FH SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES

Mifare DESfire
Eine Analyse der Implementierung

Diplomarbeit

zur Erlangung des Grades eines
Diplom-Wirtschaftsinformatikers (FH)
an der Fachhochschule Schmalkalden
Fakultät Informatik

Prof. Dr. rer. nat. Dietmar Beyer
Dipl. Inform. (FH) Lutz Jügelt

eingereicht von:
Jonas Groß
Matrikelnummer 230466
Josef-Dörflinger-Str. 14
97769 Bad Brückenau

Schmalkalden, den 27. Januar 2012

Kontaktlose Chipkarten erfreuen sich wachsender Beliebtheit. Sie werden nicht nur als Tickets sondern auch für Zugangskontrollen, Bezahlsysteme und weitere sicherheitskritische Anwendungen eingesetzt.

Für diese Einsatzbereich zeigte sich die bis dahin meist verwendete Karte, die Mifare Classic, als unzureichend gewappnet. Das dort angewandte Verschlüsselungsverfahren wies erhebliche Schwachstellen auf, die es ermöglichen die verwendeten Schlüssel innerhalb kurzer Zeit herauszufinden. Mittlerweile gilt deshalb die Mifare DESFire als sicherer Nachfolger. Ob dieser Ruf gerechtfertig ist, soll in der Arbeit untersucht werden.

Dazu werden die Grundlagen und Bestandteile der Technologie erläutert, um mit diesem Wissen ein Gerät auszuwählen. Mit diesem werden im Anschluss anhand sinnvoll ausgewählter und ausgearbeiteter Angriffe zu getestet, ob kritische Daten auf einer DESFire Karte sicher abgelegt werden können.

Nachfolgende Kapitel bilden die Diplomarbeit:

Kapitel 1 Einführung

Kapitel 2 Analyse

Kapitel 3 Abschluss

Danksagung

An dieser Stelle bedanke ich mich bei *Prof. Dr. rer. nat.Dietmar Beyer*, der mich während meiner Diplomarbeit betreut und unterstützt hat; sowie *Dipl. Inform. (FH) Lutz Jügelt*, der sich als Zweitprüfer zur Verfügung gestellt hat.
Meinen Korrekturlesern, *Kai Trott* und *Volker Zeis*, ein großes Dankeschön für ihre Zeit und ihre Geduld.
Einen besonderen Dank auch an *Marcus Denison*, meinen langjährigen Projektpartner, für seine Unterstützung und die kompetente Beratung bei kritischen Fragen.

Inhaltsverzeichnis

1 Einführung

1.1 Einleitung

RFID (Radio Frequenz Identifikation) beschreibt Techniken, die Daten mit Hilfe von elektromagnetischen Wellen übertragen. Sie dient heutzutage nicht nur rein zur Identifikation, sondern erfüllt vielfältige Aufgaben, die von einfachen Etiketten bis hin zur komplexen Zahl- und Zutrittssystemen reichen. Ihr kontaktloser Charakter vereinfacht und beschleunigt viele Vorgänge. Da dazu weder physischer noch Sichtkontakt notwendig ist, kann nur schwer nachvollzogen werden, was wirklich passiert.
Das Unternehmen NXP hat mit seiner Mifare-Technologie weltweite Verbreitung auch in sicherheitskritischen Bereichen errreicht. Doch ist das gerechtfertigt? Ermöglicht eine solche Technologie nicht vor allem unsichtbare Angriffe?
Diese Arbeit soll sich mit der Sicherheit dieser Technik am Beispiel des Mifare DESFire IC(Integrated Circuit) beschäftigen.

1.1.1 Motivation

Schon vor über 100 Jahren erkannte Auguste Kerckhoffs, dass bei einem Verschlüsselungsverfahren die Sicherheit der Informationen nur von der Geheimhaltung des Schlüssels abhängen darf (vergleiche [Sch06], S. 6). Dass dieses Prinzip noch heute Gültigkeit besitzt, wurde vielfach bewiesen. Unter anderem als 2008 das bei Mifare Classic RFID-Karten verwendete Verfahren in [Plö08] offengelegt wurde. Durch die Kenntnis des Verschlüsselungsalgorithmus und der internen Abläufe konnten so Angriffe entwickelt werden, die weder eine Interaktion des Karteninhabers noch direkten physischen Kontakt erfordern, um die kritische Funktionen wie Bezahl- und Zugangskontrollsysteme zu kompromitieren.
Geringe Kosten und die vermeintliche Sicherheit der Karte hatten ihr bis dahin zur Marktführerschaft verholfen, obwohl mit der Mifare DESFire eine etwas teuerere Variante mit offengelegtem Verschlüsselungsverfahren existierte und mit dem Advanced

Encryption Standard selbst für dieses schon seit über einem halben Jahrzehnt ein Nachfolger existierte. Daraufhin wurde mit des DESFire EV1 eine Nachfolgeversion entwickelt, die auch auf längere Sicht als sicher gelten soll.
Doch nicht alle Details der Implementierung sind frei zugänglich und es drängt sich die Frage auf, ob wirklich von den vorherigen Fehlern gelernt wurde oder nur marketingwirksam eine kostenspieligere Kartenvariante an den Mann gebracht werden soll.

1.1.2 Problemstellung

Bisherige Arbeiten haben hauptsächlich die ursprüngliche Variante des Mifare ICs untersucht. Da der DESFire IC auf den gleichen Grundlagen aufbaut, könnte er auch für die gleichen bzw. ähnliche Angriffe anfällig sein.
Um dies zu Überprüfen soll anhand sinnvoller Kriterien ein Testgerät angeschafft werden und soweit damit möglich geprüft werden, ob sich damit bekannte und/oder neue Angriffe verwirklichen lassen.

1.1.3 Ziel der Arbeit

Das Ziel dieser Arbeit ist es zu untersuchen, ob das Gesamtsystem, mit dem der Mifare DESfire IC arbeitet, geeignet ist um sensibele Daten wie Geldbeträge zu verwalten und zusätzliche sicherheitskritische Funktionen, z.B. Zutrittskontrolle und Ausweisfunktionalitäten, zu erfüllen. Dazu soll in einem vernünftigen Maße Aufwand betrieben werden, um an diese Daten zu gelangen bzw. die Funktionalitäten empfindlich zu stören oder sogar zu verhindern.

1.1.4 Abgrenzung

In 1.4 werden die momentan erhältlichen Mifare ICs genauer vorgestellt. Sie basieren alle auf dem ISO 14443 Standard, stellen jedoch andere Sicherheitsanforderungen und arbeiten dem entsprechend unterschiedlich.
Der DESFire IC zielt speziell darauf ab ein hochwertiges eigenständiges System zu verwirklichen, das bekannte und bewährte offene Verschlüsselungssysteme mit dem neuesten Speichersystem kombiniert.
Obwohl er schon einige Jahre auf dem Markt ist und vielfach eingesetzt wird, findet sich noch keine öffentliche Arbeit, die sich explizit mit ihm beschäftigt. Deshalb soll der Fokus dieser Arbeit auf ihm liegen.

1.1.5 Aufbau

Der Aufbau ist dreigeteilt. Im ersten Teil werden die Technologien und Verfahren erläutert, die bei einem DESFire System zum Einsatz kommen, und die verschiedenen ICs von NXP gegenübergestellt mit dem besonderen Focus auf ihre sicherheitsrelevanten Funktionen. Der zweite Abschnitt befasst sich mit der Suche nach einem geeigneten Testgerät und der Durchführung ausgewählter Attacken, um sicherheitsbedenkliche Lücken in der Implementierung zu finden. Dazu werden Anforderungen zur Auswahl der Hardware aufgestellt, die mit Hilfe einer Nutzwertanalyse zur Anschaffung eines Gerätes führen, und dann auch auf die Angriffe angewendet werden. Im letzen Part findet eine Zusammenfassung und Bewertung der gefundenen Erkenntnisse statt.

1.2 Geschichte

Die Geschichte der Mifare ICs(Integrated Circuit) began 1994 mit der Bekanntmachung der Mifare 1k Chipkarte (vergleiche [NXP05]), deren Markteinführung 1996 begann. Schon im darauffolgendem Jahr kam mit der Mifare Pro ein Variante mit 3DES Koprozessor auf den Markt. Ihr 1999 eingeführter Nachfolger Mifare ProX hatte zusätzlich ein kontaktbehaftetes Interface und ein Koprozessor zur Absicherung per Public-Key-Infrastruktur. Mit 50 Millionen ausgelieferten Einheiten wurde diese Karte ein großer kommerzieller Erfolg. Die dabei eingesetzte Übertragungstechnik und das unter anderem verwendete Chipkartenformat wurden in den folgenden 2 Jahren zum ISO 14443 Standard. Weitere auf diesem Standard basierende Versionen verhalfen der Mifare-Technologie im Jahr 2003 zur Marktführerschaft mit einem Marktanteil von 82%. Die Auslieferung der 2002 angekündigten Mifare DESfire startete 2004 gleich in mehreren Ländern bei namhaften Unternehmen, wie z.B. der NASA. Im Jahr 2007 gelang es erstmals die bis dahin geheimgehaltene Verschlüsselung der Übertragung zu analysieren, was in den darauf folgenden Jahren zu mehreren teils wissenschaftlichen Arbeiten zu diesem Thema führte. Die Herstellerfirma NXP richtete daraufhin eine Website([NXP08a]) ein, mittels derer sie ihre Kunden seitdem über weitere Entwicklungen informiert. Parralel dazu wurde die Produktpalette weiter überarbeitet und soll im nächsten Abschnitt vorgestellt werden.

1.3 Technische Grundlagen

In diesem Kapitel werden die grundlegenden Technologien und Normen vorgestellt, deren Zusammenspiel ein DESFire basiertes System ausmachen. Dabei wird mit der ISO Norm als physischer Grundlage begonnen. Deren Übertragungsprotokoll ermöglicht eine Authentifikation mittels der vorgestellten Verschlüsselungsverfahren um letztendlich auf die im Mifare Application Directory gespeicherten Daten zugreifen zu können.

1.3.1 ISO 14443 Norm

Die für kontaktlose Chipkarten zuständige Arbeitsgruppe WG8 der ISO (Internationale Organisation für Normung) veröffentlicht ihre Arbeitsergebnisse auf ihrer Website[1] als FCDs(Final Committee Draft). Diese werden nach der Zustimmung der ISO-Mitgleider als ISO-Norm veröffentlicht. Daher sollten sie technisch der finalen Version entsprechen und dienen für die folgenden Ausführungen als Grundlage[2].
Die ISO 14443 Norm ist eines dieser Ergebnisse und besteht aus vier Teilen, die jeweils spezifische Eckdaten und Abläufe zwischen Chipkarten und Lesegeräten beschreiben. Diese sind ausgelegt für eine Kommunikation mit einer ungefähren Reichweite von sieben bis 15 cm und sind dadurch vom Typ Proximity Coupling. Entsprechend wird für die Karten der Begriff PICC(Proximity Integrated Circuit Card) und für das Lesegerät PCD(Proximity Coupling Device) verwendet.

1.3.1.1 Part 1 - Physical characteristics

Der erste Teil der Norm befasst sich mit den PICCs und deren Eigenschaften. Hierbei wurden als empfohlene physikalische Maximalausmaße für die Antenne 86 mm * 54 mm * 3 mm festgelegt, da diese sich aus dem zweiten Teil der Norm und entsprechenden Testmethoden nach ISO/IEC 10373-6 ergeben. Für weitere physikalische Eigenschaften wird dazu geraten, sich an andere bestehende ISO-Normen wie z.B. ISO/IEC 7810 oder ISO/IEC 15457-1 zu halten. Es soll jedoch sichergestellt werden, dass Materialien und Ausmaße so gewählt werden, dass sie die Funktionsweise im alternierenden 13,56 MHz bei einer Maximalbelastung von 12 A/m für durchschnittlich 30 Sekunden gewährleisten.
Da NXP lediglich die ICs für die PICCs liefert, ist es dem Kunden überlassen welche

[1] http://www.wg8.de/
[2] Als weitere Quellen dient [Fin06], S. 270ff).

Bauform verwendet wird. Daher kann NXP nur Kompatibilität zu den anderen Teilen der Norm garantieren.
Wird die Chipkartenform nicht eingehalten spricht man im Allgemeinen von einem RFID-Tag oder einfach nur Tag.

1.3.1.2 Part 2 - Radio frequency power and signal interface

Dieser Teil der Norm legt die Energieversorgung und die Signalerkennung fest. Dabei wird die PICC durch ein von einem PCD erzeugtem Magnetfeld mit einer Sendefrequenz von 13,56 MHz mit Energie versorgt. Die magnetische Feldstärke muss zwischen 1,5 A/m und 7,5 A/m erreichen. Da für die PICCs keine aktive Stromquelle vorgesehen ist, wird somit bei einem Abstand zum PCD von 0 cm eine Ansprechfeldstärke von 1,5 A/m sichergestellt. Diese sollte bei bekannten Feldstärkeverlauf auch bei 10 cm Entfernung als Minimum zur Verfügung stehen.
Im weiteren Verlauf der Norm wird nun Typ A und Typ B unterschieden. Befindet sich der PCD im Wartezustand(Idle-State), so soll er mittels periodischem Umschalten zwischen beiden Verfahren Polling auf den jeweiligen Kartentyp ermöglichen. Besteht eine Kommunikation mit einer oder mehreren PICCs, darf kein Wechsel des Typs geschehen bis wieder der Wartezustand erreicht wird.

1.3.1.2.1 Typ A Bei dem Typ A kommt als digitale Modulationsart für den Downlink vom PCD zur PICC eine 100% ASK(Amplitude Shift Keying) Modulation mit modifizierter Millercodierung zum Einsatz. Dabei findet die Informationskodierung durch eine Lücke im Spannungsverlauf statt, die zwischen zwei und drei Mikrosekunden anhalten darf um eine ausreichenden Energieversorgung der PICC zu gewährleisten.

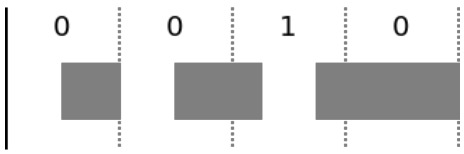


Abbildung 1.1: modifizierte Millercodierung

In umgekehrter Richtung wird durch Ein- und Ausschalten eines Lastwiderstandes, sogenanntes On-/Off-keying, eine Manchestercodierung auf eine Hilfsträgerfrequenz von 847 kHz moduliert.

1.3.1.2.2 Typ B Bei dem Uplink von Typ B wird ebensfalls eine 847 kHz Hilfsträgerfrequenz eingesetzt. Bei der Lastmodulation wird jedoch ein BPSK(Binary Phase Shift Keying) um 180 Grad eingesetzt um die Daten NRZ(Non Return to Zero) codiert zu übertragen.
Bei der Übertragung vom Lesegerät zur Karte wird ebenfalls die NRZ Codierung verwendet. Jedoch wird diese per 10% ASK-Modulation realisiert.

1.3.1.3 Part 3 - Initialization and anticollision

Nachdem die anderen Teile der Spezifikation die physikalischen Rahmenbedingungen festgelegt haben, beginnt in diesem Normteil die logische Weiterverarbeitung. Hierzu müssen PICC und PCD verschiedene Zustände und Verfahren unterstützen, die sich aufgrund der verschiedenen Modulationsverfahren des zweiten Teils der Norm unterscheiden. Gemeinsam ist beiden Typen, dass sie im Falle von Dual-Interface-Karten schon während der Inititalisierungsphase überprüfen müssen, ob sie kontaktbehaftet betrieben werden oder nicht, und dass sie jeweils ein Mechanismus zur Handhabung mehrerer im Sendebereich befindlichen PICCs haben, der letztendlich eine Selektion und Kommunikation mit mindestens einer der Karten ermöglicht.
Das Folgende bezieht sich auf den kontaktlosen Betrieb.

1.3.1.3.1 Typ A Um die logische Verarbeitung durch zu führen, muss zu erst einem Freqenzgang ein Wert zugewiesen werden. Dazu bestimmt sich eine etu(elementary time unit) mittels einem Divisor D durch die Formel:

$$128 = (D \quad fc) \tag{1.3.1}$$

Wobei fc die Feldfrequenz von 13,56 MHz ist und D die Werte 1, 2, 4 und 8 annehmen kann. Innerhalb der etu wird ein Bit übertragen. Daraus resultieren die möglichen Bitraten von 106, 212, 424 und 848 kBits/s[3]. Allerdings ist nur D = 1 gefordert und muss während der Initialisierungs- und Antikollisionsphase eingehalten werden. Die anderen Geschwindigkeiten können erst danach mittels einem Befehl aus dem ISO 14443 Part 4 eingestellt werden.
Darüber hinaus wird die Zeiteinteilung bei der synchronen Kommunikation zwischen PCD und PICC bestimmt. Zwischen den Nachrichten ist in Richtung von PCD zu

[3] z.B. aus D = 2 resultierende Bitrate: $1s = (128 = (2 \quad 13560000s^{-1})) = 211875etu \quad 212kBit/s$

PICC für jede Geschwindigkeit und jedes letzte Bit genau festgelegt, wie lange das Feld mindestens unmoduliert bleiben soll, bevor weitere Signale gesendet werden dürfen. Im Gegensatz dazu ist die unmodulierte Zeit in der Gegenrichtung fest auf $1172/f_c$ gesetzt. Einen Spezialfall stellen das REQA- und WUPA-Kommando dar. Sie dürfen nur mit einer Mindestpause von $7000/f_c$ auf einander bzw. sich selbst folgen.
Bei PICCs des Typs A gibt es neben dem „ausgeschalteten“ Zustand außerhalb eines Feldes noch die folgenden Zustände:

IDLE

READY

HALT

Selected

Active

Zwischen diesen kann der PCD mit folgenden Befehlen wechseln:

REQA

AC(ANTICOLLISION)

SEL

HLTA

WUPA

Im folgenden wird nun die Zustandstransitionen mit ihren Kommandos erläutert.
Sobald die Karte in das Feld des PCDs kommt, wird sie mit Energie versorgt. Das startet eine Initialisierungsphase. Nach deren erfolgreichem Abschluss befindet sich die PICC in dem IDLE-State. In diesem darf sie nur auf das REQA-Kommando reagieren um eventuell bestehende Kommunikation mit anderen Karten nicht zu unterbrechen. Dazu unterscheidet das Kommando sich von der restlichen Kommunikation, in dem es aus lediglich sieben Datenbits[4] besteht. Wird es ausgesandt, muss die PICC

[4] Einzig das WUPA Kommando besteht auch aus 7 Bit. Es überführt aber aus den HALT-State in den READY-State.

innerhalb von 5 ms mit einem Standard-Frame, der einen ATQA-Block enthält, antworten. Der Block besteht aus zwei Byte und deren jeweiligen Paritätsbits und dient zur Identifikation der Kartenart. Eine entsprechende Übersicht der MIFARE-Karten findet sich unter [NXP09e] auf Seite 10. Nach dem Versenden des ATQAs geht die PICC in den READY-State.
Sind mehrere PICCs im Sende-/Empfangsbereich und antworten diese mit unterschiedlichen Binärfolgen, so kann es bereits in diesem Schritt zu Kollisionen kommen. Diese entstehen bei der manchester-kodierten Übertragung dann, wenn aufgrund unterschiedlicher Binärwerte über den gesamten Takt Last auf das Feld moduliert wird. Somit ist kein eindeutiger Wert erkennbar. Das wird jedoch durch das nun folgende Antikollisionsverfahren abgefangen.

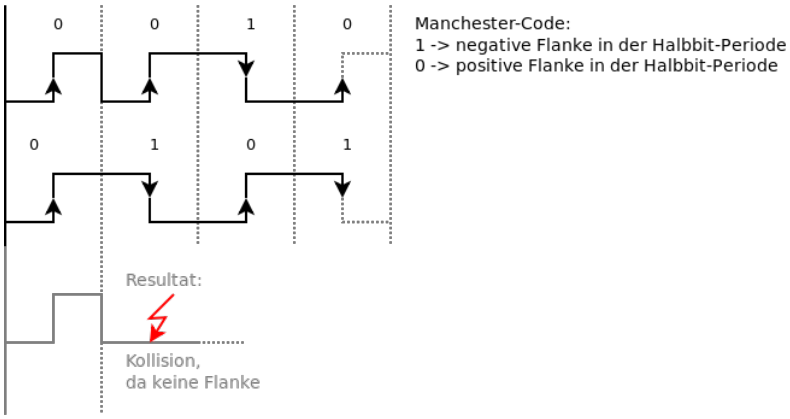


Abbildung 1.2: Kollisionsbeispiel: Manchester-Kodierung

Im READY-State wartet die Karte auf ein ANTICOLLISION-Kommando. Mit Hilfe dieses Kommandos wird ein Binary-Search-Tree-Algorithmus durchlaufen, mittels dessen anhand der UID(Unique Identifier) eine PICC selektiert wird.

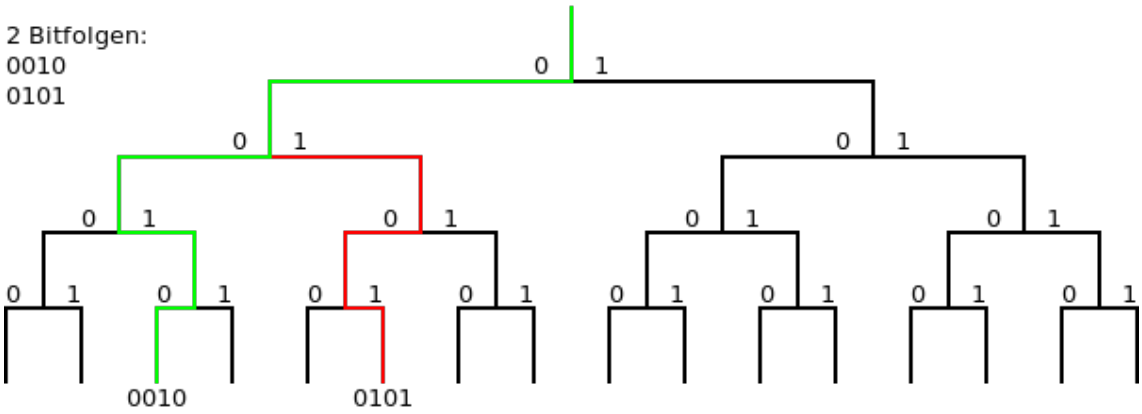


Abbildung 1.3: Kollisionsbeispiel: Binary-Tree-Walk

Da die Norm für UIDs die Längen 4(single-size), 7(double-size) und 10 (triple-size) Byte vorsieht, gibt es die entsprechenden Cascade-Level CL1, CL2 und CL3. Das Verfahren startet immer im CL1. Dazu beinhaltet die vom PCD gesendete Bitfolge sieben Byte. Das erste ist das SEL Byte und enthält je nach Cascade-Level die Bitfolgen 0x93(CL1), 0x95(CL2) oder 0x97(CL3). Im darauffolgendem NVB(Number of valid bits) Byte wird die Länge der schon erkannten und selektierten Bits angegeben. Stellt man dieses Byte hexadezimal dar, so entspricht die erste Zahl der Bytes und die zweite der Bits, ab denen der Suchalgorithmus fortfahren soll. Da das SEL und das NVB Byte selbst mit gezählt werden, kann es Werte zwischen 0x20 und 0x70 annehmen. Das Maximum kommt durch die Länge des nun folgenden UID Teils zustande. Dieser besteht aufgrund der single-size UIDs aus vier Bytes, die als erstes Byte nicht den Wert 0x88 beinhalten dürfen, da dieser als CT(Cascade Tag) dient. Kommt der Wert als erstes Byte vor, können nur die jeweils nächsten drei Byte der UID folgen. Danach wird jedoch immer ein Byte BCC(Block Check Character) angehängt, welcher per Exklusiv-Oder-Verknüpfung über die vorigen vier Byte berechnet wird. Das Cascade-Level wird erhöht, wenn das CT gesetzt ist und die folgenden UID-Byte eindeutig ermittelt wurden. Hierbei steht das NVB auf 0x70 und in diesem Fall entsteht aus dem ANTICOLLISION-Kommando durch Anhängen eines zwei Byte langen CRC_A(Cyclic Redundancy Check error detection code, Type A) das SELECT-Kommando. Die Berechnung des CRC_A geschieht nach ISO/IEC 13239, allerdings wird 6363 als Startwert verwendet und auf die Invertierung nach der Berechnung wird verzichtet.

Die PICC antwortet auf ein ANTICOLLISION-Kommando indem sie entsprechend

dem aktuellen Kaskadelevel 4 Byte ihrer UID oder das CT und 3 Byte der UID gefolgt von einen Byte BCC sendet. Bei einem SELECT-Kommando verschickt sie ein SAK(Select acknowledge). Die Bestandteile des SAK sind ein SAK Byte und der zweit Byte lange CRC_A. Aus der Bitfolge des SAK ist erkennbar, ob die UID komplett ist und ob die PICC der ISO 14443 Part 4 Norm entspricht. Ist die UID noch nicht komplett, wird das Kaskadelevel erhöht und mindestens ein weiterer Durchlauf mit dem ANTICOLLISION-Kommando folgt. Falls eine vollständig erkannte UID signalisiert wird geht die PICC in den Selected-Zustand über und ist für weitere Kommunikation bereit. Findet diese statt, ist die PICC im ACTIVE-Zustand.
Passiert ein Fehler oder empfängt die PICC ein HALT-Kommando, so geht sie in den HALT-State. Aus diesem kann sie nur per WUPA(Wake-UP Befehl vom Typ A)-Kommando in den READY-State übergehen. Wie das REQA-Kommando besteht auch das WUPA-Kommando aus 7 Datenbits, deren Versand alle PICCs im Feld aktiviert und einen erneuten Antikollisionsloop anstößt. Allerdings wird hier der Wert 0x50 übertragen.

1.3.1.3.2 Typ B Auch bei Typ B geht die PICC nach dem Eintritt in das elektromagnetische Feld und erfolgreicher Initialisierung in einen IDLE-Zustand. Allerdings wird hier schon während der Initialisierung ein vier Byte langer PUPI(Pseudo-Unique PICC Identifier, Typ B) generiert und das nun folgende REQB(REQuest Kommando vom Typ B) enthält zusätzliche Parameter um im anschließenden Slotted-ALOHA-Verfahren die Anwendungsfamilie einzugrenzen und die Anzahl der verfügbaren Slots bekannt zu geben. Im Zuge der damit verwirklichten Antikollision werden ähnlich dem Typ A verschiedene Zustände mit ähnlichen Befehlen durchlaufen bis letztendlich die Kommunikation nach ISO 14443 Part 4 zustande kommt[5]. Dabei werden alle nötigen Daten für eine spätere Protokollaktivierung bereits übertragen und entsprechende Einstellungen vorgenommen.
Die verwendeten Zeitintervalle unterscheiden sich stark vom Typ A, sind jedoch detailliert festgelegt.

1.3.1.4 Part 4 - Transmission protocols

Dieser Teil der Norm dient dazu den Transfer von APDUs(application protocol data unit) nach ISO 7816-4 Protokol T=1 zu ermöglichen und einen störungsfreien Be-

[5]Dies wird jedoch keiner genaueren Betrachtung unterzogen, da bei der Mifare DESfire Typ A verwendet wird.

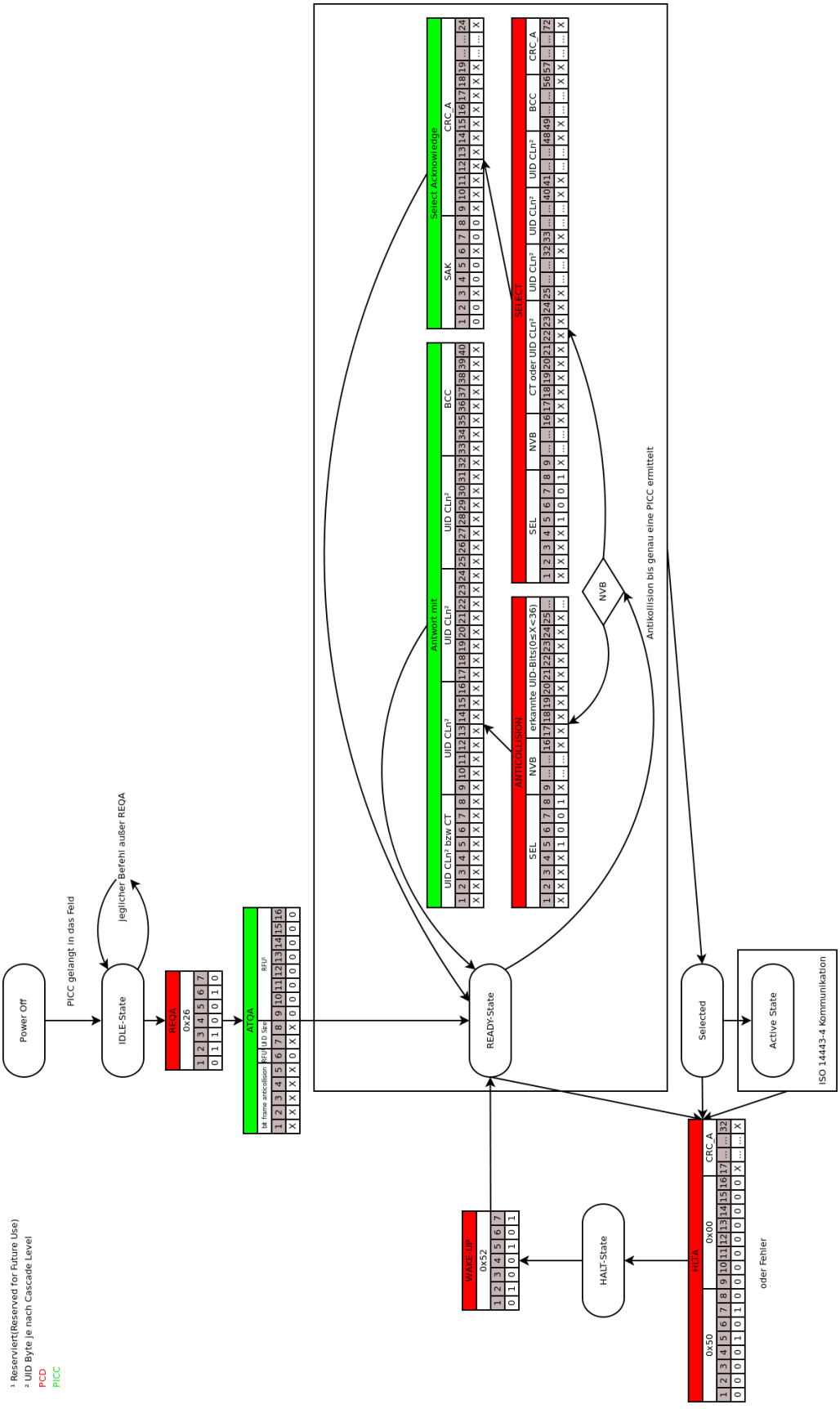


Abbildung 1.4: ISO 14443 3 A Diagramm

trieb zu ermöglichen, auch wenn sich andere PICCs nach ISO 10536 und 15693 im gleichen Feld befinden. Dazu benötigt man im Betrieb nach Typ A weitere Befehlsfolgen. Auf diese wird folgend eingegangen.
Wenn die ISO 14443 Part 4 Kompatibilität mittels des SAK bestätigt worden ist, folgt das RATS(Request for Answer To Select)-Kommando, in dem der selectierten PICC ein CID(Card IDentifier) mit ganzzahligen Werten zwischen 0 und 14 zugewiesen und die maximale Bitfolgengröße des PCDs mitgeteilt wird. Daraufhin sendet die PICC die ATS(Answer To Select). Da noch nicht bekannt ist, welche Protokollmerkmale unterstützt werden, beginnt die ATS mit einem Byte für die Länge, gefolgt von dem Format Byte. Dieses kodiert die maximale Binärfolgenlänge, die die PICC verarbeiten kann, und hat noch drei Bit die für weitere Fähigkeiten der PICC stehen. Je nachdem ob sie gesetzt sind oder nicht folgen entsprechend drei Byte mit weiteren Informationen. Das erste Byte beschreibt die Divisoren D für die beiden Kommunikationsrichtungen, das zweite die Wartezeiten zwischen Nachrichten und das dritte Unterstützung für CID und NAD(Node ADdress). Den Abschluss bilden die Historical Bytes. Sie übertragen Inhalte nach ISO 7816-4 und zwei Byte CRC.
Falls die ATS veränderbare Werte signalisiert, können diese als nächstes per Protocol and parameter selection response modifiziert werden. Dazu wird ein vier bis fünf Byte langer Request gesendet. Dieser beginnt mit dem PPSS(Protocol and Parameter Selection Start) Byte, in dem die Bitfolge 1101 die PPS(Protocol and Parameter Selection) als Erkennungsmarke dient und die restlichen Bits die CID der PICC haben. Die Bits des zweiten Bytes sind bis auf Bit fünf festgelegt und dieses eine dient nur als Ankündigung für das nächste Byte. Im optionalen dritten Byte werden der Karte die Divisoren für die Geschwindigkeiten der beiden Übertragungsrichtungen mitgeteilt. Am Ende folgen dann noch zwei Byte CRC. Als Antwort schickt die PICC nur das PPSS und die zugehörigen CRC-Bytes. Wie auf mögliche Fehlerfälle reagiert werden soll, ist auch genau festgelegt. Tritt jedoch kein Fehler auf, so ist die Protokollaushandlung für den Typ A hiermit abgeschlossen.
Stehen alle Parameter fest, kann eine synchrone wechselseitige Datenübermittlung durchgeführt werden. Hierfür stellt die ISO 14443 Norm drei Block Formate zur Verfügung. Allen gemeinsam ist, dass sie aus Prolog-, Informations und Epilogfeld bestehen, wobei das Informationsfeld optional ist. Den Epilog bildet die CRC-Checksumme je nach Typ und der Prolog enthält ein PCB(Protocol Control Byte) und optional Bytes für die CID und die NAD.

Prologfeld			Informationsfeld	Epilogfeld
PCB	(CID)	(NAD)	(INF)	EDC
1 Byte	1 Byte	1 Byte		2 Bytes

Tabelle 1.1: ISO 14443-4: allgemeines Blockformat

Die einfachsten Blöcke sind R-Blöcke. Sie enthalten kein Informationsfeld und geben im PCB eine positive oder negative Bestätigung zu dem letzten empfangenen Block. Die S-Blöcke werden für Kontrolinformationen genutzt. Dies kann die Deselektion einer PICC sein, die Verlängerung der Wartezeiten zwischen der Datenübertragung oder zum Auslesen der Stromversorgung der PICC genutzt werden.
Die dritte Art von Blöcken sind die I-Blöcke. Mit ihnen werden die APDUs übertragen. Dazu stellen sie zwei besondere Fähigkeiten zur Verfügung. Die eine ist Multi-Activation, mit der mehrere PICCs[6] gleichzeitig im ACTIVE-Zustand gehalten werden können und somit eine schnelle Umschaltung[7] ermöglicht wird. Die andere ist das Chaining. Es ermöglicht die Aufteilung von APDUs in mehrere Blöcke die nacheinander gesendet werden.
Der letzte Teil der Norm stellt einige Regeln zur Steuerung der Kommunikation und zur Fehlerbehandlung auf. Erwähnenswert erscheint noch, dass die PICC mit dem Bestätigen eines Deselektionsbefehls ihre CID freigibt.

1.3.2 Verschlüsselungsverfahren

In seiner ursprünglichen Version unterstützte der DESFire IC nur den Data Encryption Standard. Später kam der Advanced Encryption Standard hinzu. Im folgenden werden beide Verfahren vorgestellt.

1.3.2.1 Geschichte

Kryptographie diente bis Anfang der 1970ger hauptsächlich zur militärischen Kommunikation. Doch mit der zunehmenden Verbreitung der Informationstechnik wurde die Verschlüsselung sensibler Daten und sichere Authentifikation immer wichtiger. Deshalb startete das NIST 1973 eine öffentliche Ausschreibung für einen Algorithmus, der fortan als standardisiertes Verschlüsselungsverfahren zum Einsatz kommen sollte. Qualifizierte Einsendung blieben aber aus und so wurde ein Jahr später eine

[6] Die Adressierung über die CID erlaubt maximal 15 PICCs.
[7] Also ohne Deaktivierung und/oder Antikollisionsdurchlauf.

zweite Ausschreibung zu diesem Thema veröffentlicht. Auf diese reichte IBM einen Algorithmus ein, der von der NSA(National Security Agency) geprüft und akzeptiert wurde. Im nächsten Schritt wurde um eine Stellungnahme der Öffentlichkeit gebeten. Diese kritisierte zwar die undurchsichtige Rolle der NSA, aber fand keine entscheidenden Gegenargumente, so dass der Algorithmus am 15.06.1977 als Teil des Data-Encryption-Standard veröffentlicht wurde. Der Standard beinhaltete als weitere wesentliche Punkte unter anderem die Zertifizierung der DES-Implementationen durch das NIST und eine Überprüfung alle fünf Jahre. In den folgenden Jahren erkannte auch das ANSI(American National Standards Institute) den DES an und es wurden weitere Standards, vor allem bei Finanztransaktionen und in der Telekommunikation, entwickelt, die DES als Grundlage benutzten. Bis zum Jahr 1994 stand der weiteren Zertifizierung des Standard nichts entgegen. Doch in diesem Jahre wurde der DES mit zwölf HP-9735-Workstations innerhalb vom 50 Tagen zum ersten Mal offiziel gebrochen. Zwei Jahre später reagierte das NIST mit der Suche eines Nachfolgers. Dieser sollte als Advanced Encryption Standard Schlüssellängen von 128, 192 und 256 Bit unterstützen. Erst nachdem die EFF(Electronic Frontier Foundation) 1998 einen neuen Rekord aufstellte, indem sie die Schlüsselsuche mit einem Spezialchip in nur 3 Tagen bewältigte, stellte das NIST die 15 AES-Kandidaten vor, von denen fünf 1999 in das Finale kamen. Bis zum 15.5.2000 wurde der Öffentlichkeit die Möglichkeit gegeben Kommentare abzugeben und am 2.10.2000 der Gewinner bekannt gegeben. Auch hierzu wurde der Allgemeinheit Zeit gegeben um Kritikpunkte vorzubringen. Letztendlich wurde der Algorithmus Rijndael im Dezember 2001 zum offiziellen Standard erklärt und ist seit dem 26.05.2002 in Kraft(vergleiche [Ert07], S. 60 und [Ert07], S. 70).
Bis heute wurden verschiedene Rekorde in der DES-Schlüsselsuche aufgestellt und man kann relativ günstige Rechenmaschinen kaufen, die dies in weniger als einem Tag erledigen(vergleiche [sci10]). Um die Schlüsselsuche zu erschweren wird vielfach Triple-DES[8] eingesetzt. Hierbei wird DES mit zwei verschiedenen Schlüsseln dreimal hintereinander angewendet nach folgendem Muster(vergleiche [Ert07], S. 68):

$$\mathbf{C} = \mathbf{E}_{\mathbf{K}_1}(\mathbf{D}_{\mathbf{K}_2}(\mathbf{E}_{\mathbf{K}_1}(\mathbf{M}))) \tag{1.3.2}$$

Für das NIST ist diese Methode nur noch sicher genug, um bis Ende dieses Jahres an-

[8] Oft auch als 3DES abgekürzt.

gewandt zu werden. Danach sollte 3TDEA[9] angewandt werden(vergleiche [PDB10], S. 9f). Dabei werden drei unterschiedliche Schlüssel für die einzelnen Schritte des 3DES eingesetzt. Die Mifare DESfire unterstützt alle der erwähnten Verfahren[10].

1.3.2.2 Data Encryption Standard

Der DES ist symmetrischer Blockchiffre. Diese Art der Verschlüsselung unterteilt den Klartext in Blöcke festgelegter Länge und verschlüsselt sowie entschlüsselt sie mit dem gleichen Schlüssel.
Dabei wird Konfusion und Diffusion angestrebt, um die Zuordnung eines Teiles des Klartextes zu einem Chiffreteil zu erschweren. In diesem Kontext bedeutet Konfusion eine möglichst große Zerstreuung der Klartextzeichen innerhalb des Chiffres um so gut wie möglich Zufallszahlen zu ähneln. Diffusion ist die Verteilung der Klartextzeichen auf eine hohe Anzahl an Chiffrebits. Der DES arbeitet dazu mit Blocklängen von 64 Bit für Klar- sowie Chiffretext.
Auch bei dem Schlüssel kommt diese Bitlänge zum Einsatz, allerdings werden davon 8 Bits[11] zum Paritätscheck während der Schlüsselaufbereitung benutzt und erfüllen somit keine kryptografische Funktion (vergleiche [Ert07], S. 58ff).
Sie haben lediglich eine Kontrollfunktion um die Richtigkeit der Übertragung zu gewährleisten oder gegebenenfalls mit einer Fehlermeldung abzubrechen. Somit bleiben 56 Bit übrig, die in zwei Hälften zu je 28 Bit zerlegt werden. In Laufe der 16 Runden des DES werden auf diesen Hälften abhängig vom Rundenindex festgelegte Bitverschiebungen durchgeführt. Nach der jeweiligen Verschiebung werden 48 Bit ausgewählt und einer Kompressionspermutation unterzogen. Dadurch wird in jedem Teilschlüssel eine unterschiedliche Teilmenge des Schlüssels verwendet.
Auch der zu verschlüsselnde Text wird geteilt. Allerdings erst nach einer Eingangspermutation. Anschließend durchlaufen beide 32 Bit Hälften die 16 Runden. In diesen wird zu allererst die eine Hälfte zwischengespeichert und danach auf ihr eine Expansionspermutation ausgeführt, die die 32 Bit auf 48 Bit verteilt und somit einen Lawineneffekt verwirklicht. Danach wird das Ergebnis mit dem jeweiligen Rundenschlüssel XOR-verknüpft und macht dadurch Chiffrat vom Schlüssel abhängig. In der darauffolgenden S-Box-Substitution werden die 48 Bit in 6 Bit Blöcke zerlegt. Diese werden benutzt, um daraus die Adressierung in vorgegebenen Matrizen[12] abzulei-

[9] Wird auch als 3KDES oder 3K3DES bezeichnet.
[10] Diese sind: DES, 3DES, 3KDES und AES.
[11] Das letzte Bit pro Byte(vergleiche [Sch06], S. 318).
[12] Den sogenannten S-Boxen.

ten. Diese Operation ist dank der S-Boxen nicht linear und somit hauptsächlich für die Sicherheit des Algorithmus verantwortlich. Weitere Konfusion geschieht anschließend per P-Box-Permutation. Diese ordnet die entstandene Bitfolgen ein weiteres mal nach einem festen Muster um. Nach ihrem Abschluss wird das Ergebnis mit dem Zwischengespeichertem der vorherigen Runde XOR-verknüpft und schließt damit die aktuelle Runde ab.
Nach dem letzten Rundendurchlauf findet die Schlußpermutation statt. Sie ist zur Eingangspermutation invers und damit kryptografisch nicht relevant, allerdings kann sie dazu dienen, Klar- bzw Chiffretext byteweise in die entsprechende Hardware zu laden.

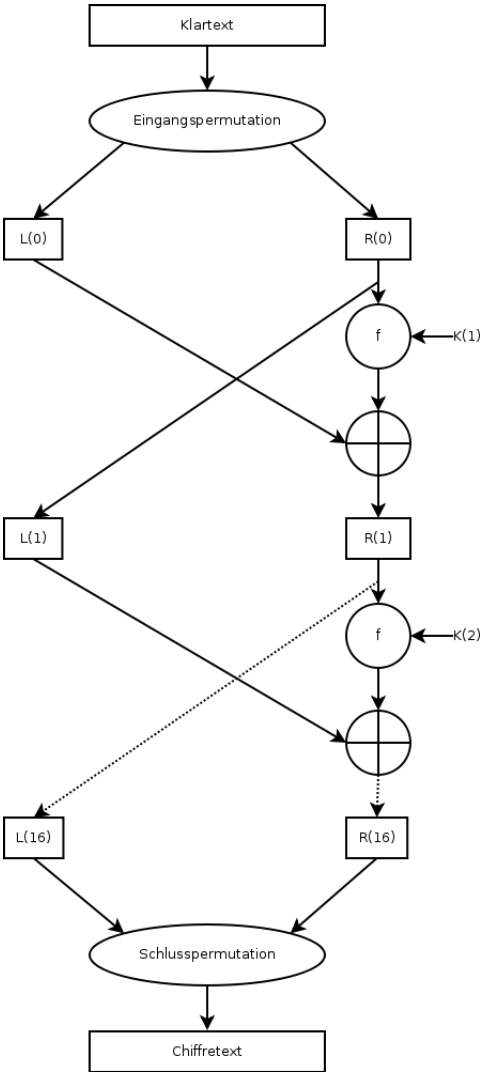


Abbildung 1.5: DES-Runden

Sämtliche vorgegebenen Werte und Berechnung sind so gewählt, dass für die Ent-

schlüsslung die gleiche Funktion verwenden kann; man muss nur die einzelnen Teilschlüssel in umgekehrter Reihenfolge anwenden. Somit kommt die Symmetrie zu Stande (vergleiche [Sch06], S. 316ff).

1.3.2.3 Advanced Encryption Standard

Der AES(Advanced Encryption Standard) hat viele Gemeinsamkeiten mit dem DES. Auch er ist ein symmetrische Blockchiffre, der rundenbasiert arbeitet. Allerdings können die Blöcke 128, 192 oder 256 Bit umfassen[13] und die Anzahl der Runden hängt von den gewählten Blockgrößen für Schlüssel und Klartext ab. Innerhalb der Runden findet keine Expansionspermutation, S-Box-Substitution und P-Box-Permutation statt, sondern die Funktionen ByteSub, ShiftRow und MixColumn werden zur Konfusion und Diffussion eingesetzt. Der Teilschlüssel wird erst nach diesen XOR-verknüpft und bei dessen Generierung verläuft die Schlüsselaufbereitung anders. Dabei wird auf Paritätsbits verzichtet.
Alle eingesetzten Funktionen basieren auf einfachen Bit-Operationen und zyklischen Verschiebungen und sind somit effizient in Hardware implementierbar(vergleiche [Ert07], S. 69ff).

1.3.3 Mifare Application Directory

Zum Speichern von Daten kommt bei den Mifare PICCs das MAD(MIFARE Application Directory) zum Einsatz. Dieses gibt es in drei Version, die alle die zu speichernden Daten in sogenannten Applikationen ablegen. Dabei ist die zweite voll kompatibel zur ersten. Der einzige signifikante Unterschied ist die Adressierung von größerem EEPROM (vergleiche [Sem05] und [NXP09b]).

1.3.3.1 MAD Version 1

In der Version 1 und 2 des MAD wird einer Applikation ein Sector zugeteilt. Dieser besteht aus vier Blöcken zu je 16 Byte. In den ersten drei können Daten gespeichert werden, deren 8 Bit umfassende CRC-Checksumme jedesmal im letzten Byte abgelegt wird.
Der jeweils letzte Block heißt Trailer und enthält den Read-key A und den Write-key B. Zwischen den fünf Byte langen Keys wird das GPB(General purpose byte)

[13] Der DESfire IC arbeitet mit 128 Bit Schlüsseln.

und die Zugriffsbedingungen gespeichert. In diesen wird festgelegt, ob die Schlüssel zum Lesen bzw. Beschreiben des Sectors benötigt werden und ob damit bestimmte Mifare-spezifische Funktionen wie z.B. Wertinkrementierung genutzt werden dürfen. Der Sector 0x00 hat einen besonderen Inhalt. Er enthält im ersten Block Herstellerdaten, wie z.B. eine Seriennummer. Der zweite und dritte Block stellen ein Inhaltsverzeichnis dar. Je nachdem an welcher Stelle ein vorgegebener AID(Application identifier) steht, finden sich die zugehörigen Daten im entsprechenden Sector.
Der AID selbst setzt sich aus einem Byte Function Cluster Code und einem weiteren Byte mit dem Application Code zusammen. Anhand des Function Cluster Codes lässt sich eine Zuordnung zu Bereichen wie z.B. Gesundheitswesen, Taxibetrieb, etc. vornehmen. Ein eindeutiger Application Code in Verbindung mit einem Function Cluster Code kann bei NXP registriert werden und gewährleitstet die genaue Zuordnung zu dem beantragenden Unternehmen und die Eintragung in eine allgemeine Datenbank. Die selbstreferenzierden Bytestellen werden mit einer CRC-Checksumme und einem Infofeld gefüllt. Dieses Feld enthält einen Pointer auf einen Sector in dem weitere Informationen zu dem Kartenherausgeber stehen sollten oder 0x00 falls dem Herausgeber keinen Sector dafür benutzt. Das GPB wird hier benutzt um zusätzliche Informationen zur Karte, wie z.B. die MAD Version, zu speichern.

1.3.3.2 MAD Version 2

Bei MAD Version 2 werden in dem Sector 0x10 der erste bis dritte Block für das Verzeichnis genutzt. Das GPB wird für die zukünftige Verwendung freigehalten[14]. Den letzten acht Applikationen stehen 16 Datenblöcke zur Verfügung. Somit kann bis zu 4 KiloByte EEPROM verwaltet werden[15].

[14] Inhalt des GPB soll 0x00 betragen.
[15] 32*4*16+8*16*16 Kilobyte

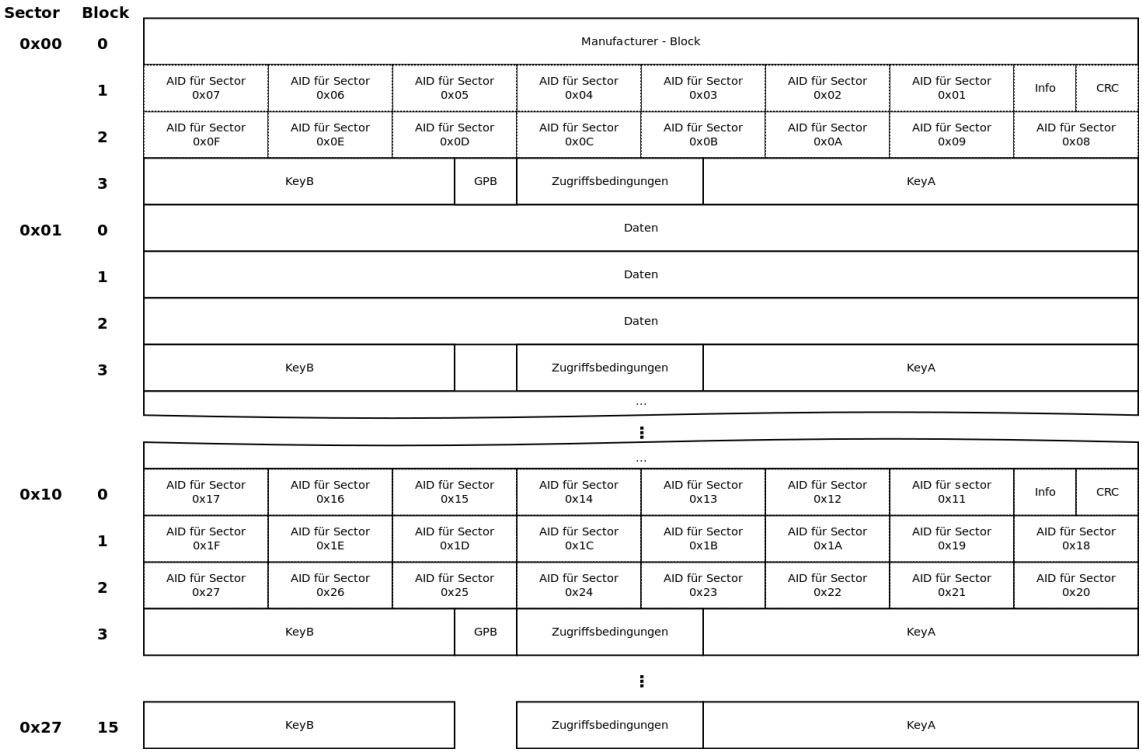


Abbildung 1.6: Grafische Darstellung: Mifare Application Directory Version 2

1.3.3.3 MAD Version 3

Diese grundsätzliche Speicherstruktur in Applikationen ist bei der dritten Version des MAD gleich. Allerding wurde das Applikationsverzeichnis abgeschafft. Der DESFire IC verwaltet automatisch alle abgelegten Daten und gibt deren Speicherstellen mit dem Befehl GetApplicationIDs heraus. Diese haben einen drei Byte langen AID. Um die Kompatibilität mit den beiden anderen Verzeichnisversionen zu bewahren, gibt es eine Reihe von Regeln, die man einhalten muss um letztendlich die MIFARE classic AID mit dem Wert 0xF als Postambel abspeichern zu können. Die ersten zwei Bits werden dann verwendet um 16 „virtuelle“ klassische Applikationsverzeichnisse an zu sprechen.
Insgesamt ist er möglich bis zu 28 verschiedene Applikation mit jeweils bis zu 32 Files im nativen Format zu speichern. Die Größe und der Typ des jeweiligen Files wird bei dessen Erstellung festgelegt. Es stehen fünf Dateitypen zur Verfügung. Diese sind:

Standard Data Files

Backup Data Files

Value Files with Backup

Linear Record Files with Backup

Cyclic Record Files with Backup

Standard Data Files und Backup Data Files könnnen beliebige unformatierte Daten aufnehmen, wobei Backup Data Files auf einen integrierten Mechanismus zur Datensicherung zugreifen und in Transaktionen bearbeitet werden können. Im Gegensatz dazu lassen sich in Value Files nur 32-Bit Ganzzahlen speichern, auf die sich spezielle Funktionen zum Erhöhen und Verringern des Wertes anwenden lassen. Auch das Setzen eines Maximalwertes ist sowohl für den Betrag selbst, als auch für dessen Erhöhung möglich. Die Linear und Cyclic Record Files arbeiten datensatzweise. Läuft der Speicher beim Schreiben eines Linear Cyclic Record voll, muss das gesamte File gelöscht werden. Bei einem Cyclic Record File wird jedoch automatisch der älteste Eintrag überschrieben (vergleiche [NXP09c] und [Sem05]).
Den größten Unterschied zu den Vorversionen stellen jedoch die möglichen Verschlüsselungsvarianten des Datenaustauschs dar. Diese sind:

Unverschlüsselte Datenübertragung

Kommunikation mit MAC(Message Authentication Code)

Vollverschlüsselte Datenübermittlung inklusive CRC.

Je nach verwendetem IC können hier unterschiedliche auf dem DES bzw. seinem Nachfolger AES basierende Verschlüsselungsverfahren zum Einsatz kommen.
Außerdem werden einige Befehle aus dem ISO 7816-4 Standard sowie das dafür notwendige APDU-Wrapping unterstützt. Ob das Wrapping zum Einsatz kommt, wird durch die erste Nachricht nach Durchlaufen des ISO 14443 Standards festgelegt. Hat diese das APDU-Format, so muss es bis zum Verlassen des Feldes beibehalten werden. Das gleiche gilt für das native Format.

1.4 Einordnung in Produktpalette

Das Unternehmen NXP hat momentan fünf verschiedene Typen von Mifare ICs im Angebot, die jeweils in verschiedenen Ausführungen erhältlich sind. Dabei sind alle vollständig ISO/IEC 14443-2 und ISO/IEC 14443-3 kompatibel und unterscheiden

sich hauptsächlich in der Verschlüsselung und der Speicherausstattung (vergleiche [NXP09e]). Deshalb soll bei der nun folgenden Vorstellung der verschiedenen Versionen auf diese beiden Punkte besondere Aufmerksamkeit liegen.

1.4.1 MIFARE Ultralight

Die MIFARE Ultralight ist in zwei Versionen erhältlich. Beide bedienen das untere Preissegment. Die entscheidenden Unterschiede sind jedoch die Verschlüsselung sowie die Größe des Speichers.

Ultralight

Der MIFARE Ultralight IC ist zum Zeitpunkt der Erstellung dieser Arbeit der billigste Chip im NXP-Angebot. Er bietet keine integrierte Verschlüsselung und hat nur 512 Bit EEPROM, das in 16 Seiten mit jeweils 4 Byte aufgeteilt ist. Von diesen 64 Byte sind „32 bit one-time programmable (OTP) area“. Dieser Bereich besteht aus Schaltungen die einmalig von Null auf Eins gesetzt werden können und danach unveränderbar bleiben (vergleiche [B.V10]). Weitere 384 bit sind für wiederbeschreibbare Nutzerdaten bestimmt. Beide Bereich können über spezielle Lock-Bits blockweise(OTP area) bzw. applikationsweise(Nutzerdaten) auf Lesezugriffe eingeschränkt werden.
Außerdem enthält der Chip eine 7 Byte lange UID. Damit soll er hauptsächlich in einer bestehenden MIFARE-Umgebung kostengünstige Einmaltickets ermöglichen, die den Komfort von RFID-Lösungen bieten und somit Papiertickets ablösen (vergleiche [NXP09a]).

Ultralight C

Mit einer 3DES-Hardware-Verschlüsselung und 1536 Bit EEPROM stellt die Variante MIFARE Ultralight C eine kostengünstige, wenn auch geringfügig teuerere, und sicherere Alternative zu der MIFARE Ultralight dar. Sie soll zum einen den Aufwand einer Integration zu einer MIFARE DESfire Umgebung minimieren, zum anderen volle Kompatibilität zu der Ultralight ohne Verschlüsselungsverfahren gewährleisten und dabei die Sicherheit verbessern (vergleiche [NXP09g]).
Dazu werden die 1536 Bit in 48 Seiten mit jeweils 32 Bit aufgeteilt. Darin gibt es einen 512 Bit großen Bereich, der direkt kompatibel zur „einfachen“ Ultralight ist. Er beinhaltet also die OTP area und ist auch ansonsten genauso aufgebaut wie bei der

Ultralight. Der restliche EEPROM beherbergt neben dem zusätzlichen Speicherplatz noch einen 16 bittigen Zähler (vergleiche [NXP09f]).

1.4.2 MIFARE 1K/4K/Mini

Der hier verwendete Chipsatz wird auch als MIFARE classic bezeichnet und ist in Varianten mit 320 Byte, 1 Kilobyte und 4 Kilobyte EEPROM erhältlich. Er unterstützt den Crypto1-Algorithmus, der bereits bei der ersten MIFARE-Generation verwendet wurde. NXP selbst rät aber zur Benutzung von DESFire EV1 und/oder MIFARE Plus, da seit dem 31.12.2007 wirksame Angriffe auf die Karte bekannt sind und selbst mit zusätzlichen Sicherheitsmaßnahmen das Risiko des Clonens einer Karte nicht mehr ausgeschlossen werden kann (vergleiche [NXP08b]).Darüber hinaus ist die enthaltene UID bei den Produktserien bis zur MF1 ICS x007 nur 4 Byte lang [NXP10c]. Damit kann die Eindeutigkeit der UID vorraussichtlich ab Ende 2010 (vergleiche [NXP10b]) nicht mehr gewährleistet werden (vergleiche [NXP10a]). Obwohl die Wahrscheinlichkeit, dass zwei PICCS mit gleicher UID gleichzeitig in Reichweite eines PCDs sind, sehr gering ist, werden die aktuellen Versionen bereits mit einer 7 Byte langen UID ausgeliefert (vergleiche [NXP09e]).

1.4.3 MIFARE Plus

Als sanfte Migrationslösung von einem MIFARE-Umfeld mit Crypto1-Algorithmus zu einer zeitgemäßeren und sichereren Umgebung ist der MIFARE Plus IC gedacht. Er ist in zwei Varianten erhältlich, die sich im Umfang der unterstützten sicherheitsrelevanten Befehle unterscheiden. Beide Versionen sind jeweils mit 2 oder 4 Kilobyte EEPROM erhältlich. Sie bieten zusätzlich zum Crypto1-Algorithmus auch die Möglichkeit die Kommunikation per AES zu verschlüsseln. Des weiteren werden für Migrationszwecke 4 Byte UIDs unterstützt. Somit ist es möglich, solange die „klassische“ Crypto1-Umgebung weiter zu betreiben bis alle Kundenkarten ausgetauscht sind und die Umgebung auf AES vorbereitet ist, um dann einfach umzuschalten ohne den Kunden zu einer speziellen Interaktion zu zwingen (vergleiche [NXP09e] und [NXP09d]).
Diese Umschaltung kann nur von einem niedrigeren zu einem höheren Level vollzogen werden (vergleiche [NXP10e]).
Ausgeliefert wird der Plus IC mit Security Level 0, in dem er voll rückwärts kompatibel zu den Mifare ICs ist, aber auch das ISO 14443 Part 4 Protokoll beherrscht.

Für die höheren Level müssen erst über eine kartenspezifische Funktion bestimmte AES-Schlüssel gespeichert werden, bevor diese aktiviert werden können.
Im Security Level 1 kann zusätzlich zu den „klassischen“ MIFARE Kommandos eine optionale AES-Authentifizierung genutzt werden.
Erst im dritten Security Level ist diese Authentifizierung verpflichtend und aus ihrem Resultat werden die Crypto1-Schlüssel sitzungweise abgeleitet. Zusätzlich zu den Crypto1-Schlüsseln werden für jeden Sector zwei entsprechende AES-Schlüssel verwaltet[16]. Die genauen Zugriffsbedingungen werden weiterhin über den Sector Trailer bestimmt.
Security Level 3 bricht mit der Rückwärtskompatibilität und wickelt die Kommunikation nur noch über das ISO 14443 Part 4 Protocol ab. Dabei werden zwei Sitzungsschlüssel aus einem gemeinsamen Schlüssel und per Zufallsgenerator erzeugten Zahlen von PICC und PCD abgeleitet. Dabei kann einer für die Übertragungsverschlüsselung und der andere als Message Authentication Code zum Einsatz kommen. Ist jedoch höhere Performanz gewünscht, kann der PCD für bestimmte Befehle die MAC-Generierung abschalten oder auch komplett unverschlüsselt arbeiten.

Plus S

Der MIFARE Plus S IC ist die Variante mit geringerer Funktionalität. Sie unterstützt nur die Security Levels 0,1 und 3. Außerdem ist der Befehlssatz an verschiedenen Stellen eingeschränkt, was hauptsachlich die Unterstützung von PICCs mit zufälliger UID und Absicherung von Kommandos mittels MAC betrifft (vergleiche [NXP10f]).

Plus X

Die Plus X Version bietet alle Security Level. Weiterhin können die Kompatibilitätskommandos mittels MAC abgesichert und der volle Befehlssatz zum Umgang mit zufällig generierten UIDs genutzt werden.
Das Herausragende an dem Plus X IC ist die integrierte Möglichkeit einen Entfernungscheck durchzuführen. Dies soll insbesondere Relay-Attacken verhindern (vergleiche [NXP10e] und [NXP09d]).

[16] Sie werden aber erst in Security Level 3 eingesetzt.

1.4.4 MIFARE DESFire

Wie der Name schon andeutet ist das Charakteristikum des MIFARE DESFire IC die DES-Unterstützung per Hardware. Das „Fire“ im Namen steht für „Fast, Innovative, Reliable and Enhanced“[17]. Bei den angegebenen Zielgruppen für diesen Kartentyp listet NXP u.a. Zutrittskontrollen auf (vergleiche [NXP08c]).
Zum Zeitpunkt der Erstellung dieser Arbeit sind zwei Varianten erhältlich.

DESFire

Der „klassische“ MIFARE DESFire IC adressiert ausschließlich 4 KByte EEPROM und unterstützt nur DES und TDES zur Verschlüsselung. Die wesentliche Neuerung war das MAD Version 3 und damit einhergehende Verschlüsselungmöglichkeiten der Übertragung. Diese werden anschließendend im Zusammenhang mit dem Nachfolger DESFire EV1 genauer beleuchtet. Die wesentlichen Unterschiede zwischen den beiden Versionen werden in [Incbe] aufgelistet.

DESFire EV1

Die aktuelle Version MIFARE DESFire EV1 bietet mit 2, 4 oder 8 Kilobyte EEPROM in der größten Version am meisten Speicherplatz unter den verfügbaren MIFARE ICs. Für die sichere Datenübertragung zum Speicher unterstützt sie die Verschlüsselungsverfahren DES, 3DES, 3KDES und AES. Diese werden für die Authentifikation gegenüber dem Tag verwendet. Desweiteren kann die Datenübertragung je nach Einstellung der selektierten Applikation erfolgen. Dafür sind prinzipiell drei verschiedene Verfahren möglich.
Das erste Übertragungsverfahren steht nur im Kompatibilitätsmodus zum Vorgänger zur Verfügung. Dabei werden die Daten komplett unverschlüsselt übertragen.
Die zweite Übertragungsmöglichkeit beinhaltet eine Absicherung mittels kryptografischer Checksummen als MAC. In der Kompatibilitätseinstellung wird hierfür jede Nachricht mit einem vier Byte MAC authentifiziert. Ansonsten wird ein acht Byte langer CMAC(Cipher-based MAC) auf Basis der zur Verfügung stehen Algorithmen verwendet.
Im dritten Übertragungsmechanismus wird ein CRC durchgeführt und dessen Summe anschließend an die Daten angehängt. Das Ergebnis wird dann anhand des ausgewähl-

[17] Zu deutsch etwa: „Schnell, innovativ, zuverlässig und verbessert“.

ten Verfahrens verschlüsselt und schließlich übertragen. Dabei ist die CRC-Summe im Kompatibilitätsmodus 16 und ansonsten 32 Bit lang (vergleiche [NXP09c]).

1.4.5 SmartMX

SmartMX ist ein Smart Card Controller, der es ermöglicht, mit weiteren Komponenten Dual Interface Karten herzustellen, die vollständig ISO/IEC 14443 A kompatibel sind. Er verfügt über eine Mifare-Emulation[18] und unterstützt die Verschlüsselungverfahren 3DES, AES und PKE(Public Key Encryption). Allerdings enthält er kein eigenes Speichersystem. Dieses muss folglich über Zusatzhardware verwirklicht werden. Im Rahmen dieser Arbeit wird dieser Controller keiner weiteren Betrachtung unterzogen (vergleiche [NXP09h]).

1.4.6 Abgrenzung und Zusammenfassung

Wie die Ultralight und classic-Varianten ist der DESfire IC als Komplettsystem für passive Transponderkarten gedacht. Allerdings verzichtet er auf die Kompatibilität zur classic-Variante und stellt das flexibelste fest verbaute Dateisystem zur Verfügung. Mit den Plus- und SmartMX-Versionen teilt er sich die AES-Verschlüsselung[19] und bietet dadurch als einziger IC die modernste Verschlüsselung ohne potentielle Sicherheitslücken durch die classic-Kompatibilität offen zu lassen.
Die wichtigsten Vergleichsdaten werden folgend tabellarisch dargestellt:

[18] Für Mifare 1K und Mifare 4k(vergleiche [Sem10]).
[19] In der EV1-Version.

	Ultralight	1K/4K/ Mini	Plus	DESFire	SmartMX
Ver-schlüs-selung	3DES (C)	Crypto1	Crypto1, AES	3DES, 3KDES(EV1), AES(EV1)	3DES, AES, PKE
Speicher	512 Bit, 1536 Bit(C)	320 Byte, 1 oder 4 Kbytes	2 oder 4 Kbytes	2, 4 oder 8 Kbytes	beliebig
Beson-derhei-ten	OTP area, Counter(C)		Stufenweise Migration		Dual-Interface
MAD Version	speziell	1 bzw 2(4K)	2	3	beliebig
classic kompa-tibel	X	(X)	X		X

Tabelle 1.2: Gegenüberstellung der Mifare ICs

2 Analyse

2.1 Selektion der Hardware

Nachdem im letzten Kapitel eine theoretische Basis geschaffen wurde, besteht der nächste Schritt zur eigentlichen Analyse in der Beschaffung eines geeigneten Testgerätes. Dazu werden im Anschluss Kriterien aufgestellt, an Hand derer die in Frage kommenden Geräte bewertet werden, um das Gerät mit dem größten Nutzwert zu selektieren.

2.1.1 Sichten

Bei dem Aufstellen der Kriterien werden zwei verschiedene Sichten deutlich. Zum einen ist dies die Herstellersicht, der prinzipbedingt bemüht ist seine Werbeversprechen von Sicherheit der Daten und deren Zugriff sowie Eindeutigkeit bei der Identifikation zu erfüllen, und zum anderen die Sicht des durchführenden Testers. Für diesen ist im Vorfeld schlecht abschätzbar, welche Möglichkeiten und Probleme auf ihn zu kommen. Die spezifischen Anforderungen beider sollen nun genauer erläutert werden.

2.1.1.1 Herstellersicht

Nachdem sich mehrere Gruppen mit der Untersuchung der Mifare-basierten RFID-Lösungen beschäftigten und das bis dahin geheimgehaltene Verschlüsselungsverfahren aufdecken konnten, hat sich auch NXP zum Thema Sicherheit geäußert (vergleiche [NXP08a]). Dabei wurde eine Liste veröffentlich, die beschreibt wodurch NXP bestehende Systeme als gefährdet betrachtet. Die einzelnen Punkte dabei sind:

> Eine Möglichkeit um erfolgreiche Kommunikation zwischen einem Reader und einer Karte abzuhören und die Daten und/oder die verwendeten Schlüssel auszulesen.

Bei nicht erfolgreicher Kommunikation den Schlüssel des Readers abhören zu können

Der Angriff braucht nur ein paar Minuten oder weniger bei Einsatz eines Laptop und zusätzlichen Gerätschaften im Wert von 100 €.

Angriffe, die nur eine Karte benötigen, können in einer Laborumgebung und mit akzeptabler Vorberechnungszeit durchgeführt werden und sich eventuell zu Angriffen ohne Laborumgebung und geringerer Vorberechnungszeit entwickeln.

Innerhalb einer Sekunde können mit genügend Vorwissen alle Daten und Schlüssel der Karte mit begrenztem Equipment und einem Laptop ausgelesen werden.

Zum Auslesen der Schlüssel und Daten wird nur 2 malige Interaktion mit der Karte benötigt

Zwar hat NXP auch Dokumente mit Gegenmaßnahmen erstellt, diese sind jedoch nur unter Zustimmung zu Geheimhaltungsklauseln zugänglich. Außerdem ließ sich noch keine Veröffentlichung zur Wirksamkeit dieser geheimen Maßnahmen finden.
Gerade deshalb gibt diese Liste Anhaltspunkte, ab wann eine RFID-Implementierung als gescheitert betrachtet werden kann.

2.1.1.2 Testersicht

Der Tester hat im Gegensatz zum Hersteller eine Blackbox-Sicht auf die tatsächliche Implementierung. Aus diesem Standpunkt heraus ist es grundsätzlich wünschenswert bei geringem finanziellen Einsatz weitreichende Analysemöglichkeiten zu bekommen. Dazu ist es nicht nur erforderlich, dass die zu beschaffende Hardware den bereits genannten Normen entspricht und die darin festgelegten Verfahren beherrscht, sondern auch deren Beeinflussung ermöglicht. Dafür muss der Treiber für das Gerät eine entsprechend mächtige Programmierschnittstelle[1] zur Verfügung stellen. Noch besser wäre es, wenn die Gerätesoftware frei und im Quelltext verfügbar wäre, da man sich dadurch bei Bedarf eventuell weitere Möglichkeiten eigenhändig schaffen könnte. Allerdings bedeutet die Verfügbarkeit dieser Optionen noch nicht, dass man sie auch benutzen kann. Daher wären Hilfestellungen durch vielfach genutze und bewährte Entwicklerprogramme, gute Dokumentation und eine aktive Entwicklergemeinschaft sowie Wege um bei Fragen mit dieser in Kontakt zu treten erstrebenswert.

[1] auch API(Application Programming Interface) genannt.

Außerdem stellt die weitere zur Verfügung stehende Hardware bestimmte Anforderung an die Geräteauswahl. Die im Rahmen dieser Diplomarbeit bereitstehenden Computer besitzen Bluetooth-, Ethernet- und USB-Schnittstellen.

2.1.1.3 abgeleitete Anforderungen

Vergleicht man nun beide Sichten so ergibt sich neben der obligatorischen Unterstützung des ISO-14443 A Standards folgende Liste von Anforderungen:

Kosten unter 100 €

Open Source Library

Treiber API

Hilfestellungen

Schnittstellen

2.1.2 Herleitung der Gewichtungsfaktoren

Nicht alle Anforderungen tragen in gleichem Maße dem letztendlich zu erwartendem Nutzen bei. Deshalb werden sie paarweise gegenübergestellt und dabei in ihrer Wichtigkeit verglichen, um eine Priorisierung zu ermöglichen.
Die Gewichtung erfolgt dabei nach folgender Tabelle:

Wenn beide Funktionalitäten gleich wichtig sind:	2:2
Wenn die erste wichtiger als die zweite ist:	3:1
Wenn die zweite wichtiger als die erste ist:	1:3
Wenn die erste wichtig und die zweite unwichtig ist:	4:0
Wenn die zweite wichtig und die erste unwichtig ist:	0:4

Tabelle 2.1: Gewichtungsgrundlage

Die Schnittstellen stellen ein Ausschlusskriterium dar,da es ohne sie nicht möglich wäre eine Analyse durchzuführen. Sie spielen zwar bei der Auswahl der Geräte eine Rolle, haben aber ebenso wie die Kosten keinen direkten Einfluss auf den zu erwartenden Nutzen für das Ziel der Analyse. Deshalb tauchen beide in der nun folgenden Tabelle nicht auf.

	Open Source Library	Treiber API	Hilfe-stellun-gen	Summe	%
Open Source Library	.	4	3	7	58
Treiber API	0	.	3	3	25
Hilfe-stellungen	1	1	.	2	17

Tabelle 2.2: Gewichtung der Anforderungen

Wie ersichtlich nehmen die Schnittstellen eine überragende Stellung ein, denn ohne sie ist eine Inbetriebnahme der Hardware von vornherein schon ausgeschlossen.
An zweiter Stelle stehen die Kosten. Sie kommen in beiden vorgestellten Sichten vor. NXP setzt diese im Vergleich zu den Einsatzzwecken der Mifare-Produkte sehr niedrig an.
Ziemlich dicht darauf folgt der offen zugängliche Quellcode. Technisch gesehen könnte eine gute Programmierschnittstelle des Gerätetreibers ausreichen bzw. Quellcodeveränderungen ersparen. Deren Notwendigkeit ist in dieser Phase jedoch noch nicht absehbar und die Einsicht in den Code könnte eventuell weitere Möglichkeiten aufdecken. Deshalb ist eine quelloffene Lösung vorzuziehen.
Ob überhaupt Bedarf an weiteren Hilfestellungen entsteht hängt von der Qualität und dem Potential der zugrunde liegenden Gerätesteuerungssoftware ab. Sie spielen deshalb eine untergeordnete Rolle.

2.1.3 Mögliche Geräte

Die aufgestellten Anforderungen führten dazu, dass bei der Recherche von Anfang an darauf geachtet wurde, nur Geräte in die engere Auswahl zu nehmen, die allen genannten Anforderungen gerecht wurden. Dabei stellte sich heraus, dass von den zur Verfügung stehenden Schnittstellen nur der USB-Anschluss in dieser Preiskategorie verfügbar war. Deshalb wird bei der folgenden Vorstellung der sich ergebenden Zusammenstellung nicht weiter darauf eingegangen.

2.1.3.1 MIFARE Pegoda Contactless Card Reader

Der MIFARE Pegoda Contactless Card Reader wird von NXP hergestellt und ist über unterschiedliche Händler, z.B [EC10], ab ca. 50 € verfügbar. Es lässt sich über Gerätetreibern unter diversen Windows-Betriebssystemen ansprechen. Auf der NXP-Website([NXP10d]) wird er als Referenzdesign angepriesen und man kann zusätzliche Programme für das Gerät herunterladen. Des weiteren stellt NXP ein Datenblatt und viele andere nutzliche Dokumente zur Eigenentwicklung zur Verfügung. Teile der Dokumentation und der Software werden aber erst nach Unterzeichnen eines Geheimhaltungsvertrages bereitgestellt.

2.1.3.2 Omnikey CardMan 5121 RFID

HID Global ist der Hersteller von zwei Geräten, die den Anforderungen entsprechen. Das ist zum Einen der Omnikey CardMan 5121 RFID. Er ist für ca. 80 € z.B. unter [Nie10] erhältlich. Da er nach dem PC/SC-Standard für Kartenlesegeräte[2] arbeitet, benötigt er keine spezielle Treibersoftware. Auf der Herstellerwebsite kann unter [Glo10a] zusätzliche Software runtergeladen werden. Es findet sich auf der Website jedoch keine weiteren Informationen zu den Programmierschnittstellen. Neben der kontaktlosen Datenübertragung im 13,56 MHz Bereich unterstützt er auch die kontaktbehaftete Kommunikation mit Chipkarten.

2.1.3.3 Omnikey 5321 Desktop USB Reader

In den technischen Daten sowie im Preis(z.B. unter [CRY10]) entspricht der Omnikey 5321 dem Omnikey CardMan 5121 RFID. Allerdings werden auf der HID Global-Website[3] wesentlich mehr Dokumente und die gleiche Software für dieses Gerät bereitgestellt. Unter [Glo10c] ist ein „Contactless Developer Guide“(siehe [Glo10b]), in dem die Programmierschnittstelle beschrieben wird. Darin ist der Zugriff auf eine PICC nur auf APDU-Ebene beschrieben.

2.1.3.4 RWM226A-USB reader/writer

Das deutsche Ingenieurbüro R. S. Systems (siehe [RSS10c]) bietet über seinen eBay-Shop([RSS10a]) in regelmäßigen Abständen den RWM226A-USB reader/writer (vergleiche [RSS10b]) an. Mit seinem Preis von ca. 100 €, dem virtual-COM-Zugriff als

[2] http://www.pcscworkgroup.com/
[3] http://www.hidglobal.com/

Treiber und der Unterstützung des ISO-14443 A Standards[4] erfüllt er zwar die Anforderungen, aber die Mifare DESfire Karte taucht in der Liste der unterstützten Karten nicht auf. Es wird auch nicht klar, ob oder wie sich eine solche Unterstützung nachrüsten ließe. Außerdem ist der RWM226A das einzige zur Wahl stehende Produkt, das nicht von einer weltweit agierenden Unternehmung hergestellt wird.

2.1.3.5 SCL010

Auch SCM Microsystems GmbH ist mit zwei PCDs vertreten. Eine weitere Gemeinsamkeit mit HID Global ist die Unterstützung des PC/SC-Standards. Der SCL010 wird per USB-Kabel angebunden und besitzt die typische Form eines RFID-Readers auf dem man eine Karte ablegen kann (vergleiche [Mic10a]). Er ist für ca. 50 € erhältlich, z.B. über [Ele10].

2.1.3.6 SCL3711

Der SCL3711 von SCM Microsystems GmbH kostet dagegen ca. 100 € [C:10] und hat die Form eines USB-Sticks. Für beide Geräte bietet SCM Microsystems auf den jeweiligen Internetseiten neben den typischen Datenblättern Referenzmanuals an [Mic10b] [Mic10c]. In diesen wird die API und ihre Benutzung übersichtlich dokumentiert und anhand von Beispielen veranschaulicht; allerdings wie bei dem Omnikey 5321 wird auch hier nur die APDU-Ebene abgedeckt.

2.1.3.7 touchatag

Mit ca. 40 € ist der touchatag von Alcatel Lucent der billigste Kandidat (bei [Sch10]). Eigentlich handelt es sich dabei jedoch um einen ACR122U von Advanced Card Systems Ltd., den Alcatel Lucent mit eigener Software und eigenen Tags vertreibt (vergleiche [Sys10]). Das verkaufte Gesamtsystem funktioniert folgendermaßen:
Wenn ein registrierter Tag in das Feld des Reader eintritt, wird dessen UID ausgelesen und an einen Server im Internet geschickt. Dieser führt daraufhin eine mit dieser UID verknüpfte Aktion aus. Lässt sie sich im Internet ausführen so leitet sie der Server ein, ansonsten schickt er eine Nachricht an das lokale System und die entsprechende Handlung wird von dort aus gestartet (vergleiche [AL10b]).
Die offen liegende API und die Unterstützung des PC/SC-Standards ermöglichen

[4] sowie der USB-Schnittstelle

dies grundsätzlich auf allen wichtigen Betriebssystemen; es werden jedoch nur aktuelle Windows- und Mac OS X-Betriebssysteme direkt von Alcatel Lucent unterstützt (vergleiche [AL10a]). Auf der Seite von Advanced Card Systems Ltd.([Sys10]) hingegen lassen sich weitere Treiber und vor allem ein API Treiber Handbuch für die Programmierung auf APDU-Ebene herunterladen.

2.1.4 Mögliche quelloffene Software

Nach dem Eingrenzen der Hardware wurde nach quelloffener Software für die Geräte gesucht. Dabei stellte sich heraus, dass es nur drei grundlegende Lösungen in diesem Bereich gibt. Diese werden nun vorgestellt.

2.1.4.1 libnfc

Der Grundgedanke hinter der libnfc ist es, eine freie Programmierschnittstelle für NFC(Near Field Communication) auf einer höherer Programmierebene bereitzustellen und damit diesen Bereich von Lizenzgebühren und Geheimhaltungsverträgen zu lösen (vergleiche [Ver10]).
Neben einer Website und dem Quellcode([lib10b]) mit Kommentaren stehen ein Forum([lib10c]), die API-Dokumentation([lib10d]) und ein Issue-Tracker([lib10e]) als weitere Hilfestellungen bereit und werden von der Entwicklergemeinde auch intensiv genutzt. Der SCL3711 und der touchatag aus der vorhergehenden Hardwareauswahl stehen auf der Kompatibilitätsliste (vergleiche [lib10a]).

2.1.4.2 librfid

Auch die librfid unterstützt zwei der in Frage kommenden Geräte (vergleiche [Wel08]). Dies sind der Omnikey CardMan 5121 und der Omnikey 5321. Sie hat zwar das selbe Ziel, bezieht sich aber speziell auf den ISO 14443 A und B Standard. Keine der Hilfs- und Kommunikationsmöglichkeiten der libnfc steht bereit und die letzte veröffentlichte Version stammt vom vierten Februar 2008.

2.1.4.3 RFDump

RFDump als dritte Open Source Lösung wird hier hauptsächlich wegen der Vollständigkeit genannt. Auch diese Software wird seit 2008 nicht weiter entwickelt (vergleiche [RFD08b]). Außerdem findet sich die unterstützte Hardware nicht in der oben

getroffenen Auswahl wieder (vergleiche [RFD08a]) und die weiteren Hilfsmittel gibt es ebenfalls nicht.

Software	Geräte
libnfc	SCL3711
	touchatag
librfid	Omnikey CardMan 5121
	Omnikey 5321
RFDump	-

Tabelle 2.3: Quelloffene Software für die mögliche Hardware

2.1.5 Nutzwertanalyse

Nachdem die möglichen Geräte und die quelloffenen Alternativtreiber im Hinblick auf die gestellten Anforderungen vorgestellt wurden, wird nun eine Bewertung durchgeführt. Ziel ist es, das Gerät mit dem größten zu erwartendem Nutzwert zu ermitteln. Als Maßstab zur Beurteilung dient folgende Tabelle:

Optimale Leistung/Funktion; in allen Punkten den Anforderungen entsprechend	100%
Kleinere Mängel und Nachteile; Leistung leicht unter den Anforderungen	80%
Ins Gewicht fallende Mängel und Nachteile; Leistung nennenswert unter den Anforderungen	60%
Ganz erhebliche Mängel und Nachteile; Leistung weit unter den Anforderungen	40%
Funktion nur zu einem geringen Teil brauchbar; Leistung nur bruchstückhaft vorhanden	20%
Funktion/Kriterium nicht vorhanden oder unbrauchbar	0%

Tabelle 2.4: Bewertungsskala für die Nutzwertanalyse

Anhand dieser Bewertungsskala wird nun eine Nutzwertanalyse durchgeführt.

Anforderungen	Gew[1]	Pegoda		Cardman 5121		5321		RWM 226A-USB		SCL010		SCL3711		touchatag	
		EG[2]	WK[3]	EG	WK	EG	WK	EG	WK	EG	WK	EG	WK	EG	WK
OS[4]	58	0	0	80	46,8	80	56,8	0	0	0		100	58	100	58
API[5]	25	80	20	20	5	60	15	20	5	60	15	60	15	60	15
Hilfe	17	40	6,8	20	3,4	40	6,8	0	0	40	6,8	100	17	100	17
			26,8		65,2		68,6		5		21,8		90		90

[1] Gewichtung
[2] Erfüllungsgrad
[3] Wertigkeit/Ergebnis
[4] Open Source Library
[5] Gerätetreiber API

Tabelle 2.5: Nutzwertanalyse

2.1.6 Fazit und Auswahl

Am besten schneiden die Geräte ab, welche von der Unterstützung der libnfc profitieren. Außerdem ist die vom jeweiligen Hersteller bereitgestellte Treiberunterstützung und Dokumentation vergleichbar. Da der touchatag aber wesentlich weniger Kosten verursacht und dadurch ein besseres Preis-Leistungs-Verhältnis zustande kommt, wird ihm der Vorzug vor dem SCL3711 gegeben.

2.2 Test der Implemetierung

Nach der Auswahl eines geeigneten Gerätes soll die DESFire Implementierung anhand von verschiedenen Tests geprüft werden.
Im Standardszenario befindet sich die PICC im Besitz eines Angreifers. Dieser hat die Intension, wie in 1.1.3 bereits erwähnt, die Funktionalität des Gesamtsystems entscheidend zu stören bzw. zu unterbinden oder die gespeicherten Daten zu seinen Gunsten zu manipulieren.
Obwohl sich der Aufwand, der für einen Angriff in Kauf genommen wird, im Normalfall nach dem zu erwartenden Ergebniss richtet, soll hier der in 2.1.1.1 vorgegebene Kostenrahmen für Zusatzgeräte eingehalten werden, da er auch als Grundlage für die Anschaffung der Hardware diente.
Soweit nicht anders erwähnt, wird der ausgewählte touchatag als PCD eingestetzt. Zur Kontrolle und als Gegenstelle kam ein Omnikey 5321 RFID Reader in Kombination mit der mitgelieferten Software zum Einsatz. Er soll das zu attackierende System darstellen, während die Angriffe mit dem touchatag durchgeführt werden.
Diese werden im Folgenden vorgestellt.

2.2.1 Zerstören

Durch die Zerstörung der PICC soll ein DoS(Denial of Service) herbeigeführt werden. Dafür muss nicht zwingend der ganze Transponder zerstört werden. Schon das Abtrennen oder das Durchtrennen der Antenne nahe genug am IC führt zu einer nicht mehr ausreichenden Stromversorgung und somit dem Verlust der Funktionsweise. Dies kann je nach Beschaffenheit der PICC unterschiedlich schwierig ausfallen. Prinzipiell dürfte sich aber jede Bauform durch geeignete physische oder chemische Einwirkung genug beschädigen lassen, um die weitere Funktion auszuschließen.
Des weiteren sieht die ISO 14443 Part 1 eine maximale Feldstärke von 12 A/m vor. Wird diese verstärkt, führt das zu erhöhter Verlustwärme oder letztendlich zu thermischer Zerstörung.
Durch fehlende Funktion können nicht nur Probleme bei der Identifikation auftreten, sondern auch weiterführende Dienste wie z.B. Bezahl- oder Transportsysteme in ihrer Funktion für den Nutzer stillgelegt werden (vergleiche [Fin06], S. 237f)

Hilfsmittel

Prinzipell kann fast alles genutzt werden, solange damit dem Tag genügend Schaden zugefügt werden kann. Examplarisch soll hier der RFID-Zapper genannt werden, der nach der Anleitung aus [zr06] aus einer handelsüblichen Einwegkamera nachgebaut werden kann. Er hat den Vorteil, dass durch ein kurzzeitig erzeugtes starkes elektromagnetisches Feld nur die Funkelektronik geschädigt wird und der Rest der PICC keine offensichtlichen Spuren einer Beeinträchtigung aufweist.

Umsetzung

Von einer Umsetzung wurde abgesehen, da nur wenige Tags zur Verfügung standen und diese für weitere Versuche benötigt wurden.

Resümee

Die Zerstörung stellt einen effektiven und einfachen Weg zur Verhinderung eines Dienstes dar. Außerdem ergibt sich eine interessante Kombinationsmöglichkeit mit dem nächsten Angriff.

2.2.2 Ablösen des Transponders

Das Ablösen des Transponders trennt ihn vom eigentlichen Gegenstand. Da in ISO-14443 Part 1 keine feste Form und kein genaues Material festgelegt ist, ist das Separieren je nach PICC mit einem unterschiedlich hohem Risiko der Zerstörung verbunden. Bei Erfolg kann der Transponder an einem anderen Objekt angebracht werden, das somit die mit der UID des ICs verknüpfte Identität annimmt sowie die damit verbundenen Dienste unter dieser nutzen kann.

Hilfsmittel

Um diesen Angriff möglichst realistisch nachzuvollziehen wurde eine PICC in Chipkartenformat gewählt. Dabei ist der IC und dessen Antenne in Thermoplaste eingebettet. Diese lässt sich mit Aceton aufquellen. Desweiteren wird ein Gefäß zur Aufnahme der Materialien benötigt, welches nicht aus per Aceton lößlichen Stoffen besteht.

Umsetzung

Vor Begin des eigentlichen Experiments wurde auf der PICC eine Standard Data File mit dem Text „Hallo Welt!“ angelegt. Danach wurde die Karte in ein Glas gelegt und diese dann mit Aceton befüllt bis die Karte vollständig bedeckt war, um eine gleichmäßige Auflösen der Thermoplasten zu erwirken. Schon nach einigen Minuten quoll die Thermoplaste auf und nach circa 45 Minuten hatten sich IC und Antenne von dem Rest gelöst.
Bei dem anschließenden Test der Karte ließen sich alle Funktionen ohne Probleme nutzen und der gespeicherte Text fehlerfrei wieder auslesen.

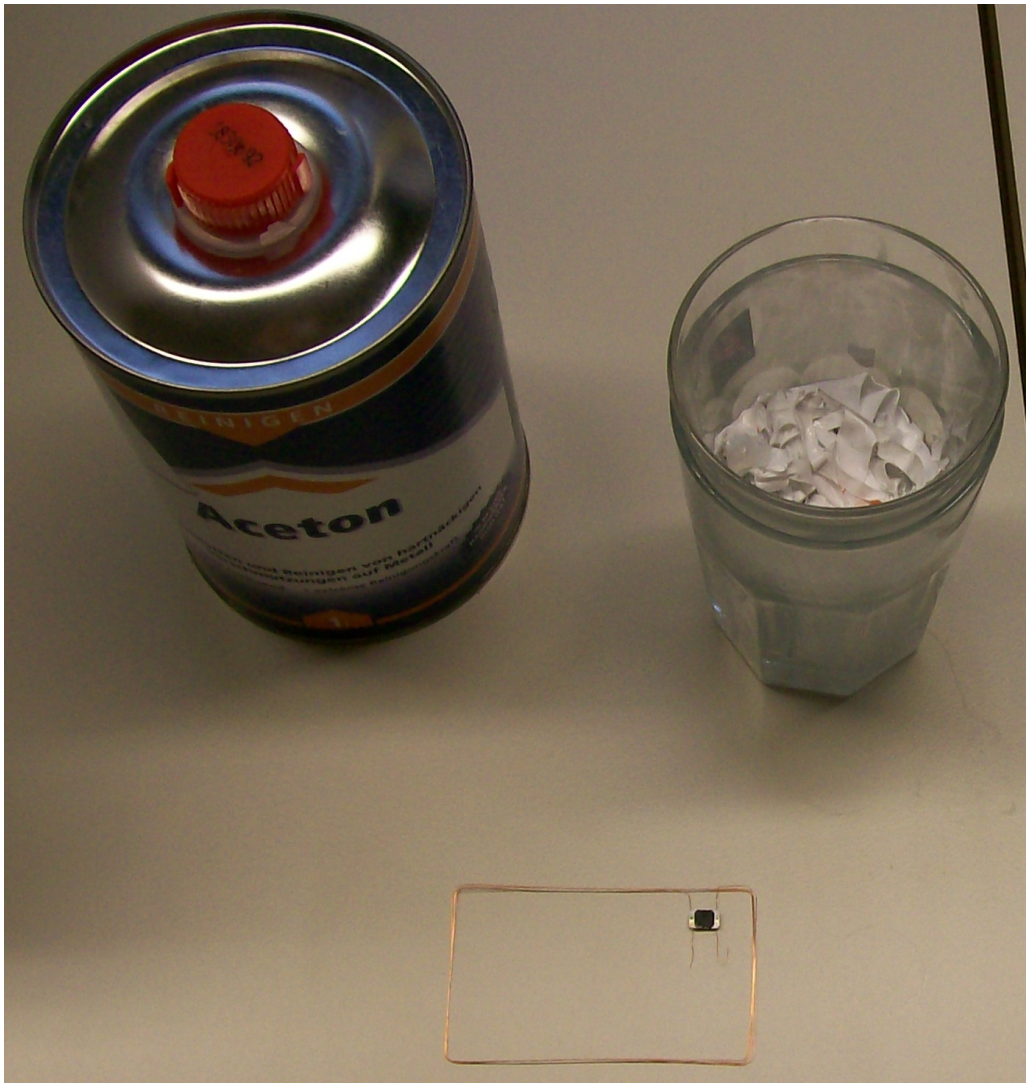


Abbildung 2.1: Acetonversuch

Resümee

Wenn keine zusätzlichen Sicherheitsmaßnahmen ergriffen werden, lässt sich der DESfire IC mit seiner Antenne sehr einfach Ablösen und an einer anderen Karte anbringen[5]. Dies ermöglicht verschiedene sicherheitstechnisch kritische Szenarien.
Als ein Beispiel soll hier das Bezahlen in einer Cafeteria oder Mensa dienen. Dort wird die Identität oftmals anhand eines Bildes und einiger zusätzliche Daten, die auf der Chipkarte aufgedruckt wurden, überprüft. Das eigentliche Bezahlterminal stellt diese aber nicht zum Abgleich zur Verfügung, die dies eine Datenbankverbindung erfordern würde und somit zusätzliche Kosten verursacht. Wird nun der eigentliche Chip deaktiviert oder zerstört, kann so mit einer gestohlenen oder sogar gefälschten Karte bezahlt werden.
Der Aufwand und die entstehenden Kosten sind gering und der Angriff ist einfach nachzuvollziehen, deshalb sollte in sicherheitskritischen Umgebungen ein anderes PICC-Format gewählt werden.

2.2.3 Abschirmen/Verstimmen

Da eine PICC ihren Strom aus dem elektromagnetischen Feld des PCD bezieht, führt das vollständige Abschirmen dieses Feld zu einem DoS. Für die Abschirmung sind alle Materialien geeignet, die elektromagnetische Wellen dämpfen. Zum Einen wird durch den Einsatz von z.B. Metallfolie der Antennenschwingkreis des Transponders verstimmt und zum Anderen entstehen Wirbelstromverluste. Je nach Grad der Verstimmung kann so die Stromzufuhr geschwächt werden bis letztendlich nicht genügend Energie für den Betrieb des IC zur Verfügung steht.
Diese Methode hat den Vorteil, dass Schaden an der PICC vermieden werden kann und durch Entfernen der Verstimmungsursache wieder die vorherige Funktion hergestellt wird. Somit kann ein passiver Transponder zeitweise „abgeschaltet“ werden (vergleiche [Fin06], S. 238).

Hilfsmittel

Es gibt verschiedene Hüllen speziell für diesen Einsatzzweck zu kaufen. Letztendlich genügt aber ein ausreichend großes Stück Alufolie.

[5] Der Autor hat ihn für bessere Handhabbarkeit anschließend an einer abgelaufenen Bahncard angebracht.

Umsetzung

Abbildung 2.2: Verstimmen bzw. Abschirmen einer PICC

Zu Beginn wurde eine eigens gebaute Metallhülle aus Stahl getestet. Sie schirmte die PICC ab, so dass kein ausreichendes Signal am PCD ankam. Auch die dünnere, kommerziell erhältliche Hülle erfüllte diesen Zweck.
Danach wurde einfache Aluminiumfolie aus dem Supermarkt ausprobiert. Stetige Verkleinerung der verwendeten Folie zeigte, dass es genügt etwas mehr als die Hälfte der PICC abzudecken, um das Signal soweit zu verstimmen, dass keine Erkennung möglich war.

Resümee

Bei DESfire PICCs ist kein physischer oder sonst irgendwie erkennbarer Kontakt zum Auslesen und Verändern der gespeicherten Daten notwendig. Durch das Abschirmen der PICC mit billigsten Mittel kann effektiv verhindert werden, dass dies ungewollt passiert.

2.2.4 Senden von Störsignalen

Die theoretisch einfachste Variante ein Störsignal zu erzeugen, wäre es eine Dauerlast auf das Feld zu schalten. Damit wäre kein Lastwechsel bei der Miller- und kein Flankenwechsel bei der modifizierten Manchester-Kodierung mehr möglich. Doch das ist gar nicht notwendig. Während der Antikollision sendet die PICC immer wieder Binärfolgen, die aufeinander folgende Null-Werte enthalten. Schon das Senden von abwechselnden Binärwerten würde folglich die Erkennung und Auswahl einer PICC verhindern und so zu einem DoS führen. Würde man die Kommunikation abhören, könnte man so auch gezielt auf einzelne Nachrichten reagieren und einen erneuten Antikollisionsdurchlauf erzwingen.

Hilfsmittel

Zur Umsetzung des Störsenders wurde der touchatag in Verbindung mit der libnfc verwendet. Als auslesendes PCD wurde sowohl ein Omnikey 5321 RFID Reader als auch ein anderer touchatag getestet.

Umsetzung

Die libnfc bringt eine Reihe von Beispielanwendungen mit. Darunter ist nfc-anticol. Diese ursprünglich zur Demonstration des ISO 14443A Antikollisionsverfahren gedachte Anwendung wurde so umgeschrieben, dass der touchatag konstant den Hexadezimalwert 0x55 versendet, da dieser einer alternierenden Binarfolge entspricht. Als Folge daraus bekommt die PICC ständig Binärfolgen zugesandt, mit denen keine sinnvolle Verarbeitung verknüpft werden kann und wird somit in ihrer Funktionsweise gestört.
Sobald der mit der Störsoftware laufende touchatag in das Feld eines anderen Lesegerätes kam, verhinderte er erfolgreich jede weitere Kommunikation.

Abbildung 2.3: Störsender

Resümee

Obwohl der touchatag als Störsender seine Funktion voll erfüllte, stellt doch die geringe Signalreichweite ein ernstzunehmendes Hinderniss für einen realistischen Angriff dar. Man muss ihn bis auf wenige Zentimeter an den eigentlichen Reader heranbringen. Dies könnte in einem Umfeld ohne zusätzliche Überwachung eventuell gelingen ohne Aufsehen zu erregen.

2.2.5 Vergrößerung der Reichweite

Beim Empfang der Mifare-Signale gibt es zwei Reichweiten. Die Energiereichweite bezieht sich auf die Entfernung, in der von dem IC noch ausreichend Energie empfangen wird, um voll funktionsfähig zu arbeiten. Die Lastmodulationsreichweite ist der Abstand, bei dem die von der PICC aufmodulierten Signale noch bei dem PCD ankommen. Um beide zu Maximieren wird der Strom in der Senderantenne erhöht

und der Durchmesser der Leserantenne vergrößert. Allerdings setzt der erste Teil der ISO 14443 Norm Grenzen für die Außmaße der Antenne im PICC und beschränkt das Ansprechfeld des PCDs.
Für den Angreifer bedeutet die Umgehung dieser Beschränkungen und damit die Erhöhung dieser Distanzen eine Verringerung des Risikos entdeckt zu werden. Allerdings konnten dabei selbst unter optimalen Bedingungen nicht mehr als 40 cm erreicht werden (verlgeiche [Fin06], S. 241f).

Hilfsmittel

Aufgrund seine elektromagnetischen Eigenschaften eignet sich vor allem Kupferdraht als Antenne.

Umsetzung

Man könnte die verbaute Antenne des touchatag durch das Anlöten eines Kupferdrahtes erweitern oder ersetzen. Die Verbindungsstellen sind deutlich zu erkennen.

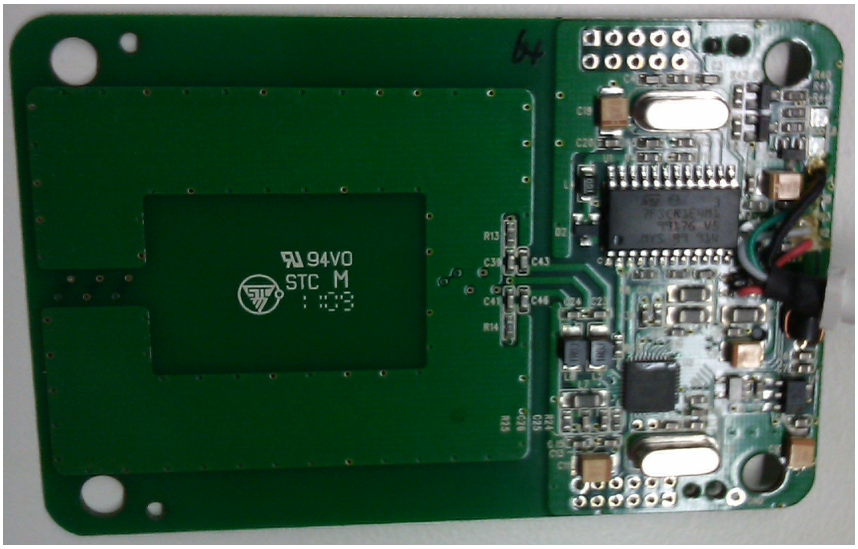


Abbildung 2.4: Unterseite der touchatag-Platine

Allerdings wird die radiofrequente Elektronik des touchatag durch einen PN532 Microcontroller gesteuert. Mit diesem ist es nicht trivial möglich die Feldspannung oder sonstige Faktoren ohne teuere Zusatzhardware zu beeinflussen.

Resümee

Auf Grund der vorhergenannten Probleme bei der Umsetzung und der verhältnismäßig geringen zu erwartenden Reichweitenvergrößerung wurde von der Verwirklichung dieses Angriffs abgesehen.

2.2.6 Emulieren

Zum Emulieren eines DESfire Tags benötigt man ein Gerät, dass den PICC-Teil der ISO 14443A Norm abbilden kann. Um dieses für einen Angriff gebrauchen zu können, muss es sich so verhalten wie es eine valide PICC würde. Dazu muss es nicht nur die Norm umsetzen, sondern auch auf entsprechende Anfragen mit den richtigen Antwortdaten reagieren um die auf einer PICC gespeicherten Daten zu imitieren.

Hilfsmittel

Der touchatag lässt sich in mehreren Modi betreiben. Einer davon ist der "Target/PICC Mode"(vergleiche [NXP07], S. 15). Zusätzlich liegen der libnfc einige Beispiele bei, die zeigen wie man diesen Modus als Emulator nutzt(z.B. nfc-emulate-uid.c und nfc-emulate-tag.c).

Umsetzung

Für die Befehle REQA, WUPA, ANTICOLLISION und SELECT wird in ISO 14443-3 eine Antwortzeit von ca. 91,1 Mikrosekunden vorgeschrieben[6]. Über die USB-Schnittstellen sind diese Zeiten praktisch nicht zu Erreichen. Deshalb ist man hierbei auf die Unterstützung eines auf dem Gerät verbauten Microcontrollers angewiesen.

[6]genauer: (n x 128 + 84)/fc mit n = 9 und fc = 13,56 MHz (1236/13560000 Hz 0.00009115044247787611 s)

Abbildung 2.5: Emulation

Wie bereits in 2.2.5 erwähnt wird die eigentliche Sendeelektronik des touchatag hinter einem PN532 Microcontroller vor dem Benutzer verborgen. Im Quellcode der Emulationsprogramme wird davor gewarnt, dass dieser als Gegenmaßnahme zur Verhinderung richtiger Emulation zwei Mechanismen implementiert hat.
Zum einen wird die Länge der zu emulierenden UID auf vier Byte beschränkt und zum anderen wird das erste Byte auf den Wert 0x08 gesetzt.
Die DESfire ICs verwenden aber durchgängig sieben Byte UIDs. Zwar wurde versucht dies zum Umgehen, aber der dem Omnikey 5321 RFID Reader empfing stets nur eine kurze mit 0x08 beginnende UID oder die erzeugte Software stürtzte reproduzierbar ab.

Resümee

Prinzipiell funktioniert das Emulieren mit dem touchatag sehr gut und einfach. Allerdings trifft dies nicht auf die DESfire ICs zu. Systeme, die auf diesem IC aufbauen, sollten schon während der Antikollisionsphase ihren Dienst mit einer Fehlermeldung einstellen und somit ein Ausnutzen der Emulationsfähigkeiten verhindern.
Diese Überprüfung fand bei der Software des Omnikey jedoch nicht statt. Folglich ist dies systemabhängig und muss für das jeweilige Angriffsziel getestet werden.

2.2.7 Relay-Attacke

Bei der Relay-Attacke wird die Reichweite vergrößert, in dem zwei weitere Geräte zwischengeschaltet werden. Eines davon befindet sich in der Lastmodulationsreichweite der anzugreifenden PICC und die andere im Feld des Ziel-PCDs. Der Angreifer muss beide unter seiner Kontrolle haben und eine Verbindung zwischen ihnen herstellen können. Über diese „Brücke“ leitet er die Kommunikation ohne dass die jeweiligen Gerätebesitzer Kenntnis davon haben. So wird dem PCD eine falsche Identität vorgetäuscht und die von der ursprünglichen Karte unterstützten Dienste können unter dieser genutzt werden.

Jede Übertragung bringt Signallaufzeiten mit sich. Wie mit diesen umgegangen wird, ist in Part 2 und 3 der ISO 14443 Norm festgelegt. Außerhalb der in 2.2.6 beschriebenen Zeiten sieht sie einen synchronen Betrieb vor, bei dem nach jeder Nachricht eine Mindestwartezeit vorgeschrieben wird.
Der Part 4 der Norm enthält zusätzlich eine maximale Wartezeit, die zwischen PCD und PICC ausgehandelt werden kann[7]. Diese errechnet sich nach der Formel:

$$\mathbf{FWT} = (256 \quad 16/\mathbf{fc}) \quad 2^{\mathbf{FWI}} \tag{2.2.1}$$

Hierbei steht das fc für den field carrier; also die 13,56 MHz Feldfrequenz. Das FWI ist ein aushandelbarer Wert zwischen 0 und 14. Somit ist eine $\mathbf{FWT_{Max}}$ von ca 4,95 Sekunden möglich[8]. Die FWT kann zwar von der PICC durch ein WTX (Frame waiting time extension) request im Einzelfall verlängert werden, allerdings höchstens auf die so eben berechnete Maximalzeit gesetzt werden.

[7] Die FWT(Frame Waiting Time)
[8] genauer: $((256 \quad 16)/13560000\mathbf{Hz}) \quad 2^{14} \quad 4 : 9490312684365781710 9\mathbf{s}$

Wartet der PCD nicht lange genug, um die Nachricht komplett zu puffern, muss die Übertragung so schnell wie möglich geschehen. Dazu ist es erforderlich, die Flanken je nach Kodierung zur richtigen Zeit zu erzeugt. Bei der Manchesterkodierung von PICC zu PCD können die Bitwerte schon direkt an der etu-Grenze erkannt werden. Die modifizierte Miller-Codierung verwendet für Nullen nach Einsen einen High-Pegel über die gesamte etu. Binäre Einsen werden mit einem Low-Pegel in der Mitte der etu kodiert. Folglich vergeht bei zwei Einsen hintereinander ein Drittel des etu-Zeitintervalls, bevor der binäre Wert festgestellt werden kann. Bei der weiteren Übertragung kommt dann noch zusätzlicher Protokolloverhead und die Geschwindigkeit des Übertragungsmediums hinzu. Überschreitet die letztendlich gesendete Flanke die halbe Dauer eines Bits, kann das zur Ablehnung der gesamten Nachricht führen.
Dabei hängt die Bitdauer wesentlich von der ausgehandelten Übertragungsgeschwindigkeit ab und ist im schlechtesten Fall 1,2 Mikrosekunden[9].

Hilfsmittel

Zur Verwirklichung diesen Angriffs sind zwei ISO 14443 Norm kompatible Geräte erforderlich, von denen eines die PICC und das andere den PCD emulieren kann.

Umsetzung

Um in dem vom Hersteller in 2.1.1.1 vorgegebenem Kostenrahmen zu bleiben und da die sonstigen zu Verfügung stehenden Geräte diesen sprengten, wurde versucht eine Weiterleitung mittels zweier touchatags zu bewerkstelligen.
Auch hierfür stellt die libnfc Beispielquellcode bereit. In den Dateien nfc-relay.c und nfc-relay-picc.c wird eine Weiterleitung auf logischer Objektebene verwirklicht.
Dabei zeigte sich, dass die Wartezeiten gerätespezifisch sind. Wurde ein dritter touchatag als Ziel-PCD verwendet, kam es häufig zu falsch erkannten oder nur halb gelesen Bytes. Diese Probleme traten bei dem Omnikey 5321 RFID Reader nicht auf.
Allerdings scheitert auch dieser Aufbau, denn hier wird ein touchatag als PICC-Emulator eingesetzt und die eingebaute Firmware enthält folglich die selben Schutzmechanismen wie in 2.2.6.

[9] Die halbe etu ist dann 0,6 Mikrosekunden. Von diesem werden 0,4 Mikrosekunden zur Erkennung des Binärwerte benötigt. Folglich verbleiben 0,2 Mikrosekunden zur Übertragung.

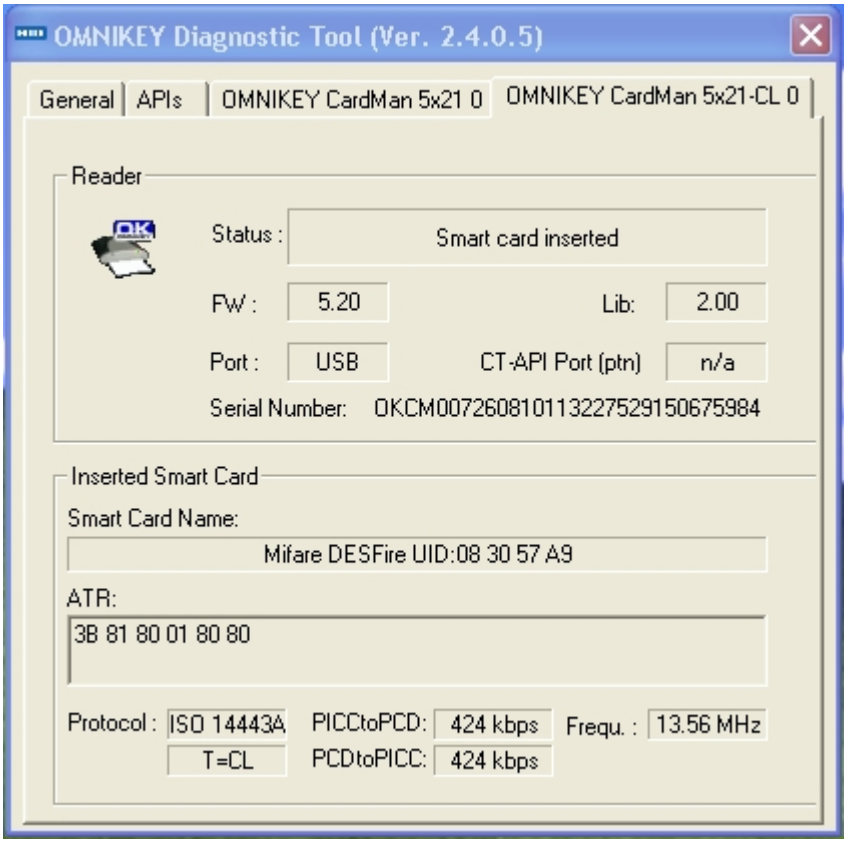


Abbildung 2.6: Ausgabe des Diagnoseprogrammes

Resümee

Wie schon beim Emulieren ist eine grundsätzliche Funktionsweise gegeben, jedoch mit entscheidenden Einschränkungen im Detail. Auch hier ließen sich die firmwareseitigen Schutzmechanismen nicht umgehen.

2.2.8 Manipulation der gespeicherten Daten

Befindet sich die PICC im Besitz des Angreifers, darf er, um das Gesamtsystems nicht zu gefährden, die gespeicherten Daten nicht beliebig verändern können. Dazu wurden von NXP verschiedene Maßnahmen getroffen.

Hilfsmittel

Es wird ein PCD benötigt.

Umsetzung

Bei dem Versuch auf die gespeicherten Daten zu zugreifen zeigt sich schnell, dass die frei erhältlichen und in 1.3 dargestellten Informationen nicht ausreichten. Zwar sind in der ISO-Norm die technischen Rahmenbedingungen und das Protokoll festgelegt und NXP hat Dokumente zur Speichertechnik offen gelegt, aber entscheidende Informationen fehlten.
In [NXP09c] werden die zur Verfügung stehenden Kommandos aufgelistet. Nur ohne die dazu gehörigen Bitfolgen ist unklar wie man diese mit der Technik aus der Norm aufrufen sollte. Die Suche nach der Binärdarstellung der Befehlsaufrufe erübrigte sich jedoch, als die libfreefare aus den nfc-tools([CT10]) offiziell Unterstützung für DESfire ICs hinzufügte.
Die nfc-tools sind eine Softwaresammlung, die auf der libnfc aufbaut. Die enthaltene libfreefare dient dabei als Funktionensammlung um eine geeignete API aufzubauen. Die Funktionen standen somit bereit, aber die Parameter der Funktionen wurden nicht erläutert. Bei Nachfragen in diversen Foren wurde stets auf ein vertrauliches Dokument verwiesen. Dieses würde einem nach der Unterzeichnung eines NDA(Non-Disclosure Agreement)[10] von NXP zur Verfügung gestellt. Dies war jedoch nicht notwendig. Einige Parameter erschlossen sich aus dem Kontext, weitere ließen sich durch Ausprobieren finden. Den entscheidenden Hinweis lieferte [Cou09], in dem die Zugriffsrechte beschrieben wurden. Die dabei gewonnen Erkenntnisse sollen nun dargestellt werden.
Per Voreinstellung werden alle neuen Schlüssel und auch der Master Key mit acht Null-Bytes belegt und per DES verschlüsselt. Im folgenden wird ein solcher Schlüssel mit Nullschlüssel bezeichnet. Diese Voreinstellung kann bei der EV1 geändert werden. Jedes Tag hat genau eine Master Application mit einem Master Key. Diese hat vier Zugriffsbeschränkungen, die in einem 8 Bit Wert verwaltet werden. Je nachdem ob ein bestimmtes Bit gesetzt ist, wird der Schlüssel für das Ausführen der jeweiligen Funktion benötigt oder nicht. Die vier beschränkten Funktionalitäten mit ihren jeweiligen Kontrollbits sind:

Ändern der Konfiguration (Bit 4)

Anlegen und Löschen von Applikationen ohne Schlüssel (Bit 3)

Auflisten der Applikationen ohne Schlüssel (Bit 2)

[10] zu deutsch: Verschwiegenheitsvereinbarung/Geheimhaltungsvertrag

Ändern des Master Keys (Bit 1)

Bei dem Anlegen einer Applikation muss eine der drei möglichen Übertragungsarten[11] ausgesucht und die Anzahl der zu verwendenden Schlüssel festgelegt werden. Eine Application kann mindestens einen und maximal 13 Schlüssel enthalten. Diese sind nach der Erstellung mit dem Nullschlüssel initialisiert. Applikationen haben die gleichen Zugriffsbeschränkungen wie die Master Application und der Master Key ist hierbei der erste Schlüssel.
Bei Files gestalten sich die Zugriffsrechte anders. Diese sind:

Lesen

Schreiben

Lesen und Schreiben

Zugriffsrechte ändern

Jedem dieser Rechte wird ein Schlüssel zugeordnet. Dabei wird jeweils die Nummer des Schlüssels verwendet. Den restlichen zwei Werten des Nibble[12] kommt eine Sonderrolle zu. Der Wert 14 bedeutet, dass kein Schlüssel, auch nicht der Nullschlüssel, benötigt wird und 15 verbietet jeglichen Zugriff. Insgesamt ergibt sich daraus dann ein 16 Bit Wert der folgenden Form:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Lesen				Schreiben				Lesen & Schreiben				Ändern			

Tabelle 2.6: Zugriffsrechte einer File

Um die jeweiligen Rechte nutzen zu können, muss man sich bei der Applikation mit dem entsprechenden Schlüssel authentifizieren.
Mit diesen Erkenntnissen war es möglich eine Brute-Force-Programm zu schreiben. Dabei stellt sich heraus, dass es ca. 4 Sekunden dauert 256 Authentifizierungsanfragen zu stellen. Als Folge daraus ergibt sich[13], dass es sogar mit der „kleinsten“

[11] siehe 1.3.3.3
[12] Als Nibble wird ein Halbbyte, also vier Bits, bezeichnet.
[13] Es wird ein uint8_t Array der Größe acht übergeben, also ergibt sich: 2^{56} **4s** = 288230376151711744**s**) 28823037615171174**4=60=60=24=365** 9139725271**:1730** Jahre

Verschlüsselung (DES) viel zu lange dauern würde eine vollständige Schlüsselsuche durch zu führen.

Resümee

Solange zur Schlüsselfindung kein anderer Weg außer der Brute-Force-Methode gefunden wird, sind die Daten sicher.

2.2.9 Abhören und Replay

Ein System auf Basis von Mifare DESfire Chipkarten basiert auf der ISO 14443 A Norm und einem der unterstützten Verschlüsselungsalgorithmen. Diese Algorithmen bestehen aus festgelegten Operationen und sind unabhängig von Zufallswerten. In der ISO Norm kann nur die UID der Karte zufällig generiert werden[14]. Dadurch müsste die gleiche Befehlsabfolge auch das gleiche Ergebnis liefern, solange die UID im Bereich der vom PCD akzeptierten liegt.
Gelingt es dem Angreifer eine Kommunikationssitzung abzuhören und zu speichern, kann er diese aufgrund der Synchronität sowie den Modulationsverfahren die Nachrichten den beiden Beteiligten zuordnen. Je nach Angriffsziel wird er dann einem PCD die Nachrichten der PICC übermitteln (z.B. bei einer Zutrittskontrolle) oder der PICC PCD-Nachrichten vortäuschen(z.B. um gespeichertes Guthaben zu erhöhen).

Hilfsmittel

Man benötigt ein Gerät, das die verschiedenen Taktflanken der Modulationsarten messen kann. Idealerweise würde es die so gewonnen Daten direkt als Bitfolgen oder Bytewerte umrechnen und zur Weiterverarbeitung an einen Computer übertragen.

Umsetzung

Wie bereits mehrfach erwähnt wird bei dem touchatag die Funkelektronik hinter einem Microcontroller vor dem direkten Zugriff verborgen. Dieser Controller ermöglicht weder das Auslesen der Taktflanken noch stellt er eine Möglichkeit bereit die Kommunikation mit zu hören.

[14] Die Möglichkeit die UID auch zufällig zu erzeugen besteht erst seit der Revision von 2008.

Resümee

Dieser Angriff ist mit einem touchatag nicht durchführbar.

2.2.10 Differenzielle elektro-magnetische Analyse

Die DEMA(Differenzielle elektro-magnetische Analyse) stellt eine Seitenkanalattacke dar, da sie nicht die eigentliche kryptographie Methode sondern eine Eigenschaft der Implementierung ausnutzt. Im Falle von passiven RFID-Systemen ist das der Stromverbrauch. Den Strom beziehen die PICCs aus der Amplitude des elektromagnetichen Feld des PCDs. Diese ist folglich etwas kleiner, wenn der Chip mehr Energie bedarf, als wenn er keine braucht. Da unterschiedliche Berechnungen mit abweichenden Werten verschiedene Energieverbrauchswerte aufweisen, kann man diese den Abweichungen von der sonst erzeugten Schwingung zuordnen.
Dazu führt man die Authentikation durch. Dabei wird der Wert nach dem Protokollkommando des PCD von der PICC verschlüsselt. Daraufhin betrachtet man die dabei resultierenden Schwingungen des Feldes.
Bei Tags, die DES als Verschlüsselungsalgorithmus verwenden, ist es in [KOP09] anhand der Schiebeaktionen zwischen den DES-Runden gelungen die Teilschlüssel der S-Boxen 1, 2, 3, 4 und 8 korrekt zu identifizieren und somit 30 Bits des Schlüssels zu rekonstruieren.

Hilfsmittel

Für diese Analyse benötigt man ein Oszilloskop, mit dem man sehr genau die Feldstärke messen kann. Zu dem Testaufbau in [KOP09] gehört weiterhin ein speziell entwickelter PCD der eindeutige Trigger-signale zur genauen zeitlichen Bestimmung aussendet.

Umsetzung

Der Preis für ein geeignetes Oszilloskop übersteigt den gesetzten Kostenrahmen, deshalb wurde von einer Umsetzung abgesehen. Warum der Angriff trotzdem teil dieser Arbeit wurde, wird im nächsten Abschnitt erleutert.

Resümee

Da die DEMA auf Messungen der Trägerwelle basiert stellt sie aus mehreren Gründen einen äußerst effektiven Angriff dar. Diese Welle lässt sich noch im Fernfeld, also aus über 22 Metern Entfernung, messen und ist nicht invasiv. Würde es gelingen dadurch einen ausreichend kompletten Schlüssel gewinnen[15], würden die meisten der bereits genannten Angriffe obsolet.
Obwohl die momentanen Kosten hoch sind, könnte sich aus den gewonnenen Erkenntnissen spezialisierte Hardware zu einem geringen Preis entwickeln. Unter diesen Gesichtspunkt ist das Setzen eines Maximalpreises pro Angriffsmethode nicht sinnvoll. Zudem wird sich der Aufwand eines Angreifers nach dem zu erwartenden Gewinn richten und dieser ist bei den Einsatzgebieten der DESfire Chipkarten durchaus beträchtlich.

[15] Die Autoren von [KOP09] legen nahe, dass dies bei DES-Verschlüsselung bereits gelungen ist.

3 Abschluss

3.1 Zielerreichung/Ergebnisbewertung

Der Auswahl der Angriffe ging ein intensives Studium der FCDs, der bisherigen Attacken auf Mifare-Systeme und der vewendeten Verschlüsselungsverfahren voraus. Dabei wurde deutlich, dass sich der Data Encryption Standard in seiner langen in 1.3.2.1 dargestellten Geschichte als äußerst resistent erwiesen hat. Der Brute-Force-Ansatz hat sich bis heute als beste Methode zur Dechiffrierung erwiesen.
Das Abschirmen der Daten durch dieses offene und viel geteste Verfahren erwies sich als größtes Hinderniss und führte dazu, dass die verbleibenden Attacken entweder generischer Art sind, z.B. Zerstören und Ablösen, oder sich gegen die kontaktlose Kommunikation wenden.
Diese sind hauptsachlich an der verwendeten Hardware, dem touchatag, gescheitert. Dessen Microcontroller PN532 wurde von NXP entwickelt und enthält effektive Sperren. Würde man den selbstgesteckten Kostenrahmen erweitern, könnte man für 160 € einen Proxmark3 unter [BKf11] kaufen. Dieser basiert auf einen offengelegtem Design und sollte keine künstlichen Hindernisse enthalten.
Insgesamt sind die erfolgreich[1] durchgeführten Angriffe zu allgemein, um speziell als Schwäche der Mifare DESFire Implementierung gelten zu können. Dennoch scheint die Mifare Plus X als einziger IC mit seinem integrierten Entfernungscheck wirklich sicher; allerdings nur, wenn er im Security Level 3 und AES-verschlüsselt betrieben wird.
Außerdem bleibt Abzuwarten wie sich die DEMA entwickelt.

3.2 Fazit

Das Zusammenspiel zwischen touchatag und libnfc (und den nfc-tools) ermöglicht einen kostengünstigen und relativ einfachen Einstieg in den RFID-Bereich. Jedoch

[1] Im Hinblick auf 1.1.3.

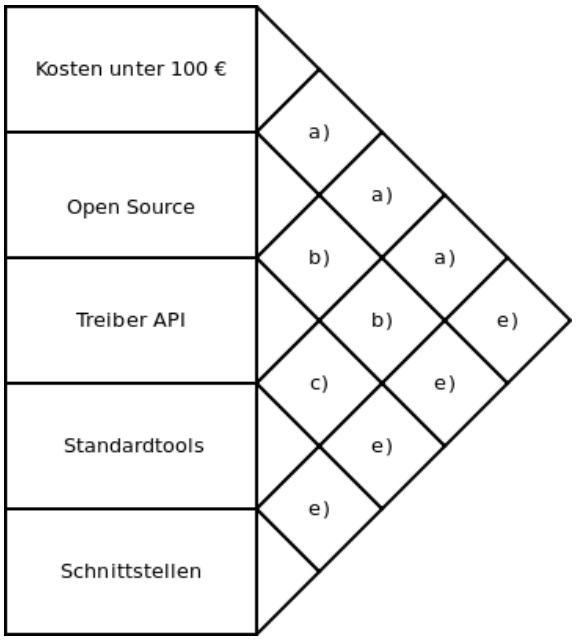
verhindern die bereits genannten Einschränkungen effektive und tiefgreifende Analysen. Dazu ist ein Gerät nötig, welches den direkten Zugriff auf die Funkhardware und die Programmierung des Microcontrollers erlaubt. Das Ziel der Arbeit (Kapitel 1.1.3) konnte deshalb nur unbefriedigend erreicht werden.
Obwohl schon vor mehr als 100 Jahren erkannt wurde, dass Sicherheit von Informationen nicht von dem verwendeten Verfahren abhängen darf[2], stellt NXP immer noch Teile des Datenzugriffsverfahrens unter ein NDA. Die Sinnlosigkeit dieses Vorgehens wurde bereits bei der Mifare Classic eindrucksvoll bewiesen. Zusätzlich entstand als Nebenprodukt von 2.2.8 eine annähernd vollständige Implementation der DESFire Funktionalitäten ohne Zugriff auf geheime Daten und ohne die Unterzeichnung einer Verschwiegensheitserklärung. Der Quellcode, sowie der Code aller in diesem Rahmen entstandenen Programme, findet sich auf dem Begleitdatenträger und ermöglicht es die vierstelligen Preise anderer Anbieter, z.B. [fMSm10], zu umgehen.
Aufbauend darauf wäre es interessant verschiedene Energieschwankungen in unterschiedlichen Szenarien, wie z.B. beim Lesen, Inkrementierung, etc., zu messen und zu untersuchen, ob damit Rückschlüsse auf den verwendeten Schlüssel möglich sind. Die DEMA allgemein erscheint momentan als vielversprechenster Kandidat, um die DESFire Implementierung zu brechen. Sie kann nicht nur erste Ergebnisse vorweisen, sondern ist auch aus größeren Entfernungen durchführbar und damit stellt einen realistisch einsetzbaren Angriff dar.
Aber auch sie basiert auf der Funkübertragung. Folglich kann der DESFire IC als sicher angesehen werden, solange außerhalb des tatsächlichen konkreten Gebrauchs 2.2.3 als Abwehrmaßnahme eingesetzt wird.

[2] Kerckhoffs'sches Prinzip

A Anhang

A.1 Präferenzanalyse

Die Präferenzanalyse dient dazu, die gefundenenen Anforderungen zu priorisieren. Dazu werden sie paarweise gegenübergestellt und in ihrer Wichtigkeit verglichen. Bei dem Vergleich scheidet die Möglichkeit „gleich wichtig“ aus. Dadurch werden Präferenzen gefunden. Um die bisher gefunden Gewichtungsfaktoren zu validieren, wurde sie deshalb zusätzlich durchgeführt.



Anhand der Anzahl der festgestellten Präferenzen lassen sich Gewichtungsfaktoren ermitteln.

Anforderungen	Kosten	Open Source	Treiber	Hilfestellungen	Schnittstellen
Nennungen	3	2	1	0	4
prozentualer-Anteil	30	20	10	0	40

Tabellenverzeichnis

Abbildungsverzeichnis

Formelverzeichnis

Literaturverzeichnis

[AL10a] Alcatel-Lucent: *Downloads*. Technischer Bericht, Alcatel-Lucent, 2010. http://www.touchatag.com/downloads 22. September 2010.

[AL10b] Alcatel-Lucent: *Using the Advanced HTTP Application*. Technischer Bericht, Alcatel-Lucent, 2010. http://www.touchatag.com/developer/docs/applications/advanced-HTTP 22. September 2010.

[BKf11] Bearstech.com, Kd85.com und faberNovel.com: *Proxmark III RFID card, "no more kittingëdition*. Technischer Bericht, hackable-devices.org, 2011. http://hackable-devices.org/products/product/proxmark-iii-rfid-card-no-more-kitting-edition/ 25. Januar 2011.

[B.V10] B.V., NXP: *MIFARE Ultralight Features and Hints*. Technischer Bericht, NXP B.V., 2010. http://www.nxp.com/documents/application_note/AN073121.pdf 08. November 2010.

[C:10] C:, INFORMAT: *SCM SCL3711*. Technischer Bericht, INFORMAT C:, 2010. http://www.informathica.de/product_info.php?info=p419_SCM-SCL3711 22. September 2010.

[Cou09] Council, Bracknell Forest Borough: *Mifare DESFire Specification*. Technischer Bericht, LASSeO, 2009. http://www.lasseo.org.uk/papers/DESFIRE_Specification_V1.0.pdf 20. Januar 2011.

[CRY10] CRYPTAS: *OMNIKEY 5321 USB RFID*. Technischer Bericht, CRYPTAS it-Security GmbH AUSTRIA, 2010. http://www.cryptoshop.com/de/products/reader/rfid/2010101023.php 22. September 2010.

[CT10] Conty, R. und Roman Tartiere: *nfc-tools - Near Field Communication (NFC) tools under POSIX systems*. Technischer Bericht, Google Project Hosting, 2010. http://code.google.com/p/nfc-tools/ 20. Januar 2011.

[EC10] Electronic-Componentsseller: *CLRD701 PEGODA Contactless smart card reader*. Technischer Bericht, eBay Inc., 2010. http://cgi.ebay.de/mifare-%ae-Pegoda-Contactless-Smart-Card-Reader-CLRD701_W0QQitemZ310230565432QQcmdZViewItem?rvr_id=143675264625\&rvr_id=143675264625\&cguid=8daac57f1290a0aad456bee6fe9f6546#ht_4441wt_934 22. September 2010.

[Ele10] Elektronik, Jacob: *SCL010 Desktop Leser*. Technischer Bericht, Jacob Elektronik GmbH, 2010. http://direkt.jacob-computer.de/Eingabeger%E4te_Diverse_Eingabeger%E4te_SCL010_Desktop_Leser_(905073)_artnr_289342.html?direkt=1\&ref=1244 22. September 2010.

[Ert07] Ertel, Wolfgang: *Angewandte Kryptographie*. Hanser Verlag, 3. Auflage, 2007.

[Fin06] Finkenzeller, Klaus: *RFID-Handbuch*. Hanser Verlag, 4. Auflage, 2006.

[fMSm10] Microprocessor-Systeme mbH, MP-Sys Gesellschaft für: *ChipMan - Schnell und einfach kodieren von kontaktbehafteten und kontaktlosen Chipkarten*. Technischer Bericht, MP-Sys Gesellschaft für Microprocessor-Systeme mbH, 2010. http://www.mpsys.de/resources/chipmaninfo.pdf 25. Januar 2011.

[Glo10a] Global, HID: *CardMan 5121 RFID*. Technischer Bericht, HID Global, 2010. http://www.hidglobal.com/driverDownloads.php?techCat=19\&prod_id=168 22. September 2010.

[Glo10b] Global, HID: *Contactless Developer Guide*. Technischer Bericht, HID Global, 2010. http://www.hidglobal.com/documents/ok_contactless_developer_guide_an_en.pdf 22. September 2010.

[Glo10c] Global, HID: *Readers-PC Connected*. Technischer Bericht, HID Global, 2010. http://www.hidglobal.com/technology.php?tech_cat=19\&subcat_id=10 22. September 2010.

[Incbe] Inc., NXP: *MIFARE DESFire Backwards compatibility*. Technischer Bericht, NXP Inc., keine Angabe. http://www.plasticard.de/fileadmin/downloads/produkte/DESFireDifference.pdf 29. Oktober 2010.

[KOP09] Kasper, T., D. Oswald und C. Paar: *New Methods for Cost-Effective Side-Channel Attacks on Cryptographic RFIDs*. In: *Workshop on RFID Security, RFIDSec*, 2009.

[lib10a] libnfc: *Compatible NFC devices*. Technischer Bericht, libnfc, 2010. http://www.libnfc.org/documentation/hardware/compatibility 22. September 2010.

[lib10b] libnfc: *libnfc - Public platform independent Near Field Communication (NFC) library*. Technischer Bericht, Google, 2010. http://code.google.com/p/libnfc/ 22. September 2010.

[lib10c] libnfc: *libnfc developers community*. Technischer Bericht, libnfc, 2010. http://www.libnfc.org/community/ 22. September 2010.

[lib10d] libnfc: *libnfc developers community*. Technischer Bericht, libnfc, 2010. http://www.libnfc.org/api/ 22. September 2010.

[lib10e] libnfc: *libnfc developers community*. Technischer Bericht, libnfc, 2010. http://code.google.com/p/libnfc/issues/list 22. September 2010.

[Mic10a] Microsystems, SCM: *SCL010*. Technischer Bericht, SCM Microsystems GmbH, 2010. http://www.scmmicro.com/products-services/smart-card-readers-terminals/contactless-dual-interface-readers/scl010.html 22. September 2010.

[Mic10b] Microsystems, SCM: *SCL010*. Technischer Bericht, SCM Microsystems GmbH, 2010. http://www.scmmicro.com/fileadmin/products/datasheets/SCL010.MANUAL.VER13.pdf 22. September 2010.

[Mic10c] Microsystems, SCM: *SCL3711*. Technischer Bericht, SCM Microsystems GmbH, 2010. http://www.scmmicro.com/fileadmin/products/datasheets/SCL3711.MANUAL.VER16.pdf 22. September 2010.

[Nie10] Niehusen, Karsten: *CardMan 5121 RFID*. Technischer Bericht, cardomatic.de, 2010. http://www.cardomatic.de/start.php?d_O20011_Omnikey_5121_RFID.php 22. September 2010.

[NXP05] NXP: *MIFARE Milestones*. Technischer Bericht, NXP Semiconductors Austria GmbH Styria, 2005. http://www.mifare.net/about/milestones.htm 27. September 2010.

[NXP07] NXP: *UM0701-02 PN532 User Manual*. Technischer Bericht, NXP B.V., 2007. http://www.nxp.com/documents/user_manual/141520.pdf 18. Januar 2011.

[NXP08a] NXP: *Break DES in less than a single day*. Technischer Bericht, NXP Semiconductors Austria GmbH Styria, 2008. http://www.mifare.net/security/mifare_classic.asp 20. September 2010.

[NXP08b] NXP: *Frequently Asked Questions*. Technischer Bericht, NXP Semiconductors Austria GmbH Styria, 2008. http://www.mifare.net/security/faq.asp 09. September 2010.

[NXP08c] NXP: *MIFARE DESFire EV1 - NXP IC solution for contactless multi-application, high speed and secure smart cards*. Technischer Bericht, NXP B.V., 2008. http://www.nxp.com/documents/leaflet/75016504.pdf 09. September 2010.

[NXP09a] NXP: *MF0ICU1 MIFARE Ultralight contactless single-trip ticket IC*. Technischer Bericht, NXP B.V., 2009. http://www.nxp.com/documents/data_sheet/MF0ICU1.pdf 09. September 2010.

[NXP09b] NXP: *MIFARE Application Directory (MAD)*. Technischer Bericht, NXP B.V., 2009. www.nxp.com/acrobat_download2/other/identification/AN10787_6.pdf 30. September 2010.

[NXP09c] NXP: *MIFARE DESFire EV1 contactless multi-application IC*. Technischer Bericht, NXP B.V., 2009. http://www.nxp.com/acrobat_download2/other/identification/145630_MF3ICD81_MF3ICD41_MF3ICD21_sds.pdf 30. September 2010.

[NXP09d] NXP: *MIFARE PlusTM; Migrate classic contactless smart card systems to the next security level*. Technischer Bericht, NXP Semiconductors, 2009. http://www.nxp.com/documents/leaflet/75016722.pdf 09. September 2010.

[NXP09e] NXP: *MIFARE Type Identification Procedure*. Technischer Bericht, NXP B.V., 2009. http://www.nxp.com/documents/application_note/AN10833.pdf 09. September 2010.

[NXP09f] NXP: *MIFARE Ultralight C*. Technischer Bericht, NXP B.V., 2009. http://www.nxp.com/documents/short_data_sheet/MF0ICU2_SDS.pdf 08. November 2010.

[NXP09g] NXP: *MIFARE Ultralight C - NXP IC solution for contactless limited-use applications with enhanced security*. Technischer Bericht, NXP B.V., 2009. http://www.nxp.com/acrobat_download/literature/9397/75016620.pdf 09. September 2010.

[NXP09h] NXP: *NXP SmartMX : high security microcontroller IC*. Technischer Bericht, NXP B.V., 2009. http://www.nxp.com/documents/leaflet/75016823.pdf 09. September 2010.

[NXP10a] NXP: *4 Byte & 7 Byte UIDs of MIFARE products*. Technischer Bericht, NXP Semiconductors Austria GmbH Styria, 2010. http://www.mifare.net/news/47byteuids_statement.asp 09. September 2010.

[NXP10b] NXP: *4 Byte and 7 Byte UID offering of MIFARE ClassicTM, MIFARE PlusTM, SmartMXTM and licensed products*. Technischer Bericht, NXP Semiconductors Austria GmbH Styria, 2010. http://www.mifare.net/downloads/Customer_Letter_UID_Topic_ENG_Version.pdf 09. September 2010.

[NXP10c] NXP: *AN10927 - MIFARE and handling of UIDs*. Technischer Bericht, NXP B.V., 2010. http://www.nxp.com/acrobat_download/other/identification/AN10927.pdf 09. September 2010.

[NXP10d] NXP: *CLRD701 PEGODA Contactless smart card reader*. Technischer Bericht, NXP Semiconductors, 2010. http://www.nxp.com/#/pip/pip=[pip=PE099231]|pp=[t=pip,i=PE099231] 22. September 2010.

[NXP10e] NXP: *MF1PLUSx0y1 - Mainstream contactless smart card IC for fast and easy solution development*. Technischer Bericht, NXP B.V., 2010. http://www.nxp.com/documents/short_data_sheet/MF1PLUSX0Y1_SDS.pdf 08. November 2010.

[NXP10f] NXP: *MF1SPLUSx0y1 - Mainstream contactless smart card IC for fast and easy solution development*. Technischer Bericht, NXP B.V., 2010. http://www.nxp.com/documents/short_data_sheet/MF1SPLUSX0Y1_SDS.pdf 08. November 2010.

[PDB10] Polk, W. Timothy, Donna F. Dodson und William. E. Burr: *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. Technischer Bericht, National Institute of Standards and Technology, 2010. http://csrc.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf 07. September 2010.

[Plö08] Pl
ötz, H.: *Mifare Classic–Eine Analyse der Implementierung*. Master's thesis, Humboldt-Universit
ät zu Berlin, 2008.

[RFD08a] RFDump.org: *Hardware*. Technischer Bericht, RFDump.org, 2008. http://www.rfdump.org/hw.shtml 22. September 2010.

[RFD08b] RFDump.org: *What is RFDump*. Technischer Bericht, RFDump.org, 2008. http://www.rfdump.org/ 22. September 2010.

[RSS10a] RSSystems: *Electronic Boards and Systems*. Technischer Bericht, eBay Inc., 2010. http://stores.ebay.de/Electronic-Boards-and-Systems 22. September 2010.

[RSS10b] RSSystems: *RFID READER/WRITER, MIFARE 13,56MHz, USB + 3Tags*. Technischer Bericht, eBay Inc., 2010. http://cgi.ebay.de/RFID-READER%2fWRITER,-MIFARE-13,56MHz,-USB-%20-3Tags_W0QQitemZ200387835226QQcmdZViewItem?rvr_id=\&rvr_id=\&cguid=3f6ed0751280a0e204c3ded3fde0c145 22. September 2010.

[RSS10c] RSSystems: *R.S.Sytems*. Technischer Bericht, RSSystems - Germany, 2010. http://www.rss-systems.de/ 22. September 2010.

[Sch06] Schneier, Bruce: *Angewandte Kryptographie*. Pearson Studium, 2006.

[Sch10] Schatz, Stern &: *Touchatag*. Technischer Bericht, Stern & Schatz GmbH, 2010. http://www.getdigital.de/products/Touchatag 22. September 2010.

[sci10] sciengines: *Break DES in less than a single day*. Technischer Bericht, SciEngines GmbH, 2010. http://www.sciengines.de/company/news-a-events/74-des-in-1-day.html 14. September 2010.

[Sem05] Semiconductors, Philips: *MIFARE DESFire MF3 IC D40 Short Form Specification*. Technischer Bericht, Koninklijke Philips Electronics N.V., 2005. www.nxp.com/documents/short_data_sheet/075532.pdf 30. September 2010.

[Sem10] Semiconductors, NXP: *Secure dual interface and contact PKI smart card controller from NXP Semiconductors*. Technischer Bericht, NXP B.V., 2010. http://www.nxp.com/#/pip/pip=[pip=P5CD016_021_041_CX081_FAM_SDS,jp=Features]|pp=[t=pip,i=P5CD016_021_041_CX081_FAM_SDS] 23. November 2010.

[Sys10] Systems, Advanced Card: *ACR122U*. Technischer Bericht, Advanced Card Systems Ltd., 2010. http://www.acs.com.hk/index.php?pid=product\&prod_sections=0\&id=ACR122U 22. September 2010.

[Ver10] Verdult, Roel: *Introduction*. Technischer Bericht, libnfc, 2010. http://www.libnfc.org/documentation/introduction 22. September 2010.

[Wel08] Welte, Harald: *libnfc developers community*. Technischer Bericht, openmrtd, 2008. http://openmrtd.org/projects/librfid/ 22. September 2010.

[zr06] zapper.20.minime@spamgourmet.com und rfid.20.mahajivana@spamgourmet.com: *RFID-Zapper*. Technischer Bericht, Chaos Computer Club, 2006. https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper_de61.html 21. Januar 2011.

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt wurde. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen oder anderen Quellen entnommen sind, sind als solche eindeutig kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form noch nicht veröffentlicht und noch keiner Prüfungsbehörde vorgelegt worden.

Schmalkalden, den 27. Januar 2012

_____

Jonas Groß