 2003 http://www.infineon.com/cgi/ecrm.dll/ jsp/showfrontend.do?lang=EN&news_nav_oid=-9979&content_type=NEWS&content_oid=94777

[13] Juels, A.: Minimalist Cryptography for Low-Cost RFID Tags, San Francisco 2003 http://www.rsasecurity.com/rsalabs/staff/bios/ ajuels/publications/minimalist/ Minimalist.pdf

[14] Knospe, H.; Pohl, H.: RFID Security. Information Security Technical Report: 9, 4, 39 - 50, 2004 http://www.securitywireless.info/upload/dl/Rfid/RFID_Security_ISTR.pdf

[15] Langheinrich, M.: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, Zürich 2004 http://www.vs.inf.ethz.ch/publ/papers/ langhein2004rfid.pdf

[16] Manghisonic, M.: Radiation Tolerance of a 0.18 µm CMOS Process. 7th International Conference on Advanced Technology and Particle Physics, Como 2001

[17] Morneburg, H. (Ed.): Bildgebende Systeme für die medizinische Diagnostik. München 1995

[18] N.N.: Predicting Displacement Damage Effects in Electronic Components by Method of Simulation-

Study Report https://escies.org/public/radiation/ esa/database/ niel-1.pdf Köln 2002

[19] Ohkubo, M.; Suzuki, K.; Kinoshita, S.: Cryptographic Approach to „Privacy-Friendly“ Tags, Yokosuka (JPN) 2003 www.rfidprivacy.org/papers/ohkubo.pdf

[20] Outpost9.com's Lab (Ed.): Wordlist, o.O. 2004 http://www.outpost9.com/files/wordlists/d8.zip

[21] Parke, S.: Comparison of existing & proposed SOI MOSFET device structures for minimizing total dose radiation. IEEE Aerospace Conference Proceedings, 2004

[22] Pohl, H.: Taxonomie und Modellbildung in der Informationssicherheit. Datenschutz und Datensicherung 28, 11, 678 - 685, 2004 http://www.inf.fh-bonn-rhein-sieg.de/data/ informatik_/fb_informatik/ personen/pohl/Aufsaetze/ Taxonomie_und_Modellbildung_in_der_ Informationssicherheit.pdf

[23] Roth, T.: Informationssicherheit von RFID-Transpondern am Beispiel von Meta-ID-Pseudonymisierungsverfahren und Passwortschutz. Diplomarbeit Sankt Augustin 2004

[24] Royal Philips Electronics (ed.): Philips erweitert RFID-Chip-Portfolio für weltweite Supply-Chain-Management-Applikationen. Eindhoven 2003 http://de.semiconductors. philips.com/news/content/file_987.html

[25] Royal Philips Electronics (ed.): Philips' Smart Label and Tag Ics. Eindhoven 2004 http://www.semiconductors.philips.com/acrobat/other/identification/label_tag_ics_linesheet.pdf

[26] Shinde, S.: Funkender Frischkäse, Hannover 2003 http://www.tebiko.de/t/s/rfid.htm

[27] Stoica, A.; Arslan, T.; Keymeulen, D.; Duong, V.; Zebulum, R.; Ferguson, I.; Daud, T.: Evolutionary recovery from radiation induced faults on reconfigurable devices. 2004 IEEE Aerospace Conference Proceedings 2004

[28] Sze, S. M.: Semiconductor Devices - Physics and Technology. New York 2002

[29] Texas Instruments Inc. (ed.):Digital Signature Transponder. Dallas 2001, http://www.ti.com/ tiris/docs/ products/transponders/RI-TRP-BRHP.shtml

[30] Universität Leipzig, Institut für Informatik(ed.): Projekt Deutscher Wortschatz. Top10000. Leipzig 2001 http://aspra9.informatik.uni-leipzig.de/Papers/top10000 en.txt

[31] US Food and Drug Administration (ed.): Guidance for Industry and FDA Staff. Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information. Washington 2004 http://www.fda.gov/cdrh/ode/guidance/1541.html

[32] Weis, S. A.; Sarma, S. E.; Rivest, R. L.; Engels, D. W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter et al. (Eds.): Security in Pervasive Computing. LNCS 2802. 201 – 212, 2004 http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf

[33] Zeitcontrol Cardsystems GmbH (ed.): KnowHow, o.O. 2004 http://www.transponder.de

---

[1] Die Arbeiten sind im Rahmen des Forschungsschwerpunkts NEGSIT – Next Generation Services in Heterogenous Network Infrastructure entstanden.

[2] Die Autoren danken der Fa. Atmel GmbH, Heilbronn ganz herzlich für die Überlassung von Mikroprozessoren und Transpondern, ohne die die Arbeiten nicht möglich gewesen wären.

[3] Herrn N. Conrads, Philips Research, Aachen danken die Autoren herzlich für die Durchführung der Röntgen-Experimente.