NFC - Mit freundlichen Grüßen*

Florian Schiele
Friedrich-Alexander-Universität
Erlangen-Nürnberg (FAU)
ich@florianschiele.de

ABSTRACT

Near Field Communication (NFC) ist eine Sammlung von Kommunikationsprotokollen, die auf der Radio-Frequency Identification (RFID) Technologie basieren. NFC wird eingesetzt, um drahtlos über kurze Distanzen Daten zu übertragen. Einer der Kommunikationspartner (Transponder) kann hierbei passiv sein. Das heißt, er wird vom aktiven Transponder mit Energie versorgt und benötigt keine eigene Stromversorgung. Dies ermöglicht NFC-Transponder in sehr kompakter Bauform mit nahezu unbegrenzter Lebenszeit herzustellen.

Zu den bekanntesten Anwendungen zählen unter anderem das kontaktlose Bezahlen, Zutrittskarten von Zugangskontrollsystemen und die keyless-entry-Systeme zur Entriegelung von Fahrzeugen. Dies ist nur ein Auszug von vielen sicherheitskritischen Anwendungen. Aus diesem Grund sind neben der einfachen Speicherung von permanenten Daten bei einigen Kartentypen auch Verschlüsselungsfunktionen implementiert, mit denen die Karteninhalte gesichert werden können oder auch ein Challenge-and-Response-Protokoll realisiert werden kann.

In diesem Artikel wird zunächst das Verfahren, welches die drahtlose Kommunikation von NFC ermöglicht, vorgestellt. Nachdem diese Grundlagen vorgestellt sind, wird die Kommunikationssicherheit von NFC untersucht. Insbesondere stellen wir die Frage, ob Angriffe wie der Man-In-The-Middle-Angriff, das aktive Auslesen und passive Abhören der Kommunikation möglich sind.

KEYWORDS

NFC, RFID, Transponder, Smartcard, Rahmenantenne, i1seminar

1 EINFÜHRUNG

Die NFC-Technologie ist heutzutage weit verbreitet und aus dem Alltag nicht mehr wegzudenken. Die Sensibilität einiger Einsatzgebiete und die benötigten Fachkenntnisse machen NFC zu einem fordernden aber zugleich auch spannenden Fachgebiet.

Um die Sicherheit von NFC verstehen und bewerten zu können, ist neben der Informatik auch ein fundiertes elektrotechnisches Verständnis notwendig.

In den folgenden Kapiteln werden zunächst die nötigen Grundlagen erläutert, um dann mögliche Angriffsvektoren zu beleuchten und auch Gegenmaßnahmen aufzuzeigen.

Das Wissen, das in diesem Artikel vermittelt wird, ist für den Leser nicht nur von theoretischem Wert. Praktisch kann die einfache Version des Relay-Angriffs mit geringem Aufwand selbst durchgeführt werden. Ausserdem kann auch ein NFC-Indikator aus einer Leuchtdiode (LED) und etwas Draht zusammengesetzt werden.

*Dieser Beitrag entstand im Rahmen des Konferenzseminars “IT Security”, das im Sommersemester 2020 vom Lehrstuhl 1 Informatik für IT-Sicherheitsinfrastruturen der FAU durchgeführt wurde. Besonderer Dank gilt hierbei Philipp Klein für die Betreuung dieser Ausarbeitung.

2 GRUNDLAGEN

NFC ist eine Sammlung von Vorgaben, die die Kommunikation zwischen einem Reader wie zum Beispiel einem Kartenlesegerät und einer Zutrittskarte standardisieren. Diese Vorgaben beziehen sich hauptsächlich auf die mittlere Schicht im ISO/OSI-Modell zwischen der Applikationsebene und der Bitübertragungsschicht.

Die Übertragungsschicht wird mittels RFID realisiert. Um die Arbeitsweise und mögliche Angriffsszenarien auf die Kommunikation einer NFC-Verbindung zu verstehen, werden zunächst die Grundlagen der RFID-Technologie beleuchtet.

Die RFID Technologie wurde bereits im zweiten Weltkrieg zur kontaktlosen Freund-Feind-Erkennung an Flugzeugen eingesetzt. Die damalige Nutzdatenmenge betrug lediglich ein Bit. Der Informationsgehalt bestand darin, ob am Flugzeug ein RFID-Transponder montiert war oder nicht. [3, S. 26]

Diese Art von Ein-Bit-Transpondern ist einfach aufgebaut und in der Herstellung sehr kostengünstig. Heutzutage werden sie zum Beispiel in großen Stückzahlen im Einzelhandel als Warensicherungsetikett eingesetzt. Nach der Bezahlung an der Kasse wird das Warensicherungsetikett entfernt oder deaktiviert. Die Deaktivierung geschieht meist durch Zerstörung eines elektronischen Bauteils innerhalb des Transponders. [1, S. 14]

Da Transponder mit nur einem Bit Nutzdaten sehr einfach kopiert werden können, wäre der Einsatz zum Zwecke der Freund-Feind-Erkennung heutzutage damit sinnlos. Der Feind könnte sich einfach durch eine Kopie des Transponders als Freund ausgeben.

Aus diesem Grund war es wichtig, Transponder mit mehr Informationsgehalt als einem Bit zu entwickeln.

Auch eine Verschlüsselung der Kommunikation zwischen Reader und Transponder ist ein bedeutsames Merkmal. Hiermit kann unter anderem ein Schutz gegen das Abhören und Kopieren (Klonen) realisiert werden. Die Möglichkeit, mehr als ein Bit Daten per RFID zu übertragen, ist in der modernen Welt nicht mehr wegzudenken.

Seither wurde ein breites Spektrum von RFID-Systemen verschiedener Anbieter entwickelt und verkauft, die untereinander inkompatibel sind. Um einen einheitlichen Standard zu definieren, haben sich Nokia, Philips Semiconductors (heute NXP) und Sony im Jahr 2002 zusammengetan und das NFC-Forum [1] gegründet. Mittlerweile sind viele weitere Hersteller dem Forum beigetreten. [10]

NFC wird unter anderem in den Normen ISO/IEC 21481, ISO/IEC 14443, ISO/IEC 18092 standardisiert. [9, S. 3]

Durch die Standardisierung und die weite Verbreitung wurde die NFC-Technik auch für Mobilfunkgeräte interessant. Sind diese mit einem NFC- Interface ausgestattet, können Sie mit allen NFC-standardisierten Transpondern kommunizieren.

[1] https://nfc-forum.org

3 GRUNDLEGENDER AUFBAU EINES RFID SYSTEMS

Der grundlegende Aufbau eines RFID-Systems besteht aus einem Reader [2] und einem Transponder. Der Reader ist stets aktiv. Das bedeutet, er verfügt über eine eigene Stromversorgung. Der Transponder kann sowohl aktiv als auch passiv sein.

3.1 Aktive und passive Transponder

Wenn es sich um einen aktiven Transponder handelt, verfügt dieser über eine eigene Stromquelle. Mobiltelefone mit NFC zählen zum Beispiel zu den aktiven NFC-Transpondern. Ein aktiver Transponder ist in der Lage, einen passiven Transponder mit Energie zu versorgen und eine Verbindung zu initiieren.

Passive Transponder hingegen werden durch ein elektromagnetisches Feld, das vom aktiven Transponder (Reader) erzeugt wird, mit Energie versorgt. Sie sind dadurch nicht in der Lage, eine Verbindung zu initiieren. [1, S. 74ff.]

Es sind zwei Paarungen möglich:

(1) Aktiv/Aktiv: Beide Teilnehmer können abwechselnd aktiv senden. Nur der jeweils sendende Teilnehmer erzeugt das elektromagnetisches Wechselfeld. Auf das Wechselfeld (Träger) werden die Daten moduliert.
(2) Aktiv/Passiv: Der aktive Teilnehmer erzeugt einen permanenten Träger. Möchte er senden, moduliert er die Daten wie im Aktiv/Aktiv Modus auf den Träger. Möchte der passive Teilnehmer senden, beeinflusst er den Träger des aktiven Teilnehmers (Lastmodulation). [3]

3.2 Energieversorgung passiver NFC Transponder

Eine Energieversorgung über die Luftschnittstelle wird immer dann benötigt, wenn der Transponder passiv ist. Der Reader versorgt den Transponder mit Hilfe von elektromagnetischer Induktion mit Energie. Im Grunde funktioniert die Energieübertragung wie ein herkömmlicher elektrischer Transformator.

3.2.1 Exkurs Transformator. Ein elektrischer Transformator besteht im einfachsten Fall aus zwei Leiterschleifen (Spulen) und einem ferromagnetischen Kern (meist geblechter Eisenkern). Wird an eine der beiden Spulen eine Wechselspannung angelegt, bildet diese durch den Stromfluss ein wechselndes Magnetfeld [4] aus, das im Eisenkern gebündelt auf die zweite Spule übertragen wird. In der zweiten Spule entsteht daraufhin wieder eine Wechselspannung, mit der ein Verbraucher versorgt werden kann. Der Wirkungsgrad kann bei qualitativ hochwertigen Transformatoren bis zu 99% betragen.

3.2.2 Rahmenantenne. Bei der RFID-Technik werden ebenfalls Spulen (eine im Reader und eine im Transponder) eingesetzt. Der Unterschied zum Transformator liegt im Fehlen des Kerns. Das magnetische Feld wird ausschließlich über die Luft übertragen. Solch eine Spule wird Rahmenantenne genannt. [1, S. 36f.] Abbildung 1 zeigt einen Transponder mit aufgedruckter Rahmenantenne.

[2] Erfassungs- oder Lesegerät, z.B. Mobiltelefon
[3] Eine ausführliche Beschreibung folgt im Kapitel Datenübertragung
[4] Die Polarität des magnetischen Feldes ändert sich analog zur Polarität des Wechselstromes

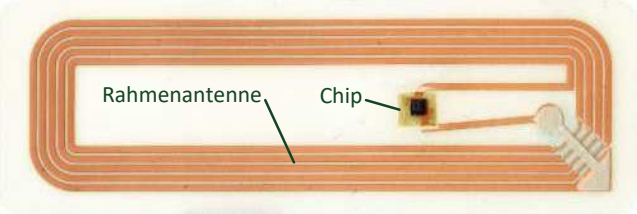

Abbildung 1: NFC Transponder mit Rahmenantenne

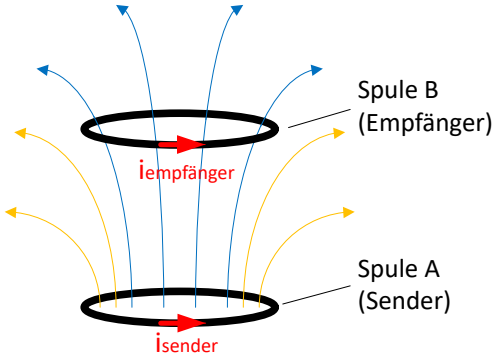

Abbildung 2: Streufluss

3.2.3 Kopplungsfaktor. Der Kopplungsfaktor gibt an, wieviel der ausgestrahlten Energie der Sendespule an der Empfangsspule wieder abgegriffen werden kann. Der Wert bewegt sich im Bereich $0 \leq k \leq 1$. Wenn die Spulen von Reader und Transponder auf einer Achse mit gleichem Durchmesser direkt aufeinander angeordnet sind ist der Kopplungsfaktor nahe 1. Sind die Spulen weit voneinander entfernt oder magnetisch abgeschirmt, geht der Kopplungsfaktor gegen 0. Typische RFID-Anwendungen arbeiten mit einem Kopplungsfaktor von bis unter 0,01 (1%) [1, S. 86ff.]

Die mathematische Herleitung des Kopplungsfaktors führt hier zu weit. Abbildung 2 soll eine Vorstellung darüber vermitteln, wie sich der Kopplungsfaktor im Verhältnis zum Abstand ändert. Die Spule A wird von einem Strom i_{sender} durchflossen. Dadurch bilden sich elektromagnetische Feldlinien entlang der Spulenachse aus. Ein Teil (blaue Feldlinien) durchqueren die Empfangsspule B. Der restliche Teil (orangene Feldlinien) verfehlen die Empfangsspule B. Hierbei handelt es sich um Streufluss. [5, S. 57]

Der Streufluss kann in diesem Kontext als Verlust [5] angesehen werden, da er nicht beim Empfänger ankommt. Um eine ausreichende Energieversorgung zu gewährleisten ist es also wichtig, die Spule des Transponders nah und in der richtigen Orientierung am Reader zu positionieren.

Zur praktischen Untersuchung, wie sich die Kopplung der Antennen verhält, dient ein einfacher Aufbau wie in Abbildung 3 dargestellt.

[5] Verlust im Sinne von nicht auf den Empfänger übertragen. Hierbei handelt es sich nicht um einen Verlust im elektrotechnischem Sinn.

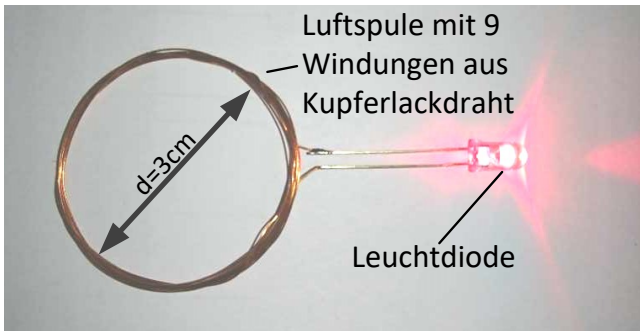

Abbildung 3: RFID Indikator mit Luftspule und LED

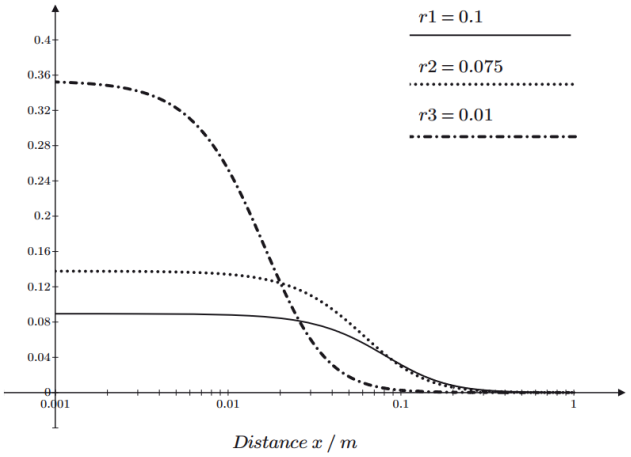

Abbildung 4: Kopplungsfaktor [1, S. 87]

Hierzu wird eine Spule mit etwa 9 Windungen [6] mit einer LED verbunden. Wird die Spule in das Wechselfeld des Readers gebracht, leuchtet (blinkt) die LED durch die induzierte Energie.

Der Durchmesser von Sende- und Empfangsspule wirkt sich ebenfalls auf den Kopplungsfaktor aus. In Abbildung 4 wird der Kopplungsfaktor einer Spule (Durchmesser 1cm) gekoppelt mit drei im Durchmesser verschiedenen Spulen abhängig vom Abstand (Luftspalt) dargestellt. Es ist ersichtlich, dass ab einem bestimmten Abstand der Kopplungsfaktor stark abfällt. Diese Stelle ist der Übergang vom Nahfeld ins Fernfeld. Im Fernfeld ist keine transformatorische (induktive) Kopplung mehr möglich. Daher ist RFID im Zusammenspiel mit einem passivem Transponder nur im Nahfeld funktionsfähig. [1, S. 138f.]

Diese Erkenntnis ist von zentraler Bedeutung, da die Sicherheit von NFC auch auf der Reichweite beruht. Dieses Sicherheitsmerkmal soll vor dem Auslesen von Transpondern aus größerer Entfernung schützen.

[6] Die Anzahl der Windungen wirkt sich auf das transformatorische Verhältnis aus und beeinflusst damit direkt die Spannung, die an der LED anliegt.

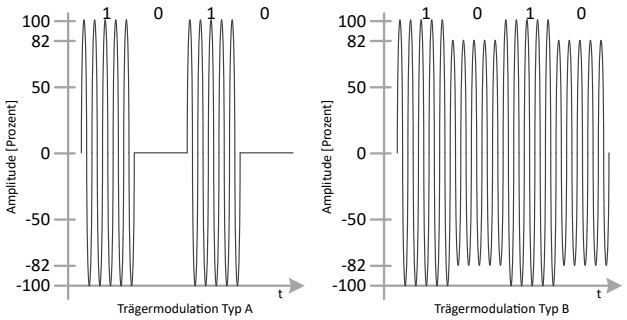

Abbildung 5: Trägermodulation Typ A, B nach [7, S. 25]

4 DATENÜBERTRAGUNG

Die Datenübertragung erfolgt drahtlos ebenso wie die Energieversorgung mittels Induktion. Zunächst betrachten wir die Senderichtung eines aktiven Transponders (folgend Reader genannt). Ziel ist es, einzelne Bits, also eine Eins oder eine Null seriell an den Kommunikationspartner zu übertragen.

Bei NFC wird Amplitudenumtastung (ASK) zur Bitmodulation angewendet. [1, S. 308]

4.1 Senderichtung Reader -> Transponder

Der Reader moduliert die Informationen unter Verwendung von ASK. ASK ist die digitale Variante der Amplitudenmodulation (AM), wie sie von einigen Radiosendern zur Tonübertragung im Radio verwendet wird. Die zwei Zustände (Eins und Null) werden bei ASK in der Höhe der Sendeamplitude abgebildet. NFC spezifiziert zwei Übertragungsmodi: Typ A und Typ B. Bei Typ A wird ein On-Off-Keying verwendet. Das bedeutet, die zwei verwendeten Amplituden sind 0% für eine binäre 0 und 100% für eine binäre 1. Bei Typ B hingegen werden Amplituden mit 100% für eine binäre 1 und 82% für eine binäre 0 angewandt. Die Trägerfrequenz beträgt bei NFC grundsätzlich 13,56 MHz. In Abbildung 5 sind die Amplituden der Spannungsverläufe eines Readers beim Senden jeweils für Typ A und für B illustriert. [2, S. 13f.]

Nun stellt sich die Frage wie ein passiver Transponder unter Verwendung des Übertragungsmodi vom Typ A bei einer längeren Sequenz von binären Nullen noch mit Energie versorgt werden kann. Bei der Übertragung einer Null mit Typ A ist die Sendeamplitude 0%, es findet also auch keine Energieübertragung statt. Die Lösung liegt in der verwendeten Bitcodierung. Bei Typ A wird eine modifizierte Miller-Codierung genutzt, bei der kurze 0%-Impulse für die Modulation ausreichen.[1, S. 220] Die kurzen Energieunterbrechungen werden mit einem elektrischen Ladungsspeicher im passiven Transponder ausgeglichen.

Im Fall des Übertragungsmodi Typ B wird jedem Binärwert eine Amplitude zugeordnet. Das stellt kein Problem hinsichtlich der Energieversorgung dar, da selbst bei einer langen Sequenz von Nullen noch kontinuierlich 82% der Amplitude zur Verfügung stehen.

4.2 Empfangsrichtung Transponder -> Reader

Ein passiver Transponder hat keine eigene Energieversorgung. Die Energie die vom Reader bereitgestellt wird reicht aus, um die Elektronik des passiven Transponders zu versorgen. Genug Energie

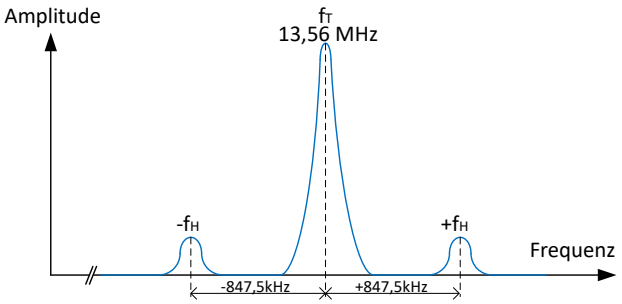

Abbildung 6: Hilfstraeger nach [1, S. 226]

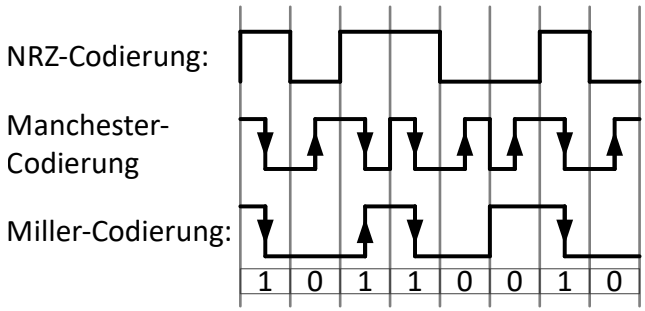

Abbildung 7: Codierungsverfahren [1, S. 221]

zum Senden eines eigenen Trägers ist allerding nicht vorhanden. Deshalb bedient man sich an dieser Stelle mit der Technik der Lastmodulation.

4.2.1 Lastmodulation. Bei der Lastmodulation verändert der Transponder seinen Energiebedarf entsprechend der zu übertragenden Informationen.

Das Funktionsprinzip kann wieder anhand eines elektrischen Transformators erklärt werden. Wir betrachten ein Handyladegerät. Steckt das Ladegerät in der Steckdose ohne, dass ein Handy angeschlossen ist, setzt es wenig Energie um (nur Wärmeverlust). Dies würde einer binären Null entsprechen. Wenn hingegen ein Handy angeschlossen ist, wird es geladen und entsprechend mehr Energie bezogen. Dies würde einer binären Eins entsprechen. Beide Fälle sind an der Steckdose in Form des Energieflusses messbar.

Genau dieses Prinzip wird auch bei der NFC-Technologie genutzt. Der Reader kann den Energieumsatz des passiven Transponders messen und entsprechend interpretieren.

Da der Energieumsatz des passiven Transponders unter anderem bedingt durch Rechenoperationen und Speicherzugriffe der Transponderelektronik schwankt, könnten diese Schwankungen vom Reader als falsche Information erfasst werden. Auch äußere Einflüsse wie Metallgegenstände können den Energieentzug des Readers beeinflussen. Die genannten Einflüsse wirken auf die Trägerfrequenz des Readers von 13,56 MHz. Somit ist der Träger für die Datenübertragung mit Lastmodulation ungeeignet.

4.2.2 Seitenbänder. Um das vorgenannte Problem zu umgehen wird die Lastmodulation auf die Seitenbänder der Trägerfrequenz verlagert. Seitenbänder sind Hilfsträger unterhalb und oberhalb der Trägerfrequenz. Der Frequenzabstand zum Träger beträgt wie in Abbildung 6 gezeigt $f_H = \frac{f_T}{16} = 847,5kHz$. [1, S. 51ff]

Die Hilfsträger werden mit on-off-keying betrieben. Das bedeutet, dass für eine binäre Eins der Hilfträger eingeschaltet und für eine binäre Null abgeschaltet wird. Die Lastmodulation auf dem Hilfsträger lässt sich durch eine simple digitale Schaltung mit einem Frequenzteiler (Binärzähler) realisieren. [1, S. 53]

4.3 Bitcodierungsverfahren

Die zu übertragenden Bits der NFC Kommunikation werden mit drei verschiedenen Verfahren kodiert. Die Senderichtung (Reader -> Transponder) wird bei Typ A mit der modifizierten Miller Codierung kodiert. Bei Typ B mit dem Manchester Code. Die Empfangsrichtung (Transponder -> Reader) wird generell, egal ob Typ A oder B mit der Non return to zero (NRZ) Codierung kodiert. Wie die eben genannten Codierungsverfahren im einzelnen funktionieren, wird in den folgenden Unterkapiteln erklärt.

4.3.1 NRZ Codierung. NRZ ist ein einfaches Codierungsverfahren. Wie in Abbildung 7 dargestellt, wird den beiden Binärzuständen 0 und 1 jeweils ein Pegel zugeordnet. Die NRZ Codierung wird bei der Lastmodulation, also dem Rückkanal via Hilfsträger angewendet.

Aus der NRZ Codierung kann keine Taktrückgewinnung [7] erfolgen. Ein Beispiel ist die Übertragung vieler gleicher Bitzustände. Hier würde sich der Pegel nicht verändern. In diesem Fall kann folgend auch kein Takt abgeleitet werden.

Im Anwendungsfall von NFC wird der Takt aus dem Sendesignal des Readers gewonnen. [1, S. 220ff]

4.3.2 Manchester. Die Manchester Codierung ordnet den Binärzuständen anstatt eines Pegels eine Flanke zu. Soll eine Eins abgebildet werden, so wird eine fallende Flanke übertragen. Für die Übertragung einer binären Null wird hingegen eine steigende Flanke übertragen.

In Abbildung 7 ist zu erkennen, dass es je Takt mindestens einen Pegelwechsel gibt. Die Frequenz des Wechsels beträgt maximal eine und minimal eine halbe Bitlänge. Mit diesem Wissen ist es nun möglich einen Takt aus dem Signal zu gewinnen.

Ein Nachteil ist, dass durch die halb-Bit-langen Pulse die doppelte Übetragungsbandbreite nötig ist. Die folgend aufgeführte modifizierte Miller Codierung umgeht diese Eigenschaft. [1, S. 220ff]

4.3.3 Modified Miller. Die modified Miller Codierung vereint die Vorteile der NRZ- und der Manchestercodierung. Sie benötigt nur die einfache Übertragungsbandbreite und trotzdem ist eine Taktrückgewinnung möglich.

Bei einer binären Eins wird in der Taktmitte eine Flanke erzeugt. Für eine binäre Null bleibt der Pegelzustand unverändert. Um einen konstanten Pegel durch folgende Nullen zu vermeiden wird, ein Flankenwechsel zwischen den Takten eingefügt. [1, S. 220ff]

[7] Ein Takt wird benötigt um das übertragene Signal in ein Raster (rote vertikale Linien in Abbildung 7) einzuordnen.

5 ANGRIFFE

Bisher haben wir viel über die physikalischen Grundlagen der Energieversorgung und die Datenübertragung gelernt. Ausserdem kennen wir die Codierungsverfahren, mit denen die Daten übertragen werden. Diese Grundlagen sollen uns dabei helfen zu verstehen, wie Angriffe auf NFC funktionieren.

5.1 Zerstörung des Transponders

Einer der wohl primitivsten Angriffe auf ein RFID System ist die Zerstörung des Transponders. Ist dieser physisch zugänglich, kann er mechanisch, zum Beispiel mittels Durchtrennen der Rahmenantenne oder Krafteinwirkung auf den Chip, zerstört werden. Ist der Transponder nicht physisch zerstörbar, kann er durch eine ausreichend große Feldstärke (größer als 12A/m [8]) zerstört werden. Durch die hohe Energie wird der Spannungsregler des Transponders thermisch zerstört.

Bei 1-Bit Transpondern, die nur aus einem Schwingkreis bestehen, kann durch hohe Energieeinwirkung der Schwingkreis verstimmt werden. Diese Eigenschaft wird oft bei Warensicherungsetiketten an der Kasse nach der Bezahlung genutzt. [1, S. 35f]

5.2 Auslesen

Um einen NFC Transponder, wie zum Beispiel eine Kreditkarte mit NFC-Funktion im Vorbeigehen auszulesen, reicht im einfachsten Fall eine App wie *NFC-Tools* [9] aus. Die Herausforderung ist hier, dass der Reader nah (einige Zentimeter) am Transponder positioniert werden muss. Hiermit können statische Daten wie Name, Kreditkartennummer und Ablaufdatum erlangt werden. Am Terminal bezahlen kann man mit den gewonnenen Daten allerdings nicht, da zwischen dem Reader und der Kreditkarte eine kryptografische Authentifizierung eingesetzt wird.

Um sich vor Datendiebstahl zu schützen reicht eine Abschirmung mittels einer Metallhülle. Die Feldlinien gelangen dann nicht mehr durch die Rahmenantenne der Kreditkarte, da das Metall diese besser leitet und damit von der Karte fern hält. [1, S. 276]

5.3 Abhören

Das Abhören des magnetischen Feldes, das für die Kommunikation dient, ist auf Grund der lokal begrenzten Ausbreitung (Abbildung 2) nur im direkten Umfeld möglich. Eine globale Aussage, aus welcher Entfernung das Abhören möglich ist, lässt sich nicht treffen. Die mögliche Entfernung ist von vielen Parametern abhängig. Hierzu zählen:

- Antennengüte, -größe und -form
- Ausrichtung der Antenne
- Empfindlichkeit des Empfängers
- Abschirmendes Umfeld, z.B. Metalle
- Rauschen, kosmische Strahlung

[4, S. 4]

Ungefähre Erfahrungswerte für den maximalen Abstand bewegen sich beim Abhören eines aktiven Readers im Bereich von zehn Metern. Das Abhören eines passiven Transponders ist durch die wesentlich geringere Sendeleistung (siehe Abbildung 6) auf den Hilfsträgern nur im Bereich von etwa einem Meter möglich. [4, S. 5]

Wenn zwei aktive Transponder wie z.B. Mobiltelefone kommunizieren, kann das Abhören aus einer Entfernung von zehn Metern mit einer entsprechend qualitativen Ausrüstung durchaus gelingen. [4, S. 5]

5.4 denial of Service (DOS)

Um die Kommunikation zwischen den NFC Kommunikationspartnern zu stören kann ein einfacher Störsender verwendet werden, der auf der NFC Trägerfrequenz von 13,56 MHz sendet. Wichtig ist, den Störträger valide zu modulieren. Das bedeutet, im richtigen Timing an- und abzuschalten. [4]

5.5 Bitmanipulation

Die gezielte Manipulation der Datenübertragung ist wesentlich anspruchsvoller. Wir haben zwei Übertragungstypen (Typ A und Typ B) kennen gelernt. für beide Übertragungstypen betrachten wir die möglichen Szenarien.

5.5.1 Bitmanipulation bei Typ A. Typ A verwendet eine 100% Modulation. Das bedeutet, der Träger ist ein- (folgend mit ”Mark” bezeichnet) oder aus- (folgend als ”Space” bezeichnet) geschaltet. Um ein Space zu einem Mark zu ändern, muss der Angreifer lediglich einen eigenen Träger mit der richtigen Amplitude senden.

Andersherum muss der Angreifer den Träger des Readers auslöschen. Das funktioniert theoretisch durch Überlagerung. Das bedeutet, der Angreifer muss neben der richtigen Amplitude auch das richtige Timing treffen. In Abbildung 8 und 9 sind jeweils das Trägersignal, das Angreifersignal und das resultierende Signal abgebildet. Im Fall von Abbildung 8 ist die Phasenlage zwischen Reader- und Angreifersignal nahezu null. Hiermit ist keine Auslöschung des Readersignals möglich. Um den Träger des Readers auszulöschen muss der Angreifer seinen Träger mit einem Phasenwinkel von 180 Grad gegenüber dem Träger des Readers aussenden. Die Randbedingungen, die hierzu notwendig sind lassen sich mit hohem Aufwand im Labor herstellen. Im praktischen Einsatz ist es jedoch sehr schwer umsetzbar. [4, S. 5]

5.5.2 Bitmanipulation bei Typ B. Da bei Typ B eine 10% Modulation verwendet wird, ist der Träger des Readers stets aktiv. Da hier das Signal nicht ausgelöscht werden muss, hat der Angreifer eine bessere Voraussetzung. Er addiert bei jedem Space des Readers einen 10% Träger auf. Jetzt gibt es aus Sicht des Transponders nur noch ein gleichbleibend starkes Signal (interpretiert als Space). Um Mark Amplituden einzufügen muss der Angreifer wie in Abbildung 10 gezeigt, einen Träger mit 10% oder 20% Amplitude aussenden.

Zusammengefasst kann man sagen, dass bei Typ A die manipulation mit einer Warscheinlichkeit von 50% gelingt, da praktisch nur Space in Mark gewandelt werden kann. Bei Typ B ist die Manipulation möglich. [4, S. 5]

5.6 Latenzausnutzung

Bisher haben wir betrachtet wie die Kommunikation vom Reader zum Transponder manipuliert werden kann. Für die Rückrichtung, also vom Transponder zum Reader, kann ein einfacherer Weg beschritten werden. Wenn der Transponder für die Antwort lange

[8] Spezifiziert in ISO/IEC 14443 und ISO/IEC 15693
[9] Im Android Appstore erhältlich.

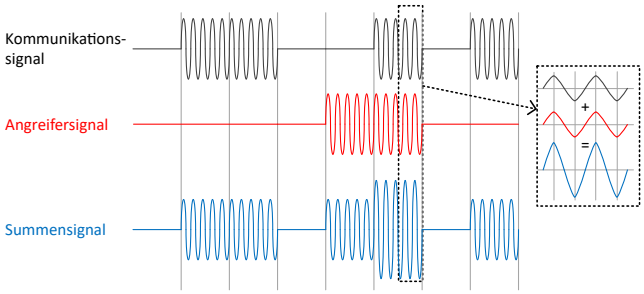

Abbildung 8: Addition Signale von Typ A nach [4, S. 9]

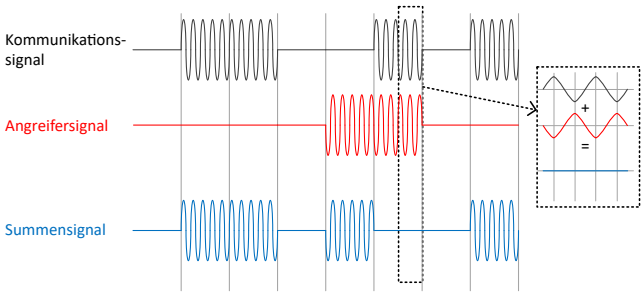

Abbildung 9: Subtraktion Signale von Typ A nach [4, S. 9]

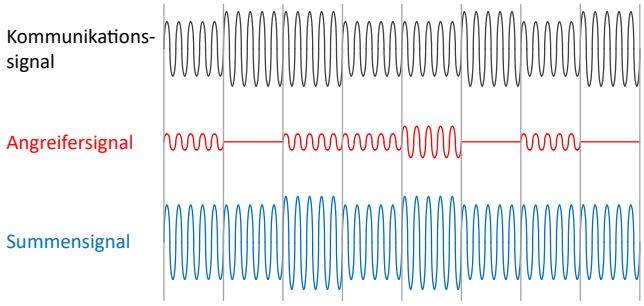

Abbildung 10: Addition Signale von Typ B nach [4, S. 9]

braucht, kann der Angreifer diese Zeit nutzen und früher antworten. Hierzu muss der Angreifer lediglich einen Träger auf den Seitenbändern modulieren. [4, S. 6]

5.7 Man-In-The-Middle

Bei einem klassischen Man-In-The-Middle Angriff versucht, wie in Abbildung 11 dargestellt, ein Angreifer den Kommunikationskanal zwischen den Kommunikationspartnern zu übernehmen. Dafür muss er zunächst zwei Dinge erreichen: Er muss erstens die Kommunikation zwischen Reader und Transponder unterbinden und zweitens selbst eine Kommunikation zu Reader und Transponder aufbauen.

In den vorherigen Kapiteln wurde untersucht, wie die Kommunikation unterbunden werden kann und wie die Kommunikation modifiziert werden kann.

Es wird nun folgendes Szenario betrachtet: Der Reader und der Transponder möchten einen sicheren Kanal aufbauen. Ein Weg

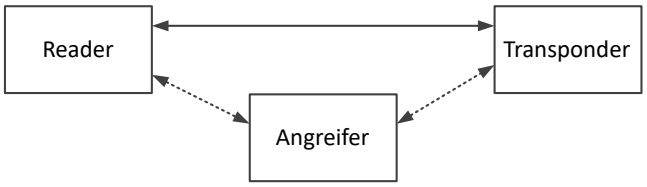

Abbildung 11: Man-In-The-Middle Angriff nach [4, S. 6]

dies zu realisieren ist der Diffie-Hellman (DH) Schlüsselaustausch. Sobald der Transponder in die Reichweite des Reader kommt startet der Schlüsselaustausch. Nun muss der Angreifer den Kanal stören und mit beiden Kommunikationspartnern eine eigene Verbindung aufbauen. Dazu sendet der Angreifer einen eigenen Träger. Bis hierhin hat der Angriff funktioniert. Der Reader kann allerdings in der Lage sein, den zweiten Träger des Angreifers über seine Empfangsstufe zu detektieren. An dieser Stelle wird der Angriff vom Reader erkannt und bricht den Schlüsselaustausch ab.

Somit ist NFC gegen den Man-In-The-Middle Angriff, bei richtigem Einsatz resistent. [4, S. 6f]

5.8 Relay-Angriff

Ziel des Relay-Angriffs ist es, die Kommunikation zwischen Reader und Transponder herzustellen ohne den Transponder in die Lesereichweite des Readers zu bringen. Besonders interessant ist dieser Angriff bei Transpondern, die nicht kopierbar sind. [10]

5.8.1 Relayangriff durch elektrische Verlängerung. Die wohl einfachste Methode ist die elektrische Verlängerung. Hierzu werden zwei Spulen (Rahmenantennen), wie in Abbildung 12 gezeigt, über eine Leitung elektrisch miteinander verbunden. Die eine Antenne wird in die Reichweite des Readers gebracht und die andere Antenne in die direkte Nähe des Transponders.

Aber wie kann mit diesem kabelgebundenen Aufbau ein Angriff stattfinden? Ein denkbares Szenario ist, sich hiermit an einem mit NFC gesichertem Zugang Zutritt zu verschaffen. Angenommen, ein zutrittsberechtigter Mitarbeiter eines Unternehmens trägt seinen NFC-Betriebsausweis offen am Hosenbund und macht neben einem gesicherten Zugang eine Raucherpause. Der Angreifer befestigt sich die Antennen an den Händen (z.B. in Handschuhe eingenäht). Die Antennen sind durch die Jacke des Angreifers mit einer Leitung verbunden. Eine Hand legt er auf das Lesegerät und die andere Hand führt er in einem kurzen Schwung am offen getragenen Betriebsausweis vorbei. Die elektrisch gekoppelten Antennen des Angreifers ”verlängern” das induktive Feld des Readers zum offen getragenen Betriebsausweis. Die Kommunikation findet statt und der Zugang wird freigegeben.

5.8.2 Relayangriff mit Mobiltelefonen. Wenn ein Relay-Angriff kabellos durchgeführt werden soll, muss das elektrische Signal über eine Funktechnik übertragen werden. Maass et al. haben hierzu zwei auf Android basierende Mobiltelefone verwendet, die mit NFC Hardware ausgestattet waren. Eine Herausforderung war die Fälschung der Unique Identifier (UID) des NFC-Chips. Die UID ist bei

[10] Smartcards mit sicherer integrierter Verschlüsselung

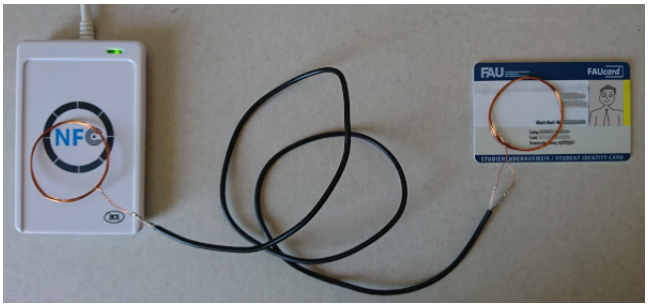

Abbildung 12: Einfacher Relay-Angriff

handelsüblichen Transpondern fest vergeben und kann nicht geändert werden. Die UID wird häufig vom Reader zur Identifikation des Transponders herangezogen. Sie verschafften sich Rootzugriff und konnten dann direkt mit den NFC Treiberbibliotheken interagieren. Das ermöglichte das direkte Konfigurieren des NFC-Chips und dadurch auch das Setzen der UID [8]

Ein Mobiltelefon wurde für den Readermodus konfiguriert und das andere im Transpondermodus. Die Übertragung zwischen den Telefonen kann auf verschiedenen Wegen, wie Bluetooth oder Wlan [11], realisiert werden.[8]

Ein Problem ist die Latenz von einigen Millisekunden, bedingt hauptsächlich durch die Übertragung zwischen den Mobiltelefonen. Dadurch ist es dem Reader technisch möglich diesen Relay-Angriff zu detektieren.[8]

Die Applikation ist auf GitHub [12] gehostet.

5.9 Fälschen von Transpondern

Das Fälschen oder Klonen ist bei einfachen (nur permanenter Speicher) Transpondern, folgend Tag genannt, mit geeigneter Technik, wie zum Beispiel mit dem USB-Reader ACR122 und einigen Software-Tools, möglich.

Die Identität eines handelsüblichen Tags wird anhand einer unveränderbaren UID auf dem Tag gespeichert. Da diese UID vom Reader oft als Identitätsmerkmal verwendet wird, muss neben den inhaltlichen Daten auch die UID des Klons mit der des Originals übereinstimmen. Zu diesem Zweck gibt es die so genannten "Magic Chinese Cards". Bei diesen Karten kann über einen speziellen Befehl die UID beliebig angepasst werden.

Aber auch hier gibt es eine Möglichkeit, wie der Reader solche Kopien erkennen kann. Der Reader versucht, den Befehl zur Änderung UID auf dem Tag auszuführen. Sollte der Befehl erfolgreich ausgeführt werden, kann der Reader die Karte als gefälscht einstufen. [6, 23:00]

6 ZUSAMMENFASSUNG

Wir haben die Grundlagen der von NFC genutzten RFID-Kommunikationsschnittstelle kennengelernt und können nun auch nachvollziehen warum NFC nur, wie der Name schon sagt, im Nahfeld von wenigen Zentimetern funktioniert.

Das Mithören aus größerer Entfernung ist mit einem entsprechend qualitativen Equipment durchaus möglich. NFC ist robust gegen Man-In-The-Middle Angriffe. Somit kann zwischen den Kommunikationspartnern ein sicherer Kanal aufgebaut werden. Abgehörte Daten sind dann nutzlos.

Die gezielte Manipultaion der Kommunikation ist nur bedingt möglich, da der Reader den Träger des Angreifers detektieren kann.

Ein Relay-Angriff kann leitungsgebunden mit einfachsten Mitteln durchgeführt werden. Um größere Distanzen zu überbrücken kann aktive Technik, wie ein NFC fähiges Mobiltelefon, eingesetzt werden. Durch die daraus resultierenden erhöhten Laufzeiten ist auch dieser Angriff detektierbar.

Gegen das unerlaubte Auslesen kann man sich durch eine metallische Abschirmung, wie zum Beispiel eine Metallhülle, schützen.

Einfache Speicher-Tags können kopiert werden. Sogar die UID kann auf speziellen Tags verändert werden. Ein Reader, der dies testet, kann solche speziellen Tags jedoch erkennen.

Die NFC-Technologie ist durchaus als eine Technologie mit hohem Sicherheitsniveau einzustufen.

Wie bei vielen Sicherheitsthemen in der Informatik spielt auch hier die richtige Implementierung und Anwendung eine große Rolle.

Um die Technik vollumfänglich zu beherrschen ist ein fundiertes Fachwissen der Elektrotechnik (HF-Technik, EMV), der Informatik bis hin zur Kryptographie notwendig. NFC hat sich in den vergangenen Jahren zu einem komplexen und interdisziplinären Fachgebiet entwickelt. [1, S. 1]

LITERATUR

[1] Klaus Finkenzeller. 2015. *RFID-Handbuch: Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC* (7 ed.). Hanser, München. DOI: http://dx.doi.org/10.3139/9783446444393

[2] Tim Grießhammer. 2017. Entwicklung einer NFC-Antennenanpassung mit kopplungsabhängiger Leistungsregelung. (2017).

[3] Willibald A Günthner, Julia Boppert, and Michael Schedlbauer. 2005. RFID–Es funkt gewaltig. *Zukunft im Brennpunkt* 04 (2005), 25–30.

[4] Ernst Haselsteiner and Philips Semiconductors. 2006. Security in Near Field Communication (NFC). *Workshop on RFID Security* (01 2006).

[5] Heuck Klaus. 2013. *Elektrische Energieversorgung* -. Springer-Verlag, Berlin Heidelberg New York.

[6] G. Klostermeier. 2018. RFID/NFC-Grundlagen - A Pentesters Perspective. (2018). https://www.youtube.com/watch?v=06nal8BuB2w&t=1779s

[7] Josef Langer and Michael Roland. 2010. *Anwendungen und Technik von Near Field Communication (NFC).* DOI: http://dx.doi.org/10.1007/978-3-642-05497-6

[8] Max Jakob Maaß, Uwe Müller, Tom Schons, Daniel Wegemer, and Matthias Schulz. 2015. NFCGate - An NFC Relay Application for Android. In *Proceedings of the 8th ACM Conference on Security \& Privacy in Wireless and Mobile Networks (WiSec).* http://tuprints.ulb.tu-darmstadt.de/5414/

[9] Reinhard Meindl. 2009. NFCIP-1 Security Standard Protects Near Field Communication. *4th ETSI Security Workshop* (01 2009).

[10] NFC-Forum. 2020. NFC Forum 15-Year Position Paper. (1 2020).

[11] Als Direktverbindung oder über das Internet

[12] https://github.com/nfcgate/nfcgate