Durchführung einer Relay Attacke durch Interception der Android NFC-Schnittstelle

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Software & Information Engineering

eingereicht von

Michael Peyerl
Matrikelnummer 1326027

ausgeführt am
Institut für Information Systems Engineering
Forschungsgruppe Industrial Software
der Fakultät für Informatik der Technischen Universität Wien

Betreuung: Thomas Grechenig
Mitwirkung: Clemens Hlauschek

Wien, 3. Juli 2018

Kurzfassung

Über diese Vorlage: Dieses Template dient als Vorlage für die Erstellung einer wissenschaftlichen Arbeit am INSO. Individuelle Erweiterungen, Strukturanpassungen und Layout-Veränderungen können und sollen selbstverständlich nach persönlichem Ermessen und in Rücksprache mit Ihrem Betreuer vorgenommen werden.

Aufbau: In der Kurzfassung werden auf einer 3/4 bis maximal einer Seite die Kernaussagen der Diplomarbeit zusammengefasst. Dabei sollte zunächst die Motivation/der Kontext der vorliegenden Arbeit dargestellt werden, und dann kurz die Frage-/Problemstellung erläutert werden, max. 1 Absatz! Im nächsten Absatz auf die Methode/Verfahrensweise/das konkrete Fallbeispiel eingehen, mit deren Hilfe die Ergebnisse erzielt wurden. Im Zentrum der Kurzfassung stehen die zentralen eigenen Ergebnisse der Arbeit, die den Wert der vorliegenden wissenschaftlichen Arbeit ausmachen. Hier auch, wenn vorhanden, eigene Publikationen erwähnen.

Wichtig: Verständlichkeit! Die Kurzfassung soll für Leser verständlich sein, denen das Gebiet der Arbeit fremd ist. Deshalb Abkürzungen immer zuerst ausschreiben, in Klammer dazu die Erklärung: z.B: “Im Rahmen der vorliegenden Arbeit werden Non Governmental-Organisationen (NGOs) behandelt, . . . ”. In LaTeXwird diese bereits automatisch durch verwenden des Befehls `\ac` erreicht. Für Details siehe Paket `glossaries`.

Schlüsselwörter

Abstract

About this template: This template helps writing a scientific document at INSO. Users of this template are welcome to make individual modifications, extensions, and changes to layout and typography in accordance with their advisor.

Writing an abstract: The abstract summarizes the most important information within less than one page. Within the first paragraph, present the motivation and context for your work, followed by the specific aims. In the next paragraph, describe your methodology / approach, and / or the specific case you are working on. The third paragraph describes the results and the contribution of your work.

Comprehensibility: People with different backgrounds who are novel to your area of work should be able to understand the abstract. Therefore, acronyms should only be used after their full definition has given. E.g., "This work relates to non-governmental organizations (NGOs), . . . ".

Keywords

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Liste der Listings

Liste der Algorithmen

1 Einleitung

In der Einleitung soll die Zielsetzung der Arbeit beschrieben, ihre Einordnung in einen übergeordneten Kontext hergestellt und die Bedeutung des Themas erörtert werden. Zu diesem Zweck ist die Einleitung in folgende Unterkapitel unterteilt:

- Problemstellung
- Motivation
- Zielsetzung
- Aufbau der Arbeit

Organisatorisches Der Umfang einer Diplomarbeit beträgt üblicherweise 90 bis ca. 120 Seiten und bei Bachelorarbeiten 40 bis ca. 60 Seiten. Beurteilungskriterien für eine Diplomarbeit ist nicht nur die Qualität der praktischen Arbeit, sondern auch Aufbau, Inhalt und Formulierung der schriftlichen Arbeit. Insbesondere sind die Grundregeln wissenschaftlichen Arbeitens (z.B. richtiges Zitieren) zu beachten.

Allgemeines Achtung beim Setzen von Absätze.

Fußzeilen: Bei technischen Arbeiten eher unüblich.
In den Sozialwissenschaften (z.B. BWL) ist es üblich, die Referenz in eine Fußnote zu setzen.
In den technischen Wissenschaften ist es üblich, im Text ein Kürzel (Dorn et al. 1999) oder eine Zahl [1] zu verwenden, um dann im Anhang der Arbeit alle Referenzen detailliert aufzuführen, wobei jede Referenz mit dem Kürzel beginnt.

Bei einer wissenschaftlichen Arbeit wird Wert auf die Einhaltung formaler Aspekte des guten Schreibens gelegt. Es ist hilfreich, wenn man seinen eigenen Schreibstil kritisch in Bezug auf folgende Punkte überprüft:

- Einfachheit (das Keep It Sober and Significant (KISS)-Prinzip gilt nicht nur für die Softwareentwicklung, sondern auch für wissenschaftliche Arbeiten: Mach es schlicht und wesentlich/Keep It Sober and Significant)
- Gliederung/ logische Ordnung (vom Allgemeinen zum Konkreten, nachvollziehbare Kette von einer Fragestellung/ einem Problem über die Bearbeitung und Zerlegung in Detailprobleme zur Lösung und der Ableitung von Erkenntnissen)
- Kürze/Prägnanz (keine Schachtelsätz, Wiederholungen vermeiden – “Don’t repeat yourself”)
- Anregende Zusätze (erläuternde/ interessante/ spannende Praxisbeispiele etc.)
- Sprache/Stil (kein Erzählstil, möglichst keine “ich”-Form, objektiv)
- Korrekte Formeln und Abbildungen
- Korrekte Zitierweise (siehe Kapitel Literaturverzeichnis)

- Einhaltung definierter Rahmenbedingungen (z.B. diese Vorlage)
- Vermeiden von Anglizismen. Grundsätzlich sollte in einer in Deutsch verfassten Diplomarbeit immer das deutsche Wort verwendet werden, wenn es unmissverständlich und akzeptiert ist. Ein Eindeutschen um jeden Preis ist allerdings zu vermeiden, da dies zu schwer lesbaren Texten führt. Beispiele: Der Begriff "Unterbrechung des Programmflusses" ist angebrachter als "Interrupt des Programmflusses", und "verdeckte Kanäle" ist als akzeptierter deutscher Begriff für "Covert Channels" zu verwenden. Umgekehrt ist aber "Cursor" das bessere Wort als "Lichtmarke". Anglizismen können als Stilmittel genutzt werden, etwa wenn man von einer "Quick and Dirty" Implementierung spricht.

Typographie Grundsätzlich sollten nicht mehr als drei unterschiedliche Schriftarten verwendet werden. Grundsätzlich sollte die Typographie sowie die Anordnung von Bildern, Tabellen, etc. LaTeXüberlassen werden. Allerdings können Silbentrennungen durch \- gesteuert werden.

Abweichungen nach persönlichem Geschmack und in Rücksprache mit Ihrem Betreuer sind zulässig. Als Stilmittel werden üblicherweise nur die Fettschrift und Kursivschrift verwendet - Unterstreichungen, Schattenschriften etc. sind zu vermeiden. Blocksatz bitte mit automatischer Silbentrennung verwenden, Rechtschreibprüfung aktivieren.

Generell kann bei der Einleitung eine modifizierte Version des Exposés als Basis verwendet werden.

1.1 Problemstellung

Formulierung der Problemstellung, Einbettung in das Forschungsumfeld und Theorie, auf die sich die Arbeit beziehen. Tendenziell kurz, allgemeiner und sehr gut verständlich – detaillierter im Kapitel "Grundlagen".

Die formulierte Fragestellung soll das Interesse an der Lösung wecken (eine langweilige oder triviale Problemstellung lässt meistens auch eine eher weniger interessante wissenschaftliche Arbeit erwarten).

1.2 Motivation

In diesem Kapitel wird der Forschungsbedarf aufgezeigt. Nach dem Lesen dieses Kapitels sollten folgende Punkte klar dargestellt sein:

- Aktueller Stand der Wissenschaft in Bezug auf die zuvor formulierte Problemstellung und klare Darstellung, was hier unzureichend/offen ist.
- GGf. Darstellung des größeren Forschungsbereichs, in den die Diplomarbeit eingebettet ist.
- Darlegung der Bedeutung des Themas für den Stand oder die Weiterentwicklung eines Bereichs der Informatik (z.B. Datenbanksysteme, Mobile Anwendungen, Java-Programmierung, Rechenzentrumsbetrieb, ...) oder eines Fachbereichs (z.B. Bankwesen, Wertpapierhandel, Gesundheitswesen, Transportwesen, Flugsicherheit ...). Erklärung, was durch die Lösung des Problems z.B. kostengünstiger/schneller/hochwertiger/sicherer/anwendbarer/"schöner" etc. wird.

1.3 Zielsetzung

Nachdem die Problemstellung und die Motivation zu deren Lösung formuliert wurden, wird in diesem Kapitel das zu erarbeitende Resultat beschrieben.

2 Grundlagen und Hintergründe

Dieses Kapitel beschreibt Grundlagen und Konzepte, die eine wichtige Rolle als Fundament für das Verständnis der Arbeit einnehmen. In erster Linie wird die Kommunikationstechnologie Near Field Communication (NFC) und ihre Funktionsweise vorgestellt. Es soll behandelt werden, wie NFC technisch umgesetzt ist und mithilfe welcher Komponenten und Methoden die drahtlose Kommunikation erfolgt. Außerdem soll auf die Ausführung der Technologie auf mobilen Android Geräten eingegangen und Sicherheitsrisiken und -konzepte beschrieben werden. Ein äußerst relevanter Punkt im Zusammenhang mit dieser Arbeit ist die Relay Attacke. Das Prinzip hinter diesem Angriff und dessen praktische Ausführung werden ebenfalls behandelt.

2.1 Near Field Communication (NFC)

Near Field Communication ist eine drahtlose Datenübertragungstechnologie ähnlich wie Bluetooth oder WLAN, mit der auf einfachem und schnellem Weg kleinere Datenmengen über kurze Distanzen übertragen werden können. Im Vergleich zu anderen kontaktlosen Übertragungsmöglichkeiten muss bei NFC allerdings keine Kopplung der Geräte, die an der Datenübertragung teilnehmen wollen, stattfinden. Befindet sich ein NFC-kompatibles Gerät in der Nähe eines anderen, wird das Senden und Empfangen von Informationen automatisch gestartet, was die Benützung der Technologie sehr angenehm und einfach gestaltet.

Erstmals wurde die Entwicklung von NFC im Jahr 2002 von Philips und Sony bekanntgegeben [4], die zwei Jahre darauf gemeinsam mit Nokia das NFC Forum, einen Non-Profit Industrieverband zur Entwicklung der Technologie und deren Spezifikation, gründeten [13, 21]. Die Organization hat bis zum Jahr 2018 insgesamt 16 Spezifikationen der NFC Technologie veröffentlicht und zählt zahlreiche einflussreiche Unternehmen wie Apple, Google, Intel, Sony, Visa, Mastercard und viele weitere zu seinen Mitgliedern [21].

Zusätzlich zu den Spezifikationen des NFC Forums ist NFC durch den ISO 18092 Standard sowie ETSI TS 102 190 Standard standardisiert, der die Kommunikationsmodi für das NFC Interface und das NFC Protokoll beschreibt [14, 31].

2.1.1 Die Funktionsweise von NFC

Die Basis für die Funktionsweise von NFC bildet das Prinzip der magnetischen Induktion [34]. Dieses allgemein bekannte Prinzip besagt, dass ein sich ändernder elektrischer Strom ein Magnetfeld hervorruft und umgekehrt ein sich änderndes Magnetfeld, elektrischen Strom in einem Leiter erzeugt. Ein NFC Chip besteht daher grundlegend aus einer Spule, die mit elektrischem Strom versorgt werden kann und dadurch ein elektromagnetisches Feld hervorruft. Dieses besitzt eine festgelegte Frequenz im 13,56 MHz Bereich [34] und kann in der nahen Umgebung des Erzeugers genutzt werden, um einen Kommunikationskanal aufzubauen. NFC-fähige Geräte können grundsätzlich in zwei Modi operieren: aktiv und passiv.

Passiver Modus

Im passiven Modus nehmen an der Kommunikation sowohl ein aktiver als auch ein passiver Partner teil. Der aktive Teilnehmer versorgt den NFC Chip des Gerätes mit elektrischem Strom wo-

durch ein elektromagnetisches Feld erzeugt wird. Wird ein passiver NFC Chip ohne eigene Stromversorgung, auch Tag genannt, in die Nähe des aussendenden Gerätes gebracht, verursacht dies in der Spule des passiven Chips wiederum einen elektrischen Strom, der für den Betrieb genutzt werden kann. Mithilfe dieser Methode können Daten übertragen werden indem der aktive Erzeuger sein Feld direkt verändert. Diese Änderungen können als Daten wahrgenommen und gesendet werden. Der passive Kommunikationspartner modifiziert das Feld durch das Entziehen von Energie, wodurch Feldschwankungen, die vom Feldverursacher als Informationen identifiziert werden können, entstehen [18].

Aktiver Modus

Im aktiven Modus generiert und verändert jeder der Kommunikationspartner sein eigenes elektromagnetisches Feld, was vom jeweils anderen Teilnehmer als Information interpretiert werden kann [18].

Geräte, die NFC unterstützen, sind typischerweise in der Lage zwischen aktivem und passivem Modus zu wechseln und befinden sich standardmäßig im passiven Zustand [5]. Vor der Initiierung einer Verbindung über NFC wird jedem Kommunikationsteilnehmer eine aktive bzw. passive Rolle zugeteilt [18].

Neben den Modi, in welchen ein Gerät, das zur Datenübertragung mittels NFC fähig ist, sich befinden kann, unterscheidet man bei der Kommunikation über die drahtlose Technologie zwischen den drei Modi Peer-to-Peer, Read/Write und Card Emulation, die nachfolgend genauer beleuchtet werden. Um eine Datenübertragung über diese Modi zu ermöglichen, besitzt ein NFC-fähiges Gerät einen Host Controller, ein Secure Element (SE) sowie den NFC Chip. Der Chip sorgt für die Umwandlung der digitalen Signale in die analogen Feldveränderungen und umgekehrt. Das Secure Element ist eine sichere und modifikationsgeschützte Umgebung zur Ausführung von Code und beinhaltet typischerweise mehrere Applikationen, die gestartet werden können. Die Implementierung des SE kann auch vollständig softwarebasiert erfolgen und im Regelfall ist es dazu in der Lage, echte Smartcards zu emulieren. Der Host Controller ist verantwortlich für die Steuerung des NFC Chips sowie für die Kommunikation mit dem Secure Element [18]. Diese Komponente sorgt demnach dafür, dass die Signale des elektromagnetischen Feldes, die vom NFC Chip empfangen werden, nach deren Umwandlung an das SE weitergeleitet werden, um dort bestimmte Anweisungen auszuführen.

Die Kommunikation über NFC kann in einem der folgenden drei Modi durchgeführt werden:

Peer-to-Peer Modus

Befinden sich zwei Geräte im Peer-to-Peer Modus, können Daten über eine bidirektionale Verbindung in beiden Richtungen untereinander ausgetauscht werden. Diese Daten können Nachrichten, Kontakte, Bilder oder jegliche andere Art von Informationen beinhalten. Beim Senden der Nachrichten befindet sich der Sender im aktiven Modus und erzeugt somit sein eigenes elektromagnetisches Feld. Der Empfänger der Nachrichten befindet sich beim Empfangen der Informationen im passiven Modus [18, 32].

Read/Write Modus

Ein NFC Gerät, dass sich im Read/Write Modus befindet, ist in der Lage, Informationen von passiven NFC Tags, die keine eigene Energieversorgung besitzen, zu lesen, sowie Daten auf ihnen zu speichern bzw. zu modifizieren. Auf den Tags können sich unterschiedlichste Informationen wie Weblinks oder WLAN Verbindungsinformationen befinden. Je nach Art der gespeicherten Infor-

mation führt das NFC Gerät diverse Aktionen, wie beispielsweise ein Video im Webbrowser zu öffnen oder Treuepunkte auf einer Kundenkarte zu verändern, aus [18, 32].

Card Emulation Modus

Der Card Emulation Modus dient dazu, eine kontaktlose Smartcard zu emulieren. Smartcards verfügen über keine eigene Energieversorgung weshalb sich das sie emulierende NFC Gerät im passiven Modus befindet. Card Emuation ist das Gegenteil des Read/Write Modus, da hier das NFC Gerät die exakt umgekehrte Rolle bei der Datenübertragung einnimmt. Mithilfe dieser Datenübertragungsmethode kann eine kontaktlose Zahlung mit dem NFC Gerät anstelle einer echten Karte durchgeführt werden. Durch die Virtualisierung der Smartcard wird darüber hinaus die Möglichkeit geboten, vielfache unterschiedliche Karten auf demselben Gerät zu simulieren und Zahlungen damit durchzuführen [18].

2.1.2 Zahlungen mittels NFC

Um kontaktlose Zahlungen über NFC durchzuführen, werden in erster Linie eine Smartcard sowie ein Smartcard-Reader benötigt, die das NFC Protokoll unterstützen. Nachfolgend sollen diese Komponenten sowie der Ablauf einer kontaklosen Zahlung über die NFC Technologie genauer erläutert werden.

Smartcards

Unter einer Smartcard, die auch als Integrated Circuit Card (ICC) bzw. Chipkarte bezeichnet wird, versteht man in erster Linie eine Plastikkarte, die einen integrierten Schaltkreis besitzt. Dieser kann sowohl zur Speicherung von Dateien sowie zur Verarbeitung von Instruktionen und zur Ausführung von Programmen verwendet werden [17]. Beispiele für Smartcards sind handelsübliche Debit- und Kreditkarten sowie Subscriber Identity Module Karten (SIM Karten), die in Mobiltelefonen Verwendung finden. Üblicherweise besteht eine Chipkarte aus einem Read Only Memory (ROM) Speicher oder einem Flash Speicher, einem Electrically Erasable Programmable ROM (EEPROM) Speicher und einer Central Processing Unit (CPU). Auf diesen Hardware Komponenten befindet sich darüber hinaus ein Dateisystem sowie ein Betriebssystem [24]. Da dies gleichermaßen die Kernbestandteile eines Computers sind, könnte man eine Smartcard ebenfalls als solchen bezeichnen. Wie auf Computern befinden sich auf einer Smartcard unterschiedliche ausführbare Applikationen, die unabhängig voneinander ausgewählt und gestartet werden können [24].

Das Dateisystem einer Chipkarte besteht aus einem übergeordneten Master File (MF), das vergleichbar mit dem Root Ordner eines Linux Betriebssystems bzw. eines MS-DOS Systems ist und alle anderen Dateien und Verzeichnisse sowie Dedicated Files (DF) und Elementary Files (EF) enthält. Als Dedicated Files bezeichnet man hierbei wiederum Verzeichnisse während Elementary Files einzelne Dateien beinhalten. Eine einzelne Applikation auf der Chipkarte befindet sich hierbei in einem einzelnen DF. Variationen eines Programms können sich in untergeordneten DFs befinden während sich die Programmdaten selbst in den EFs finden [24]. Die nachfolgende Abbildung dient zur Veranschaulichung des Dateisystems auf einer Chipkarte.

Hier Abbildungen eines Dateisystems einfügen (Single sowie Multi Application)

Smartcards werden im ISO/IEC 7816 Standard definiert. Dies ist ein umfangreicher 15-teiliger Standard, der alle Eigenschaften von Chipkarten detailliert festlegt. In ISO/IEC 7816 werden physikalische Eigenschaften wie Abmessungen, elektrische Kontakte, elektrische Signale und Datenübertragungsprotokolle sowie -kommandos präzisiert. Darüber hinaus werden Kommunikati-

onsprotokolle, Dateistruktur der Karten, Programmschnittstellen, Datenelemente, kryptografische Funktionen, Sicherheitsmechanismen und viele weitere Eigenschaften festgelegt [**15 Quellen zitieren?**]. Die kontaktlose Kommunikation über NFC sowie Kommunikationsprotokolle zur kontaktlosen Übertragung von Daten und zugehörige physikalische Eigenschaften wie die des elektromagnetischen Feldes werden hingegen im vierteiligen ISO/IEC 14443 Standard festgelegt [27–30]. Zusätzlich wurde bereits zu Beginn der 90er Jahre von den Kartengesellschaften Europay, Mastercard und Visa, der nach den Autoren benannte EMV-Sicherheitsstandard entwickelt. Dieser Standard wurde speziell für Kartenzahlungen eingeführt und soll dazu dienen eine grenzübergreifende einheitliche Schnittstelle für Kartenzahlungen bereitzustellen sowie die Sicherheit bei Zahlungen zu erhöhen und Kartenmissbrauch zu verhindern [19, 20]. Der EMV Standard wird seit dem Jahr 1999 von einer eigenen Organisation, der EMVCo, verwaltet und weiterentwickelt. Am Ende des Jahres 2017 waren 63,7% aller weltweiten Transaktionen EMV-Transaktionen sowie 54,4% aller weltweit ausgestellten Karten waren mit dem EMV-Chip versehen [7].

Funktionsweise einer Zahlung mit einer kontaktlosen Smartcard

Die Kommunikation eines handelsüblichen Point-of-Sales (POS) Terminals mit einer Smartcard erfolgt in erster Linie über sogenannte Application Protocol Data Units (Apdus). Diese Datenblöcke sind in zwei unterschiedliche Arten unterteilt: Command-Apdus dienen zum Senden einer Instruktion, die ausgeführt werden soll, während Response-Apdus, die Antwort auf einen ausgeführten Befehl enthalten. Ein Command-Apdu tritt immer paarweise mit einem Response-Apdu auf [26]. Die Struktur eines Command-Apdus wird in Abbildung 2 beschrieben.

Hier Command Apdu Abbildung

Abbildung 2.1: Struktur eines Command-Apdus

Wie aus Abbildung 2 zu entnehmen ist, besteht ein Command-Apdu aus einem Header sowie einem Body, die die folgenden Elemente enthalten:

- Class: Die Art des Kommandos
- Instruction: Das Kommando selbst
- P1 und P2: Parameter für das Kommando (unterschiedlich je nach Instruktion)
- Lc: Die Länge der Daten
- Data: Die Nutzdaten
- Le: Die erwartete Länge des Response-Apdus

Nachdem vom POS-Terminal ein Command-Apdu an die Chipkarte gesendet wurde, wird von dieser erwartet, ein kompatibles Response-Apdu als Antwort zu senden . Die Struktur eines Response-Apdus wird in Abbildung 3 veranschaulicht.

Abbildung 2.2: Struktur eines Response-Apdus

Ein Response-Apdu besitzt die folgenden Elemente:

- Data: Die Antwortdaten auf das zuvor gesendete Kommando, die um mit ISO 7816 kompatibel zu sein, eine bestimmte Struktur aufweisen müssen. Diese Struktur ist entweder für das

betreffende Kommando im Standard dokumentiert oder das Kommando ist TLV-enkodiert. Ein TLV ist eine Datenstruktur, die aus einem Tag(T), der den Typ der Daten angibt, einer Länge(L) der betreffenden Daten und den Daten selbst(V für Value) besteht.

- SW1 und SW2: Ein aus zwei Teilen bestehendes Statuswort, das den Status der Verarbeitung angibt (erfolgreich/Fehlercode)

Typischerweise wird bei einer Kartenzahlung über NFC zuerst die Applikation ausgewählt, die zur Zahlung verwendet werden soll. Sowohl das Terminal als auch die Karte können mehrere Zahlungsanwendungen unterstützen. Welche davon ausgewählt wird, hangt somit von der Priorität der Anwendung ab. Um eine Zahlungsapplikation auszuwählen, wird ein SELECT APPLICATION Apdu an die Karte gesendet, das die ID der auszuwählenden Anwendung enthält. Die Karte antwortet auf dieses Kommando mit diversen Applikationsdaten wobei die ID der Anwendung in der Antwort ein weiteres Mal enthalten ist [9, 11].

Nach der Auswahl der Anwendung wird im Regelfall ein GET PROCESSION OPTIONS (GPO) Kommando an die Karte gesendet. Als Antwort auf diese Instruktion werden von der Chipkarte Informationen gesendet, die sich Application Interchange Profile (AIP) und Application File Locator (AFL) nennen. Das AIP dient in erster Linie zur Angabe von Informationen über die unterstützten Authentifikationsmethoden während der AFL angibt, wo die zahlungsanwendungsspezifischen Dateien zu finden sind [9, 11]. Die Daten des AFL sind vergleichbar mit Pfadangaben auf einem Computer.

Im nächsten Schritt können die vom AFL angegebenen Dateien gelesen und daraus Informationen wie die Kreditkartennummer sowie der Name des Inhabers gewonnen werden [11]. Wurden die Applikationsdaten erfolgreich gelesen, wird ein Authentifizierungsschritt durchgeführt, der die Daten auf der Karte verifiziert. Hierzu werden die Informationen des AIP verwendet, um festzustellen, welche Authentifizierungsmethoden die Chipkarte unterstützt. Die Methoden, die sowohl vom Terminal als auch von der Karte angewendet werden können, werden durchgeführt [22].

Nach der Authentifizierung überprüft das Terminal, ob die auszuführende Transaktion von der Smartcard erlaubt wird sowie ob die Karte gültig ist. Nach erfolgreicher Überprüfung wird falls notwendig der Schritt zur Besitzer-Authentifizierung eingeleitet, der häufig durch Eingabe einer persönlichen Identifikationsnummer (PIN) erfolgt [22].

Anschließend wird eine Risikoanalyse des Terminals ausgeführt. Diese dient zum Schutz vor Betrug und unrechtmäßiger Durchführung von Transaktionen und evaluiert, ob eine Transaktion offline ohne Authorisierung durch den Kartenaussteller oder online mit Authorisierung durchgeführt werden soll. Im Zuge der Risikoanalyse werden die zuvor abgeschlossenen Transaktionen derselben Karte betrachtet. Hierbei wird überprüft, ob die letzte durchgeführte Transaktion gemeinsam mit der im Moment durchgeführten ein gewisses Limit überschreitet [9]. Dieses Limit wird Floor Limit genannt und dient dazu, eine Grenze anzugeben, über welcher eine Authorisierung durch den Kartenaussteller beantragt werden muss. Dies dient der Verhinderung von Schäden durch das Bezahlen größerer Summen ohne Authorisierung. Transaktionen, deren Betrag sich unter dem Floor Limit befindet, können während der Risikoanalyse dennoch zufällig für eine Online-Authorisierung ausgewählt werden [9, 23]. Darüber hinaus wird kontrolliert, wann zuletzt eine Online-Authorisierung ausgeführt wurde [9].

Die Risikoanalyse liefert das Ergebnis, ob die Transaktion abgelehnt, online, oder offline durchgeführt werden soll. Basierend auf dem Resultat wird ein GENERATE APPLICATION CRYPTOGRAM (AC) Kommando an die Smartcard gesendet. Diese führt ihrerseits auf Basis der im Befehl gesendeten Informationen eine Risikoanalyse durch, auf welche Art und Weise die Trans-

aktion fortgesetzt werden soll. Nach Abschluss dieses Schrittes wird ein Kryptogramm[1] generiert, das die Entscheidung der Karte über die Fortführung der Transaktion angibt. Nach Abstimmung mit der eigenen Entscheidung beendet das Terminal die Transaktion offline oder online [9, 22].

Anmerkung: Bei der Online-Authorisierung werden weitere Schritte durch den Kartenaussteller durchgeführt, die nicht im Rahmen dieser Erläuterung liegen. Nach Antwort des Kartenausstellers wird ein weiteres abschließendes GENERATE AC Kommando an die Karte übermittelt [22].

2.2 NFC Sicherheitsrisiken und Gegenmaßnahmen

Obwohl die Übertragungsdistanz der Informationen über die NFC Technologie sehr gering ist, sorgt dieser Umstand nicht für eine sichere Datenübermittlung. In der Literatur sind bereits mehrere unterschiedliche Gefahren und Angriffsarten für NFC Kommunikation bekannt, die in diesem Kapitel erläutert werden sollen.

Yes-Card Attacke

Für EMV Smartcards existieren drei verschiedene Möglichkeiten, eine Datenauthentifizierung durchzuführen: statische, dynamische und kombinierte Datenauthentifizierung. Diese Mechanismen werden bei der Zahlung an einem POS-Terminal im Authentifizierungsschritt nach dem Lesen der Applikationsdaten durchgeführt [1, 9]. Bei der Ausführung der statischen Datenauthentifizierung (SDA) wird eine digitale Signatur, die vom Kartenaussteller verschlüsselt wird, zur Offline-Authentifizierung verwendet [3]. Die Signatur kann vom POS-Terminal zur Verifizierung der Daten verwendet werden. Diese Authentifizierungstechnik ist verwundbar gegenüber der sogenannten Yes-Card Attacke. Bei diesem Angriff werden die statischen Daten (die Signatur) der Smartcard kopiert und die kopierte Karte wird modifiziert, sodass sie jeden PIN akzeptiert. Dadurch können statisch signierte Offline-Transaktionen durchgeführt werden [1, 18].

Als Gegenmaßnahmen für die Yes-Card Attacke dienen die beiden Authentifizierungsmechanismen der dynamischen sowie der kombinierten Datenauthentifizierung [1]. Bei der DDA wird von der Karte selbst bei jedem Bezahlvorgang eine Signatur erstellt, die eindeutig ist, weil sie eine zufallsgenerierte Zahl des Terminals enthält [2]. Eine auf diese Art generiert Signatur kann nicht mehr gespeichert und in nachfolgenden Zahlungen verwendet werden, da sie bei jedem Zahlvorgang unterschiedlich ist. CDA ist eine Erweiterung der DDA und erzeugt zusätzlich eine dynamische Signatur, die mit dem im späteren Schritt erzeugten Kryptogramm der Karte zur Verifizierung an das Terminal gesendet wird [8].

Eavesdropping

Mithilfe einer Antenne ist es möglich, NFC Signale, die zwischen zwei NFC Geräten übertragen werden zu lesen bzw. zu modifizieren [15]. Geräte, die in der Lage sind, RFID Kommunikation abzuhören, können beispielsweise für Eavesdropping verwendet. Diese Art von Geräten ist darüber hinaus öffentlich zugänglich [25]. Die Durchführbarkeit von Eavesdropping hängt von unterschiedlichen Charakteristika, wie der Angriffsantenne, der Qualität des Empfängers oder der Signalstärke des aussendenden Gerätes ab [12].

Als Gegenmaßnahme zu Eavesdropping muss zwischen den kommunizierenden Geräten eine gesicherte Verbindung aufgebaut werden. Dies kann mithilfe von Verschlüsselungsmethoden durchgeführt werden [15].

[1] Als Kryptogramm wird ein Hashwert von Transaktionsdaten bezeichnet, der zur Verifikation der Transaktion durch den Kartenaussteller genutzt werden kann [22].

Data Modification

Dieser Angriff beschreibt das Abfangen, Verändern und Weiterleiten der gefälschten Informationen von NFC Nachrichten. Data Modification ist sehr schwierig durchzuführen, weil das gefälschte Signal nach wie vor das richtige Format haben muss, um vom Empfänger akzeptiert zu werden [15]. Abgesehen davon ist diese Attacke sehr abhängig von der verwendeten Signalstärke des NFC Signals [12].

Um Data Modification zu verhindern, kann ein NFC Sender aus den nächstgelegenen Empfängergeräten das mit der höchsten Signalstärke auswählen, weil dieses mit hoher Wahrscheinlichkeit den beabsichtigten Empfänger darstellt. Darüber hinaus kann der Sender während der Datenübertragung überprüfen, ob weitere RF Signale entdeckt werden, die Daten aussenden. Dadurch kann Data Modification entdeckt und verhindert werden [15].

Data Corruption

Im Gegensatz zur Data Modification wird bei der Data Corruption nicht versucht die Informationen abzufangen oder zu verändern. Data Corruption zielt darauf ab, eine NFC Verbindung zwischen zwei Geräten so zu stören, dass die übertragenen Daten für den Empfänger nutzlos werden bzw. die Verbindung selbst zu blocken. Dieser Angriff ist daher eine Art der Denial-of-Service (DOS) Attacke. Das Blocken oder Stören der Verbindung kann durch vom Angreifer ausgesendete Signale, die Rauschen in der ursprünglichen Verbindung erzeugen und diese damit unbrauchbar machen, erfolgen [15].

Data Corruption kann wie Data Modification gleichermaßen durch das Überprüfen auf weitere NFC Sendequellen entdeckt und verhindert werden.

Spoofing Grundsätzlich wird beim Spoofing die eigene Identität verschleiert bzw. eine falsche Identität vorgetäuscht. Übertragen auf die NFC Technologie könnte ein Angreifer einen NFC Tag, der ursprünglich einen anderen Zweck erfüllt, so programmieren, dass schädlicher Code auf dem Gerät, das versucht den Tag zu lesen, ausgeführt wird. Handelsübliche Smartphones bzw. NFC Lesegeräte sind häufig so konfiguriert, dass der auf einem NFC Tag vorhandene Code ohne zusätzliche Überprüfungen automatisch ausgeführt wird [15].

Um Spoofing zu verhindern, ist es notwendig, NFC Lesegeräte so zu konfigurieren, dass vor der Ausführung jeglichen gelesenen Codes eine Meldung für den Benutzer des Gerätes angezeigt wird [15].

Relay Attacke

Die Relay Attacke ist ein äußerst relevantes Sicherheitsrisiko vor allem im Bereich der kontaktlosen Zahlung mittels NFC. Aufgrund ihrer großen Relevanz für diese Arbeit wird die Relay Attacke detailliert in Kapitel 2.3 beschrieben.

2.3 Die Relay Attacke

Die Relay Attacke ist ein Angriff, der verwandt mit der Man-in-the-Middle Attacke ist und jegliche Sicherheitsmaßnahmen, die auf Applikationsebene implementiert werden, umgehen kann. Sichere Kommunikationskanäle sowie kryptographisch verschlüsselte Nachrichten bieten daher keinen Schutz vor dieser Art des Angriffs. Relay Attacken ermöglichen bei der Zahlung mittels NFC eine beliebig große Distanz zwischen Sender und Empfänger der Daten, wodurch die Sicherheit durch die kurze Übertragungsdistanz von NFC ebenfalls nicht mehr gegeben ist [1]. Es

besteht daher bei der Durchführung einer Relay Attacke die Möglichkeit an einem POS Terminal mit einer Smartcard (real oder emuliert) zu zahlen, die sich tausende Kilometer entfernt befindet.

Dieser Angriff galt lange Zeit aufgrund physischer Limitationen des Kommunikationskanals sowie der zur Ausführung notwendigen speziellen Hardware als schwierig durchzuführen. Die Einführung NFC fähiger Mobilgeräte änderte diesen Umstand allerdings gravierend. Seit mehreren Jahren ist die Ausführung einer Relay Attacke mit jedem handelsüblichen Smartphone, das NFC unterstützt, möglich [33]. In der Literatur wurde die Durchführbarkeit dieses Angriffes vielfach bestätigt (siehe Abschnitt 5 - Related Work).

2.3.1 Man-in-the-Middle Angriffe

2.3.2 Prinzip der Relay Attacke

Vorgestellt wurde das Prinzip der Relay Attacke zum ersten Mal von John Conway im Jahr 1976 in dem Buch „On Numbers and Games"**[Buchzitat]**. Er beschreibt, wie es möglich ist, dass ein Schach Laie ohne Wissen über die Spielregeln, einen Großmeister im Spiel schlägt. Der Laie bzw. Angreifer spielt gleichzeitig gegen zwei Schach Meister, wobei er in beiden Partien unterschiedliche Farben einnimmt. Die Meister des Spiels wissen nichts voneinander und sind in dem Glauben, sie spielen nur gegen den Angreifer. Dieser leitet nun jeden Zug des einen Meisters an den anderen weiter, wodurch die beiden Experten des Spiels effektiv gegeneinander spielen **[Buchzitat]**.

Dieses Verfahren angewendet auf die Kommunikation mittels NFC wird folgendermaßen umgesetzt: Der Angreifer benötigt zwei NFC fähige Geräte, die in der Literatur auch "Ghost“und "Leech"genannt werden [16]. Der Ghost dient dazu eine falsche Chipkarte zu simulieren, während der Leech verwendet wird, um ein falsches POS Terminal dazustellen. Der Leech wird im Read/Write Modus in unmittelbarer Nähe der Smartcard bzw. des die Smartcard emulierenden Gerätes platziert. Mit dem Ghost wird nun versucht, mithilfe des Card Emulation Modus eine kontaktlose Zahlung an einem realen POS Terminal durchzuführen. Jegliche vom Terminal gesendeten Befehle, die vom Ghost empfangen werden, werden unverändert über einen sekundären Kommunikationskanal, der bereits vor der Attacke aufgebaut werden kann, an den Leech übertragen. Dieser übermittelt die Daten nun über NFC an das Opfer, welches daraufhin die passenden Antworten zu den Befehlen liefert. Diese werden umgekehrt an den Ghost und über diesen an das reale Terminal gesendet. Nachdem alle Befehle und Antworten nur weitergeleitet, aber nicht verändert werden, kann die Zahlung problemlos durchgeführt werden, als ob sie mit der echten Chipkarte ausgeführt worden wäre [16].

Abbildung 2.3 veranschaulicht das Prinzip der Relay Attacke.

Abbildung 2.3: Prinzip der Relay Attacke

Dieser Angriff eröffnet zahlreiche Möglichkeiten, Schaden anzurichten. Ein großes Sicherheitsrisiko, das diese Attacke nach sich zieht, ist, Zahlungen mit fremden Karten ohne das Wissen der Besitzer an POS Terminals durchzuführen. Darüber hinaus könnte sich ein Angreifer mithilfe dieser Technik Zugang zu für ihn nicht freigegebenen Bereichen verschaffen, indem die Relay Attacke verwendet wird, um eine NFC Sicherheitskontrolle für Zugangskarten zu umgehen [16].

2.3.3 Gegenmaßnahmen

Relay Attacken sind schwierig zu verhindern, da Sicherheitsmaßnahmen auf Applikationslevel keine Wirkung zeigen [1]. Verschlüsselte Nachrichten bzw. dynamisch generierte Daten werden durch den Ghost und den Leech ebenfalls weitergeleitet, wodurch eine Verifizierung immer dann erfolgreich ist, wenn sie es ohne die Relay Attacke auch wäre.

Gegenmaßnahmen können demnach in zwei Kategorien eingeteilt werden: Schutz der Karte (des Opfers) und Schutz des Systems selbst [1]. Die einfachste Art, um Schutz vor Relay Attacken zu gewährleisten, ist das Abschirmen der Karte gegenüber jeglicher RF Kommunikation. Dies kann beispielsweise mithilfe von RFID Hüllen oder Metallfolie erfolgen [1]. Bei die Karte emulierenden NFC Geräten, sollte daraus schlussfolgernd die NFC Funktion bei Nichtverwendung ausgeschaltet werden. Weiters können Relay Attacken durch sekundäre Authentifizierungsmechanismen wie biometrische Merkmale, PIN Codes oder Passwörter verhindert werden [1]. Diese würden allerdings viel Verantwortung auf den Benutzer übertragen und teilweise voraussetzen, dass Detailwissen über die Transaktionen bekannt ist. Zusätzlich wird die angenehme Art und Weise, mit der Zahlungen mittels NFC abgewickelt werden können, zerstört werden [10].

Typischerweise wird für die Kommunikation zwischen Ghost und Leech zusätzliche Zeit benötigt, was bedeutet, dass die Transaktion insgesamt eine längere Zeitspanne in Anspruch nimmt. Theoretisch könnten Relay Attacken daher verhindert werden, indem für jede Karten-POS-Terminal-Kombination eine maximale Zeitspanne festgelegt wird, die die Transaktion dauern kann. Dies ist allerdings aufgrund der unzähligen unterschiedlichen Kartentypen nicht möglich. Eine allgemeine Obergrenze für die Zeitdauer einer Transaktion reicht im Normalfall nicht aus, um eine Relay Attacke zu verhindern [1].

Dass eine allgemeine Obergrenze nicht ausreicht, kann man folgendermaßen schließen: Unterschiedliche Chipkarten benötigen unterschiedliche Zeiten, um Transaktionen auszuführen. Eine allgemeine Obergrenze müsste daher die langsamste Karte in Betracht ziehen, um die maximale Zeit einer Transaktion festzulegen. Würde die Obergrenze auf Basis anderer Kriterien festgelegt, könnten valide Transaktionen mit langsamen Karten ansonsten verworfen werden. Dies bedeutet allerdings, dass Relay Attacken, deren insgesamte Transaktionsdauer geringer als die der langsamsten Karte sind, ohne Probleme durchgeführt werden können.

Ein Ansatz zur effektiven Verhinderung von Relay Attacken ist das sogenannte Distance Bounding. Bei diesem Verfahren wird davon ausgegangen, dass sowohl Karte als auch POS Terminal messen, wie lange eine initiale Nachricht (Secret) benötigt, um gesendet und empfangen zu werden. Aus dieser Zeit und der Übertragungsgeschwindigkeit kann die Entfernung der beiden Komponenenten bestimmt werden. Theoretisch könnte eine Relay Attacke dann nur mehr durchgeführt werden, wenn die eingesetzten Geräte Daten mit nahezu Lichtgeschwindigkeit übertragen könnten [1]. Die Sicherheit von Distance Bounding ist allerdings abhängig von der Übertragungsgeschwindigkeit und es hat sich gezeigt, dass NFC nicht geeignet dafür ist [10].

Wird die Smartcard mithilfe eines mobilen NFC Gerätes emuliert, können Ortsinformationen dabei behilflich sein, Relay Attacken zu unterbinden. Die Ortsinformationen können beispielsweise durch Ermittlung der Daten des nächstgelegen Funkmastens oder durch GPS Daten festgestellt werden. Durch die Integration der ortsbasierten Daten in die NFC Kommunikation können demnach Relay Attacken verhindert werden [10]. Dennoch gibt es Limitationen bei der Ermittlung des Ortes eines Gerätes und dessen Verwendung bei der Zahlung wie beispielsweise Ungenauigkeit der Messung oder die Nichtfreigabe der Ortsinformationen durch den Mobilfunkbetreiber [10].

In diesem Kapitel werden die theoretischen Grundlagen und alle in der Arbeit verwendeten und für das Verständnis relevante Begriffe erläutert. Kapitelnamen spezifizieren, anpassen an die Fragestellung der Arbeit.

Gerade im Bereich der Grundlagen wird viel Literatur zitiert – Details zum Zitieren finden Sie im Kapitel 4. Da keine Diplomarbeit so innovativ ist, dass sie nicht auf vorhandenes Wissen aufbaut und in ein entsprechendes Forschungsumfeld eingebettet ist, kommt an dieser Stelle der Literaturrecherche eine besondere Bedeutung zu. Als Daumenregel gilt, dass der aktuelle Stand der Wissenschaft in der Informatik üblicherweise durch Publikationen v.a. der letzten 2 – 4 Jahre repräsentiert wird.

2.4 Aktueller Stand der Technik

In diesem Kapitel wird ein Überblick über bereits existierende Lösungen für die Problemstellung bzw. verwandte Problemstellungen gegeben. Dabei ist eine Klassifizierung der existierenden Lösungen empfehlenswert. Eine Analyse der Lösungen, nach Kriterien sortiert, sollte insbesondere auch die Defizite der existierenden Lösungen erläutern und damit insbesondere auch eine Begründung liefern, warum diese Lösungen für die Problemstellung der Arbeit nicht herangezogen werden können.

2.4.1 Unterkapitel

Bei der Verwendung von Gliederungsebenen gibt es Folgendes zu beachten:

- Es sollten nicht mehr als 3 Gliederungstiefen nummeriert werden.
- Unterkapitel sind nur dann sinnvoll, wenn es auch mehrere Untergliederungen gibt. Ein Kapitel 2.1.1 sollte somit nur dann verwendet werden, wenn es auch 2.1.2 gibt.
- Oft ist es einfacher und besser verständlich, Aufzählungen als Text zu formulieren und somit weitere Gliederungsstufen zu vermeiden.

2.4.2 Abbildungen

Beschreibungen zu Abbildungen und Tabellen stehen unter dem Bild. Jede Abbildung muss im Fließtext referenziert werden. In LaTeXbesitzen Abbildungen typischerweise Labels, welche zum referenzieren verwendet werden. Zudem plaziert LaTeXdie Abbildungen an geeigneten Stellen, was meistens auch wünschenswert ist. Falls das nicht gewünscht wird, kann es durch Optionen beeinflusst werden.

Abbildung 2.4 verdeutlicht ...
(siehe Abbildung `\ref{<label>}`)

2.4.3 Tabellen

Jede Tabelle muss im Fließtext referenziertw werden. Für Tabellen gelten die selben Regeln, wie für Abbildungen (siehe dazu Abschnitt 2.4.2).

Eine Beispiel einer Tabelle ist in Tabelle 2.1 zu finden:

Bitte beachten Sie, dass Tabellen generell so einfach wie möglich gehalten werden sollen. Tabelle 2.1 dient unter anderem dazu Studierenden zu zeigen, wie Tabellen in LaTeX erstellt werden können und wie Farben verwendet werden.

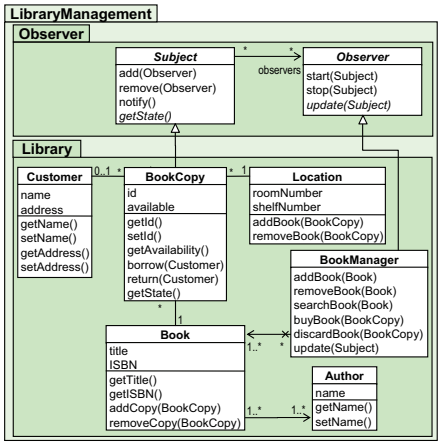

Abbildung 2.4: xxx (Quelle zitieren, wenn nicht selbst erstellt)

Linksbündig	Zentriert	Rechtsbündig
Zeile 1	xxx	xxx
Zeile 2	xxx	...
Zeile3	xxx	xxx
	xxx	xxx
xxx		

Tabelle 2.1: xxx (Quelle angeben)

3 Implementierung der Relay Attacke

Ziel dieses Kapitels ist die Beschreibung der praktischen Durchführung der NFC Relay Attacke. Es soll gezeigt werden, dass es mithilfe weniger Modifikationen am Android Betriebssystem möglich ist, die NFC Signale eines POS Terminals an ein zweites mobiles Gerät weiterzuleiten und auf diesem eine mobile Zahlung zu initiieren. Es wird dargestellt, auf welche Art und Weise ein Eingreifen in die Kommunikation der Zahlungsanwendung mit der NFC Schnittstelle möglich ist und wie die Antwortsignale der Zahlung an das weit entfernte POS Terminal zurückgesendet werden können.

Ebenfalls soll diskutiert werden, welche unterschiedlichen Komponenten zum Aufbau und zur Durchführung der Relay Attacke notwendig sind, wie diese implementiert wurden und welche Rolle sie bei der Durchführung der Attacke einnehmen. Auftretende Schwierigkeiten sowie getroffene Entscheidungen sollen ebenfalls dargelegt werden.

Am Ende dieses Kapitels soll eine funktionsfähige Proof-of-Concept Implementierung der Relay Attacke stehen, deren Umsetzung mit einfachen Methoden des Android Frameworks realisiert wird und die als Grundlage für weiterführende Forschungen dienen soll.

3.1 Aufbau der Implementierung

Zur Durchführung der Attacke wurden zwei handelsübliche, NFC-fähige Android Smartphones für die Rolle des Angreifers sowie des Opfers verwendet. Auf dem Angreifer-Gerät, einem HTC U11, war hierbei die Android Version 8.0.0 (API 26) vorhanden, auf dem Opfer-Gerät, einem Google Nexus 5X wurde eine modifizierte Version des Android Open Source Projektes mit der Version **XXX** installiert. Welche Modifikationen an diesem Betriebssystem vorgenommen wurden, wird in Kapitel **XXX** detailliert beschrieben.

Umgesetzt wurde die Relay Attacke durch die Entwicklung einer Proof-of-Concept Hostcard Emulation App, die eine handelsübliche mobile Payment Applikation wie beispielsweise Android Pay simulieren soll. Diese Anwendung wurde auf dem Opfer-Gerät installiert und als Ziel der Attacke sollte die HCE App zur Durchführung einer Zahlung und Weiterleitung der Daten an den Angreifer angeregt werden, ohne dass sich das Opfer in der Nähe eines POS Terminals befindet. Die Entwicklung der HCE App wird in Kapitel **XXX** dargelegt.

Die Kommunikation der Geräte wurde durch eine weitere mobile Anwendung, welche unabhängig von der HCE Applikation operiert, realisiert. Diese existiert sowohl auf dem Angreifer- als auch auf dem Opfer-Gerät und sorgt für eine Verbindung zwischen den Kommunikationspartnern über ein Wireless Local Area Network (WLAN).

Diese Anwendung kommuniziert darüber hinaus auch mit dem Android Betriebssystem und sorgt für die Ausführung der HCE App, sobald ein Signal vom Angreifer-Gerät empfangen wird. Darüber hinaus wird auch die Antwort der HCE App, die eigentlich an die NFC Schnittstelle gesendet wird, ebenfalls von der Kommunikationsanwendung abgefangen und an den Angreifer weitergeleitet. Mit welchen Mechanismen die unterschiedlichen Kommunikationswege umgesetzt wurden, wird in Kapitel **XXX** genauer ausgeführt.

Zur erfolgreichen Durchführung der Attacke sind Modifikationen am Android Betriebssystem notwendig. Diese sorgen dafür, dass die entwickelten Anwendungen die passenden Signale erhalten,

Abbildung 3.1: Übersicht der Relay Attacke

um korrekt operieren zu können. Bei der Durchführung der Attacke wird angenommen, dass eine modifizierte Version des Android Source Codes auf dem Opfergerät installiert werden kann. Die genaue Durchführung der Änderungen am Android Betriebssystem wird in Kapitel **XXX** beschrieben.

In folgender Abbildung ist eine Übersicht der Relay Attacke und der zur Durchführung entwickelten Komponenten gegeben.

In Abbildung **XXX** ist in erster Linie ein POS Terminal sowie ein Angreifer- und ein Opfer-Gerät dargestellt. Das POS Terminal wird durch eine Terminal Simulator Software auf dem Computer dargestellt. Über eine Universal Serial Bus (USB) Verbindung wird von einem NFC Reader die NFC Funktionalität zur korrekten Funktionsweise der Terminal Software bereitgestellt.

Bei Kontakt mit dem Angreifer wird vom POS Terminal eine kontaktlose Zahlung über NFC eingeleitet. Die Commmand Apdus werden hierbei direkt in der Kommunikationsanwendung empfangen. Diese nutzt nach dem Empfang eines Kommandos die WLAN Verbindung, um das Apdu an das Opfer weiterzuleiten. Die Kommunikationsanwendung, die auf dem Opfer-Gerät standardmäßig im Hintergrund aktiv ist, empfängt die Signale, woraufhin sie eine Kommunikation über das Betriebssystem mit der auf dem Opfer vorhandenen HCE Applikation startet. Die Rolle dieser HCE Applikation kann im Prinzip von jeder handelsüblichen Mobile Payment Anwendung übernommen werden. Diese Anwendung ist das eigentliche Ziel des Angriffes. Nachdem sie vom Betriebssystem gestartet wurde, wird eine mobile Zahlung in die Wege geleitet. Bei der Durchführung der Zahlung von der Zahlungsapplikation Response Apdus an die NFC Schnittstelle des Gerätes gesendet, nachdem die HCE Anwendung davon ausgeht, durch NFC aufgerufen worden zu sein. Das modifizierte Betriebssystem leitet nun diese Antworten an die Kommunikationsanwendung zurück, welche diese über WLAN wiederum dem Angreifer mitteilt. Vom Angreifer-Gerät werden die Apdus schlussendlich an das POS Terminal zurückgeleitet und die Relay Attacke wurde erfolgreich durchgeführt.

In den nachfolgenden Kapiteln wird ausgeführt, wie die einzelnen Komponenten im Detail umgesetzt wurden, um die beschriebene Funktionalität bereitzustellen.

3.1.1 Die Hostcard Emulation Anwendung

Das Android Framework stellt zur Implementierung einer Hostcard Emulation Anwendung die Klasse HostApduService zur Verfügung. Diese Android-Service Klasse sorgt für das Annehmen von Command Apdus, nachdem diese von der NFC Schnittstelle empfangen wurden. Um diese empfangenen Apdus verarbeiten zu können, muss die Klasse erweitert und die processCommandApdu Methode überschrieben werden. Welche Applikation auf ein eintreffendes Command Apdu gestartet werden soll, wird vom Betriebssystem festgestellt. Diese besitzt einen Routing Mechanismus, der auf den sogenannten Application IDs (AIDs) aufgebaut ist [6]. Dies sind Identifier, die Zahlungsanwendungen eindeutig identifizieren können und sie müssen bei der Installation einer Mobile Payment App von dieser beim Betriebssystem durch eine XML-Datei in der Anwendung registriert werden [6].

Die in dieser Arbeit dargestellte Proof-of-Concept Umsetzung einer HCE Applikation verwendet die AID einer Mastercard MAESTRO Debitkarte, die durch die Hexadezimal Darstellung A0000000043060 identifiziert wird. Gemeinsam mit den Standard Identifiern für Zahlungssysteme, die genau genommen noch vor der eigentlichen Anwendung ausgewählt werden, wird die MAESTRO-AID in der aids.xml Datei festgelegt.

Diese Datei wird bei der Registrierung der HostApduService Klasse in der AndroidManifest.xml Datei referenziert, um dem Betriebssystem mitzuteilen, welche AIDs von der HCE Anwendung verarbeitet werden können.

Wird eine Smartcard bzw. ein NFC fähiges Mobilgerät, auf dem eine Zahlungsanwendung vorhanden ist, in die Nähe eines POS Terminals gebracht, so wird von diesem das aus den Grundlagen bekannte SELECT PPSE Kommando gesendet. Nach der Antwort, welche AIDs verarbeitet werden können und dem SELECT AID Kommando wird die implementierte HCE Anwendung über die erweiterte HostApduService Klasse aufgerufen. Nach Auswahl der Applikation zur Verarbeitung der Zahlung werden, solange die NFC Verbindung nicht unterbrochen wird, alle nachfolgenden Apdus ebenfalls an diese Klasse weitergeleitet [6].

Um eine echte Zahlungsanwendung zu simulieren wurden in der implementierten App die ersten Response Apdus einer echten MAESTRO Debitkarte gespeichert. Als Reaktion auf ein ankommendes Command Apdu wird deshalb das passende Response Apdu zurückgeliefert.

In diesem Kapitel wird die eigentliche Problemlösung in einem oder mehreren Unterkapiteln ausgeführt. Die Strukturierung dieser Kapitel ist naturgemäß sehr stark von der konkre Aufgabenstellung abhängig. Der Name dieses Kapitels ist anzupassen, z.B. Umfeldbeschreibung – Fallbeispiel . . . , konkreter schreiben je nach Art Diplomarbeit/Fragestellung.

4 Hinweise zur Literatur

4.1 Literatursuche

Der Vollzugang zu einigen Publikationen ist nur intern aus dem TU-Netz möglich. Um auf möglichst viele Papers extern zugreifen zu können, wird von der TU Wien eine VPN-Zugangsmöglichkeit angeboten, diesen VPN-Zugang bitte gleich einrichten.

Besonders ergiebig sind folgende Search-Engines:
Microsoft Academic
ACM-Datenbank
Google Scholar

Wir empfehlen, vor Beginn Ihrer Arbeit einige Diplomarbeiten, die am INSO oder generell an der Fakultät für Informatik verfaßt wurden, zu Ihrem Themenbereich zu suchen und Aufbau, Schreibstil, Art der Abbildungen etc. durchzuschauen. Arbeiten finden Sie hier.

Weitere Datenbanken und Suchmaschinen:
Elektronische Zeitschriftenbibliothek der TU Wien
Scientific Literature Digital Library (CiteSeer)
Ingenta
INSPEC

Journals:
IEEE - Institute of Electrical and Electronics Engineers, Inc. - Library
Verlag Springer - Springer Link
Elsevier

Bibliotheken und Online-Kataloge:
Online-Kataloge des Österreichischen Bibliothekenverbundes
Online-Katalog der TU Wien (ALEPH)
Digital Bibliography & Library Project (DBLP) of University of Trier
The Collection of Computer Science Bibliographies

4.2 BibLatex

Biblatex bietet verschiedene Möglichkeiten an, um Literatur zu referenzieren. Die beiden häufigsten Befehle sind `\cite` und `\citeauthor`.

Beispiele wie referenziert werden kann:
fankhauser:2009:softwaretechnik-security beschreiben in [**fankhauser:2009:softwaretechnik-security**]
...
In [**schanes:2011:voip-fuzzer**] zeigen **schanes:2011:voip-fuzzer** wie ... Weitere Informationen können in [**oasis:2010:homepage**] von **oasis:2010:homepage** entnommen werden.

Wir empfehlen JabRef, um die Literaturdatenbank zu verwalten.

5 Algorithmen und Quellcode

5.1 Beispiele für Quellcode

Beispiel eines Quellcodes ist im Quellcode 5.1 zu finden.

```
1 //Start Program
2 System.out.println("Hello World!");
3 //End Program
```

Listing 5.1: Short code

5.2 Beispiele für Algorithmen

Algorithmus 5.1 dient als Beispiel.

input : A bitmap Im of size $w \times l$
output : A partition of the bitmap

```
1  special treatment of the first line;
2  for i ← 2 to l do
3      special treatment of the first element of line i;
4      for j ← 2 to w do
5          left ← FindCompress(Im[i, j − 1]);
6          up ← FindCompress(Im[i − 1, ]);
7          this ← FindCompress(Im[i, j]);
8          if left compatible with this then ;                    // O(left, this)==1
9
10             if left < this then Union(left,this);
11             ;
12             else Union(this,left);
13             ;
14         end
15         if up compatible with this then ;                      // O(up, this)==1
16
17             if up < this then Union(up,this);
18             ;
               // this is put under up to keep tree as flat as
                  possible
19             else Union(this,up);
               ;                                          // this linked to up
20         end
21     end
22     foreach element e of the line i do FindCompress(p);
23 end
```

Algorithmus 5.1 : Sample algorithm

6 Ergebnisse

Die Resultate der Arbeit präsentieren und nach Möglichkeit aussagekräftige, eigenständige Abbildungen einbauen. Namen des Kapitels konkretisieren, an jeweilige Arbeit anpassen – Lösungsvorschlag/Implementierung im Titel des Kapitels benennen.

7 Zusammenfassung und Ausblick

Literatur

Wissenschaftliche Literatur

[1] Thomas Bocek u. a. “An NFC Relay Attack with Off-the-shelf Hardware and Software”. In: *10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2016* (2016). URL: https://link.springer.com/chapter/10.1007/978-3-319-39814-3_8 (besucht am 15. 01. 2018).

[5] Andrea Cuno. *Near Field Communication*. 2010. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.395.8428&rep=rep1&type=pdf#page=11 (besucht am 19. 04. 2018).

[8] EMVCo. “Integrated Circuit Card Specifications for Payment Systems: Book 2 - Security and Key Management”. In: 2011. URL: https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_2_Security_and_Key_Management_20120607061923900.pdf (besucht am 10. 05. 2018).

[9] EMVCo. “Integrated Circuit Card Specifications for Payment Systems: Book 3 - Application Specification”. In: 2011. URL: https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_3_Application_Specification_20120607062110791.pdf (besucht am 29. 04. 2018).

[10] Lishoy Francis u. a. “Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones”. In: *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (2010). URL: https://link.springer.com/chapter/10.1007/978-3-642-16822-2_4 (besucht am 15. 01. 2018).

[12] Ernst Haselsteiner und Klemens Breitfuß. *Security in Near Field Communication (NFC)*. 2006. URL: https://s3.amazonaws.com/academia.edu.documents/8360228/002%20-%20security%20in%20nfc.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1516912912&Signature=sib36KcnIO0AAbNxqdEjxuId6TY%3D&response-content-disposition=inline%3B%20filename%3DSecurity_in_near_field_communication_NFC.pdf (besucht am 25. 01. 2018).

[16] Z. Kfir und A. Wool. “Picking Virtual Pockets using Relay Attacks on Contactless Smartcard”. In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)* (2005). URL: http://ieeexplore.ieee.org/abstract/document/1607558/ (besucht am 15. 01. 2018).

[18] Gerald Madlmayr, Christian Kantner und Thomas Grechenig. “Near Field Communication”. In: *Secure Smart Embedded Devices, Platforms and Applications*. Hrsg. von Konstantinos Markantonakis und Keith Mayes. Springer New York, 2014.

[24] Wasim Raad, Tarek Sheltami und Mohammad Sallout. *A Smart Card Based Prepaid Electricity System*. Aug. 2007.

[25] Henning Siitonen Kortvedt und Stig Mjølsnes. “Eavesdropping Near Field Communication”. In: *The Norwegian Information Security Conference (NISK) 2009* (2009). URL: https://www.researchgate.net/publication/265976861_Eavesdropping_Near_Field_Communication (besucht am 10. 05. 2018).

[32] A. Supriya, S. Ramgopal und S. M. George. “Near field communication based system for health monitoring”. In: *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT)*. 2017, S. 653–657. DOI: 10.1109/RTEICT.2017.8256678.

[33] José Vila und Ricardo J. Rodríguez. “Practical Experiences on NFC Relay Attacks with Android”. In: *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (2015). URL: https://link.springer.com/chapter/10.1007/978-3-319-24837-0_6 (besucht am 15. 01. 2018).

[34] R. Want. “An introduction to RFID technology”. In: *IEEE Pervasive Computing* 5.1 (2006), S. 25–33. ISSN: 1536-1268. DOI: 10.1109/MPRV.2006.2.

Online-Referenzen

[2] CardContact Software & System Consulting. *Dynamic Data Authentication*. URL: https://www.openscdp.org/scripts/tutorial/emv/dda.html (besucht am 10. 05. 2018).

[3] CardContact Software & System Consulting. *Static Data Authentication (SDA)*. URL: https://www.openscdp.org/scripts/tutorial/emv/SDA.html (besucht am 03. 05. 2018).

[4] Sony Corporation und Philips. *PHILIPS AND SONY ANNOUNCE STRATEGIC COOPERATION TO DEFINE NEXT GENERATION NEAR FIELD RADIO-FREQUENCY COMMUNICATIONS*. 2002. URL: https://www.sony.net/SonyInfo/News/Press_Archive/200209/02-0905E/ (besucht am 24. 01. 2018).

[6] Android Developers. *Host-based Card Emulation*. URL: https://developer.android.com/guide/topics/connectivity/nfc/hce.html (besucht am 25. 01. 2018).

[7] EMVCo. *EMVCo - Webseite*. URL: https://www.emvco.com/ (besucht am 28. 04. 2018).

[11] *Getting information from an EMV chip card with Java*. 2006. URL: https://blog.saush.com/2006/09/08/getting-information-from-an-emv-chip-card/ (besucht am 29. 04. 2018).

[13] *History of Near Field Communication*. URL: http://nearfieldcommunication.org/history-nfc.html.

[14] European Telecommunications Standards Institute. *ETSI TS 102 190: Near Field Communication (NFC) IP-1; Interface and Protocol (NFCIP-1)*. 2003. URL: http://www.etsi.org/deliver/etsi_ts/102100_102199/102190/01.01.01_60/ts_102190v010101p.pdf (besucht am 15. 04. 2018).

[15] Infosec Institute. *Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema*. 2013. URL: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/ (besucht am 24. 01. 2018).

[17] Prof. Dr. Richard Lackes. *Gabler Wirtschaftslexikon: Chipkarte*. URL: https://wirtschaftslexikon.gabler.de/definition/chipkarte-27504#authors (besucht am 24. 04. 2018).

[19] Mastercard. *EMV Chip*. URL: https://www.mastercard.at/de-at/haendler/sicherheit-geschaeft/emv-chip.html (besucht am 26. 04. 2018).

[20] Österreichische Nationalbank. *Standardisierung und SEPA*. URL: https://www.oenb.at/Zahlungsverkehr/Kartenzahlungen/Standardisierung-und-SEPA.html (besucht am 26. 04. 2018).

[21] NearFieldCommunication.org. *NFC Forum*. URL: http://nearfieldcommunication.org/history-nfc.html (besucht am 15. 05. 2018).

[22] Jeroen Netten. *Step by step: How does a EMV contact card payment work?* 2016. URL: https://www.quora.com/Step-by-step-How-does-a-EMV-contact-card-payment-work (besucht am 29. 04. 2018).

[23] *POS Terminal Risk Management Rules You Need to Know*. URL: http://blog.unibulmerchantservices.com/pos-terminal-risk-management-rules-you-need-to-know/ (besucht am 02. 05. 2018).

[26] International Organization for Standardisation (ISO). *ISO/IEC 7816-4:2013 Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange*. 2013. URL: https://www.iso.org/standard/54550.html (besucht am 28. 04. 2018).

[27] International Organization for Standardization. *ISO/IEC 14443-1:2016 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 1: Physical characteristics*. URL: https://www.iso.org/standard/70170.html (besucht am 26. 04. 2018).

[28] International Organization for Standardization. *ISO/IEC 14443-2:2016 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface*. URL: https://www.iso.org/standard/70170.html (besucht am 26. 04. 2018).

[29] International Organization for Standardization. *ISO/IEC 14443-3:2016 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision*. URL: https://www.iso.org/standard/70170.html (besucht am 26. 04. 2018).

[30] International Organization for Standardization. *ISO/IEC 14443-4:2016 Identification cards – Contactless integrated circuit cards – Proximity cards – Part 4: Transmission protocol*. URL: https://www.iso.org/standard/70170.html (besucht am 26. 04. 2018).

[31] International Organization for Standardization (ISO). *ISO/IEC 18092:2013: Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*. 2013. URL: https://www.iso.org/standard/56692.html (besucht am 15. 04. 2018).

A Anhang

Quellcode, Datenmodell, Fragebögen, ...