

Kontaktlose Smartcards Angriffe und Gegenmaßnahmen

Hendrik Dettmer

1. Februar 2007

1 Einführung und Geschichte

Kontaktlose Smartcards sind eine Verbindung von RFID Chips und Smartcards, die in Kreditkarten, Reisepässen oder Ähnlichem eingelassen sind. RFID steht für Radio Frequency Identification und beschreibt damit Karten, die berührungslos eine Identifizierung oder mehr senden können. Die eigentliche Smartcard ist eine Identifikationskarte, die einen eingebauten Schaltkreis hat.

Geschichtlich gesehen gibt es die Idee schon seit dem zweiten Weltkrieg. Durch die Erfindung des Radars und des Funkverkehrs fingen die Alliierten an erste Freund-Feind-Erfassungssysteme für Flugzeuge zu entwickeln und einzusetzen, um so die Abschüsse durch die eigenen Truppen zu minimieren. Durch weitere Radarinstallationen wurden so genannte Transponder, die in Flugzeuge und Bodentruppen eingebaut wurden, abgefragt und die Standpunkte der Einheiten konnten so festgestellt werden. Auch schon in diesen Anfangsjahren der kontaktlosen Identifizierung wurden Methoden von den Gegnern entwickelt, um diese Systeme auszuschalten oder sie für sich zu nutzen. So wurden Transponder aus abgeschossenen englischen Flugzeugen ausgebaut und in deutsche Maschinen eingebaut, um die Erfassungssysteme zu täuschen. Die weiterentwickelten Systeme, die nicht mehr so anfällig gegen einfache Attacken sind, werden auch heute im Militär eingesetzt [1].

Erst nach dem Krieg wurde die kontaktlose Identifikation auch in der freien Wirtschaft eingesetzt, um Bauteile eindeutig zu identifizieren. Diese Systeme wurden in der Produktion eingesetzt und konnten durch ihre Größe zunächst nur bei großen Produktionsteilen (z.B. Eisenbahnwaggons) verwendet werden. Die eingebauten Hohlraumresonatoren konnten durch Schrauben so eingestellt werden, dass sich eine eindeutige "ID" ergab. Diese Technik mag in der Produktion von Autos oder anderen großen Teilen noch einsetzbar sein, jedoch ist sie für kleinere Teile nicht zu realisieren.

Um 1975 wurden elektronische Warensysteme eingeführt. Mit diesen Systemen konnte man auch kleinere Teile bestücken und so zum Beispiel vor Diebstahl schützen. Da die Transponder jedoch nur 2 Zustände darstellen konnten (vorhanden/fehlt) waren kompliziertere Aufgaben (z.B. Zahlungsverkehr) nicht denkbar für diese Technik. Diese Systeme werden mit zwei



Abbildung 1: Der ePass - eine kontaktlose Smartcard

Möglichkeiten betrieben, nämlich einem induktiven Nahfeld, das magnetisch erzeugt wird oder einem elektromagnetisch erzeugten Fernfeld (Mikrowellentechnik).

Ab den 80ern kamen vollwertige RFID-Systeme auf den Markt. Diese konnte man nun auch für Mautstellen, Skipässe, und viele Dinge mehr einsetzen. Im Jahre 1999 begann am MIT die Entwicklung eines globalen Standards zur Warenidentifikation. Es wurde der Elektronische Produktcode (EPC) erarbeitet, der eine weltweite eindeutige Kennzeichnung von Objekten ermöglicht. Dieser Produktcode wird nun von der EPCglobal, einem Non-Profit-Unternehmen, verwaltet und gefördert. Dies war der Anfang einer Welle von RFID-Applikationen, eine Welle die sich noch im Aufbau befindet und viele Authentifizierungs- und Bezahlmechanismen ablösen wird. Die aktuellsten Chips haben eine Von-Neumann-Architektur und besitzen

einen Mikrocontroller. So bietet Philips ein Tag namens SmartMX, welches 72 KByte Speicher besitzt, eine Datenrate bis zu 848 KBit/s unterstützt und einen Krypto-Co-Prozessor besitzt. Diese Chips sind nun wirklich kontaktlose Smartcards, da sie einen richtigen Mikrocontroller haben und kryptographisch Protokolle unterstützen [1].

2 Das RFID System

Ein RFID-System besteht im Wesentlichen aus einem Lesegerät (Reader) und einem Transponder auf dem die Daten gespeichert werden (Tag).

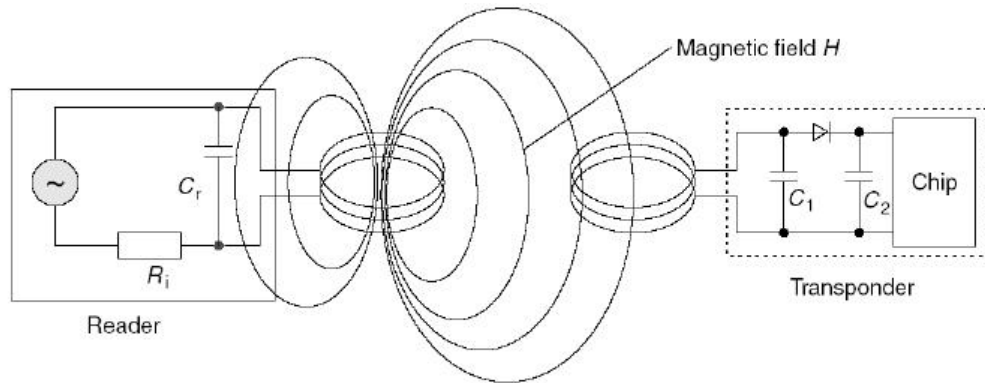


Abbildung 2: Ein grundlegendes RFID System

Es gibt zwei große Gruppen von RFID-Tags. Einmal solche, die in Industriebetrieben eingesetzt werden und dort eine höhere Reichweite erzielen müssen, um zum Beispiel Lagerräume überwachen zu können. Dort sind große Massen von RFID-Chips im Einsatz. Normalerweise hat Sicherheit nicht die oberste Priorität, da jeder Chip nur seine eindeutige Identifikationsnummer (z.B. eine Global Trade Item Number (GLN) oder eine European Article Number (EAN)) schicken soll. Die weiteren Arbeiten werden von einem Datenbanksystem (Back-End) übernommen, um die Lagerverwaltung zu übernehmen. Der Preis ist oft das wichtigste Kriterium beim Aufbau einer RFID-Lösung für ein Unternehmen. Lagerbestände müssen schnell und präzise ausgelesen werden können. Die Meisten dieser eingesetzten Systeme besitzen zu wenig Leistung, um kryptografische Protokolle nutzen zu können. Natürlich gibt es auch Industriezweige, in denen auf Sicherheit Acht gegeben wird. Die Lösungen, die dort eingesetzt werden, sind die Gleichen wie bei Nahbereichschips. Die Nahbereichschips werden für die bekannten Aufgabenbereiche eingesetzt, wie z.B. Reisepässe, Zutrittskontrollen oder auch auf unserem Studierendenausweis, mit dem man auch bezahlen kann. Diese Chips funktionieren meistens bis zu einer Entfernung von einigen Zentimetern vom Lesegerät. Nur wenige Nahbereichschips sind aktive Chips, die eine eigene Stromquelle (z.B.

eine Batterie) auf ihrer Karte benötigen. Diese Chips sind meist zu teuer und auch zu groß für normale Anwendungen.

Passive Chips werden dagegen oft eingesetzt. Sie beziehen ihre Energie normalerweise aus einem magnetischem Feld und speichern sie in einem Kondensator zwischen, um so eine relativ konstante Stromquelle zu haben. Nur so können sie den Datenstrom des Lesegerätes überhaupt empfangen. Meistens wird auf den Speicher zugegriffen, den der Chip mitbringt (bis zu mehreren Kilo Bytes), um Daten entweder zu lesen oder zu schreiben.

Diese Nahbereichschips arbeiten meistens nach dem ISO Standard 14443A oder 14443B und somit auf einer Frequenz von 13,56 MHz(Hochfrequenz). Die anderen Standards für diese Frequenz sind der ISO 15693 und der ISO 18000, wobei auch andere Frequenzen benutzt werden.

Die Niedrigfrequenzen (zwischen 125 und 134 kHz) bieten einen kurzen Leseabstand (ähnlich den 13,56 MHz Chips) und erreichen nur eine geringe Datenübertragungsrate. Sie werden über den ISO Standard 11784/85 und 14223 abgedeckt.

Die Ultrahochfrequenz-Chips haben eine hohe Datenübertragungsrate und benutzen die Frequenzen 868 MHz und 915 MHz. Ihr Leseabstand beträgt bis zu 4 Meter. Sie müssen jedoch teilweise vor der Übertragung richtig positioniert werden, damit man sie auslesen kann.

Wenn ein Tag in die Nähe eines Readers kommt wird es durch die Energie, die das Tag nun aufnehmen kann, eingeschaltet. Der Reader sendet immer ein elektromagnetisches Feld aus, das genügend Leistung für die Tags liefert. In einem gewissen Intervall schickt der Reader eine Anfrage, um zu prüfen ob Tags in seine Nähe gekommen sind.

Die Kommunikation von der Seite des Readers wird mit dem modifizierten Miller Code zum Tag gesendet. Das bedeutet, dass der Reader Pausen in das Energiefeld einbaut, um die Informationen in diesem Energiefeld zu übertragen. Das Tag kann Energie über kurze Zeitabstände speichern, so dass es während der Pausen weiter arbeiten kann. Wenn dies nicht so wäre würden die Pausen das Tag jedesmal in den stromlosen Zustand bringen und damit einen Reset ausführen.

Das Tag antwortet mit einer Lastmodulation, für die es zwei Frequenzbänder nutzt, oberhalb und unterhalb (± 847 kHz) der 13,56 MHz. Hier wird mit der Manchester-Codierung gearbeitet und die Informationen durch eine Veränderung des Pegels codiert. Prinzipiell funktioniert das Verfahren der Lastmodulation wie bei einem Transformator. Durch Veränderungen des Stroms der sekundären Spule (Tag) wird auch der Strom in der primären Spule (Rea-

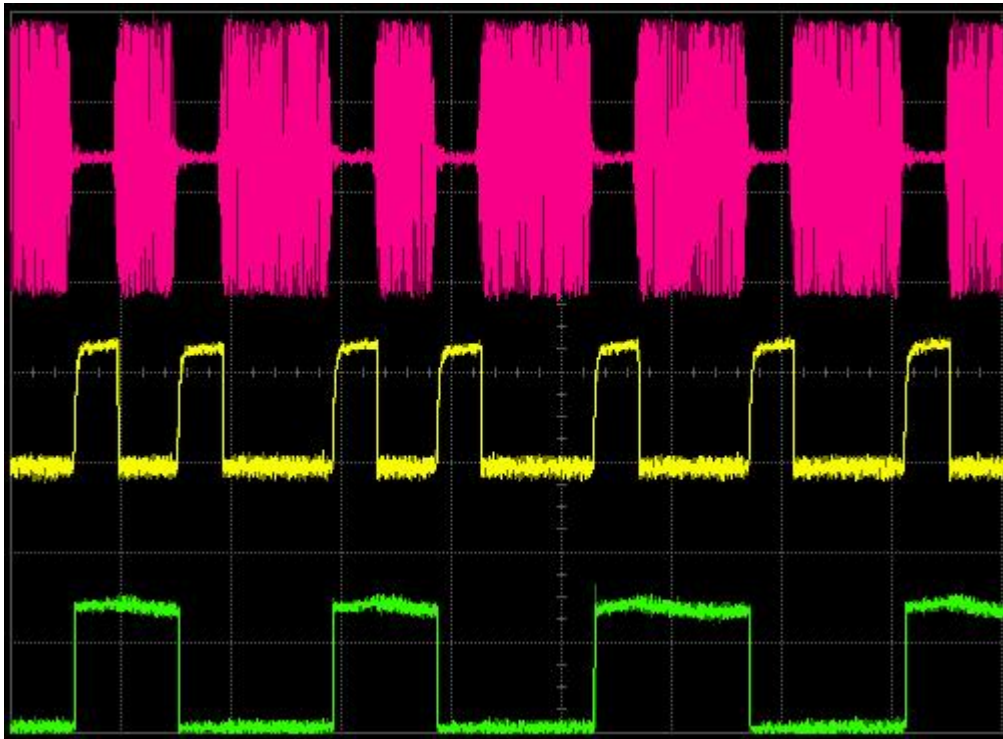


Abbildung 3: **Modifizierter Miller code**

- Oben das Feld des Readers (rot)
- Mitte ein Millercode aus Pulsen (gelb)
- Unten ein Millercode (grün)

der) verändert. Diese Veränderungen kann der Reader feststellen und so die Antwort des Tags empfangen. So wird eine Datenübertragungsrate von wenigstens 106 kBit/s erreicht [2].

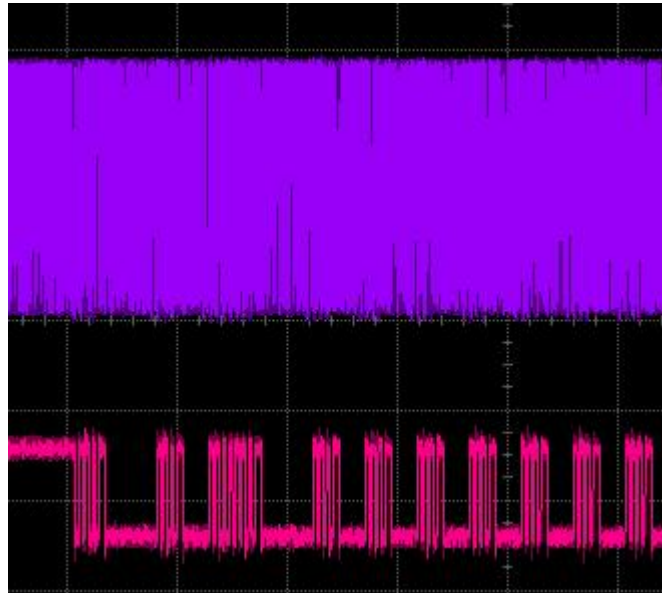


Abbildung 4: **Manchester code**

→ Oben das Feld des Readers (blau)

→ Unten die Signale, die das Tag sendet (rot)

3 Angriffsarten

Hier werden die bekannten Angriffsarten aufgelistet. Die Liste wurde aus [3] übernommen und erweitert. Dies ist ein Überblick über die möglichen Angriffe, im nächsten Kapitel werden deren Ausführungen besprochen.

3.1 Inhalt des Tags fälschen

Durch einen Schreibzugriff werden die Daten auf einem Tag verändert. Die wichtigen Daten (ID und Schlüssel) des Tags bleiben jedoch unverändert. So wird das Tag von einem Reader noch als “echt” erkannt, die Daten sind jedoch nicht mehr die Originalinformationen. Natürlich müssen auf dem Tag auch Daten gespeichert worden sein. Wenn man sich z.B. nur mit seiner ID identifiziert, sonst jedoch nichts auf dem Tag steht funktioniert dieser Angriff nicht.

Es gibt auch die theoretische Möglichkeit RFID-Tags mit einem Virus zu infizieren. So könnte man den Reader dazu bringen weitere Tags zu infizieren

oder eine Buffer-Overflow-Attacke auf das Back-End durchzuführen.

3.2 Tag klonen

Der Angreifer stellt mit Hilfe der wichtigen Daten eines Tags, der ID und eventueller Schlüssel, neue Tags mit den gleichen Attributen her (Cloning). Bei manchen schlecht gesicherten Systemen kann man sogar ohne die wichtigen Daten ein Tag klonen. So sind viele Tags mit der gleichen Identität im Umlauf.

Die Cloning Attacke funktioniert sogar bei vielen E-Pässen, so kann der Angreifer sich als eine andere Person ausgeben. Nur durch Signaturen und Hash-funktionen kann verhindert werden, dass der Angreifer die Daten auch noch verändern könnte [6].

3.3 Deaktivieren

Der Angreifer schafft es mit Kill- oder Löschbefehlen auf das Tag zuzugreifen und es zu deaktivieren. Diese Befehle sind meistens passwortgeschützt. In einfachen und alten Versionen können Tags Passwörter für diese Befehle haben, die nur 8 Bit lang sind. In aktuellen Versionen der Tags sind die Passwörter mindestens 32 Bit lang.

Das Tag kann auch mit einfachen physischen Mitteln zerstört werden. So kann ein Reader das Tag und die Identität des Trägers nicht mehr feststellen.

3.4 Ablösen

Ein Angriff, der nur darauf beruht, dass man das Tag von seinem Trägerobjekt entfernt und es auf einem anderen Objekt befestigt. Sozusagen wie ein "Umkleben" von Preisschildern.

3.5 Abhören

Der Angreifer hört den Luftkanal zwischen dem Tag und dem Reader mit einem selbst gebauten oder gekauften "Sniffer" ab [7]. So kann er auf dem Kanal die Kommunikation belauschen (Eavesdropping) und die Informationen, die er empfängt, auswerten. Dies ist eine wirkliche Bedrohung für kontaktlose Smartcards, da man den Luftkanal schlecht abschirmen kann. Außerdem

sind “Sniffer” so klein, dass man sie verstecken kann und so diesen Angriff schlecht bemerkt.

3.6 Relay

Die Kommunikation kann nicht nur mit einem “Sniffer” mitgehört werden, sondern auch über eine Kombination aus Sniffer und Reader weitergeleitet werden (relay). So werden alle Informationen in Echtzeit zwischen dem Reader und dem Tag über die Station des Angreifers gelenkt und können dort mitgeschnitten werden. Man kann sie sogar während der Übertragung verändern.

3.7 Replay

Auch diese Attacke baut auf das Abhören des Kanals auf. Wenn der Angreifer eine Kommunikation auf dem Luftkanal abgehört hat speichert er diese ab. Nun kann er sich gegenüber dem Reader als Tag oder gegenüber dem Tag als Reader ausgeben, indem er die aufgezeichnete Kommunikation wieder abspielt. Mit Challenge und Response Protokollen kann man diese Attacke verhindern.

3.8 Blocken

Ähnlich dem Cloning werden viele Blocker-Tags hergestellt. Diese müssen das verwendete Antikollisionsprotokoll des ISO-Standards unterstützen. Dann werden die Blocker-Tags in die Nähe des Readers gebracht und blockieren so mit ihrer großen Anzahl alle Kanäle für normale Tags. Natürlich gibt es auch Blocker-Tags, die immer wieder ihre ID ändern um so alle Anfragen des Readers zu beantworten. Diese aktiven Tags sind jedoch komplizierter und teurer und funktionieren nur mit einem bestimmtem Antikollisionsprotokoll.

3.9 Stören

Der Datenaustausch zwischen Sender und Empfänger kann durch passive oder aktive (z.B. Störsender) Maßnahmen gestört werden. Da es keine große

Robustheit bei der Übertragung gibt, kann sie schon mit einfachen passiven Mitteln gestört werden, zum Beispiel durch Alufolie, mit der man einen Faradayschen Käfig um den RFID-Chip aufbaut.

3.10 Verfolgen eines Tag

Es ist auch möglich ein Tag mit einer eindeutigen Kennzeichnung zu verfolgen. So kann man automatisch die Bewegung des Trägers mitverfolgen, wenn es sich bei dem Tag zum Beispiel um ein wichtiges Dokument wie den ePass handelt. So kann ein Angreifer kontaktlose Smartcards missbrauchen, um mehr Daten über den Träger zu gewinnen. Außerdem ist mit den richtigen Mitteln die Überwachung einer sehr großen Gruppe von Menschen möglich.

3.11 Identität fälschen (Reader)

Der Angreifer täuscht mit seinem Reader vor, dass er autorisiert ist Tags zu lesen, damit er an die Daten auf den Tags kommen kann. Es kommt auf die Realisierung des RFID-Systems an um einzuschätzen zu können, wie schwer dieser Angriff wirklich ist. Oft muss auf das Back-End-System zugegriffen werden damit man an die Daten kommen kann, die es dem Reader ermöglichen sich vor einer Karte zu authentifizieren.

Natürlich kann man nicht nur den Reader und das Tag angreifen sondern auch direkt das Back-End-System, in dem normalerweise die meisten Daten gespeichert sind. So kann man zum Beispiel bei Bezahlssystemen direkt auf die Schattenkonten zugreifen und so das System aushebeln. Solche Angriffe sind Attacks auf Computernetzwerke oder einzelne Rechner. Diese Attacks fallen in die Kategorien der Netzwerk- oder Betriebssystem-Sicherheit und haben somit nicht mehr direkt etwas mit dem Thema kontaktlose Smartcards zutun. Jedoch sind Angriffe von Smartcards auf Netzwerke oder umgekehrt denkbar und möglich.

4 Ausführung von Attacken

1. Der Angreifer kann die Kommunikation zwischen Tags und Reader abhören, indem er ein Abhörgerät (Sniffer) in die Nähe des eigentlichen Readers bringt. Mit bestimmten Techniken kann man die Reichweite, in der man standardmäßige Tags auslesen kann, stark erhöhen. Hancke hat gezeigt, dass man die Kommunikation zwischen Reader und Tag aus 4 Metern Entfernung empfangen kann. Sicherlich sind mit besseren Geräten auch höhere Reichweiten erreichbar [4].

Wenn der Angreifer mit einer Relay Attacke arbeitet, können die Weiten zwischen dem echtem Reader und dem echten Tag sehr groß werden. Es spielen dann nur noch die Toleranzgrenzen des echten Readers eine Rolle da es unvermeidlich ist, dass das Signal eine gewisse Verzögerung aufweist. Diese Grenzen sind in der Praxis meist sehr hoch ausgelegt und so kommen manche Versuche auf eine Reichweite von bis zu 50 Metern.

Bei einer Replay Attacke ist die Entfernung zwischen dem Reader und dem Tag unerheblich, da eine Kommunikation wieder abgespielt wird, die schon einmal stattgefunden hat. So braucht der "echte" Reader oder das "echte" Tag nicht in der Nähe zu sein.

2. Der Angreifer könnte einen Virus in ein Tag einpflanzen. Wenn dann ein Reader dieses Tag liest wird das Virus auf das Back-End-System überspielt. So kann ein Virus nur bei bestimmten Back-End-Systemen funktionieren. Da jedoch die meisten dieser Systeme auf Datenbanken basieren ist die Wahrscheinlichkeit groß, dass der richtige Angriff, wie zum Beispiel eine SQL-Injektion, zum Tragen kommt. So wird dieser Virus auch auf weitere Tags überspielt, die danach mit dem Reader gelesen werden.

Riebach, Simpson, Crispo und Tanenbaum haben schon in Tests gezeigt, dass dieser Angriff möglich ist. Jedoch ist darauf hin zu weisen, dass es nur mit ganz bestimmten Systemen funktioniert. Ähnlich funktionieren auch Buffer-Overflow-Attacken. Bei diesen Attacken werden Befehle ausgeführt, die einen Buffer zum Überlaufen bringen. Daten, die nicht mehr in den Buffer passen, werden in andere Teile des Speichers geschrieben und befinden sich so in ausführbaren Bereichen des Speichers. So könnte vielleicht schadhafter Code ausgeführt werden [5].

3. Nachdem sich ein Tag mit seiner ID angemeldet hat kann er die Daten verändern, die das Tag sendet (aktive Man-in-the-Middle-Attacke). So kann er falsche Daten des Tags vortäuschen, indem er das echte Tag stört und mit seinem falschen Tag weitere Informationen sendet. Jedoch werden in den meisten Anwendungen die wichtigen Daten im Back-End-System gespeichert, womit dieser Angriff meistens fehl schlägt. Der Bau eines Systems, mit dem der Angriff gelingen kann, ist mit unter 100 Euro nicht besonders teuer.
4. Um ein anderes Tag emulieren und konfigurieren zu können, muss der Angreifer schon in den Besitz von sensiblen Informationen, wie der ID und Schlüsseln des Tags, kommen. Erst dann kann er eventuell eine geklonte Karte verändern und die Daten fälschen.
5. Die Kommunikation zwischen Reader und Tag lässt sich sehr gut und sehr schnell unterbinden. So genannte Denial of Service Attacken gibt es viele. So kann man das Tag einfach zerstören oder das Tag und den Reader mit Metall oder Wasser ummanteln.

Es entstehen auch neue Bedrohungen für die Träger von kontaktlosen Smart-cards. So kann man Personen über mehrere Orte verfolgen, oder autorisierte Stellen können mehr Daten auswerten als nach den Datenschutzbestimmungen erlaubt ist. Durch diese Technik stehen ihnen mehr Daten über Personen und deren Handlungen zur Verfügung. So ist es einfach möglich nachzuvollziehen, wie oft eine Person mit ihrer kontaktlosen Kreditkarte bezahlt hat seitdem sie das letzte Mal ein bestimmtes Lesegerät benutzt hat. Dies sind größtenteils jedoch keine Angriffe, sondern es wird oft von den Betreibern des Systems gewollt [3].

5 Gegenmaßnahmen

5.1 Authentifizierung

Reader und Tag versuchen zu beweisen, dass sie berechtigt sind miteinander zu kommunizieren. Auch der Reader muss sich vor dem Back-End-System authentifizieren.

- Wenn die ID von einem Tag eindeutig ist kann über ein Back-End-System verhindert werden, dass Klon-Attacken erfolgreich sind, indem das doppelte Auftreten einer ID im System einen Alarm auslöst. Ausserdem können Karten ohne eine Nummer im System nicht mit dem Reader kommunizieren. Jedoch wird diese Methode bei einer großen Anzahl von möglichen Karten sehr langsam und damit irgendwann nicht mehr einsetzbar, da viele Karten an verschiedenen Stellen (z.B. an allen Flughäfen) auf die gleiche Datenbank zugreifen müssen.
- Ein Möglichkeit der Authentifizierung ist das Challenge-und-Response-Verfahren. Als erstes schickt der Reader dem Tag die Aufforderung eine

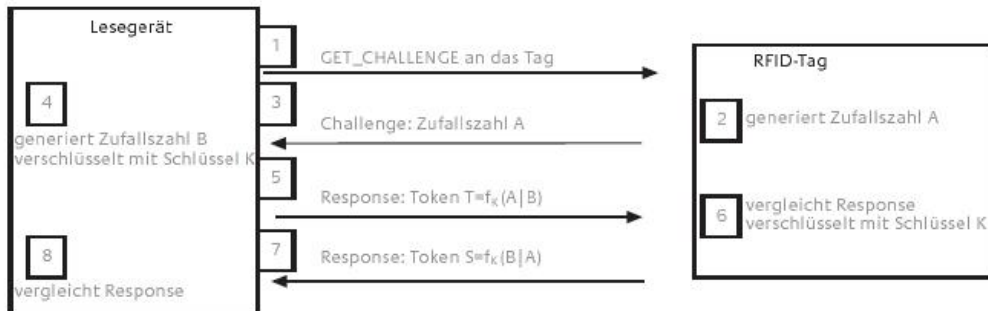


Abbildung 5: Das Challenge-und-Response-Verfahren

Challenge zu schicken. Das Tag verschlüsselt mit einem symmetrischen Verfahren und dem gemeinsamen Schlüssel eine Zufallszahl. Das Tag schickt nun seine verschlüsselte Zufallszahl zum Reader. Dieser entschlüsselt die Challenge und verschlüsselt nun die Zufallszahl des Tags

und seine eigene Zahl mit dem gemeinsamen Schlüssel. Dies schickt der Reader als Response zurück zum Tag. Wenn das Tag die Response entschlüsselt, haben beide einen neuen gemeinsamen symmetrischen Schlüssel für die weitere Kommunikation, der aus den beiden Zufallszahlen besteht. Dieser Schlüssel wird nur für eine Sitzung benutzt. Dadurch, dass eine Zufallszahl verwendet wird, ist diese Methode besonders gut zum Verhindern einer Replayattacke. Ein Angreifer kann auch ohne Kenntnis des symmetrischen Schlüssels sich nicht mehr als autorisierter Reader ausgeben.

Wenn ein Angreifer an den Sitzungsschlüssel kommt kann er sich für eine Sitzung authentifizieren. Sollte er jedoch den symmetrischen Schlüssel für die Verschlüsselung der Zufallszahlen bekommen, kann er die Kommunikation jedes Mal komplett entschlüsseln. Wenn er den Kanal abhört, kann er per Brute-Force-Methode versuchen den Schlüssel herauszubekommen. Um diesen Schlüssel aus seinen Speicherzellen auszulesen muss man schon sehr aufwendige Labortechnik haben (z.B. "Focused Ion Beam").

- Das Tag hat auch Möglichkeiten den Reader zu identifizieren. Bei sehr einfachen Systemen gibt es Tags, die eine bestimmte Anzahl von Schlüsseln gespeichert haben, die ihnen der Reader zuschicken muss um an die Daten des Tags zu kommen. Mehr Sicherheit bietet das Hash-Lock-Verfahren. Das Tag hat eine eigene Meta-ID und bleibt gesperrt. Wenn es in die Nähe eines Readers kommt sendet es nur diese Meta-ID. Der Reader holt dann aus dem Back-End den Schlüssel, der zur Meta-ID gehört und sendet ihn zum Tag. Das Tag berechnet mit diesem Schlüssel, seiner ID und einer Hashfunktion einen Wert und vergleicht ihn mit seiner Meta-ID. Wenn diese beiden Werte übereinstimmen entsperrt sich das Tag für diese Kommunikation. Eine Replayattacke ist jedoch bei diesem Verfahren nicht ausgeschlossen. Deswegen wird dieses Verfahren meist nur bei kontaktlosen Smartcards angewendet, die zu wenig Rechenleistung besitzen um das Challenge-und-Response-Protokoll zu durchlaufen.
- Asymmetrische Verfahren werden zur Authentifizierung seltener eingesetzt, da sie sehr viel Zeit und Energie brauchen. Auch sind die Daten-

mengen größer, um die gleiche Sicherheit bei Brute-Force-Attacken zu liefern wie symmetrische Verfahren.

5.2 Verschlüsselung

Da der Luftkanal zwischen Reader und Tag leicht abgehört werden kann ist es wichtig die Daten verschlüsselt zu übertragen. So kann eine Verschlüsselung einen Abhörangriff verhindern. Diese Verschlüsselung hängt aber stark mit der Authentifizierung zusammen, da beim Challenge-und-Response-Verfahren ein Sitzungsschlüssel ausgetauscht werden kann, der dann für eine symmetrische Verschlüsselung genutzt werden kann. Eine wesentlich höhere Sicherheit bietet natürlich das Ablegen von den Daten im Back-End, solange dieses keinen bestimmten Restriktionen unterliegt. So müssen so gut wie keine Daten übermittelt werden und man kann auf die Verschlüsselung verzichten, womit man wieder billigere Chips benutzen kann.

5.3 Abhörsichere Antikollisionsprotokolle

Bei RFID kommen Antikollisionsprotokolle vor, da sich mehr als ein Tag im Bereich des Readers aufhalten kann. Durch diese Protokolle kann der Reader die Tags einzeln ansprechen und auseinander halten.

Dabei haben sich zwei Protokolle durchgesetzt, das Tree-Walking- und das Aloha-Protokoll. Von beiden Protokollen wurden auch abhörsichere Varianten entwickelt, um einem Angreifer das Mithören von Tag IDs zu erschweren. Denn ohne eine ID kann der Angreifer ein Tag nicht verfolgen oder deaktivieren, wobei der Kanal vom Reader zum Tag viel leichter abzuhören ist als der vom Tag zum Reader.

- Der Tree-Walking-Algorithmus: Der Grundalgorithmus funktioniert so, dass der Reader durch eine Überlagerung der Signale erkennen kann, an welcher binären Stelle der ID zwei Tags ein unterschiedliches Bit haben, wenn mehrere Tags ihre ID senden. Dann wird wie bei einem binären Baum einer der beiden Zweige ausgewählt, und die ID bis zu dieser ausgewählten Stelle an alle Karten gesendet. Die Karten, bei denen die ID übereinstimmt, dürfen nun ihre restliche ID wieder senden. So geht dieser Algorithmus durch den binären Baum bis er nur noch eine Karte ausgewählt hat. Der abhörsichere Silent-Tree-Walking funktioniert wie

schickt. Wenn jedoch die ID einzigartig sein muss oder es wichtig ist, dass man das Tag an seiner ID erkennt kann man mit Meta-ID's verhindern, dass man den Träger identifizieren kann. Man kann jedoch überwachen, wo sich diese Meta-ID aufgehalten hat, da sich eine Meta-ID nie ändert.

- Das Verfahren Randomized-Hash-Lock funktioniert so, dass das Tag seine ID mit einer Zufallszahl zusammen hasht. Die Zufallszahl und der gehashte Wert werden an den Reader geschickt, der mit allen für diese Applikation freigegebenen ID's und dem Zufallswert Hashwerte ermittelt bis er einen gefunden hat, der mit dem zugeschicktem Wert übereinstimmt. Dieses Verfahren ist gerade bei einer größeren Anzahl möglicher Karten unpraktikabel.
- Bei dem Verfahren Chained-Hashes wird die Meta-ID mit zwei unterschiedlichen Hashfunktionen nochmal gehasht. Danach hört das Tag auf die erste neue Meta-ID. Die zweite neue Meta-ID wird an den Reader geschickt, der die Hashfunktion kennt. Er bildet mit der letzten Meta-ID und der Hashfunktion die aktuelle Meta-ID zurück und spricht damit das Tag an.
- Bei dem Verfahren von Henrici und Müller gibt es auf dem Tag und dem Back-End zwei Transaktionsnummern. Bei jeder Transaktion nimmt das Tag eine Nummer und errechnet einen Hashwert aus seiner ID und dieser Nummer. Der Reader kann die ID dann zurückrechnen und sie validieren. Dann überträgt der Reader wieder zwei neue Transaktionsnummern. Zwei werden übertragen, damit ein Übertragungsfehler ausgeglichen werden kann.

5.5 Verhindern des Auslesens

Da man RFID-Chips eigentlich immer auslesen kann und ein Benutzer nicht unbedingt feststellen kann, ob seine Tags gerade ausgelesen werden oder nicht, kann man einem unbefugten Auslesen eines RFID-Chips nur schwer entgegen wirken. Bei manchen Tags ist die Antenne so angebracht, dass man

sie entfernen kann. Doch in manchen Fällen sind die Antennen in einer Chipkarte, wo man sie nicht einfach trennen und verbinden kann. Man kann versuchen seine Tags abzuschirmen, jedoch weiß man nicht, ob bestimmte Abschirmungen für bestimmte Chips funktionieren. Man kann aber auch Blocker-Tags einsetzen, um sich gegen ein unberechtigtes Auslesen zu schützen. Diese Blocker-Tags emulieren jede ID Nummer, womit es zu einem Konflikt beim Auslesen mit dem Reader kommt. Jedoch funktionieren Blocker-Tags nur für ein bestimmtes Antikollisionsprotokoll und ein bestimmtes Frequenzband.

5.6 Verhindern einer Relay-Attacke

Eine Relay Attacke ist nicht einfach zu verhindern. Die Kommunikation zwischen Reader und Tag ändert sich nicht, wenn der Angreifer über sein System weiterleitet. So kann man die Kommunikation mitschneiden und persönliche Trägerinformationen, wie zum Beispiel eine Kontonummer, erfahren. Wobei der Angreifer diese Attacke auch ausführen kann, wenn alle Informationen verschlüsselt übertragen werden und er nichts mitlesen kann.

In einem Paper wird eine Möglichkeit aufgezeigt, wie man eine Relay Attacke verhindern kann. Dafür wird ein weiteres Frequenzband (zwischen 3,1 und 10,6 GHz) genutzt, das UWB (Ultra Wide Band). Mit diesem Frequenzband kann man auch auf kleineren Entfernungen genauere Weiten (wenige Zentimeter) abmessen.

Die Gegenmaßnahme basiert auf einem Challenge-und-Response-Protokoll. Der Reader schickt dem Tag einen Zufallswert zu. Dieser Zufallswert wird dann vom Reader und vom Tag zusammen mit ihrem geheimen Schlüssel gehasht. Das Tag spaltet dann den so erhaltenen Wert in zwei gleich große Werte auf und lädt diese in Shift Register. Dann schickt der Reader Challenge Bits und das Tag wählt nach dem empfangenen Bit einen Ausgang der beiden Shift Register aus. Dies bedeutet, dass wenn der Reader eine 0 sendet der Ausgang des ersten Shift Registers benutzt wird und bei einer 1 der Ausgang des Zweiten. Dieses Bit aus dem Shift Register wird zurück gesendet und der Reader validiert das empfangene Bit, da er weiß welches Shift Register ausgewählt wurde und welcher Wert in den Shift Registern liegt. Nun kommt das UWB zum tragen. Der Reader weiß, wie lange das Tag braucht um das Bit auszuwählen und kann nun, wenn es die Antwort erhält, errechnen, wie weit das Tag entfernt ist. So kann der Reader Tags ausschließen, die zu weit entfernt sind. Auch weiß der Reader nun wie lange das Tag für eine Antwort

braucht und kann beim Überschreiten von Toleranzen die Kommunikation abbrechen [4].

5.7 Virusabwehr

Um ein RFID-System gegen einen Virus zu schützen, kann man die gleichen Vorgehensweisen anwenden, wie bei einem normalen Computer-System. Um sich dann zum Beispiel gegen eine SQL-Injektion zu schützen, muss man jeden eintreffenden Befehl auf seine Richtigkeit überprüfen und die Befehle herausfiltern, die Steuerzeichen enthalten und so gefährlichen Code einschleusen können. Natürlich sind die Schritte um ein System gegen einen Virus zu schützen unterschiedlich, so wie es auch die Software ist, die auf ihm betrieben wird.

5.8 Dauerhafte Deaktivierung

Außer den physischen Möglichkeiten ein Tag zu zerstören gibt es auch noch die Möglichkeit einen Kill Befehl zuschicken. Dieser Befehl ist passwortgeschützt, so will man die Löschung durch unautorisierte Gruppen verhindern. Jedoch wird der Chip nur softwaremäßig gelöscht, so dass die ID immer noch ausgelesen werden kann. Wodurch man den Träger immer noch nach verfolgen kann.

Eine andere Möglichkeit einen Chip zu deaktivieren, z.B. durch eine Sollbruchstelle, wird bei Tags angeboten, die als Ersatz für Barcodes dienen.

Literatur

- [1] Wikipedia - Radio Frequency Identification
<http://de.wikipedia.org/wiki/RFID>
- [2] Timo Kasper - Embedded security analysis of rfid devices
<http://www.crypto.ruhr-uni-bochum.de/theses.html>
- [3] Bundesamt für Sicherheit in der Informationstechnik
Risiken und Chancen des Einsatzes von RFID-Systemen
<http://www.bsi.de/fachthem/rfid/studie.htm>
- [4] Gerhard Hancke - An RFID distance bounding protocol
<http://www.cl.cam.ac.uk/~gh275/>
- [5] Department of Computer Science Vrije - Universiteit Amsterdam
<http://www.rfidvirus.org>
- [6] E-Pass geklont
<http://www.golem.de/0608/46966.html>
- [7] OpenPCD: RFID Sniffer
<http://www.openpcd.org/rfiddump.0.html>