Information Security

Digitale Zahlungssysteme

Analyse der Sicherheit von digitalen Zahlungssystemen in Österreich

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Biehl Stefan

Autor/Autorin
Matrikelnummer
Biehl Stefan IS151501

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Univ.-Doz. Dipl.-Ing. Dr. Ernst Piller

Rekawinkel,10.08.2018

(Unterschrift Autor/Autorin)

(Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

Rekawinkel,10.08.2018

(Unterschrift Autor/Autorin)

Zusammenfassung

Die Masterarbeit *„Digitale Zahlungssysteme - Analyse der Sicherheit von digitalen Zahlungssystemen in Österreich“* befasst sich mit den vorhandenen und zukünftigen Zahlungssystemen auf dem österreichischen Markt. Dabei wird technisch und organisatorisch veranschaulicht, wie sich digitale Zahlungssysteme von konventionellen unterscheiden. Einen zentralen Punkt stellt dabei die kontaktlose NFC Übertragung dar, die in den unterschiedlichsten Geräten untergebracht werden kann, um digitalen Geldtransfer zu ermöglichen. Im Zuge dessen werden auch die möglichen Angriffsszenarien auf die NFC Schnittstelle vorgestellt und erklärt. Basierend auf den vorgestellten Angriffsvektoren werden mögliche zukünftige Szenarien erörtert oder die vorhandenen Attacken an die derzeit gegeben technischen Möglichkeiten adaptiert. Nachfolgend beschäftigt sich die Arbeit mit digitalen Identitäten, die in einem wichtigen Zusammenhang mit dem digitalen Zahlungsverkehr stehen. Der Schutz und sachgemäße Umgang mit einer digitalen Zahlungsidentität spielt vor allem für Endbenutzer einen entscheidenden Punkt, wenn es um die Sicherheit bei einem Zahlungsvorgang geht.

Ein weiterer Schwerpunkt dieser Arbeit liegt in der Erläuterung von zukünftig in Österreich verfügbaren digitalen Zahlungsmethoden. Es handelt sich um die derzeit verbreitetsten Ökosysteme, wie Google-Wallet und ApplePay. Die vorgestellten digitalen Zahlungssysteme bieten unterschiedliche Konzepte, Implementierungen, technische Umsetzungen und organisatorische Unterschiede. Speziell bei der Implementierung eines sicheren Zahlungsvorgangs auf einem mobilen Endgerät haben die Hersteller unterschiedliche Konzepte gewählt. Im Detail geht es dabei um die aktuelle Umsetzung von Apple in ApplePay mit der Implementierung des „Secure-Elements“ und Google-Wallet mit der Umsetzung der „Host-Card-Emulation“-Technik. In weiterer Folge wird veranschaulicht wie sich diese Ansätze mit modernen Techniken wie dem Cloudcomputing verbinden lassen, um den Endkunden ein möglichst flexibles und sicheres Zahlungssystem zu bieten.

Um ein möglichst vollständiges Bild über eine digitale Transaktion zu generieren, wird auch die „Tokeninzation“ beschrieben. Dieser Vorgang stellt den eigentlichen Hintergrundprozess des Geldtransfers zwischen möglichen Zahlungsinstitutionen dar. Es gibt bei den Tokensystemen verschiedene Arten von generierbaren Token. Je nach vorliegendem Anwendungsfall und Anforderungen müssen Serviceanbieter mit einem passendem Tokensystem versehen werden, um den Ansprüchen der Kunden zu genügen.

Der letzte Schwerpunkt befasst sich mit den Angriffsvektoren auf den verschiedenen Ebenen solcher komplexen Zahlungssysteme. Die daraus resultierenden Angriffsvektoren werden auf Basis der darunterliegenden Technologie aufgezeigt und konkretisiert. Je nach Zielsetzung der Angreifer/innen werden entweder einzelne Usergruppen, Businessprozesse oder aber die Providerinfrastruktur attackiert und reichen dabei von Übergriffen auf Identitäten, mobilen Zahlungen, Softwaremanipulation bis hin zu direkten Attacken auf Hardware-schwachstellen. Abschließend kann gesagt werden, dass es in absehbarer Zeit noch zu weiteren Entwicklungen in den Bereichen der digitalen Transaktion kommen wird und diese mit Spannung zu beobachten sind.

Abstract

The master theses *"Digital Payment Systems - Analysis of the Security of Digital Payment Systems in Austria"* represents existing and future payment systems in Austria. Technically and organizationally it portrays how digital payment systems differ from conventional ones.

A central point of digital payment is the contactless NFC transmission, which can be accommodated in a variety of devices to enable digital payments. Therefor the possible attack scenarios on the NFC interface are presented and explained. Based on the introduced attack vectors, possible future scenarios are discussed, or the existing attacks are adapted to the current technical possibilities. The following chapter deals with digital identities, which are important in connection with digital payments. Scenarios are explained, which show the existing dangers in the payment process in connection with stolen identities. The protection and proper handling of a digital payment identity plays a crucial role, especially for the end user, when it comes to the security of a payment transaction.

Another focus of this work is the explanation of future digital payment methods available in Austria. These will be the most widespread ecosystems, such as Google-Wallet and ApplePay. The presented digital payment systems offer different concepts, implementations, and organizational differences to offer the customer a secure and flexible payment service.

Especially in the implementation of a secure payment transaction on mobile devices, manufacturers have chosen different technological concepts. In detail, it is about the current implementation of Apple in ApplePay, with the implementation of the "Secure-Element" and Google-Wallet with the implementation of the "Host-Card-Emulation" technology. To show the different specifics of these, it will be illustrated how these can be combined with modern technologies. For example cloud computing, in order to offer the end customer a flexible and secure payment system.

To present a complete picture of a digital payment transaction, the "tokenization" is also described. This process represents the actual background process of a payment between possible payment institutions. There are various types of token, which are generated in the token systems. Depending on the particular application and requirements, the service provider must be provided with a suitable token system to meet the requirements of the customer.

The final focus will be on attack vectors at the various levels of such complex payment systems. The resulting attack vectors are identified and substantiated basically on the underlying technology. Depending on the final goal of the attacker, either individual user groups, business processes or the provider infrastructure are attempted to attack in order to reach their destination. The possibilities of attack range from identity theft, mobile payments, software manipulation to targeted attacks on hardware vulnerabilities. In conclusion there will be further developments in the area of digital payments and these can be observed with great excitement.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung zum Thema Zahlungssysteme

Mobile und digitale monetäre Systeme werden schon seit einigen Jahren erforscht und stetig weiterentwickelt. Jedoch sind die Akzeptanz und die tatsächliche Marktverbreitung eine sehr länderspezifische Angelegenheit, die aber eine stetig wachsende Tendenz zeigt. Der neue aufgekommene Trend von „smarten Geräten“, wie Smartphones, Smartwatches oder anderen Varietäten mobiler Einrichtungen, erleichtern die Verankerung solcher Techniken am Markt. Smartdevices haben oft eine Vielzahl an Kommunikationsschnittstellen. Diese können universell gehalten sein oder aber es werden spezielle technische Bestandteile dafür benützt, um z.B. Zahlungsabläufe zu ermöglichen. Die fortschreitende Verbreitung moderner Geräte, schafft über einen mittel- bis langfristigen Zeitraum einen immer größeren Bedarf an neuen Zahlungsmöglichkeiten. Ob sich eine neue Transaktionssart im alltäglichen Umfeld für die breite Masse etabliert, oder aber nur für spezielle Anwendungsfälle eingesetzt wird, kann nur schwer prognostiziert werden. Um diese Technik besonders interessant zu machen, benötigt der/die Endbenutzer/in auf jeden Fall eine bestimmte Situation oder die Notwendigkeit für die Verwendung im alltäglichen Leben. Jedoch liegt es nicht allein im Einflussbereich der Endbenutzer/innen ganze Ökosysteme zu etablieren, sondern überwiegend an den Herstellern, die ihre Zahlungslösungen an die Kundenbedürfnisse anpassen sollten. Es existieren noch viele andere wichtige Faktoren, die erfüllt werden müssen, wie z.B. die Schaffung der nötigen Infrastruktur, das Einbinden der Händler- und Bankinstitute, das Schaffen von Sicherheitsbewusstsein etc. Dafür müssen einige Gegebenheiten stimmen, um mit einem Schlag einen großen Bereich von Zielgruppen, Händler/innen und Institutionen anzusprechen, damit sich ein digitales Zahlungssystem in einem Land durchsetzt [1, p. 1].

Was sind mobile Zahlungen?

Eine mobile Zahlung ist die Übertragung eines digitalen Wertes mit Hilfe eines mobilen Endgerätes. Aufgrund der vielfältigen Schnittstellen ergeben sich bei der Initiierung oder Bestätigung des Zahlungsverkehres, mehrere technologische Umsetzungen. [1, p. 2].

Um nun einen technologischen Überblick der Einsatzmöglichkeiten zu bekommen, muss man folgende Bereiche miteinbeziehen:

- Art der Anwendung
- Bereich der Zahlung
- Transaktionsart
- Innovation

Die **Anwendungsszenarien** mobiler Zahlungen unterscheiden sich in zwei grundsätzlichen Ansätzen, der **lokalen** und der **server-** oder **cloudbasierten** Zahlung. Die lokale Anwendung ist eine Transaktion, die direkt vom mobilen Endgerät aus durchgeführt werden kann, vorausgesetzt es erfüllt die technischen Anforderungen. Wird alles über einen Server oder eine cloudbasierte Plattform abgewickelt, muss nur sichergestellt sein, dass der Client einen Zugriff auf das Zahlungsservice besitzt. Server- und cloudbasierte Ansätze ermöglichen dabei, Geräteschnittstellen unabhängige Zahlungen durchzuführen. [1, p. 3].

Der **Bereich** einer Zahlung gliedert sich dabei in drei Arten:

- Direkte Zahlung Bsp. Der/Die Käufer/in und Verkäufer/in stehen sich persönlich gegenüber.
- Internet-Zahlung Bsp. Der/Die Käufer/in und Verkäufer/in sind über eine Internetplattform verbunden.
- Mobile Zahlung Bsp. Der Kauf wird über ein mobiles Gerät abgewickelt (direkt oder über das Internet) [1, p. 3].

Das maximale **Transaktionsvolumen** ist vom Zahlungsinstitut abhängig und ein Einflussfaktor, der die einzelnen Zahlungsarten unterscheidet. Man kann diese in Makro- und Micro-Transaktionen unterteilen. Von einer Micro-Transaktion spricht man, wenn es sich um Geldbeträge kleiner gleich 5 € handelt. Bei einer Makro-Transaktion spricht man von einem Betragsvolumen von größer gleich 5€. [1, p. 3].

Der **Innovationsgehalt** eines solchen Zahlungssystems zeigt sich, wenn ein neuer Zahlungskanal geschaffen wird, der der Zielgruppe einen zusätzlichen Mehrwert bietet. Die Innovationen der Anbieter betreffen dabei unterschiedliche Bereiche, welche jene von der Schaffung einer ausschließlich digitalen Währung bis hin zur Integrationen auf mobilen Geräten umfassen. Bei letzterer ist im Hintergrund schon ein bekanntes und verifiziertes „Konto“ vorhanden, von dem aus der monetäre Wert übertragen wird. Dabei wird auf bestehenden Strukturen aufgesetzt und gegebenenfalls erweitert. Die Vorteile von elektronischem Geldtransfer sind für Endbenutzer/innen nicht immer auf den ersten Blick ersichtlich, da der Verbraucher nur am Ergebnis interessiert ist. Die nachfolgende Aufzählung zeigt einige Vorteile der neuen Zahlungsstrukturen:

- Universelle Verwendbarkeit
- Universelle Zahlung
- Sperrmaßnahmen bei Diebstahl oder Verlust
- Schutz vor falscher Währung
- Schnelle und sichere Transaktion
- Haftung

Spricht man ausschließlich von elektronischem Geld, spielen andere Aspekte eine Rolle, beispielsweise die ordnungsgemäße **Speicherung** einer digitalen Wertanlage auf einem mobilen Endgerät.

Unter der Hinzunahme weiterer Faktoren, wie eines konkreten Zahlungsszenarios und -bereiches spielen auch Mobilfunkanbieter eine nicht unerhebliche Rolle. Diese betreiben und warten das Netzwerk, über das der Transaktion übertragen wird. Abhängig vom jeweiligen Zahlungskonzept und Anwendungsfall kann hier auf unterschiedliche Infrastrukturtechnologien gesetzt werden. [1, p. 3].

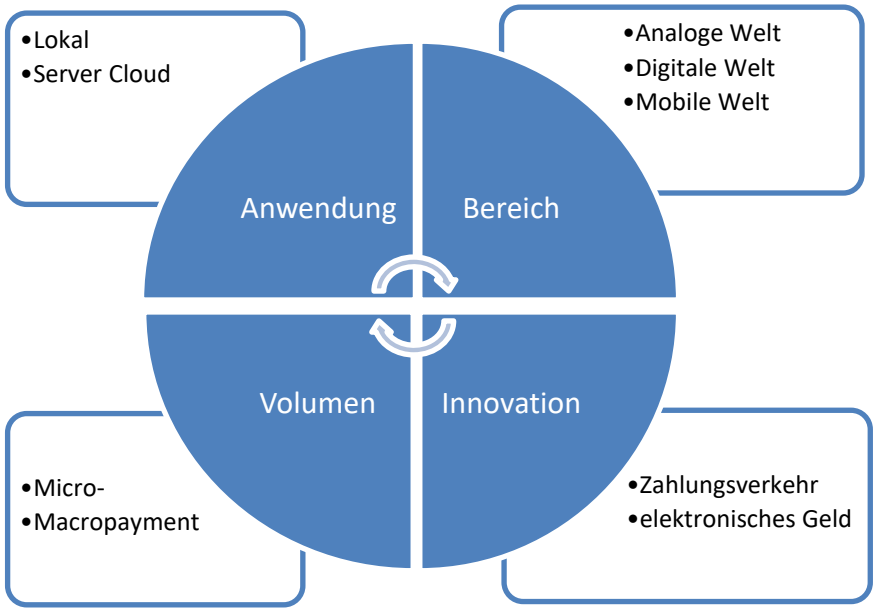

Abbildung 1 Kategorisierung von Mobile Payment nach [1, p. 2]

Darstellung der derzeitigen Marktsituation in Österreich

Die derzeitige Situation in Österreich ist, dass die Mehrheit der Bevölkerung im Alltag bevorzugt mit Bargeld bezahlt. Vor allem die Kleinstbeträge um die ~20 € werden in Österreich meist mit dem Bargeld beglichen. Bei größeren Beträgen kommen vorranging andere Zahlungsarten zum Einsatz, nämlich vor allem Kredit- und Debitsysteme. [2, p. 1]

Die Wahl eines Zahlungsmittels ist oft eine sehr emotionale Entscheidung. Menschen, die sich mit einer bestimmten Zahlungsart arrangiert haben, verändern diese Gewohnheit nur mehr selten oder nur unter spezifischen Umständen. Die Assoziationen, die mit physischem Geld gemacht werden, sind oft komplett andere, als zum Beispiel mit Kredit- oder Debitzahlungen, wo es sich aus Kundensicht hauptsächlich um Buchgeld handelt. Ähnlich ist das auch mit mobilen Zahlungssystemen, bis sich diese in der breiten Bevölkerung gedanklich verankert haben. Je öfter die Endverbraucher/innen einer direkten Konfrontation mit neuen Zahlungssystemen gegenüberstehen, desto wahrscheinlicher ist die zukünftige Wiederverwendung. [2, pp. 2-3]

Bargeld hat in seiner jetzigen Form auch Nachteile, bezogen auf die Verteilungs-, Instandhaltungs- und Betriebskosten. Bei der Aufrechterhaltung eines physischen Zahlungssystems wie wir es kennen, entstehen oft Kosten, die vom Konsumenten und vom Anbieter getragen werden müssen. Beispielsweise besteht Papiergeld aus speziellen Herstellungsverfahren, Materialzusammensetzung und diversen Sicherheitsmerkmalen[1]. Diese „Betriebskosten“ sind bei mobilen Zahlungssystemen tendenziell geringer und steigen auch nicht so drastisch bei großflächigem Einsatz. Für die zukünftigen Generationen wird der mobile Zahlungsverkehr schon tief in der Gesellschaft verankert sein und steht somit in direkter Konkurrenz zu den konventionellen Zahlungsmöglichkeiten. [2, p. 3]

Anhand von der Österreichischen Nationalbank zur Verfügung gestellten Daten, kann man Österreich grundsätzlich als ein bargeld-affines Land bezeichnen. Derzeit befinden sich im europäischen Raum ca. 20,72 Milliarden herausgegebene Banknoten im Umlauf:

Jahr	Euro-Banknoten	Steigung zum Vorjahr in %
2014	26.237	n.A
2015	27.795	~6%
2016	28.893	~4%
2017	30.035	~4%

Tabelle 1 Banknotenumlauf [3]

Österreichische Insellösungen

In Österreich gab es seit 1990 eine eigenständige digitale Geldbörse, die auch unter dem Namen „Quick“ bekannt ist. Jener Vorreiter moderner digitaler Zahlungssysteme sollte eine Art von digitalem Bargeld mit all den Vorteilen wie Anonymität und Sicherheit werden. Es war möglich seine „Quick“-Geldbörse mit einem Maximalbetrag von bis zu 400€ aufzuladen. Die Implementierung dieser Funktion geschah über die Jahre auf fast allen in Österreich ausgegeben Bankomatkarten. Alternativ konnte man auch Quick-Pre-Pay-Karten kaufen und diese mit Geld befüllen. Die Funktionalität und Integration in schon vorhandene Zahlungssysteme entwickelte sich fortlaufend und erlangt mit der Umsetzung von „Quick Neu“ seinen technischen Höhepunkt. Es war unter anderem möglich eine Internetbezahlung mittels einer Quick-Karte durchzuführen, dazu wurde aber ein eigenständiges Kartenlesegerät benötigt. Eine kontaktlose Zahlungsfunktion in Form einer „Hybrid-Karte“ stand ab 2012 zur Verfügung.

[1]Bei den Sicherheitsmerkmalen handelt es sich um Wasserzeichen, Sicherheitsfaden, Hologramm, Glanzstreifen und Wertzahldruck.

Die großen Vorteile von Quick waren die Anonymität der Methode und dass man Zahlungen mit einem Betragsvolumen von kleiner gleich 400€ vornehmen konnte. Bei dem Begleichen des Zahlungsbetrags blieben Kontoinformationen und Kundendaten geheim. Bankbuchungen, Zeilengebühren oder aber andere Verwaltungskosten fielen erst gar nicht an. Quick-Transaktionen wurden über ihren Einsatzzeitraum in vielen Anwendungen implementiert, wie unter anderem in:

- Bankomatkassen
- Waschküchen
- Getränke-, Snack- und Zigarettenautomaten
- Schulmensen und anderen Kantinen

Die Quick-Zahlungslösung bekam 2013 starke Konkurrenz durch die standardisierte NFC[2]-Zahlungsmöglichkeit. Jene Funktion erlaubt es, über eine kontaktlose Strecke von wenigen Zentimetern eine Transaktion durchzuführen. Um den Geldtransfer anzustoßen, wird die Karte einfach über oder auf das mit dem NFC gekennzeichneten Symbolbereich gehalten. Wenige Sekunden später ist die Zahlung abgeschlossen. Über NFC können Beträge bis zu 25€ ohne die Eingabe eines PIN-Codes durchgeführt werden. Die maximale Wiederholungsfrequenz ist auf drei Transaktionen begrenzt, danach ist eine erneute PIN-Bestätigung erforderlich. Bei Beträgen höher als 25€ ist die Eingabe des PINs immer notwendig.

Das Ende von Quick

Im September 2013 wurde das Unternehmen PayLife von dem Schweizer Finanzdienstleister „SIX-Payment-Service“ aufgekauft. Der neue Betreiber entschied sich, dass Quicksystem nicht mehr weiterzuführen, obwohl es ein gewinnbringender Geschäftszweig war. Laut den damaligen SIX Statistiken waren noch ca. 140.000 Karten im Umlauf, mit denen noch Transaktionen möglich waren. Aufgrund des parallelen Aufkommens von NFC und anderen mobilen Zahlungsmodalitäten konnte die Quickzahlung ab 2016 einen starken Rückgang der Kundenbasis von ca. 20% verzeichnen. In der breiten Masse setzte sich Quick aber nicht durch, verlor dadurch potentielle Kunden und somit auch Marktanteile. Mit der Entscheidung des Anbieters SIX-Payment-Service endete Quick mit der Einstellung der Zahlungsfunktionalitäten am 31.Juli 2017.

Die Restguthaben der Kunden, die sich auf den im Verkehr gebliebenen Karten befanden, können bis Ende des Jahres 2017 und darüber hinaus direkt bei dem dementsprechenden Anbieter SIX oder Pay-Life zurückgefordert werden. [4] [5]

Derzeitige Entwicklungswege von bargeldlosen Geldtransfer

Die Entwicklung von bargeldlosen Zahlungssystemen ist stark mit dem Aufkommen von Smartphones verknüpft. Laut einem Bericht der Firma „Tune-Markting-Console“ waren schon 2015 ca. 50% der Weltbevölkerung mit Smartphones ausgestattet. Im Zusammenhang mit den Verkaufsstatistiken von diversen Online-Handels-plattformen wurden bei diesen ca. 53% der Erlöse durch mobile Geräte generiert. Allgemein wird ein klares Bild von einem schnell wachsenden Markt vermittelt. [6, p. 2]

Technologische Trends

- Mobile Zahlungssysteme basierend auf vorhandenen Methoden wie Debit und Kredit
  - AndroidPay, ApplePay, SamsungPay und weitere Anbieter
- Host-Card-Emulation, abgekürzt HCE
  - Erstellung einer virtuellen Chipkarte in einer reinen Softwareumgebung
- Bitcoin und andere digitale Zahlungsmittel
  - Dezentrale digitale Währung mit kryptographischen Wurzeln
- Blockchain-Systeme
  - Verkettung aller Transaktionsdaten zur transparenten Nachverfolgbarkeit des gesamten Geldtransfers

[2] NFC bezeichnet die Nahfeldkommunikation oder wird auch "Near-Field-Communication" genannt.

- Mobiles Zahlungssystem Peer-to-Peer
    - Direkte Geldüberweisung zwischen zwei Personen auf Basis eines Zahlungsinstitutes

Alle genannten Trends zeigen, dass der Markt des Zahlungsverkehres im Umbruch ist. Das bisher verwendete klassische Bargeld und Buchgeld bekommt durch neue Technologien und Modetrends einen frischen Aufwind. In der Zahlungsmittelbranche bilden sich zunehmend kleine Start-ups, die mit ihren Ideen den Zahlungsverkehr verbessern oder gar revolutionieren wollen. Diese werden in der Fachliteratur auch „Fintech" Start-ups genannt, der Begriff setzt sich aus **Fin**anz und **Tech**nologie zusammen. Oft haben diese Firmen auch spezifische Schwerpunkte in Themen wie Zahlungsverkehr, Onlinehandel und -banking, Sicherheit und Privatsphäre, digitalen Geldbörsen oder anderen Zahlungsinnovationen. [6, pp. 2 - 3]

Regulatorische Anpassungen und Vorbereitungen

Je globaler ein Zahlungssystem etabliert wird, desto größer ist der Nutzen für die Endverbraucher/innen. Aus diesem Grund schlug die Europäische Kommission schon 2015 eine Strategie für einen Binnenmarkt vor. Das Kernelement dieser Strategie bestand darin, die Grundvoraussetzungen für die jetzigen Standards der im europäischen Raum etablierten digitalen Zahlungssysteme zu schaffen. Die so entstandenen Systeme sind von essentieller ökonomischer und sozialer Bedeutung. Die Weiterentwicklung des Binnenmarktes kann man auch als digital fokussierten Binnenmarkt bezeichnen.

Es wurde auf internationaler Ebene erkannt, dass derartige digitale Binnenmärkte wesentlich für die Verbreitung eines digitalen Zahlungssystems sind. Dabei muss der Fokus auch auf dessen Bedürfnisse gerichtet werden, wie:

- digitale Sicherheit bei der Transaktion,
- Einfachheit in der Benutzung,
- Missbrauchssicher und
- Global verfügbare Infrastruktur

In genannten Belangen nimmt Cybersicherheit einen zentralen Punkt ein. Dafür wurden zwischen Mai und Oktober 2015 konkrete Richtlinien[3] entworfen, welche einen Schwerpunkt auf Rechtsvorschriften und technische Sicherheit für Käufer/innen und Verkäufer/innen legten. Mit Januar 2018 traten diese neuen Regelungen in Kraft. [6, pp. 4 - 5]

Die Direktive legt klar offen, dass Zahlungssicherheit gegenüber den zahlenden Parteien ein fundamentaler Grundbaustein ist. Das immer häufigere Auftreten von Sicherheitsproblemen aufgrund der tiefen Integration in komplexen Systemen soll dadurch minimiert werden. Die digitale Kriminalität entwickelt sich stetig und darf nicht ignoriert werden. Vor allem wenn es um digitale Währung, Geldtransfer und Zahlungsservices geht, speziell aus Sicht eines Zahlungsanbieters. Gut durchdachte Sicherheitsmechanismen schützen vor möglichen Schäden und reduzieren die Angriffsfläche auf ein Minimum.

Der schnelle technologische Fortschritt aufgrund von Innovationen, aber auch die systemübergreifenden Funktionen, enden in zunehmend komplexeren Hintergrundsystemen, die es dementsprechend zu designen und anhand von verfügbarer Technik abzusichern gilt. [6, p. 5]

3 Official Journal of the European Union, L 337, 23 December page 35-127

Folgende Auflistung zeigt einige wichtige Punkte, mit denen man sich während der Designphase eines solchen Zahlungssystems befassen sollte:

- Neutrale Definition einer Zahlungsmethode
- Schaffen einer geprüften Lieferantenkette
- Strikte Sicherheitsanforderungen
- Kundensicherheit in Bezug auf ausgeglichene Handelskonditionen
- Kundentransparenz
- Verbot von Zahlungsintransparenz
- Technische Richtlinien, um die Missbrauchsmöglichkeiten gering zu halten
- Rechtliche Anforderungen und Rahmenbedingung im nationalen oder internationalen Umfeld
- Weiterentwicklung und Marktanpassung
- Systemspezifikationen

Diese Themenschwerpunkte sind nur einige von vielen, sollen aber den Umfang eines digitalen Zahlungssystems vor Augen führen. [6, pp. 5- 6]

Einflussbereich von Onlineplattformen

Mit dem Aufkommen des Internets und der Etablierung von digitalen Marktplätzen mit permanenter Verfügbarkeit im internationalen Umfeld, mussten sich neue Zahlungskonzepte etablieren, die diesen neuen Ansprüchen genügen. Der Onlinehandel von Gütern und Services hat einen großen Einfluss auf die Verbreitung und Verwendung von digitalen Zahlungssystemen. In erster Linie wurden diese Zahlungsmethoden hauptsächlich in Webshops oder anderen Onlineplattformen eingesetzt. Dort etablierten sie sich zuerst im digitalen Umfeld, konnten aber aufgrund ihrer Universalität schnell den Sprung in die reale Zahlungswelt bewältigen. Viele Online-Verkaufsplattformen haben erkannt, wie wichtig ihr Angebot an unterschiedlichen Zahlungsmöglichkeiten ist, um auf dem globalen Markt zu bestehen. Die Plattformbetreiber müssen dabei Schnittstellen für stationäre Clients, aber auch zunehmend für mobile Clients unterschiedlichster Art bereitstellen und absichern. Die weitere Integration von neuen Zahlungsmethoden in bestehende Plattformen hat einen maßgeblichen Einfluss auf die anzusprechenden Kundenkreise. Jedoch stellen die neuen und oft sehr unterschiedlichen Zahlungskonzepte die Plattformbetreiber vor große Herausforderungen. Diese können technologischer aber auch politischer Natur sein und müssen dementsprechend gelöst oder als legal eingestuft werden.

Die immer stetige Weiterentwicklung und Integration der schon jetzt vorhanden digitalen Zahlungsverfahren, wie GooglePay und ApplePay, um nur einige prominente Vertreter zu nennen, schafften eine immer breitere Akzeptanz auf Kundenseite. Das spiegelt sich unter anderem in einer jährlichen Steigerung der Benutzung solcher Dienste oder im Transaktionsvolumen von mobilen Endgeräten wieder. [6, pp. 7 - 8]

Technisches Umfeld für kontaktlose Zahlung

Unser derzeitiges Zahlungssystem ist traditionell aus dem Tauschhandel entstandenen. In seinen anfänglichen Zügen war es das Eintauschen von Rohstoffen bis es sich zu der jetzigen Form, bei der Güter und Dienstleistungen mit einer Währung bezahlt werden, entwickelt hat. Um kontaktlosen Geldtransfer zu erläutern, wird zuerst veranschaulicht, wie ein generisches digitales Zahlungssystem aussehen könnte. [7, p. 6]

Definition Multi-Side-Plattform

Bei einer **M**ulti-**S**ide-**P**lattform[4], handelt es sich um ein System, das zwei oder mehreren Parteien ermöglicht, direkt miteinander zu interagieren. Aus dieser direkten Verbindung generiert eine MSP einen Wert. [7, p. 6]

Populäre Beispiele aus analoger und digitaler Welt sind Börsen, Suchmaschinen und Zeitungen, die zwischen Suchenden und Werbenden vermitteln und viele mehr, die zahlreich am Markt vorhanden sind und die unterschiedlichsten Geschäftsbereiche besiedeln. MSPs finden auch bei digitalen Zahlungssystemen Verwendung, da diese zwischen den Kund/inn/en und Verkäufer/inne/n ver- und übermitteln. Dabei bietet der MSP-Provider beiden Seiten ein System an, das eine digitale physische Infrastruktur oder eine Kombination daraus besitzt. Beide Zahlungsparteien können sich sicher miteinander verbinden, um die Zahlungsinteraktion durchzuführen. Der Anbieter stellt dabei die Rahmenbedingungen auf, unter denen sein System genutzt werden kann:

- Interaktionsbedingungen zwischen den zahlenden Parteien
- Interaktionsbedingungen zwischen Zahlungsinstitutionen und Händlern
- Universelle technische Aktionsplattformen z.B. in:
    - Betriebssystemen
    - Zahlungsterminals
    - Spielkonsolen
    - Geschäftslokalen
    - anderen Zahlungsumgebungen

Die Effektivität der MSP lässt sich dann über recht einfache Kennzahlen feststellen, wie z.B. über die Nutzeranzahl und tatsächliche Marktverbreitung. Die Kunden- und Händleranzahl ist dabei auch ein gutes Maß, um digitale Zahlungsplattformen untereinander zu vergleichen. Die MSP muss sich der Herausforderung stellen, den Anforderungen und Trends beider Seiten zu genügen, um auch am Markt erfolgreich zu sein. [7, p. 6]

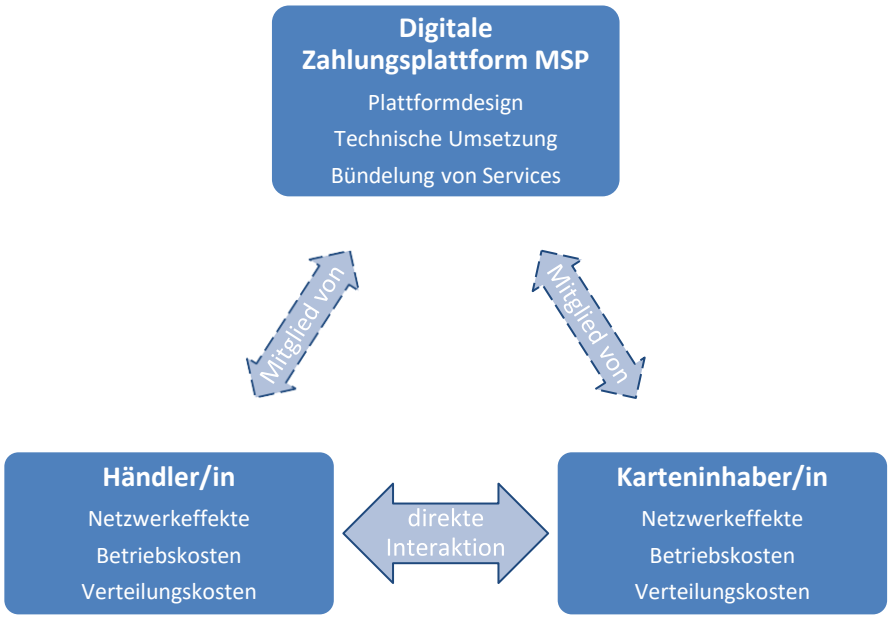

Abbildung 2 Multi-Side-Plattform nach [7, p. 6]

[4] Abgekürzt durch den Term MSP

Detailbeschreibung des digitalen Frameworks

In nachfolgender Beschreibung werden die Teilbereiche der einzelnen Beteiligten erklärt und ihr Nutzen erläutert.

Direkte Interaktion

Die direkte Interaktion zwischen den Handelspartnern ist ein Schlüsselkriterium für einen Service bzw. für den Güteraustausch. Wobei es irrelevant ist, ob es sich um ein physisches oder digitales Gut handelt. Die MSP verknüpft den gekauften analogen oder digitalen Inhalt mit dem Käufer. Zum Beispiel stellen der Google Playstore und der Apple App-Store solche MSPs dar. Derartige „Stores“ schaffen einen Softwarekatalog und damit die direkte Verbindung zwischen Käufer/innen, Entwickler/innen oder Händler/innen. Die digitale Zahlungsumgebung spielt dabei eine eher untergeordnete Rolle, solange sich die Parteien bei der Zahlungsmethode einig sind.

Als Abgrenzung dazu kann man beispielsweise den iTunes Music und Film bzw. Google Video Store sehen, die **keine** MSPs darstellen. Basierend auf den AGBs der Anbieter wird hier der Vertrag zwischen dem Kunden/der Kundin und der Verleihfirma geschlossen, also Google oder Apple. Dadurch wird eine Handelsbeziehung geschaffen. In dem vorgestellten Beispiel existiert keine direktere Zahlungsbeziehung zwischen dem Kunden/der Kundin und dem Filmstudio, und fällt damit nicht mehr in die Definition eines MSPs. [7, p. 6]

Netzwerkeffekte

Jene beschreiben Community-gesteuerte Vorgänge bzw. Phänomene, wie sich z.B. der Nutzen einer Plattform für jeden/jede zusätzlichen/zusätzliche User/in verändert. Man teilt diese Netzwerkeffekte in die nachfolgenden Kategorien ein:

- **Same-Side-Netzwerkeffekte oder auch direkte Netzwerkeffekte**
  Der Nutzen der Plattform (vertikaler Nutzen) kann direkt mit der Anzahl der zur Verfügung stehenden Güter in Verbindung gebracht werden. Als Beispiel sei hier ein Spielernetzwerk genannt, bei dem die Größe des Netzwerkes eine direkte Auswirkung auf den Nutzen der Teilnehmer/innen hat. Ein solcher Netzwerkeffekt kann in die positive aber auch in die negative Richtung ausschlagen.
    - **Positive**, direkte Netzwerkeffekte: Der/Die Benutzer/in hat die Möglichkeit mit sehr vielen Teilnehmer/inne/n zu kommunizieren, zu interagieren, zu spielen und digitale Güter zu handeln. Durch eine größere Anzahl an Spieler/inne/n besitzt dieser mehr Interaktionsmöglichkeiten.
    - **Negative**, direkte Netzwerkeffekte: Aufgrund der vielen Nutzer/innen ist der Wettbewerb zu hoch, um dem User/der Userin ein für ihn angemessenes Umfeld zu bieten.
- **Cross-Side-Netzwerkeffekte oder auch indirekte Netzwerkeffekte genannt**
  Der indirekte Nutzen entsteht erst, wenn die Nutzung nicht direkt auf dem Produkt selbst basiert. Diese Phänomene lassen sich anhand einer Gaming-Community wie Xbox Live veranschaulichen, welches ein Micropayment-System für digitale Güter beinhaltet. Außerdem bietet es zusätzliche Spielinhalte oder Verbesserungen, die mit Geld nachgekauft werden können.
    - **Positive**, indirekte Netzwerkeffekte: Der/Die Benutzer/in kann ergänzende Erweiterungen nachrüsten, um den Spielinhalt, Spaß, Dauer, usw. zu erhöhen.
    - **Negative**, indirekte Netzwerkeffekte: Die Benutzer/innen fühlen sich durch vermehrtes Anbieten von zusätzlichem Inhalt und digitalen Gütern, die mit Kosten verbunden sind, gestört und lehnen das Produkt ab.

Je nach Entscheidung wie die MSP aufgestellt ist, können sich diese Eigenschaften zunutze gemacht werden, aus Businesssicht sind meist die gewinnbringenden Effekte stärker im Fokus der Plattform. [7, pp. 6 - 7]

„Homing“-Kosten oder Betriebskosten

Man spricht von Betriebskosten oder „Homing“-Kosten, welche bei einem Verbindungsaufbau eines Users/einer Userin mit der Plattform entstehen. Sie beziehen sich hauptsächlich auf folgende drei Komponenten:

- Investitionskosten, z.B. Forschung, Anfangsinvestitionen und Ausbildungen.
- Laufende Kosten, z.B. Instandhaltungs- und Wartungskosten, Anpassungskosten und Lizenzkosten.
- Ausstiegskosten, z.B. Hardware- und Software-Wiederbeschaffung oder aber Kosten einer Kündigung.

Außerdem seien noch die Referenzkosten genannt, die eine mögliche Aussage darüber treffen, wie groß die Einarbeitungszeiten in das System für den/die Nutzer/in sind. Ist das System folglich einfach zu verwenden, weist es einen hohen Usability-Grad auf und erreicht eine große Nutzergruppe. [7, p. 7]

„Switching“-Kosten oder Wechselkosten

Wenn sich der/die Benutzer/in entscheidet das Service zu wechseln, fallen Wechselkosten, oder „Switching“-Kosten an. Die Entscheidung auf eine andere Plattform umzustellen, kann aus diversen Gegebenheiten resultieren, beispielsweise das Aufkommen einer neuen oder effizienteren Technologie oder geringeren Kosten. Der Wechsel wird dadurch erschwert, dass der Kunde schon Einkäufe in dem vorangegangenen System getätigt hat. Jene digitalen Güter wie Musik, Filme etc. können nur in den wenigsten Fällen übertragen werden. Für die Kund/inn/en sind diese Inhalte durch den „Lock-Out[5]“-Effekt verloren oder nur beschränkt zugänglich. Es ist die Kehrseite zu den Betriebskosten auf Kundenseite. Im Business spricht man von einer möglichen Lock-In Situation, bei der ein Ausstieg schwierig ist. [7, p. 7]

„Bundeling and Envelopment“ oder Bündeln von Services genannt

Je nach Marktpositionierung eines MSPs ist das Bereitstellen eines Dienstes ausreichend. Wie schon gezeigt, ist der Kundenstamm ein maßgebliches Kriterium, ob sich ein MSP-Service bewährt. Für die Erreichung einer guten Marktposition ist es oft hilfreich, das eigentliche Service mit zusätzlichen Diensten zu kombinieren, daher das Wort „Bundeling“. Dieses Vorgehen hebt einerseits den Nutzen der Plattform, stärkt aber auch die Marktposition und Verfügbarkeit. Die Konkurrenz ist je nach Sparte groß, denn am Markt tummeln sich viele Mitbewerber/innen, die möglicherweise ähnliche oder gar gleiche Services anbieten. [7, p. 7]

Plattformdesign

Beim Plattformdesign handelt es sich um architektonisch grundlegende Entscheidungen, wie die MSP-Plattform zu entwickeln ist. Hier bieten sich zwei grundsätzlich verschiedene Ansätze:

- Open-by-Design
    - Bsp.: Googles Android Betriebssystem ist prinzipiell Open-by-Design, was Drittherstellern eine umfangreiche Modifikation des Systems erlaubt.
- Closed-by-Design
    - Bsp.: Apples IOS-Betriebssystem ist ein sogenannter „Wallet-Garden“, das bedeutet, nur der Hersteller selbst hat die legitime und/oder technische Möglichkeit das Produkt zu verändern.

Beide Ansätze haben sicherheitstechnische Vor- und Nachteile, die je nach vorliegendem Konzept richtig umgesetzt werden müssen. [7, pp. 7 - 8]

[5] Gewisse digitale Inhalte und Services sind nur in einem bestimmten Hersteller spezifischen Ökosystem vorhanden. Sollte der Kunde diese Güter und Dienste nutzen wollen, ist er also gezwungen bestimmte Systeme zu verwenden.

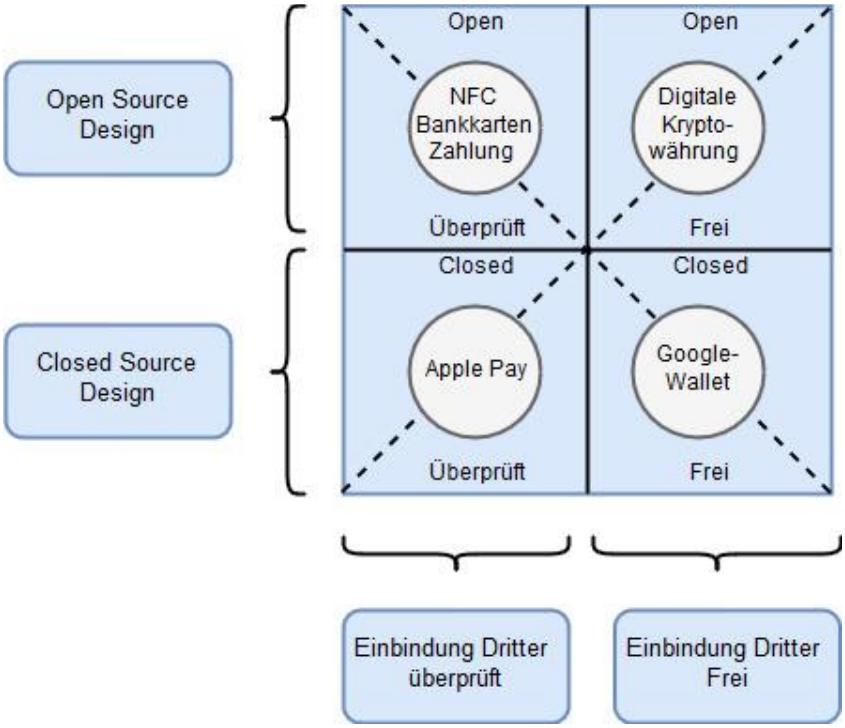

Abbildung 3 Architekturdesign nach [7, p. 8]

„Technological Solution“ oder Technologische Lösungen

Die am Markt auftretenden Lösungen zum Zahlungsverkehr haben jeweils auch unterschiedliche Kontrollmöglichkeiten. Die erste Kontrollinstanz bildet die technische Architektur, in der die notwendigen Sicherheitsmechanismen konzeptuell einzubinden sind. Aber auch die Überprüfungen von externen Einflüssen müssen regelmäßig stattfinden. Drittanbieter und Lieferanten müssen zusätzlich im Auge behalten werden, da diese auch maßgebliche Einflüsse auf die Kund/inn/en und die allgemeine Zahlungskette ausüben. Die ständigen Kontrollen sind für den Serviceanbieter eine zusätzliche Einnahmequelle, da hier die Erhebung von Bearbeitungsgebühren anfallen. Als andere mögliche Einnahmequellen aus der Sicht eines Providers kann es sich aber auch um die Herausgabe von Hardwarekomponenten handeln. Jene Hardware reicht von POS-Terminals[6] bis hin zu Infrastrukturkomponenten. Vor allem im direkten Verkauf wird meist über spezielle Terminals gezahlt. Die Zahlungssystemanbieter stellen dafür meist eigene entwickelte Hardware zur Verfügung, die z.B. über eine öffentliche- oder private Infrastruktur angebunden ist. Die Bereitstellung einer eigenen Infrastruktur ermöglicht es in Zahlungssystemen, Sicherheitskontrollen gezielter und effektiver umzusetzen und zu messen. Technologische Kontrollen über die integrierte Hardware zu implementieren, stellt eine zusätzliche konzeptionelle Verteidigungsstrategie dar. Die Schaffung einer eigenen Zahlungsinfrastruktur mit genau definierter Hardware, wie Zahlungsterminals, Zahlungskarten und den dahinterliegenden Prozessen, bietet genau diese gewünschten Kontrollen. [7, p. 8]

Bei den Zahlungssystemen wird von revolutionären und evolutionären Konzepten gesprochen, die wesentlichen Unterschiede werden nachfolgenden in einer Liste beschrieben.

[6] Der Begriff POS stellt die Abkürzung zum sogenannten Point-of-Sale-Terminal dar. Es beschreibt das Gerät beim Händler, auf dem gezahlt wird.

	Revolutionär	Evolutionär
Neue Funktionen	Bietet eine neue Möglichkeit der Zahlung (meist technologisch getriebene Innovationen).	Kann mit ergänzenden Funktionen ausgestattet werden (basierend auf der darunterliegenden Technologie).
Rückwärtskompatibel	Technisch nur schwer möglich in ein bestehendes System zu integrieren.	Ist in den meisten Fällen rückwärtskompatibel.
Schnelle Zahlung	Aufgrund des Einsatzes moderner Technologien sind die Zahlungsvorgänge schneller.	Die Geschwindigkeit ist basierend auf dem vorherigen Zahlungsdesign.
Effiziente Zahlung	Durch moderne Techniken haben revolutionäre Systeme eine hohe Effizienz.	Die Effizienz ist vom bestehenden Plattformdesign abhängig.
Sicherheitsbedenken	Hoch, da es sich um eine neue, noch nicht lange etablierte Technologie handelt. Es herrscht möglicherweise Ungewissheit.	Gering, es handelt sich schon um etablierte Systeme, die schon vollständig im Alltag verankert sind.

Tabelle 2 Zahlungssysteme - Konzepte nach [7, p. 8]

Um die Funktionslogik von modernen Zahlungsplattformen zu verstehen, muss also das oben angesprochene Plattformdesign im Zusammenhang mit den eingesetzten Technologien gesehen werden. [7, p. 8]

Veranschaulichung von traditionellen Kartenzahlungen und Mobile-Payment-Prozesse

Um nun ein mobiles Zahlungssystem zu erläutern, wird zuerst ein klassisches Karten-Zahlungssystem dargestellt, um später Vergleiche ziehen zu können. Ein traditionelles Zahlungssystem mit einer Kartenzahlung beinhaltet die folgenden Kernkomponenten und wird in Abbildung 4 dargestellt:

- Karteninhaber/in
- Bankomatkarte, verbunden mit dem dahinterliegenden Account
- Händler/in
- Händler/in, verbunden mit einem Bankkonto
- Zahlungsgesellschaft (MasterCard, Visa American Express etc.)
- Produkt- oder Serviceübergabe

Jeder dieser fünf Kernkomponenten muss technisch aufeinander abgestimmt, verbunden und verifiziert sein, um eine transparente Zahlungskette für den Kunden/die Kundin zu gewährleisten. [8, pp. 1 - 2]

Darstellung traditioneller Kartenzahlungen

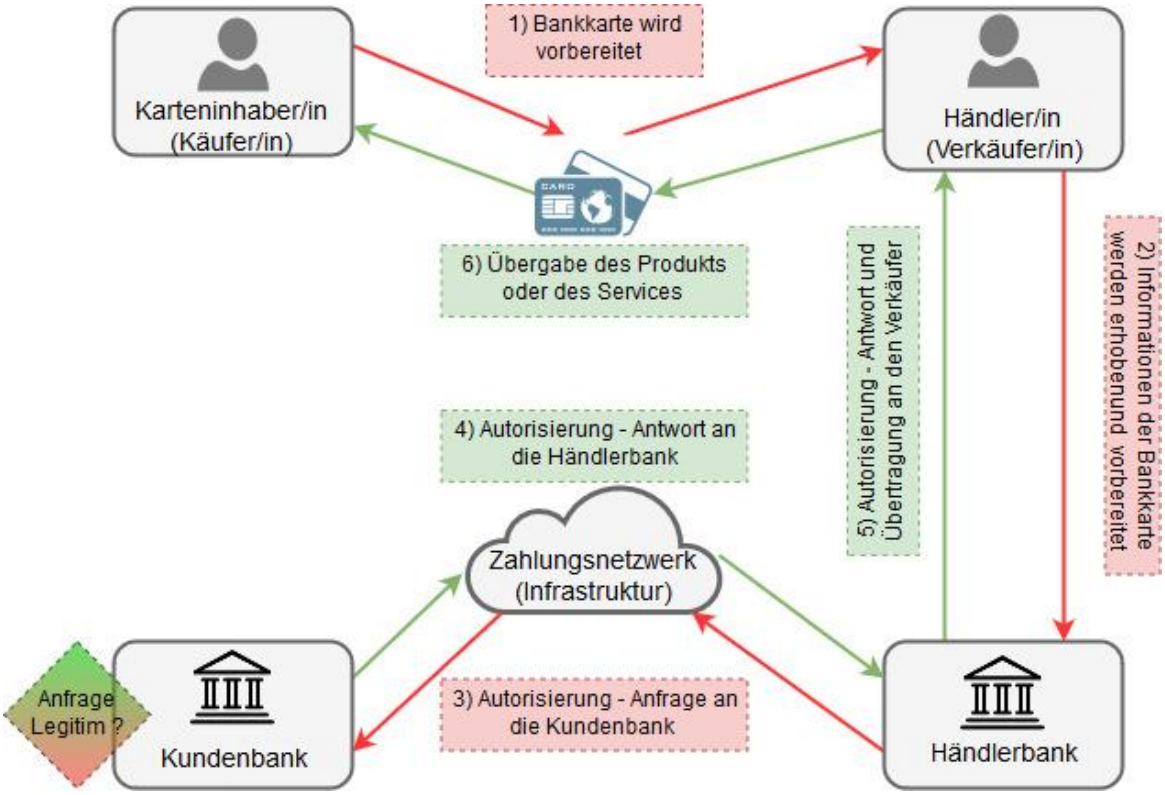

Abbildung 4 Traditionelle Kartenzahlung nach [8, p. 2]

Grundsätzlich stößt der Kunde/die Kundin die Zahlung an, dabei wird die Bankkarte in das von dem/der Verkäufer/in bereitgestellte Zahlungsterminal[7] eingesteckt (1). Das Zahlungsterminal des Verkäufers/der Verkäuferin sammelt nun alle benötigten Zahlungsdaten, um die Echtheit der Zahlung überprüfen zu können. Die Händlerbank, die den Transaktionstoken erhält, der für die Zahlung notwendig ist, routet diese Zahlungsaufforderung weiter. Wie der Transaktionstoken mit den gesammelten Daten transferiert wird, hängt vom Zahlungsnetzwerk ab (2). In der letzten Phase der Übertragung erhält die zuständige Kundenbank den Token über das Zahlungsnetzwerk (3). Die Bank des Kunden/der Kundin empfängt den eingehenden Transaktionstoken und kann diesen nun mit den empfangenen Daten verifizieren. Ja nach Entscheidung der Kundenbank wird der Zahlungsvorgang genehmigt oder abgelehnt (4). Das Ergebnis wird wiederum über das Zahlungsnetzwerk und die Händlerbank an das POS-Terminal gesendet (5). Nach dem Abschluss der Transaktion bekommt der Kunde/die Kundin sein „Gut oder Service“ übergeben (6). [8, p. 2]

Darstellungsmöglichkeit mobiler digitaler Zahlung:

Der Zahlungsverkehr bei mobilen digitalen Transaktionen gestaltet sich im Gegensatz zur traditionellen etwas komplexer. Im Vergleich zum klassischen Zahlungsverkehr erweitert sich das Konzept um zwei Kernelemente:

- Mobilfunkanbieter bzw. dessen Netzwerk[8]
- Mobile-Payment-Service-Provider [9]

[7] Wird auch oft POS genannt.

[8] In der Literatur auch MNOs genannt und bedeutet „Mobile Network Operators“.

[9] In der Literatur auch MPSPs genannt und bedeutet „Mobile Payment Service Providers“.

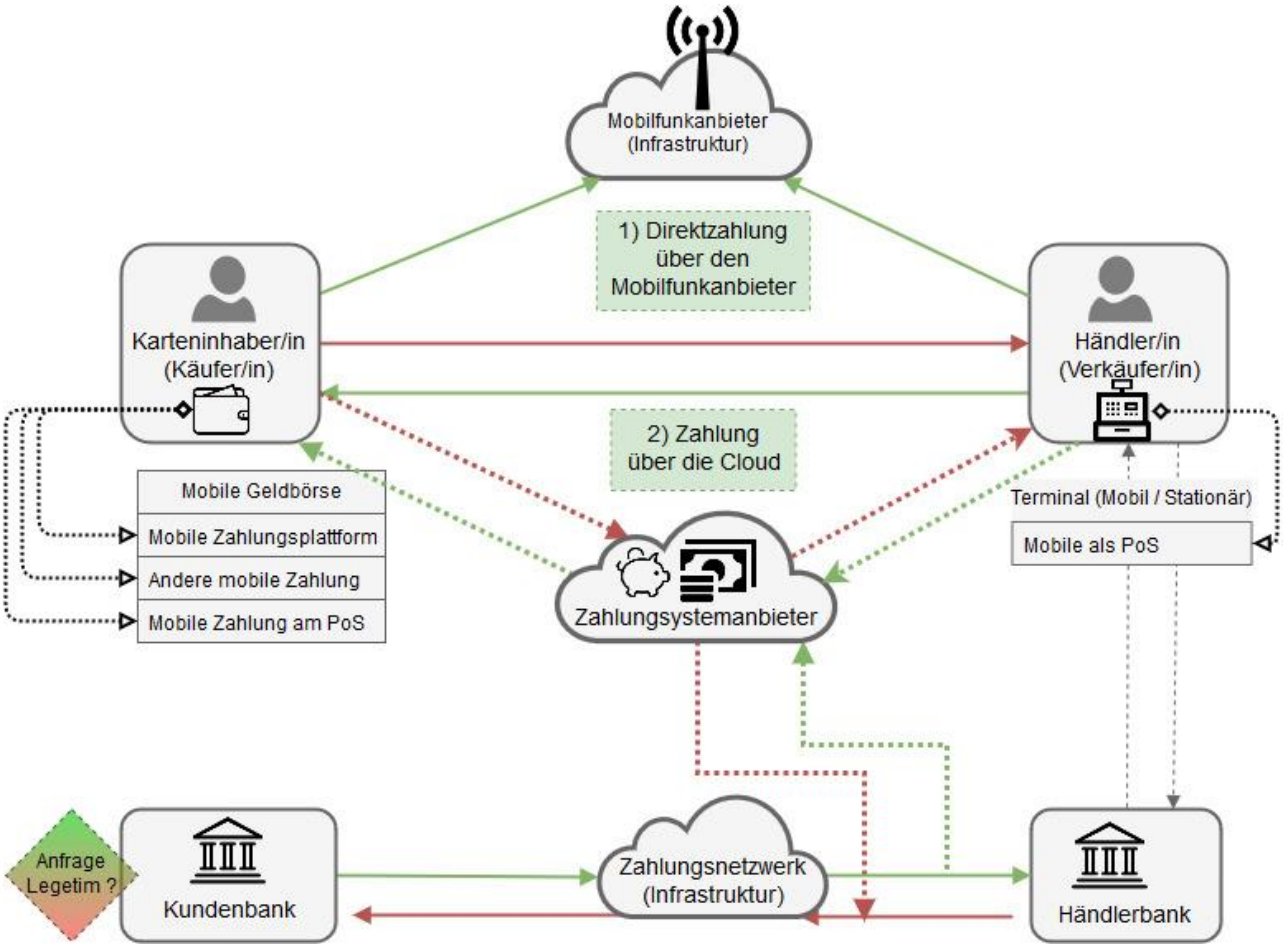

Abbildung 5 Mobile Zahlung nach [8, p. 2]

Das Ziel eines MPSP ist, dem Kunden eine Möglichkeit anzubieten, mittels derer eine direkte Zahlung von einem mobilen Gerät auf ein anderes getätigt werden kann. Je nach Aufstellung des MNO oder des MPSP kann das den Zahlungsprozess auch verkürzen (1). Das geschieht, wenn der MNO oder der MPSP direkt als „Kundenbank“ auftritt, dabei wird nur eine Verlinkung zu dem eigentlichen Zahlungskonto benötigt. Die angesprochene Verlinkung kommt beispielsweise schon von einem gebündelten Service, hier können die Zahlungsreferenzen dem MNO schon bekannt sein, z.B. aufgrund der Rechnungslegung. Alternativ könnte der Geldtransfer auch über ein Cloudsystem des Zahlungssystemanbieters transferiert werden (2). [8, p. 2]

Abhängig von vorheriger Umsetzung und bestehenden Anforderungen, können solche Konstrukte eines mobilen Zahlungssystems auch als Insellösung betrieben werden. Je nach Situation ergeben sich Vor- und Nachteile, wenn auf Händler/innen, Verkäufer/innen, Erwerber/innen oder Zahlungsgesellschaften verzichtet wird, da diese Prozesse intern abgebildet sind, z.B. WeChat. [8, p. 2]

Beschreibung mobile Zahlung am POS

Die mobilen Zahlungsmöglichkeiten auf der Kundenseite können in fünf Kategorien eingeteilt werden:

- Mobile Zahlung am POS
- Mobile Zahlung am POS per Software
- Mobile Zahlung über die Mobile Payment Plattform
- Mobile Zahlung über ein eigenständiges Zahlungssystem
- Direkte Zahlung über das mobile Netzwerk

Diese Möglichkeiten beschreibt die Zahlung am POS-Terminal via Smartphone. Die häufigste Technik für die Übertragung einer Zahlung bildet dabei NFC. Die bekanntesten Anbieter dieser Zahlungsmethode sind:

- Apple Pay
- Google-Wallet

Das mobile Zahlungssystem ist hierbei ein schon im Betriebssystem verankerter Mechanismus, der auch auf die Schutzfunktionen des eingesetzten mobilen OS[10] zurückgreift. Als Beispiele kann man Goolge-Wallet und ApplePay heranziehen, welche für den Kunden/die Kundin Zahlungsservices anbieten, die große technische Unterschiede aufweisen. [8, pp. 2 - 3]

NFC

NFC, oder auch „Near-Field-Technologie“, ist eine auf Radiowellen basierte Technologie, die eine Kommunikation auf kurze Distanzen ermöglicht. NFC stellt dabei eine Reihe an standardisierten Kommunikationsprotokollen dar und ist eine Weiterentwicklung der RFID-Technologie[11]. Die zugrunde liegende RFID-Technologie beschreibt eine Methode zur kontaktfreien Übertragung von Informationen oder Daten. Um die Datenübertagung zu ermöglichen, muss nur einer der beiden Kommunikationspartner aktive Energie zur Verfügung stellen. Das elektromagnetische Feld stellt die benötigte Energie bereit. Diese Eigenschaft zeigt die Möglichkeiten von aktiven wie auch passiven Kommunikationselementen. Die aktive Komponente, die im Zahlungsvorgang meist das POS-Terminal ist, erzeugt dann das elektromagnetische Feld, das für Energie-versorgung und Kommunikation genutzt wird. Der passive Kommunikationspartner stellt eine einfach gehaltene elektronische Schaltung dar. Dieser wird auch RFID oder NFC-Tag genannt und besitzt nur eine sehr begrenzte Anzahl an Funktionen bzw. Ressourcen. Der passive NFC-Tag verfügt über eine spezielle Antenne, mit der die erzeugte Energie aufgenommen und gleichzeitig eine Kommunikation ermöglicht werden kann. [9, pp. 4 - 5]

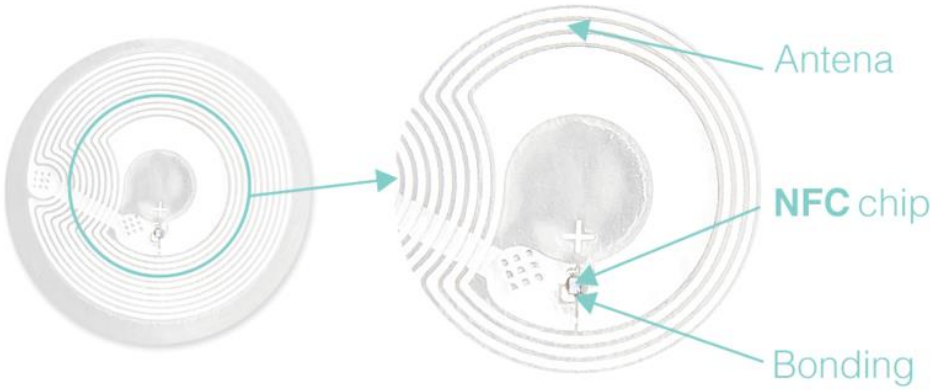

Abbildung 6 NFC-Tag nach [10]

Die Kommunikation findet dabei über einen sogenannten „Air-Gap[12]“ statt, da die Geräte physisch getrennt sind. [9, pp. 4 - 5]

Der NFC-Standard als Erweiterung zum RFID bietet dabei eine bidirektionale Verbindung (Half-Duplex) zwischen den Kommunikationspartnern. NFC operiert auf einer Frequenz von 13,56MHz, der global verfügbar ist und keiner speziellen Regulierung unterliegt. Die laut dem Standard vorgegeben Übertragungsraten sind dabei 106kbit/s, 212 kbit/s oder 424 kbit/s auf einer maximalen Distanz von 10-20cm je nach eingesetzter Hardware. Eine weitere NFC spezifische Eigenschaft ist es, eine Überprüfung durchzuführen, ob kein anderes

[10] Abkürzung für Operating System

[11] Radio Frequency Identification

[12] Ist eine physische und logische Trennung von Kommunikationspartnern, die aber miteinander kommunizieren können. Man betrachtet diesen „Luftspalt“ in der Informatik als starke Barriere, die mögliche Angriffsflächen verhindern soll.

NFC-Gerät eine aktive Übertragung hat. Man spricht hier in der Fachliteratur von „listen-before-talk“-Protokollen, jedoch ist dies aufgrund der kurzen kontaktlosen Übertragungswege eine eher nebensächliche Funktion. [11, pp. 1 - 2]

NFC - technologische Gerätetypen

Aktiver NFC-Modus

Im aktiven NFC-Modus strahlen beide Kommunikationspartner ein Radiofrequenzfeld aus, überlappt sich deren Bereich, kann ein Kommunikationskanal hergestellt werden. Beispielsweise ist das der Fall, wenn zwei Smartphones einen Datenaustausch vornehmen. Dieser Modus ist nicht gedacht, um eine hohe Datenrate zu bieten und hunderte von Megabytes auszutauschen, sondern um eine kurze oder mittelfristige Kommunikation zu ermöglichen. [12]

Passiver NFC-Modus

Im passiven NFC-Modus wird nur vom Initiatorgerät ein Radiofrequenzfeld aufgebaut. Dieses Feld versorgt die passive NFC-Schaltung mit Strom und einem Kommunikationsweg. Der passive Token bricht bei Verbindungsverlust sofort jegliche Operationen ab. Jener ist für die Durchführung seiner Tätigkeit vollständig von der Energieversorgung und dem Datenfeld des aktiven Gerätes abhängig. [12]

NFC Operationsmodus

NFC-Geräte können laut der Spezifikation[13] in drei verschiedenen Modi betrieben werden. Je nach angewendetem Modus kann das NFC-Gerät nur mehr spezifische Aufgaben erfüllen und ist für andere Operationen nicht mehr zugänglich. Abhängig vom vorliegenden Gerät ist ein Wechsel der Betriebsarten aber jederzeit möglich. In anderen Fällen ist das NFC-Gerät auf spezifische Aufgaben zugeschnitten und es steht nur ein Betriebsmodus bereit. Die zur Verfügung stehenden Betriebsmodi gliedern sich wie folgt. [12]

- Der **Schreib- /Lesemodus** ist ein Operationsmodus, zum Übertragen von Daten.
    - Aktiver **Lesemodus**, das NFC-Gerät agiert wie ein klassisches NFC-Lesegerät. Es können passiv betriebene NFC-Tags aus den unterschiedlichsten Anwendung gelesen werden. Im Falle von zwei erkannten NFC-Tags, wählt der „Anti-Kollisions-Algorithmus“ die passende Verbindung. Basierend auf dem ISO Standard (ISO/IEC 14443) muss im aktiven Lesemodus das Lesegerät erkennen, um welchen NFC-Tag-Typen es sich handelt, um im späteren Verlauf mit diesem zu kommunizieren.
    - Aktiver **Schreibmodus**, um nun einen NFC-Tag mit dem gewünschten Inhalt zu befüllen, muss das NFC-Gerät in den Schreibmodus versetzt werden. Dies kann über eine Softwarelösung geschehen, wie z.B. das Wechseln einer Einstellung in einer App, oder aber manuelles Aktiveren mittels eines Hardwareschalters.
- Der **NFC-Karten-Emulationsmodus** ermöglicht es einem NFC fähigem Gerät, eine unverschlüsselte NFC-Smartkarte zu simulieren. Dabei wird die zu simulierende Karte zuerst einmal auf dem Gerät initialisiert. Danach verhält sich das NFC-Gerät bei Bedarf wie die Smartkarte und bietet im Anschluss dieselben Funktionen.
- Der **Peer-to-Peer-Modus** unter NFC bietet Möglichkeiten abseits des Zahlungsverkehrs. Mit ihm lassen sich zwei oder mehrere NFC fähige Geräte auf „Link-Level“ miteinander verbinden. Über diesen Modus können Netzwerke geschaffen und Informationen ausgetauscht werden. Es gibt jedoch eine Einschränkung, diese Funktionalität wird nicht von der kontaktlosen Kommunikations-API[14] unterstützt. [12]

[13] In der ISO/IEC 18092 NFC IP-1, JIS X 6319-4 und ISO/IEC 14443 contactless smart card standards
[14] Allgemeine Abkürzung für eine Programmierschnittstelle

Mögliche NFC Konstellationen

Geräte X Modus	Gerät Y Modus	Beschreibung des NFC-Feldes
Aktiv	Aktiv	Im aktiven Modus sendet das NFC-Gerät ein Funkfeld aus, dass Informationen beinhaltet. Dabei senden beide Geräte X wie auch Y.
Aktiv	Passiv	Nur Gerät X sendet ein Funkfeld aus.
Passiv	Aktiv	Nur Gerät Y sendet ein Funkfeld aus.
Passiv	Passiv	Geräte X wie auch Y warten im passiven Modus auf ein Signal. Das damit verbundene Energiefeld und die Informationen bleiben aus.

Tabelle 3 NFC-Konstellationen nach [11, p. 1]

NFC-Software

Die Softwarelandschaft von NFC-Applikationen ist sehr umfangreich und findet in den unterschiedlichsten Bereichen Anwendung. Die Vielfalt und die sich ergebenden Szenarien sind daher schwer einzuschätzen. NFC an sich bietet nur das Interface, über das die Software schlussendlich eine Kommunikation anstößt und nachfolgend Daten austauscht. Es existieren jedoch einige „klassische Szenarien“, um die Einsatzmöglichkeiten dieser Technologie aufzuzeigen. [11, p. 3]

Kontaktlose Token Applikationen

In dieser Kategorie finden sich alle Systeme, die ein Token-Management als Ziel haben und beinhaltet hauptsächlich Applikationen, die eine Kommunikation mit einem passiven Token anstreben. Dieser nimmt dabei sehr variable Formen an, je nach Benützung ist es eine Schaltung beispielsweise auf kleinsten Raum oder auf Langlebigkeit optimiert, um nur ein paar Möglichkeiten aufzuzeigen. Die wohl verbreitetsten Formen sind Smartcards, NFC-Sticker oder aber auch Schlüsselanhänger. Der dabei eingesetzte NFC-Token kann aufgrund seiner variablen Bauform leicht in Geräte integriert werden. Jene Eigenschaft bietet wiederum einfache Möglichkeiten zum Nachrüsten, ohne die vorhandene Schaltung zu modifizieren. Die einzige Kommunikations-art, die diese NFC-Token beherrschen, ist über das kontaktlose Interface. Sollte es beschädigt oder korrumpiert sein, ist das Kommunizieren nur mehr sehr eingeschränkt bzw. gar nicht mehr möglich. Da der passive Token nur über sehr begrenzte Ressourcen verfügt, ist die Auswahl der zu verwendenden Protokolle ebenfalls sehr begrenzt. Der Haupteinsatzzweck jenes Token besteht darin, Daten zu speichern und bei Kontakt mit einem aktiven NFC-Gerät diese Daten zur Verfügung zu stellen. [11, p. 3]

Beispiele im Alltag

- Den Hyperlink zu einer Website speichern, der nach dem Kontakt mit dem passiven NFC-Tag aufgerufen wird.
- Ablegen von Zahlungsinformationen
- Das Speichern von GPS-Daten[15], um einen spezifischen Standort zu finden.
- Das Verwalten von WLAN[16] Zugangsdaten. [11, p. 3]

[15] Beschreibt das **G**lobale **P**ositionsbestimmungs**s**ystem.
[16] Beschreibt eine standardisierte drahtlose Übertagungstechnologie.

Gerätekopplung

Eine andere Möglichkeit für den Gebrauch von NFC-Tags ist die Gerätekopplung, dabei werden die zu koppelnden Geräte mittels der NFC-Schnittstelle zu einem Verbindungsaufbau angestoßen. Die NFC-Schnittstelle dient dabei nicht als Übertragungsschnittstelle, sondern nur als Initiator. Ein Beispiel dafür wäre die Verbindung zwischen einem Smartphone und einem Autoradio. Ziel der Kopplung ist die Freisprecheinrichtung des Autos zu nutzen. Bei diesem Beispiel wird dem Smartphone per passivem NFC-Token mitgeteilt, sich über die Bluetooth-Schnittstelle mit dem Autoradio zu verbinden, wo auch der eigentliche Datenaustausch erfolgt. Der NFC-Token fungiert als Initiator, um dem Smartphone mitzuteilen, die Bluetooth-Schnittstelle zu aktivieren und eine Kopplung mit dem Radio anzustoßen. [11, p. 4]

Ticket und Micropayment

In Hinblick auf mobile Zahlungssysteme ist dieser Bereich im Zusammenhang mit kontaktlosem Zahlungsverkehr besonders interessant. Hier wird das NFC-Interface genutzt um einen Zahlungsverkehr durchzuführen. Es ist daher nötig, die im NFC-Chip gespeicherten Daten in einem sicheren physischen Gerät unterzubringen. Dafür eignen sich die verschiedensten Formen, die von Smart-Cards bis hin zu Sim-Cards reichen, oder aber direkt intern auf dem Smartphone integriert sind.

Sollte sich nun der Kunde/die Kundin für eine Zahlung oder das Benutzen des Tickets entscheiden, startet er seine Transaktion in dem er den NFC-Chip aktiv in die Reichweite des NFC-Lesegerätes bringt. Dieses kann dann mit Hilfe der dahinterliegenden Applikation eine Gültigkeitsüberprüfung starten und das Einlösen oder die Zahlung durchführen.

In vielen Smart-Card-Szenarien ist es oft der Fall, dass eine einfache Leseoperation nicht ausreicht. Da der Endkunde/die Endkundin wieder Guthaben auf seine Karte aufladen will, sollten keine Einweg-Zahlungssysteme designt werden. Der NFC-Chip hat in den meisten Fällen nur die Ressourcen, um einfache Operationen durchzuführen, deswegen wird das eigentliche Verschlüsseln der Daten meistens von einer anderen Plattform[17] vorgenommen. Die verschlüsselten Informationen werden nun wieder auf dem NFC-Chip abgelegt, um sie beim nächsten Einsatz an einem gültigem Terminal wieder verwenden zu können. [11, p. 3]

NFC und Biohacking

Mit der vielseitigen Anwendung von NFC und deren Tokensystemen hat sich eine neue Technologiesparte etabliert. „Bio-Hacking“ ermöglicht mittels derzeit noch kleinen, aber zukunftsträchtigen technischen Errungenschaften, eine einfachere Interaktion zwischen automatisierten Systemen zu schaffen.

Das Implantieren von RFID-Chips wird schon in vielen Bereichen eingesetzt, angefangen von medizinischen Anwendungen bis hin zu Firmen, die dies ihren Mitarbeiter/inne/n anbieten. Folglich eignen sich jene Implantate auch für den Zahlungsverkehr. Zukünftig könnten sich Standards dafür entwickeln, die breite Interaktions-möglichkeiten bieten, wie Identifikation, Zugangsberechtigungen, Interaktion mit anderen digitalen Systemen und auch den Zahlungsverkehr ergänzen. Zusammenfassend ist zu sagen, dass es sich bei diesem Thema nicht nur um Fälle im Bereich des mobilen Geldtransfers handelt, sondern um weitaus umfangreichere Einsatz-möglichkeiten. Um derartige dynamische Technologien einzuführen, müssen erst gesellschaftliche Akzeptanz geschaffen und die möglichen Applikationen entwickelt werden.

Die Community der „Do-It-Your-Self“-Biohacker/innen wächst aufgrund des schnellen technologischen Fortschrittes und legt vielleicht die Grundsteine dieser Entwicklung. [13]

[17] Z.B. einer Cloud Applikation, der Smartphone CPU, an einem Zahlterminal oder Anderen.

NFC - Angriffsvektoren

Drahtlose Übertragungstechnologien bieten dem/der Nutzer/in ein hohes Maß an Flexibilität auf Kosten der Sicherheit. Da NFC nur für Übertragungen im kurzen Bereich eingesetzt wird, versucht man über die Funkfeldgröße, Kryptographie, Tokensystem und zusätzlichen organisatorischen Maßnahmen eine Minimierung der Angriffsflächen zu erreichen.

Einer der größten Hauptunterschiede zu kabelgebunden Übertragungen ist der schwer zu kontrollierende tatsächliche Abstrahlungsbereich. Das heißt, ein/e Angreifer/in in der unmittelbaren Umgebung stellt immer eine große Gefahr dar. [14, pp. 2 - 3]

Lauschangriff

NFC ist eine auf Radiofrequenzen aufgebaute Funktechnologie, daher ist eine Lauschattacke, ein permanentes nicht zu unterschätzendes Risiko. Das Belauschen durch einen Dritten ist mit Hilfe einer dementsprechenden Antenne ohne weiteres möglich. Das technische Hintergrundwissen und die nötige Literatur stellen für einen/eine Angreifer/in keine Herausforderung dar, da diese Standards frei eingesehen werden können. Die benötigte Hardware ist ebenfalls in der Kategorie handelsübliche Elektronik einzuordnen.

Dadurch dass die von Standards definierten Übertragungsstrecken auf sehr kurze Distanzen optimiert sind, ergibt sich nur ein sehr kleiner Operationsradius für einen Lauschangriff. Man spricht im Zahlungsverkehr von üblichen Distanzen bis zu maximal 10cm. Eine wichtige Unbekannte ist dabei, wie nahe sich ein/e Angreifer/in unbemerkt an das Frequenzfeld nähern kann, um seinen Übergriff durchzuführen. Dabei spielen aber noch andere Schlüsselfaktoren eine Rolle, einige davon sind:

- Funkfeld-Charakteristiken des Sendegerätes wie Antennenausrichtung und die Abschirmung gegenüber anderen Frequenzen
- Antenne des Angreifers und dessen Antennenausrichtung, Sende- und Empfangsleistung, wie auch Portabilität
- Qualität des Empfängers auf Angreiferseite
- Qualität des Funkfeld-Encoders
- Raum und Umgebungscharakteristiken
- Leistung des Sendegerätes wie Strom- und Sendeleistung
- Etc.

Die Liste der Faktoren ist bei weitem nicht vollständig angeführt, zeigt aber schon, dass das physische Umfeld einen sehr hohen Individualitätsfaktor hat. Aus diesem Grund ist es schwer, allgemeingültige Sicherheits-richtlinien dafür zu schaffen.

Außerdem sind noch andere Parameter ausschlaggebend und zwar in welchem Modus sich das Gerät befindet, ob das Gerät ein aktives Frequenzfeld erzeugt oder es ein passiver NFC-Chip ist. Bei beiden Modi müssen unterschiedliche Verfahren angewendet werden, um den Datenverkehr zu belauschen. [11, pp. 4 - 5]

Distanzverhältnis für einen möglichen Aktive- und Passive-Mode-Angriff

Modus	Mögliche Abhördistanz
Aktive NFC- Datenübertragung	~10m, stark abhängig von den oben genannten Faktoren
Passive NFC-Datenübertragung	~1m

Tabelle 4 Distanzverhältnis nach [11, p. 5]

Jene Verhältnisse stellen keine endgültigen Entfernungen dar, sollen aber einen Überblick über mögliche Angriffsdistanzen geben. Je nachdem, welche Betriebsumgebungen zum Einsatz kommen, können diese Entfernungen stark variieren. [11, p. 5]

Praktisches Angriffspotential

Die technischen Konzepte hinter NFC erschweren mögliche Lauschattacken prinzipiell, hinzu kommen die kurzen Übertragungsdistanzen. Die Konstellation eines aktiv-/passiven Tokensystems bietet für einen Lauschangriff eine schwierige Ausgangslage. Dennoch ist das Angriffspotenzial vorhanden. [11, p. 7]

Daten korrumpieren

Ein mögliches Angriffsszenario auf Basis einer Serviceunterbrechung ist die Datenkorruption. Ziel dieses Übergriffs ist es, die Kommunikation zwischen Sender und Empfänger zu stören und somit eine Serviceunterbrechung hervorzurufen. Das gelingt z.B. indem der Kommunikationspartner mit valide aussehenden Signalen und Paketen attackiert wird. Das Empfangsterminal ist somit verwirrt und die gewünschte Serviceunterbrechung ist erreicht. Grundvoraussetzungen und technische Mittel für eine derartige Attacke sind als gering einzustufen. Je nach Reaktion des technischen Empfängers, könnte in weiterer Folge der Zahlungsdienst auf dem Terminal eingestellt werden, was eine Serviceunterbrechung gegenüber dem Endkunden zufolge hätte. [11, p. 5]

Praktisches Angriffspotential

Im NFC-Standard sind Möglichkeiten definiert, mit denen ein aktives NFC-Gerät während einer Datenübertragung den Übertragungskanal auf Störungen überprüfen kann. Sollte eine durch den/die Angreifer/in verursachte Störung entdeckt werden, wird die Übertragung abgebrochen. Der Angriff ist technisch nicht schwierig durchzuführen, hat jedoch keinen direkten monetären Nutzen für den/die Angreifer/in. [11, p. 7]

Daten modifizieren

Man spricht bei der Datenmodifikation von einem gezielten Manipulieren bestimmter Parameter oder dem Flippen von Bits. Im Falle einer Zahlung könnte das, das Ändern eines Vorzeichens oder eines Betrages sein. Das beschriebene Szenario ist grundsätzlich komplexer, als die einfache Datenkorruption. Die Angreifer/innen müssen hier die vielen Parameter nachstellen, wie z.B. die entsprechend richtigen Encodierungsalgorithmen, die richtige Signalstärke, das passende Datenformat, etc. Der Eindringling müsste zuerst Pakete erstellen, die ein gültiges Format aufweisen und die manipulierten Informationen zum richtigen Zeitpunkt aussenden. Infolge dessen müsste das Terminal jene manipulierten Daten akzeptieren und weiterverarbeiten. Dieser Anwendungsfall ist nur für bestimmte Bits unter speziellen Codierungsverfahren möglich, zugleich ist es unmöglich für den/die Angreifer/in alle Bits gleichzeitig zu manipulieren. [11, p. 5]

Praktisches Angriffspotential

Das praktische Angriffspotential für ein gezieltes Manipulieren einzelner Werte ist gering und nur unter speziellen Voraussetzungen im technischen Rahmen möglich. [11, p. 7]

Daten einschleusen

Das Einschleusen von Daten ist aufgrund der technischen Gegebenheiten von NFC nur möglich, wenn die Antwortzeiten des Senders sehr hoch sind. Die oben dargestellten Faktoren zur Erstellung eines gültigen Paketes müssen ebenfalls auf der Angreiferseite erfüllt sein. Sollte es dieser gelingen, schneller eine Antwort zu senden, als der eigentliche Sender, könnte das Terminal das gefälschte Paket für legitim halten und jenes weiterverarbeiten. Ist aber der Fall gegeben, dass Sender und Angreifer/in gleichzeitig übertragen bzw. antworten, so überlappen sich die Kanäle. Am Terminal selbst kommen dadurch nur mehr korrumpierte Daten zur Weiterverarbeitung an.

Um jedoch eine Sicherheit gegenüber dieser Art von Attacke zu gewährleisten, existiert die Möglichkeit einer verschlüsselten Datenübertragung, welche mittels eines „Secure-Channel“ erreicht wird. [11, p. 6]

Praktisches Angriffspotential

Folgende drei Angriffsszenarien existieren, die das Einschleusen von Daten begünstigen:

- Angriff auf die langsame Geräte-Kommunikation
- Datenkorrumption beim gleichzeitigen Senden der Information
- Angriff auf unverschlüsselte Übertragung

Die möglichen Gegenmaßnahmen für eine verschlüsselte Übertragung finden sich im Kapitel *Secure-Channel-Methode von NFC (S. 30)*.

Man-In-The-Middle-Attacke

Das Man-In-The-Middle Angriffsszenario, das schon länger aus der klassischen IT bekannt ist, beschränkt sich nicht nur auf den IT-Sektor, sondern stellt auch ein Sicherheitsrisiko für den NFC-Zahlungsverkehr dar. Dabei versucht der/die Angreifer/in sich in die „Mitte“ der Kommunikation zu setzen. Gelingt dies, glauben nun beide Partner des Zahlungsverkehres, dass sie mit dem legitimen Kommunikationspartner Daten austauschen. Der Angreifer in der Mitte hat die Möglichkeit, manipulierte Daten an beide Seiten weiterzugeben. Die eigentlichen Kommunikationspartner glauben jedoch, dass sie mit der legitimen Gegenstelle kommunizieren und tauschen dabei gültige Kommunikationsdaten aus, die den/die Angreifer/in in beide Richtungen legitimiert. Dieser Typ von Übergriff ermöglicht es, verschlüsselt übertragenen Inhalt zu Entschlüssen. Dabei können die Inhalte gelesen und manipuliert, in späterer Folge wieder in ein legitim aussehendes Format gebracht und anschließend verteilt werden. In einem NFC-Umfeld würde ein möglicher „**M**an-**i**n-**t**he-**M**iddle[18]“-Angriff wie folgt aussehen. [15, p. 9]

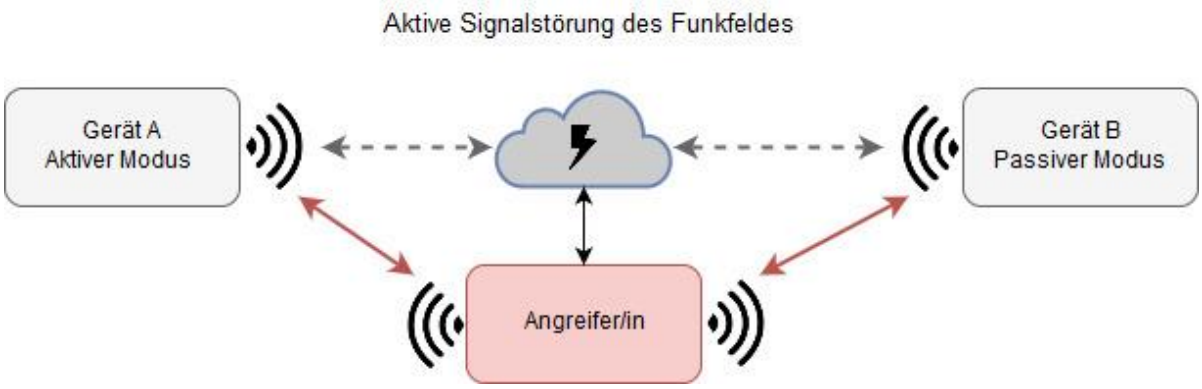

Abbildung 7 MitM-Angriff NFC nach [11, p. 6]

Ein Schutzmechanismus um zu verhindern, dass ein Signal manipuliert oder gestört wird, ist im NFC-Standard verankert. Jener Mechanismus kann aktiv eine Störung im Signal erkennen und den Schlüssel- bzw. Datenaustausch abbrechen. Diese Gegebenheit erschwert das Angriffsszenario einer MitM-Attacke erheblich. [11, pp. 6 - 7]

Praktisches Angriffspotential

Die Möglichkeit MitM-Angriffe auf NFC-Systemen durchzuführen besteht durchaus, ist jedoch nur unter gewissen Voraussetzungen und technischen Umsetzungen erfolgreich. Der Operationsradius ist dabei aber auf kurze Distanzen möglich, was einen erschwerenden Faktor darstellt. [11, p. 8]

[18] **M**an-**i**n-**t**he-**M**iddle wird auch mit dem Term **MitM** abgekürzt.

Secure-Channel-Methode von NFC

Die einzige Möglichkeit sich vor Attacken, wie dem „Mitlauschen“ oder anderen Modifikationen, zu schützen, ist eine verschlüsselte Übertragung der Kommunikationspartner. Dabei kommen klassische Verfahren aus der IT zum Einsatz, wie die Diffie-Helman-Verschlüsselung in Kombination mit elliptischen Kurven. Jene stellen eine asymmetrische Verschlüsslung dar. Das nun auf beiden Seiten erzeugte „Geheimnis“ wird verwendet, um einen symmetrischen kryptografischen Schlüssel mithilfe dem 3DES[19]- oder dem AES[20]-Verfahren auszutauschen. Dieser Schlüssel wird für den Aufbau eines sicheren Kanales benötigt. Das hat zur Folge, dass die Vertraulichkeit, Integrität und Authentizität der aufgebauten Verbindung gewährleistet werden kann. Außerdem ist noch zu erwähnen, dass die Möglichkeit besteht, andere Verschlüsselungsmethoden einzusetzen, jedoch sollte hier die geringe Rechenkapazität der meisten NFC-Geräte als zusätzlichen Entscheidungsfaktor herangezogen werden. [11, p. 8]

Bekannte NFC-Angriffsszenarien auf Basis von NFC

Aufgrund der vorliegenden Gegebenheiten der NFC-Technologie haben sich im Laufe des Gebrauchs einige praxisrelevante Angriffsmuster entwickelt. Besonders für Anbieter mobiler Zahlungsverkehrssysteme waren erfolgreich durchgeführte Attacken sehr interessant, um aus ihnen zusätzlich geeignete technische Barrieren abzuleiten oder andere aktive Gegenmaßnahmen zu entwickeln. [16, p. 2]

NFC-Relay-Attacke

Der Grundbaustein dieses Übergriffs bildet die Erhöhung der Reichweite einer NFC-Transaktion mittels eines oder mehreren Übertragungsgeräten. Die zum Einsatz kommende Funktechnologie[21] spielt dabei eine eher untergeordnete Rolle, solange sie schnell genug ist, die benötigten Daten in dem vorgesehen Zeitfenster zu übermitteln. [16, p. 2]

Technische Grundvoraussetzungen für derartige Attacken bilden ein:

- Kartenlesegerät (Zahlungsterminal)
- Karten-Emulationsgerät
- Schneller Kommunikationskanal zwischen diesen zwei Geräten

Angriffsablauf

Der/Die Angreifer/in stationiert sich mit seinem Übertragungsgerät (Mole oder Maulwurf genannt) in unmittelbarer Umgebung zum „Opfer“. Das bedeutet, dieser muss sich mit seinem „Mole-Geräte“ auf kürzeste Distanz an der auszulesenden Karte positionieren.

Zur gleichen Zeit startet der/die Angreifer/in selbst oder eine zweite involvierte Person eine Zahlungsabfrage auf den offiziellen Kauf-Terminal[22]. Die durch eine der beiden Parteien ausgelöste Zahlungsanfrage wird nun vom „Proxygerät“ an das „Mole-Gerät“ übertragen. Die Zahlungsanfrage selbst wird dabei nicht manipuliert oder abgeändert, somit beinhaltet sie ausschließlich legale Informationen und Zahlungsanweisungen. Das „Mole-Gerät“, das auf kurzer Distanz zur Smartcard platziert ist, überträgt nun alle legitimen Zahlungsaufforderungen an das NFC-Interface der Smartcard bei der Zielperson.

[19] Ist eine mehrfache Verschlüsselung auf Basis des Data Encryption Standard.

[20] Beschreibt den Advanced Encryption Standard, dieser ist der Nachfolger des Verschlüsselungsstandart DES.

[21] Weiterleitungen durch z.B. WLAN oder Bluetooth sind möglich, um hier nur ein paar technologische Vertreter zu nennen.

[22] Kann auch Point-Of-Sale-Terminal genannt werden.

Das NFC-Interface verarbeitet die Anfrage und leitet die bestätigte Zahlung über das „Mole-Gerät“ und das „Proxygerät“ zurück an das eigentliche Kaufterminal. Sollte das POS-Terminal keine technischen Gegenmaßnahmen zu dieser Angriffsklasse implementiert haben, wird die Zahlung akzeptiert. Damit ist der Übergriff erfolgreich durchgeführt. [16, p. 2]

Vergleich einer regulären Zahlung und einer Zahlung über ein mögliches Relay

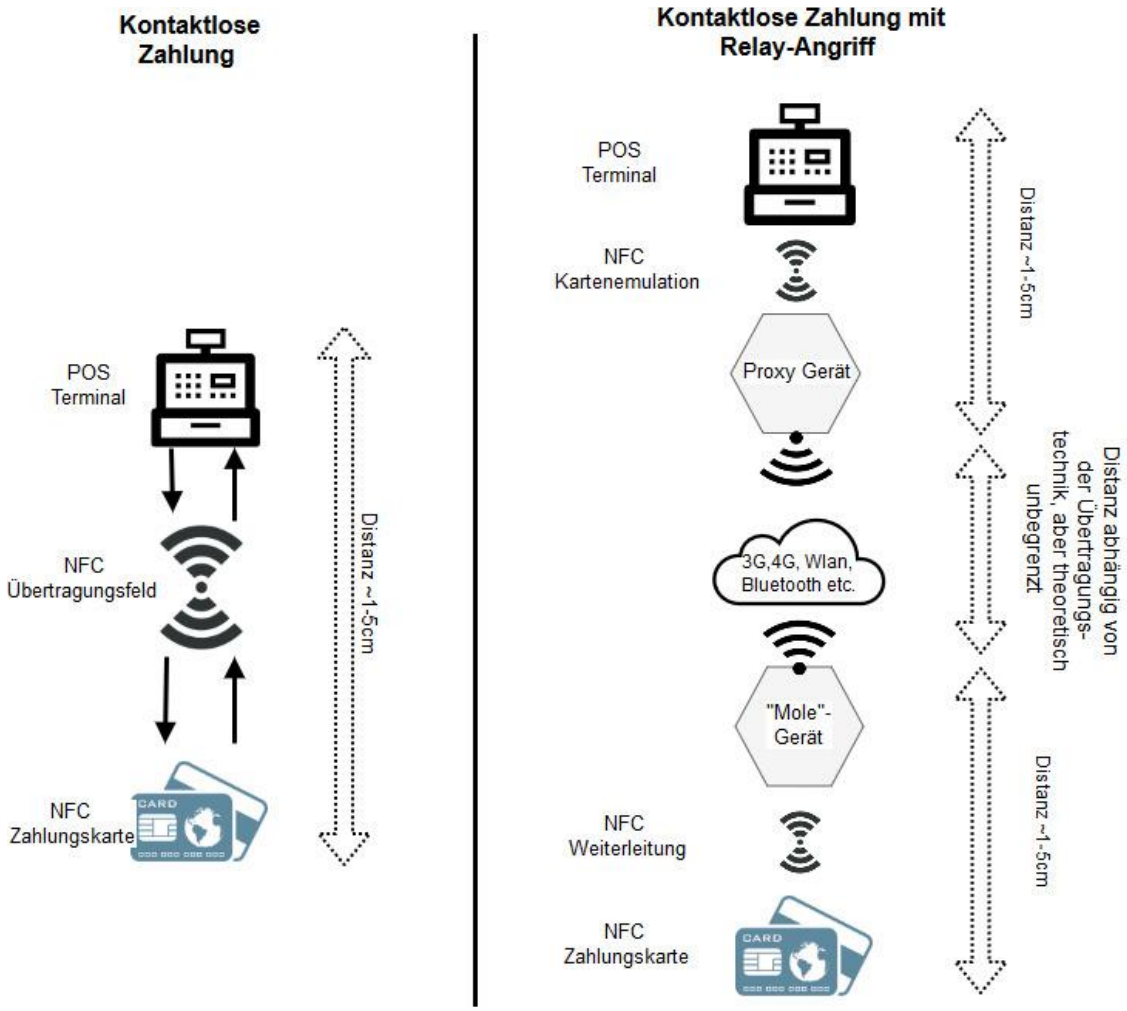

Abbildung 8 Relay-Zahlung nach [16, p. 2]

Relay-Angriffsanalyse

Eine Attacke auf Basis der Relay-Technik unterliegt dem simplen Prinzip der Reichweitenerhöhung, um sich einen Zugang zu einer Zahlung zu gewähren. Die dazu verwendeten Geräte (Proxy und Mole) stellen simple Übertragungsmechanismen zur Verfügung und sehen aus der Sicht der NFC-Schnittstelle (mobil, am Smartphone oder per eingebautem Chip auf der Bankkarte) legitim aus. Wie schon erwähnt, werden effektiv **keine** Daten manipuliert, sondern zwei oder mehrere, im Standard nicht vorgesehenen, dritte Geräte zu einer Reichweitenerhöhung missbraucht, um die kurze Übertragungstrecke auszuhebeln.

Das zusätzliche Hinzufügen von „Sicherheitsschichten“ auf Anwenderebene, wie zum Beispiel verschlüsselte Übertragung, bietet auf dieser Ebene keinen weiteren Schutz. [16, p. 2]

Schutzmaßnahem vor Relay-Attacken

Ein möglicher Angriff trifft auf alle Wireless-Technologien zu, da die Abstrahlung des Funkfeldes nur eine schwer zu steuernde Variable ist. Im Zusammenhang mit NFC und mobilen Zahlungen wurde versucht die maximale Reichweite bewusst klein zu halten, um Attacken dieser Art vorzubeugen bzw. zu erschweren.

Verteidigungsmechanismen vor derartigen Übergriffen sind hauptsächlich physischer Natur, um eine unbemerkte Zahlung über größere Distanz zu verhindern.

Mögliche Verteidigungsstrategien:

- Abschirmen der NFC-Schnittstelle mittels RF-Shield[23]
- Ein bewusster An- und Ausschaltmechanismus der NFC-Schnittstelle
  - Gesten wie z.B. das Umdrehen des Smartphones oder der Bankkarte
  - Ein- und Ausschalten per Hardware oder Software
- Erweiterung um einen zweiten Faktor
  - Biometrische Merkmale wie Fingerabdruck oder Gesichtserkennung
  - PIN oder Passwortabfrage
  - Zusätzliche Sensoren zur Aktivitätsabfrage, mehr dazu im Kapitel *Verteidigung von NFC-Relay-Attacken auf Basis von Ambientesensoren (S. 35)*.

Anmerkung: Ein Schutzmechanismus basierend auf der „reinen“ Transaktionslaufzeit hat sich in der Praxis nicht bewährt, dafür ist das alleinige Heranziehen der Zeitkomponente zu ungenau. [16, p. 3]

Weiterentwicklung der Relay-Attacke

Die Grundvoraussetzung für derartige Angriffe war die Herstellung einer physikalischen Übertragung. Dies musste in unmittelbarer Umgebung des Opfers geschehen, was für den/die Angreifer/in ein großes Risiko darstellt, erwischt zu werden. Die Erweiterung solcher Ansätze unterliegt einem rein softwarebasierten Angriffsvektor.

Anstelle einer physikalischen Übertragung oder deren Interface anzugreifen, wird versucht, einen softwarebasierten Relay am Endgerät zu erzeugen. Das Ziel ist dabei der Applikationsprozessor und dessen Interface. Die Infizierung eines Gerätes kann in Form einer schadhaften Anwendung oder Ähnlichem geschehen. Die Applikation wartet z.B. auf die Zahlungsaufforderung per mobiler Funkschnittstelle (3G, 4G Wifi-Direct oder Bluetooth etc.) und leitet diese softwaregesteuert an das Gerät weiter. [16, p. 3]

Grundvoraussetzung Beschreibung	Herrschaft
Karten-Emulationssoftware	Angreifer/in
Relay-Software auf dem Zielgerät mit den Kontoinformationen	Angreifer/in
Karten Emulations-Software	Angreifer/in
Zugang zu einem legitimen Zahlungsterminal (POS-Terminal)	Hersteller und Partner oder Angreifer/in
Mobiles Endgerät	Kundengerät
Geeignete Datenverbindung in ein öffentliches Netzwerk	Kundengerät

Tabelle 5 Voraussetzungen Software-Relay-Attacke nach [16, p. 3]

[23] Für die Abschirmung eignen sich die verschiedensten Materialen, abhängig von der verwendeten Frequenz reichen diese von Haushaltsutensilien wie Alufolie bis hin zu kommerziellen Schutzhüllen sehr weit.

In Abbildung 9 zeigt den Grundaufbau einer Software gesteuerten Relay-Attacke.

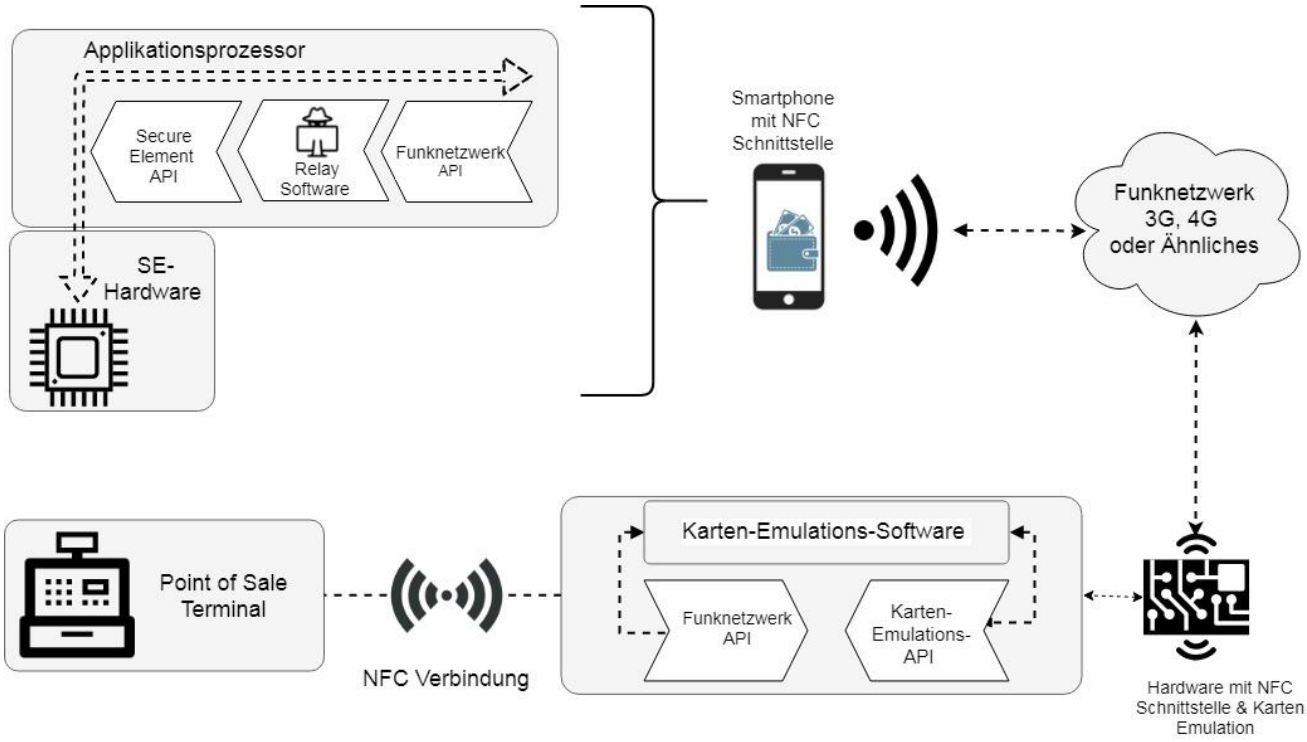

Abbildung 9 Aufbau Software-Relay-Angriff nach [16, p. 3]

Beschreibung einer Software-Relay-Attacke

Im ersten Schritt muss die schadhafte Relay-Software auf dem Smartphone installiert werden. Die Infektionsvektoren können dabei sehr vielfältig sein und erstrecken sich von Fake- oder manipulierten Apps bis hin zu nicht gepatchten Sicherheitslücken im Betriebssystem oder anderen Teilelementen der smarten Geräte. Unter der Annahme, dass ein Angreifer erfolgreich die Relay-Software am Zielgerät installiert, muss dieser außerdem die nötigen Berechtigungen besitzen, eine solche Zahlungsaufforderung an die zugehörigen Schnittstellen weiterzuleiten. Für den/die Angreifer/in gibt es mehrere Möglichkeiten sich die zuvor erwähnten Berechtigungen zu beschaffen, z.B. die App[24] sieht legitim aus und der/die Benutzer/in akzeptiert blindlings die vorgeschlagenen Berechtigungen bei der Installation[25]. Welche entweder während der App-Installation gewährt oder aber im Verlauf der Attacke, über eine zusätzliche Sicherheitslücke[26] im Betriebssystem, erschlichen werden. Diese Schritte passieren meist ohne weitere Auffälligkeiten in der Userumgebung. Ein Großteil der Vorbereitungen für den Angriff sind nun abgeschlossen und die schadhafte Applikation wartet auf Zahlungsanfragen über eine Datenschnittstelle wie 3G oder 4G. Wenn über die mobile Schnittstelle nun Zahlungsaufforderungen empfangen werden, folgt eine Übergabe an das Secure-Element, das die anschließenden Zahlungsanfragen durchführt. Das Secure-Element verarbeitet die Zahlungsanfrage und sendet die Transaktion wieder zurück. Der/die Angreifer/in befindet sich am POS-Terminal und legitimiert bzw. vollendet seine Zahlung mit den empfangenen Daten. [16, p. 3]

[24] Das Wort App beschreibt im allgemeinem ein Programm für ein mobiles Gerät.

[25] Ein exemplarischer Fall dafür wäre die „Taschenlampen-App“, die Zugriff auf das Kontaktbuch, oder gar Zugriff auf eine mögliche Zahlung verlangt.

[26] Privileg Eskalation, Buffer Overflow oder ähnliche bekannte Übergriffe kommen zur Anwendung.

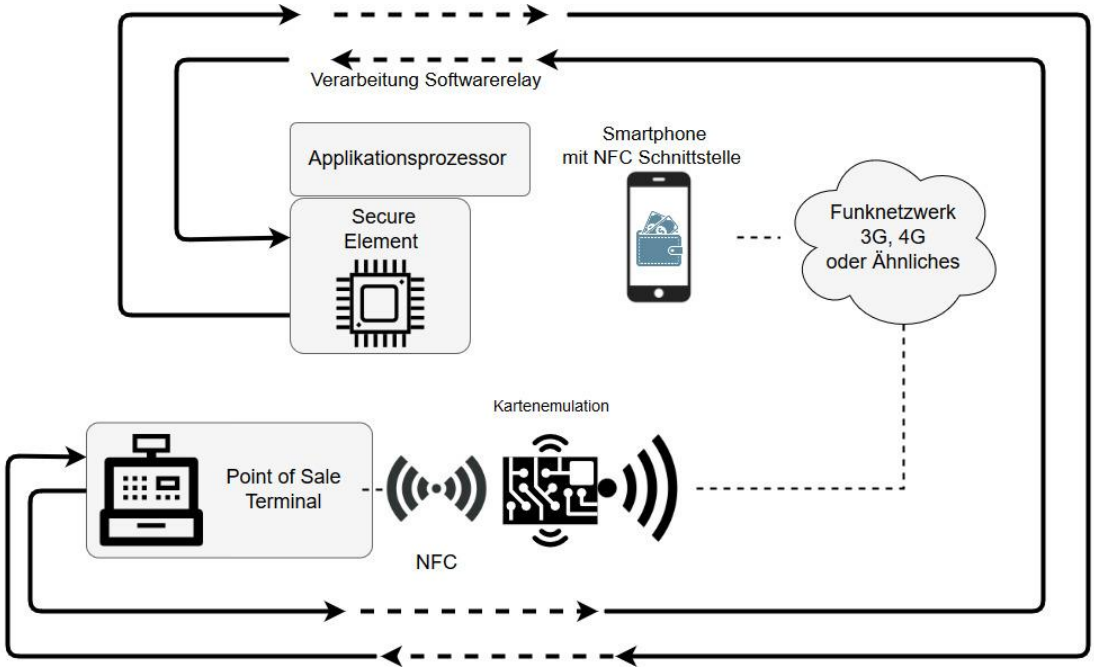

Abbildung 10 Geldfluss Relay-Attacke nach [16, p. 3]

Skalierung zu Software-Relay-Angriffen

Das Szenario einer Software-Relay-Attacke ist in seiner beschriebenen Form skalierungsfähig. Ein/e Angreifer/in der über einen Zugriff auf einen POS-Terminal verfügt, könnte selbst Nutzen aus den geringen Teilbeträgen ziehen. Die Zahlungsgrenze von beispielsweise 25€ wird dabei durch die Summe der Opfer ausgeglichen, um höhere Beträge zu erbeuten. Sollte man aus Angreifersicht für eine exemplarische Kalkulation von möglichen Gewinnen als Basis die Anzahl von veralteten Android-Geräten nehmen, ergeben sich erstaunlich hohe Benutzerzahlen und damit potentielle Opfer. [16, p. 3]

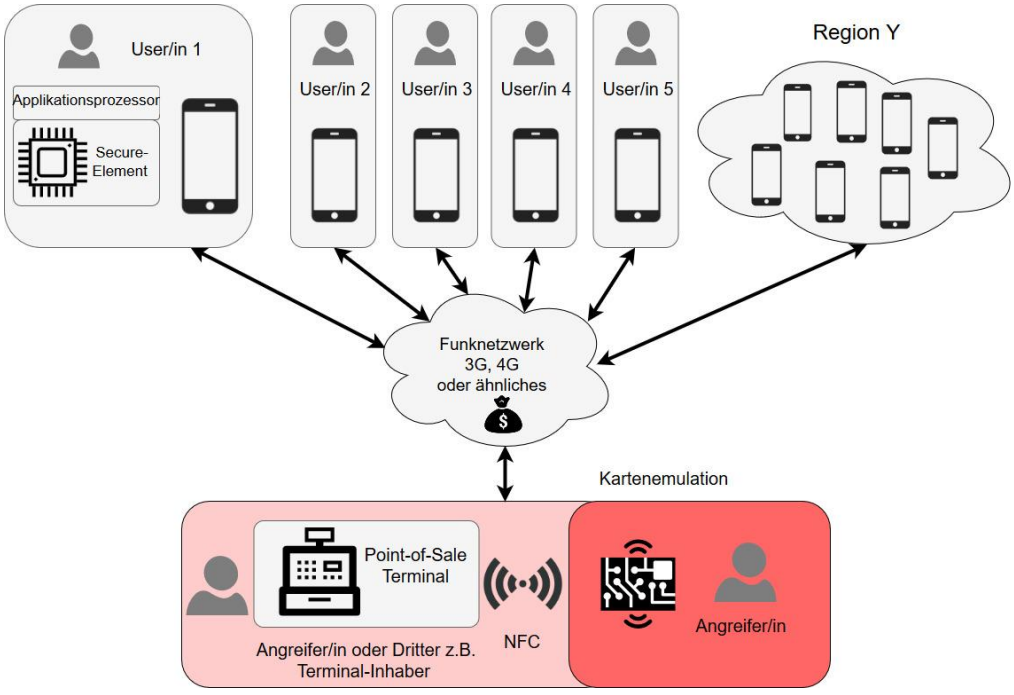

Abbildung 11 Skalierter Relay-Angriff nach [16, p. 3]

Verteidigung von NFC-Relay-Attacken auf Basis von Ambientesensoren

Wie im Kapitel *NFC-Relay-Attacke (S. 30)* kurz beschrieben, können auch Ambientesensoren benützt werden, um mögliche Übergriffe dieser Art zu verhindern. Dabei wird der zusätzliche Sensor dazu verwendet eine bewusste Tätigkeit oder Geste zu setzen, um die eigentliche NFC-Schnittstelle zu aktivieren. Ambientesensoren beschreiben unterschiedliche Typen von Inputsensoren, die gut messbare Umwelteinflüsse aufzeichnen und wiedergeben. Je nach Zahlungsgerät werden auf den Sensoren basierend verschiedene Bauformate eingesetzt und in das Gerät integriert. Eine wichtige Konstante bei der Wahl des Ambientesensors sollte beispielsweise die Umwelt sein. Je genauer die Faktoren der Umgebung eingegrenzt oder bestimmt werden können, desto effektiver lässt sich der geeignete Ambientesensor auswählen. Derartige Sicherheitsnetze könnte man auch weitläufig als zweiten Faktor für die Authentifikation bei der Zahlung bezeichnen. [17, pp. 1 - 2]

Aufstellung von möglichen praktisch messbaren Umwelteinflüssen für Sensoren

- Beschleunigungssensor
  - Linear
  - Rotation
- Anziehungskraft
- Licht
- Magnetfeld
- Temperatur
- GPS
- Bluetooth
- Wifi
- Luftfeuchtigkeit
- Luftdruck
- Netzwerkposition
- Geräuschkulisse
- Etc.

Die Liste stellt keine vollständige Abhandlung der möglichen messbaren Umwelteinflüsse dar, jedoch vermittelt diese eine Übersicht, welche physikalischen Messerwerte sich für die Absicherung einer Transaktion eignen könnten. [17, p. 8]

Ambientesensoren - Szenarien und der Bezug zu modernen Zahlungen mittels eines Smartphones.

Ein modernes Smartphone oder anderes smartes Gerät, das für den Zahlungsverkehr geeignet ist, hat üblicherweise eine Vielzahl an Sensoren, die Umwelteinflüsse oder bestimmte Gesten erkennen. Für die Verwendung solcher Sensoren bei einer Zahlung eignen sich grundsätzlich drei Szenarien, die modifiziert oder adaptiert werden können:

- Prüfung durch einen Backend
- andere einzigartige Überprüfung
- Zahlungsterminal leitet die Überprüfung weiter
- Lokale Überprüfung am Zahlungsterminal

Eine Detailbeschreibung der Anwendungsfälle finden Sie im nachfolgenden Kapitel *Überprüfung des Ambientes, der Umwelt (S. 36)*. [17, p. 3]

Beschreibung Verteidigungsstrategien auf Basis eines Ambientesensors

Der Grundbaustein der zuvor genannten Relay-Attacke ist die schlichte Ergänzung der Funkverbindung. Durch das Hinzukommen eines zusätzlichen Wertes, der die unmittelbare Umgebung wiederspiegelt, werden derartige Angriffe erschwert oder unterbunden. Der Zahlungsvorgang zwischen User und Terminal wird um eine Tätigkeit erweitert, bevor die eigentliche Transaktion durchgeführt wird.

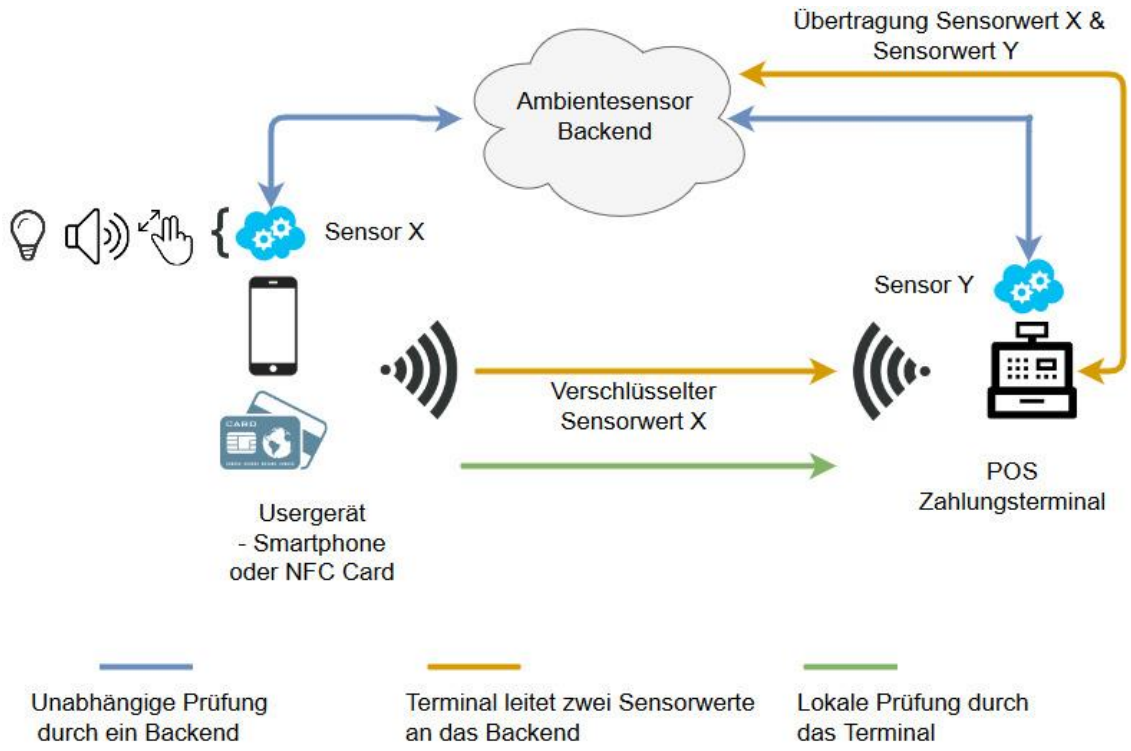

Abbildung 12 Zahlung NFC-Ambientesensor nach [17, p. 4]

Die an der Zahlung beteiligten Geräte definieren einen Zeitpunkt, an dem die „Umwelt“ gemessen wird. Sollte dieser Messwert auf beiden Seiten zum definierten Zeitraum gleich sein oder im Toleranzbereich liegen, kann die nachfolgende Transaktion durchgeführt werden. Außerdem können auch mehrere Messwerte (z.B. der Durchschnitt von 3-5 Messungen) oder gar die Kombination von mehreren Sensoren (z.B. Licht und Geräuschkulisse) zur Berechnung des Ambientewertes herangezogen werden. Dadurch sind solche Daten für den/der Angreifer/in zunehmend schwerer abzufangen, selbst zu erzeugen oder zu fälschen. Derartige Methoden sollen sichererstellen, dass sich der Zahlende und das Terminal auch wirklich in dem dafür vorgesehenen Umfeld befinden und sich kein Dritter durch eine einfache Datenweiterleitung Zugriff auf eine Zahlung verschafft.

Der Einsatz eines oder mehrerer Ambientesensoren ist auch auf Bankkarten möglich, jedoch müssen auf der Bankkarte zusätzliche Gegebenheiten beachtet werden, beispielsweise Sensortyp, Messgenauigkeit, Platzierung, Lebensdauer und Fehlertoleranz. Bankkarten haben im Vergleich zu Smartphones jeglicher Art eine sehr geringe Rechenkapazität, das Ergänzen von Sensoren ist komplex und muss vorher im Design der jeweiligen Infrastruktur berücksichtigt bzw. eingeplant werden. [17, pp. 3 - 4]

Überprüfung des Ambientes, der Umwelt

Die hier vorgestellten Konzepte, wie der Gebrauch eines Ambientesensors, kommen grundsätzlich aus der klassischen IT. Das eingesetzte Systemdesign muss in der Konzeptionsphase eines solchen Zahlungssystems möglichst genau definiert werden:

- 1. Prüfung durch einen Backend oder eine andere einzigartige Überprüfung
  - Smartphone und Terminal senden jeweils eine unabhängige Prüfungsanfrage an das Backend des Zahlungsproviders. Welcher nun die eingegangenen Ambientewerte überprüft und mit den definierten Werten aus der Designphase vergleicht. Ist die Übertragung auf beiden Seiten (mobiles Endgerät und POS-Terminal) abgeschlossen, trifft das Backend die Entscheidung, ob sich die Geräte in unmittelbarer Umgebung befinden und autorisiert die Transaktion in nachfolgenden Schritten.

- 2. Das Zahlungsterminal leitet die Überprüfung weiter
    - Das Smartphone sendet seinen Ambientewert über einen gesicherten Kanal an das Empfangsterminal. Welches nun seinen und den vom Smartphone empfangenen Umgebungswert an die Überprüfungsstelle sendet. Wie vorher schon beschrieben, trifft diese auf Basis der empfangenen Werte eine Entscheidung über die Gültigkeit der Zahlung und leitet die Antwort wieder an das POS-Terminal zurück.
- 3. Das Zahlungsterminal führt eine lokale Überprüfung durch
    - Der dritte Fall beschreibt eine lokale Überprüfung am Terminal selbst. Dabei überträgt das Smartphone den Umgebungssensorwert an das Zahlungsterminal. Welches nun eine lokale Überprüfung der Sensorwerte startet, über die Gültigkeit entscheidet und in weiterer Folge, wie die Zahlung durchgeführt wird.

Die drei oben vorgestellten Konzepte sind bei weitem nicht die einzig möglichen Systemarchitekturen. Sie zeigen aber, dass die Systemlandschaft von lokalen On-Side-Systemen[27] bis hin zu Cloud-Systemen sehr modular aufgestellt werden können. Außerdem sind diese Methoden für Ambientesensoren auch auf Bankkarten übertragbar und beschränken sich bei weitem nicht nur auf Smartphones.

Technisch existieren viele Möglichkeiten die Überprüfung eines oder mehrerer Ambientewerte auf dem Smartphone zu starten, um eine Zahlung zu verifizieren. Ob das Smartphone jedoch als geeignetes Gerät für den Geldtransfer eingestuft wird, ist eine reine Gestaltungsentscheidung des Zahlungssystemanbieters, da es bestimmte technische Voraussetzungen erfüllen muss. Ein anderer wichtiger Punkt ist, dass das Smartphone sich in der Hand des Users/der Userin befindet und somit von diesem/dieser selbst oder einem/einer Angreifer/in direkt manipuliert werden könnte. Das Smartphone an sich, hat eine große Angriffsfläche, vieles davon kommt aus der klassischen IT, einiges ist aber auch speziell aus dem mobilen Bereich. Solche Angriffsvektoren sind aus Sicht eines Zahlungssystemanbieters oft nur schwer unter Kontrolle zu bringen. [17, p. 4]

Digitale Identitäten

Das Werk Verkettung digitaler Identitäten des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein definiert digitale Identität[28] folgendermaßen:

> *(…)"Digitale Identitäten repräsentieren die Nutzer in der Informationsgesellschaft. Solche digitalen Identitäten bestehen aus technisch abgebildeten Attributen der Nutzer, den Identitätsdaten." [18, p. 22](…)*

[27] On-Side beschreibt, dass die Hardware bzw. das Service vom Hersteller intern betrieben und gemanagt wird.

[28] Der Begriff „Identitätsdaten" wird manchmal auf diejenigen personenbezogenen Daten beschränkt, anhand derer eine Person identifiziert werden kann und/oder für einen bestimmten Lebens- oder Sachbereich auf Eigenschaften dieser Person rückgeschlossen werden können.

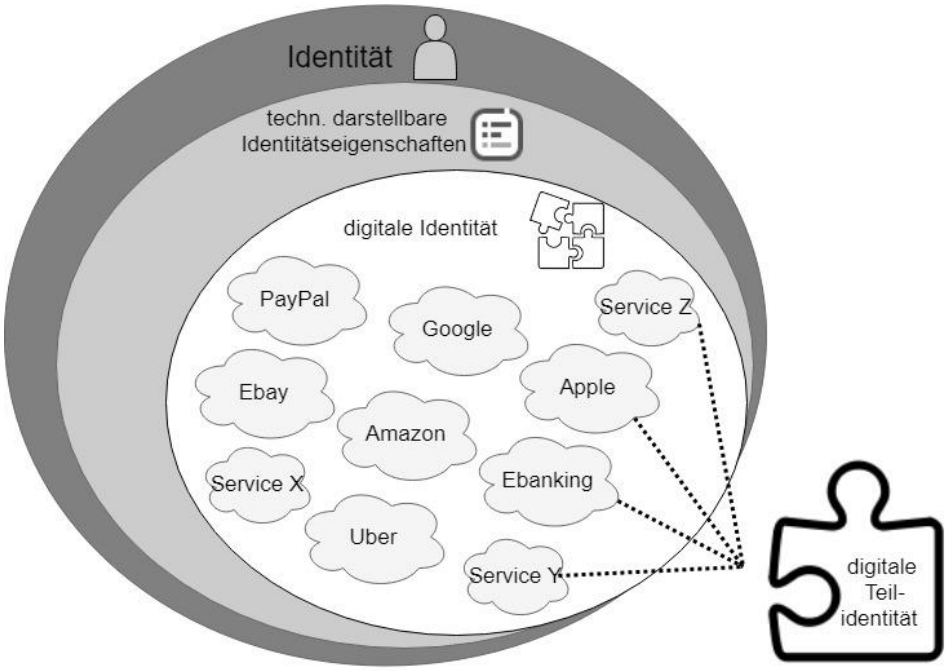

Abbildung 13 Teilidentität nach [18, p. 23]

Digitale Identitäten und ihr Gebrauch sind in unserem Zeitalter allgegenwärtig. Das Erstellen einer neuen Identität geschieht schon beim Anlegen eines Accounts für einen ausgewählten Dienst, unabhängig davon ob Zahlungsverkehr damit getätigt werden kann. Das Thema von Identitäten und deren Management beschäftigt uns schon seit den Anfängen des Internets, die gängigste Form dabei war bis ca. 2005 die Erstellung einer Userkennung und einem dazugehörigen Passwort. Viele digitale Systeme aus dieser Zeit sind darauf ausgelegt, einen singulären Identitätsnachweis zu erfüllen, nämlich ausschließlich im eigenen Ökosystem. Eine solche Umsetzung wird auch „Insel- oder Silo"-Lösung genannt. Derartiges lokales Identitätsmanagement erfüllt die modernen Anforderungen nicht mehr. Hier müssen wesentlich flexiblere und globalere Ansätze für den/die Endbenutzer/in geschaffen und angewendet werden. Eine Möglichkeit eines zentralen Identitätsmanagements kann zum Beispiel über die Regierung in Form eines eGovernment-Systems oder eines dritten globalen Identity-Providers etabliert werden.

Während der Erschaffung und der Weiterentwicklung bis hin zu unserem heute vorherrschenden Internet, war eine Identität technisch meist an einen physischen Endknoten, eine Maschine, gebunden. Mit diesem Konzept im Hintergrund war es nicht möglich oder vorgesehen eine einheitliche „Identitätsschicht" global zu etablieren, bei dem nicht Maschinen, sondern Menschen identifiziert werden konnten. [19, p. 3]

Jene konzeptionelle Gegebenheit brachte Serviceanbieter in den Zugzwang, sich selbst um das Identitätsmanagement zu kümmern. Dadurch ergaben sich die ersten Schritte in Richtung der heutigen Systeme mit User- und Passwort-Datenbanken, die sich bei den Serviceanbietern in Form von Daten-Silos zeigen. Die angelegten Identitäten existieren in den einzelnen Datensilos nur im Kontext der genutzten Services. Sollte der User/die Userin das gewünschte Service nicht mehr nutzten, ist diese Identität wertlos. Das Abhandenkommen oder der Verlust jener kann infolgedessen durch Missbrauch einen enormen Schaden verursachen. Erschwerend kommt hinzu, dass der praktische Umgang mit der Verwaltung von persönlichen User-IDs und Passwörtern bei einer Vielzahl an Endbenutzer/inne/n sehr fragwürdig ist und nicht die Aufmerksamkeit bekommt, die von Nöten wäre. Einige der alltäglichen Probleme von Endverbraucher/innen:

- Große Anzahl der zu verwaltenden Identitäten
- Geringe Passwortkomplexität
- Wiederverwendung der gleichen Passwörter
- Wenig Awareness

Die Auflistung ist unvollständig, soll aber einige bekannte Probleme auf Userseite aufzeigen. Die Lösungen zum Identitätsmanagements auf Benutzerseite lassen sich nicht allgemein beschreiben, da hier die Vorlieben und Gewohnheiten des Nutzers eine große Rolle spielen. Die derzeit vorhandenen Lösungen richten sich meist an spezifische Benutzergruppen mit unterschiedlichen Bedürfnissen. Einige komplett unterschiedliche technologische Beispiele sind:

- Gedächtnis
- Notizbuch
- Passwortmanager Lokal
- Passwortmanager Cloud
- andere Methoden zum sicheren Ablegen

Davon ausgehend, dass ein/e User/in, der im Internet aktiv ist, über mehrere oder sogar hunderte Identitäten bei verschiedenen Anbietern von Services hat, ist die sichere Verwaltung ein erheblicher Aufwand. [19, pp. 3 - 4]

Probleme mit digitalen Identitäten und mobilem Zahlungsverkehr

Die derzeitig bekannten Problemfälle in Bezug auf digitale Identitäten und einem mobilen Zahlungsverkehr sind zahlreich und können viele Ausprägungen haben. Um einen kleine Überblick zu schaffen in welche Richtungen sich solche Angriffsszenarien bewegen, werden folgende Fälle betrachtet.

- Missbräuchliche Benützung von Identitäten bei Zahlungen
- Verknüpfbarkeit von anderen Identitätsmerkmalen
- Diebstahl oder anderweitiger Missbrauch
- Wiederverwendung von schon vorhandenen Identitäten
- Identitätsverwaltung

Eine einzigartige Identität stellt den Grundbaustein für viele mobile Zahlungssysteme und die dahinterliegenden Businessprozesse dar. Unabhängig davon, ob mit der genannten Identität personenbezogene Daten verknüpft sind oder nur in einer anonymen Form zur Verfügung stehen. [20, pp. 9 - 16]

Der wirtschaftliche Schaden, der rein aus dem Diebstahl und anschließendem Handel von digitalen Identitäten entsteht, zeigt, dass sich daraus ein gewinnversprechender Schwarzmarkt entwickelt.

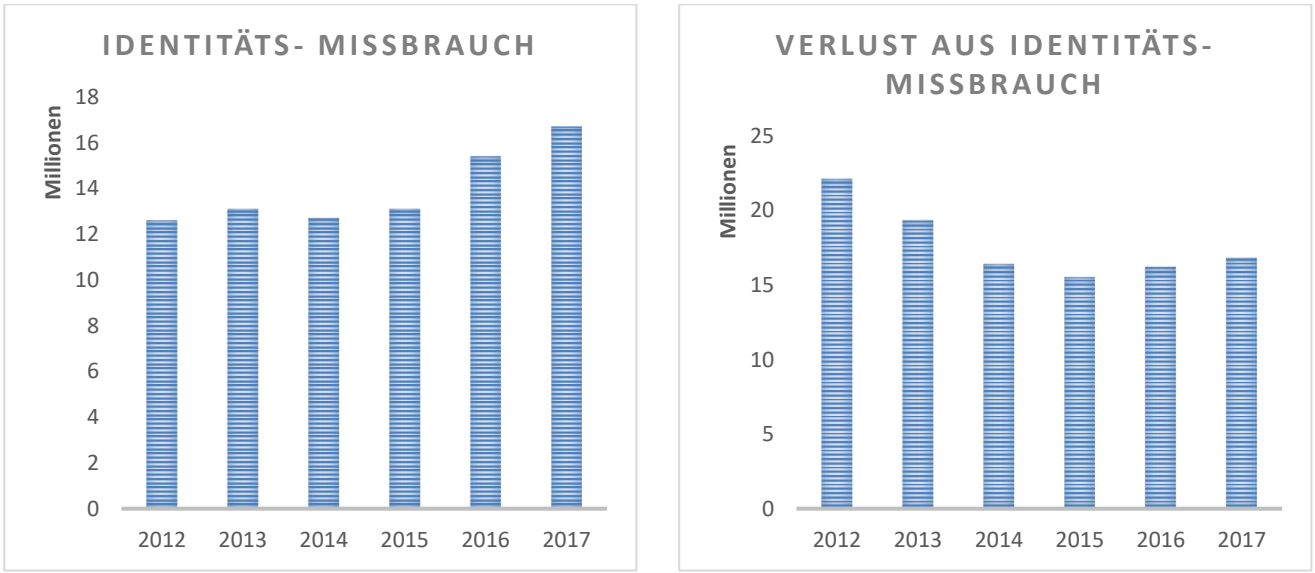

Abbildung 14 Identitätsmissbrauch nach [21]

Die Statistik zeigt, dass ein hohes Interesse an gestohlenen Identitäten besteht. Das Vorgehen der Kriminellen passt sich an das jeweilige Identitätsszenario an, beispielsweise:

- Kartenbetrug mit Hilfe von gestohlen Karteninformationen
- Mailboxübernahme für eMail basierte Zahlungen
- Internetkonten ausspionieren
- Bankinformationen abgreifen
- Vermittlungskonten übernehmen
- und vieles mehr

Durch die große Beliebtheit von Debit, Kredit und anderen ähnlichen Zahlungsmethoden verlagerte sich seit einigen Jahren die Art des Identitätsbetruges von den physischen Geschäften hin zur „digitalen" Handelswelt. Der Umfang an technologischen Möglichkeiten solche Zahlungssysteme abzusichern, hat sich stark weiterentwickelt, das resultiert in komplexeren Angriffsmustern auf Angreiferseite. Aber es erhöht auch den Arbeitsaufwand in Themenbereichen wie der Infrastruktur- und Applikationssicherheit, der sich wiederum auf die Initial- und Instandhaltungskosten auswirkt. [21]

Methoden zum Identitätsdiebstahl

In der Fachliteratur lassen sich einige Methoden von Angreifer/innen ableiten, mit denen jene zu einer gefälschten Identität kommen, beispielsweise:

- Physische Tätigkeiten
- Social Engineering
- Phishing
- Spyware, Viren und Trojaner
- Gezieltes Hacking
- (Web) Stalking
- Sorgloser Umgang durch den Endbenutzer
- Aneignung über das Dark-Web

Die Methoden für einen Identitätsdiebstahl sind vielfältig und technisch meist nicht sehr anspruchsvoll. Außerdem lassen sie sich, je nach vorherrschender Situation, auch leicht anpassen, um an das gewünschte Ziel einer falschen Identität zu kommen. [20, pp. 24 - 25]

Varianten von Identitätsdiebstahl

Die Art eines Identitätsdiebstahls lässt sich in zwei Arten gliedern. Das ist zum einen die Generierung eines neuen Accounts mit Hilfe von gestohlenen Teilidentitäten und stellt dann eine generische Identität dar. Je nach Service wird der Identitätsdatensatz auch einer einfachen Validierungsprüfung unterzogen. Und zum anderen besteht die Möglichkeit der Übernahme eines Accounts, beispielsweise durch die Veröffentlichung von geheimen User- und Passwortdaten.

	Fakten zum Angriff	Erkennung	Status
Generische Fake-Identität	Einsatz von (teilweise) echten Daten • Kontoeröffnung USA → Social-Security-Number • Kontoeröffnung AT → Name, Postanschrift & Lichtbildnachweiß Generische Daten für die Vervollständigung: • Beruf, Alter, Geschlecht etc. Generische Daten, um Glaubwürdigkeit zu erhöhen • Lebenslauf, Rechnungen, uvm.	• Daten sind nur teilweise valide. • Eigentlicher Identitätsinhaber bekommt den Missbrauch mit. • Bei manueller Kundenüberprüfung	Meist schwierig zu erkennen
Account-Übernahme	Übernahme einer gültigen digitalen Identität • Phishing oder persönlicher Kontakt, uvm. • Webbrowser Attacken wie Session-Riding, DNS-Manipulation etc… • Malwarebefall • Social-Engineering	• Der Betroffene bekommt Rechnungen oder ähnliche Zahlungsaufforderungen, die er nicht getätigt hat. • Zugriff auf die Identität erfolgt außerhalb der normalen Region des Kunden. • Sicherheitswarnungen des Serviceanbieters	Meist leicht zu erkennen

Tabelle 6 Varianten von Identitätsdiebstahl nach [20, pp. 26 - 30]

Smartphone Zahlungen und POS-Systeme

Die Grundvoraussetzung auf technischer Ebene für Zahlungen am Smartphone ist ein sicherer Umgang mit den von dem/der Benutzer/in bereitgestellten Zahlungsinformationen und einer sichereren Arbeitsumgebung. Die Techniken, die sich auf den Smartphones oder ähnlichen mobilen Geräten durchgesetzt haben, sind die Verwendung des Secure-Elements oder ein ausschließlich auf Software basierender Schutz wie z.B. HCE.

Die Zahlungsdaten und -informationen haben für den Kunden/die Kundin wie auch den Serviceanbieter einen sehr hohen Stellenwert und benötigen aufgrund dieser Umstände, einen besonders guten Schutzmechanismus gegen einen Diebstahl, Verlust oder sonstiges Abhandenkommen [22, p. 9].

Das Secure-Element

Das Secure-Element, oder auch SE abgekürzt, bietet einen abgeschotteten Bereich am Gerät, welcher in Form einer eigenständigen Hardwareschaltung implementiert ist. Die technische Umsetzung kann je nach eingesetztem SE auch unterschiedliche Vor- und Nachteile mit sich bringen, die im Gesamtkonzept zu berücksichtigen sind. Wie schon oberhalb dargestellt, kommt jenes in den unterschiedlichsten Ausprägungen, Bauformen und Situationen vor, jedoch verbindet sie ein gemeinsames Ergebnis. Ungeachtet wie das SE technisch aufgebaut ist hat es zwei wesentliche Hauptaufgaben:

- Einerseits die in ihm enthaltenen Elemente sicher und zuverlässig zu schützen.
- Andererseits die kryptographischen Rechenoperationen und Ableitungen z.B. für den Zahlungsvorgang oder die Tokenableitung zu betreiben.

Die SE-Funktionalität findet derzeit bei dem Zahlungsverkehr über ApplePay Anwendung. Das Google-Wallet bedient sich im Gegensatz dazu einer anderen Funktion, die im nachfolgenden Kapitel *Host-Card-Emulation oder HCE (S. 44)* angeführt ist. [22, pp. 9 - 10]

Implementierung einer SE-Schaltung

Je nach Umsetzung des Zahlungskonzeptes ist der Gebrauch der SE unterschiedlich. Jedoch zeigt das Gesamtbild, dass der Einsatzzweck für den Kunden/die Kundin immer derselbe ist, nämlich die Zahlung eines Service oder Gutes durchzuführen. Genauere Details zur Anwendung des SE in Apples Ökosystem sind im nachfolgenden Kapitel *ApplePay (S. 50)* aufgelistet.

Ein Kernbestandteil des Sicherheitskonzeptes des SE ist, dass jenes niemals direkt mit dem OS oder deren CPU kommuniziert. Diese Barriere ist sehr wichtig, um einen abgeschotteten Bereich auf dem mobilen Gerät zu schaffen. [22, pp. 9 - 10]

Generischer Ablauf einer NFC-Kommunikation mit dem SE

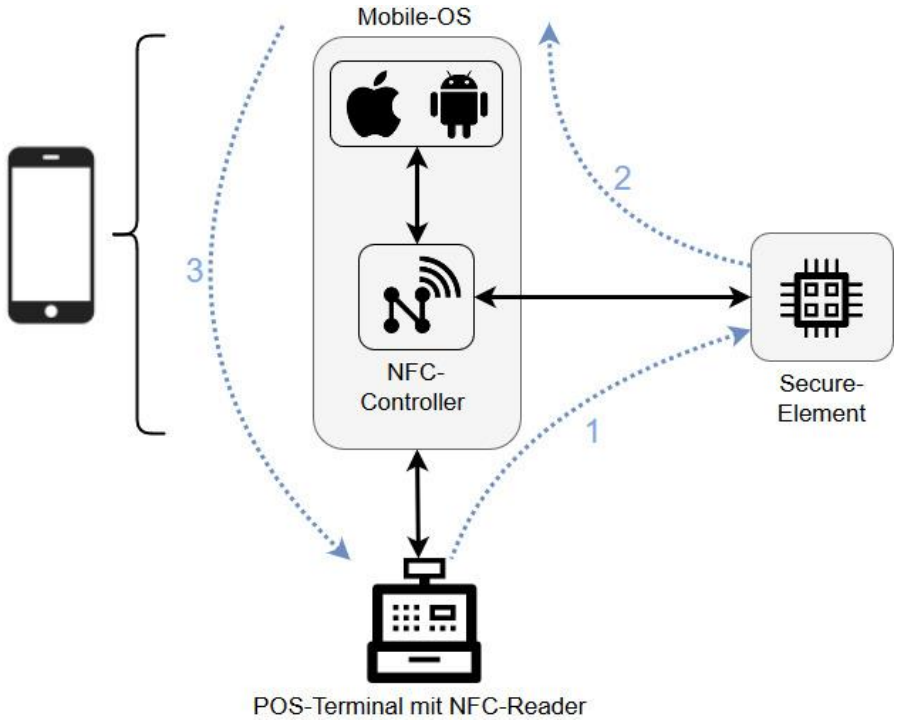

Abbildung 15 SE-Geldfluss nach [22, p. 9]

Beschreibung des Geldflusses:

- 1. Das NFC-POS-Terminal stellt die kontaktlose Verbindung mit dem NFC-Controller her und startet hiermit den Zahlungsvorgang. Der NFC-Controller überträgt die Anfrage an das SE.
- 2. Das SE verarbeitet die empfangene Anfrage und reicht jene zurück an den NFC-Controller. Der NFC-Controller leitet die Daten wiederum an das OS weiter, von welchem diese authentifiziert oder verifiziert werden.
- 3. Die verifizierten Daten werden wieder an den NFC-Controller zurückgegeben und nachfolgend an das Terminal übertragen.

In der letzten Phase einer Transaktion überträgt das NFC-Terminal die Anfragen je nach dahinterliegender Infrastruktur an das Zahlungsinstitut. [22, pp. 9 - 10]

SIM basiertes NFC

Nicht jedes Smart- oder Featurephone bietet von Haus aus eine NFC-Funktion bzw. eine eigenständige SE-Schaltung. Aus diesem Grund bieten manche Mobilfunkprovider eine SIM mit integrierter NFC-Funktionalität an. Die Sim arbeitet dabei als Secure-Element, auf der sich alle sensitiven Kontoinformationen des Inhabers/der Inhaberin befinden. Dabei wird auf das gleiche Konzept wie bei der herkömmlichen Kommunikation zurückgegriffen, die Kommunikation läuft ausschließlich über den NFC-Controller.

Überblick über österreichische Mobilfunkprovider und SIM mit NFC-Funktion:

Die drei am stärksten in Österreich vertretenen Provider bieten SIM-Karten mit NFC-Funktion wie folgt an:

Mobilfunkbetreiber	Status	Beschreibung
A1	verfügbar	Das Bankinstitut und A1 müssen sich über einen internen Prozess abstimmen und danach wird dem Kunden die SIM mit NFC-Funktion zur Verfügung gestellt.
DREI	verfügbar	Über eine Funktion namens „3Geldbörse“des Kundenportales auf seitens von DREI kann eine NFC-SIM-Karte beantragt werden.
T-Mobile	verfügbar	Die Bestellung der NFC-SIM läuft bankunabhängig, z.B. über das digitale Kundenportal oder bei einem direkten Kontakt.

Tabelle 7 NFC-SIM-Provider nach [23]

Die Verbreitung von NFC-SIM-Karten ist allerdings als gering einzuschätzen, da die NFC-Schnittstelle schon zur Standardausstattung eines modernen Smartphones gehört. Dieser Fakt macht das Nachrüsten einer NFC-Funktion, die nur für Zahlung zur Verfügung steht, teilweise obsolet. Jedoch existieren Anwendungsfälle, die technologische Begrenzungen oder andere Einschränkungen haben, bei denen auf derartige Lösungen zurückgegriffen wird. [22, pp. 10 - 11]

Technische Vor- und Nachteile der SIM mit integrierter NFC-Funktion

SIM mit NFC	Vorteil	Nachteil
	Universell mit Geräten verwendbar, die keine eigene NFC-Schnittstelle bieten.	Die Endkund/inn/en sind noch mehr in einem geschlossenen System gefangen und es ist aufwändig den Anbieter zu wechseln.
	Die SIM mit NFC kann leicht ausgetauscht bzw. in ein anderes Gerät transferiert werden.	Kann nicht mit Endgeräten benützt werden, die eine fest eingebaute SIM besitzen (CDMA[29] Telefone).

Tabelle 8 Vor- und Nachteile NFC-SIM-Karte [22, pp. 10 - 11]

[29] Die Abkürzung CDMA steht für Code-Division-Multiple-Access und bildet eine Multiplexing-Technik, die es ermöglicht über ein gemeinsam genutztes Frequenzspektrum mehrere Nutzerdatenströme zu übertragen.

Die geringe Verbreitung und die hohe Individualisierung, durch den Serviceanbieter und das Zahlungsinstitut, machen eine Attacke auf solche technologischen Umsetzungen, wie die NFC-SIM, zu einem weniger lukrativen und eher aufwendigen Ziel. [22, pp. 10 - 11]

Secure-Element in Form eines eigenständigen Chips

Im Falle von mobilen Zahlungssystemen wie bei ApplePay, kommt als SE ein eigenständiger Chip zum Einsatz. In Apples Ökosystem wird das SE auch „Secure-Enclave“ genannt. Dieser Chip bietet die Funktion des SE und verwaltet besonders sensible Inhalte, wie die für den Zahlungsverkehr, biometrische Informationen oder andere Geheimschlüssel. Die Integration des SE am Gerät besteht dabei schon ab dem Herstellungsprozess, daher ist das Hinzufügen über eine spezielle Erweiterung, wie die SIM-NFC-Lösung, nicht notwendig. Außerdem ist das SE ein fest verankerter Bestandteil der Geräteplatine mit unterschiedlichen Hardware-Schutzmechanismen versehen. Somit ist es nicht ohne weiteres möglich den sicheren Baustein einzeln zu entfernen oder auszulesen. Die Vor- und Nachteile, die sich aus diesem Gebrauch des SE ergeben sind nachfolgend angeführt. [22, p. 11]

Technische Vor- und Nachteile von SE-Elementen

Vorteil	Nachteil
Erhöhtes Sicherheitsniveau	Muss in der Produktion berücksichtigt werden, Hardware und Software
Kein Nachrüsten der SIM wird benötigt	Keine Übertragbarkeit der Informationen am SE
Keine Bindung an den mobilen Provider durch Zahlungsverkehr	Bewusstes Deaktivieren durch den Angreifer möglich → Austauschen sehr schwierig bis unmöglich

Tabelle 9 Vor und Nachteile von SE-Elementen nach [22, p. 11]

SD-Karten Secure-Element

Eine alternative Methode ist die Integration eines SE in einer externen Speicherkarte und hat eine unübersehbare Ähnlichkeit mit der Umsetzung der NFC-SIM-Karten. Statt der SIM-Karte wird das Speichermedium inklusive eines SE eingesetzt. Jenes Lösungskonzept entstand in den Anfangstagen der NFC-Technik und wurde als zukunftssichere Integrationsmethode propagiert. Damals wie auch heute konnten sich solche Techniken nicht am Massenmarkt etablieren und so verloren sie mit der Zeit zunehmend an Bedeutung. Für den privaten Kundenmarkt war diese Lösung ebenfalls nicht erhältlich, was zu ihrer Unbekanntheit beitrug. Außerdem verfügten einige mobile Geräte über keine SD-Karten-Erweiterungsschnittstelle, wodurch der Gebrauch nicht möglich war. Durch fortwährende Marktentwicklungen verlor diese Technik zusätzlich Unterstützer und wurde mit der Zeit zu einer Randerscheinung. [22, p. 12]

Host-Card-Emulation oder HCE

Die HCE, oder auch “Host-Card-Emulation” genannte Technik, stellt eine Implementierung dar, die einen auf Software basierenden Ansatz verfolgt. Somit gibt es keine Grundvoraussetzungen bzgl. zusätzlicher Hardware und der darin integrierten Elemente. Die benötigte Hardware zur Durchführung des Zahlungsverkehres befindet sich nämlich nicht am Gerät selbst, sondern liegt beim Bankanbieter, welcher sein Zahlungsservice „in-house“ betreiben oder aber auf moderne Hosting-Elemente, wie die Cloud, zurückgreifen kann. Literarisch bedingt wird diese Technik auch als “Cloudbased-SE“ beschrieben. Je nach Bankanbieter und deren Zahlungssystem sieht das dahinterliegende Back-End allerdings unterschiedlich aus. Die erste Unterstützung für HCE entwickelte die Firma Blackberry im Jahr 2012, die zu jenem Zeitpunkt noch einen erheblichen Marktanteil bei mobilen Geräten vorweisen konnte. Die Funktion für HCE wurde in späterer Folge, ebenfalls vom Android-Hersteller Google, auf

Android OS portiert. Die Integration für HCE bei Android fand ab der Version 4.4[30]statt. Seit ca. 2014 wird HCE als einzige Zahlungskarten-Emulation unter Android unterstützt, in seiner heutigen Form auch Google Pay[31] genannt und wurde über die Jahre stetig weiterentwickelt. Somit liefert Google für seine eigenen Plattformen ein vollständig auf Software basiertes Zahlungs-Ökosystem. Wodurch sich der Vorteil ergibt, dass für den Hersteller des mobilen Gerätes keine zusätzlichen Kosten anfallen bzw. keine ergänzend integrierte Hardware benötigt wird. Der Ressourcenaufwand bei einer Integration dieses Zahlungssystems ist somit geringer, als die einer Hardwarelösung. [22, p. 12]

Generischer Ablauf einer HCE-Kommunikation

Um eine direkte Kommunikation zu umgehen, wird bei HCE auf OS-Ebene auf sogenannte „Libraries und APIs“ gesetzt. Jene übernehmen die Kommunikation mit dem NFC-Controller, um die benötigten Informationen auszutauschen. Der angesprochene NFC-Controller übernimmt die Kommunikation mit dem NFC-Terminal (z.B. einem POS), um die Zahlung durchzuführen. [22, pp. 12 - 13]

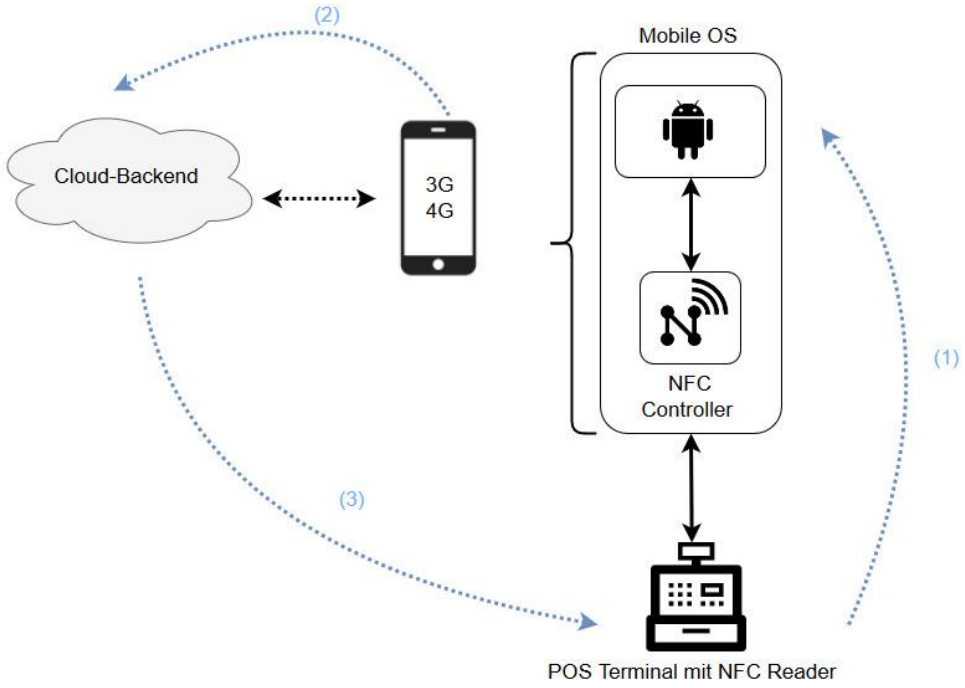

Abbildung 16 Cloud HCE-Geldfluss nach [22, p. 13]

Beschreibung des HCE-Geldflusses

- 1. Das NFC-POS-Terminal stellt die kontaktlose Verbindung mit dem NFC-Controller her und startet hiermit den Zahlungsvorgang. Der NFC-Controller leitet die Anfrage über die „Libraries und APIs“ an das OS weiter.
- 2. Das OS stellt die Verbindung mit dem Cloudbackend her und übergibt diesem die Zahlungsanfrage.
- 3. Im Cloudbackend wird die Anfrage verifiziert und mit den hinterlegten Zahlungsmitteln verknüpft. Ist jene erfolgreich, wird dem Client eine Bestätigung zurückgesendet.

[30] Android wurde ab der Version 4.4.X unter dem internen Code: “Kit Kat“ geführt.

[31] Das mobile Zahlungssystem von Google hat in seiner heute bekannten Form unterschiedliche Namen (Google Checkout, Google-Wallet und derzeit Google Pay) und Integrationen als Stand-A-Lone-App oder als integrierte Funktion in schon vorhandene Services wie Google Play.

Im letzten Schritt der Transaktion bekommt das POS-Terminal die bestätigte Begleichung, überprüft diese mit den vorgeschriebenen Parametern und akzeptiert die Zahlung. [22, pp. 12 - 13]

Technische Vor- und Nachteile von HCE

HCE Gegebenheiten	Vorteil	Nachteil
	Es muss keine SE-Hardware eingebaut werden.	Die OS-Sicherheit hat Einfluss auf die HCE.
	Smarte Geräte haben mehr Leistung und Speicher als ein SE.	Es sind nur Software-Abstraktionen möglich.
	Entwicklungs-, Betriebs-, und Wartungskosten sind geringer.	APIs können eine Angriffsfläche bieten.
	Service-Provider unabhängig	Allgemeine Software Exploits

Tabelle 10 Vor- und Nachteile HCE nach [22, p. 13]

Zusätzliche Aspekte eines cloudbasierten HCE

Die flexibelsten HCE-Ansätze werden auch „Full-Cloud-Based“-Ansätze genannt. Dabei wird versucht, so wenige sensitive Informationen wie möglich auf dem mobilen Gerät zu speichern. Vom Smartphone aus wird nur die Authentifikation gehandhabt und der eigentliche Zahlungsverkehr wird rein cloudbasiert gelöst.

Bei diesem technischen Aufbau ist die Verbindungs- und Backendsicherheit ein wesentlicher Bestandteil der Gesamtsicherheit. Ein sicheres Session-Handling und die geeignete Authentifikation der einzelnen Transaktionen ist eine Grundvoraussetzung. Weitere Aspekte der Clientsicherheit im Zahlungsverkehr finden sich im Kapitel *Mobilgeräte – mögliche Schnittstellen für mobile Angriffsszenarien (S. 58)*. Jedoch können nicht alle Elemente der Transaktion vom Zahlungsanbieter gesteuert werden, denn er hat keinen Einfluss auf das tatsächliche Endgerät, sein Datenvolumen und die Upload- und Download-Geschwindigkeit. [22, pp. 13 - 14]

Technische Vor- und Nachteile von HCE in der Cloud:

HCE in der Cloud	Vorteil	Nachteil
	Am mobilen Gerät selbst werden keine bzw. nur sehr wenige sensitive Informationen abgelegt.	Ein erfolgreicher Angriff auf das Cloudsystem (Backend) kann unvorhergesehene Folgen mit sich bringen.
	Flexibler Nutzen auf den unterschiedlichsten Endgeräten.	Es wird zwingend eine mobile Datenverbindung mit dem Cloud-Service benötigt.

Tabelle 11 Vor- und Nachteile HCE nach [22, pp. 13 - 14]

Tokenisierung

Basierend auf den bisher beschriebenen technologischen Umsetzungen von mobilen Zahlungssystemen wurden Tokensysteme eingeführt, um die Sicherheit zu erhöhen und die Menge an übertragenen Informationen zu minimieren. Dafür existieren auf dem Zahlungsmarkt etablierte Standards, wie PCI-Security-Standard-Council [32] und PCI-Data-Security-Standard[33], nach denen auch eine Zertifizierung möglich ist. Das Ziel ist, die Sicherheit von Zahlungssystemen weiter zu erhöhen. Auf Basis der vorgestellten Token-Technologie ist es dem/der Angreifer/in, selbst beim Mitschneiden einer dieser Token, unmöglich eine Attacke zu starten. [24, p. 4]

Wenn man ein solches Tokensystem betrachtet, müssen die nachfolgenden Faktoren in die Umsetzung miteinfließen:

- Technologien und Mechanismen, die die eigentlichen Kundendaten enthalten werden PAN[34]-Daten genannt.
- Wie die Transaktion durch das Zahlungssystem geleitet wird.
- Die Übertragung vom POS-System bis hin zum autorisierten Backend.
- Wie die übertragenen Token vom Backend verarbeitet werden.

Um einen tatsächlichen Angriffsvektor festzustellen, müssen bei einem Tokensystem alle Komponenten einzeln betrachtet werden. Es muss sichergestellt sein, dass jede einzelne Komponente den Grundprinzipien der Sicherheit entspricht. [24, p. 4]

Klassifizierung von Token basierten Systemen

Hier werden nachfolgend die Unterschiede von irreversiblen und reversiblen Tokensystemen gezeigt. Je nach Einsatzzweck existieren Vor- und Nachteile, die in der Designphase eines Geldsystems beachtet werden müssen. Die Gegebenheiten, die diese Designentscheidungen mit sich bringen, haben weitläufige Auswirkungen auf die Architektur des Zahlungssystems. [24, p. 7]

Irreversibles Tokensystem

Wie der Name schon anklingen lässt, handelt es sich hierbei um ein Konzept, bei dem es nicht vorgesehen bzw. möglich ist, für jegliche Teilnehmer/innen oder Angreifer/innen die PAN-Daten widerherzustellen. Die Token werden hierbei in authentifizierbar oder nicht authentifizierbar eingeteilt.

- Man spricht von einem **authentifizierten** irreversiblen Token, wenn es sich bei deren Erstellung, um eine mathematische Einweg-Funktion handelt, die sicherstellt, dass PAN-Daten verfügbar sind. Diese Art von Token kann unter **keinen** Umständen wieder zurück in die ursprünglichen PAN-Daten transformiert werden.
- Die zweite Form ist der **nicht authentifizierbare** irreversible Token, welcher nach der mathematischen Operation nicht mehr zu spezifischen PAN Daten zurückgeführt werden kann, aber im späteren Verlauf zu einem spezifischen Konto hinter der Transaktion verknüpft wird. [24, p. 7]

[32] PCI Security Standards Council abgekürzt **PCI SSC**

[33] PCI Data Security Standard abgekürzt **PCI DSS**

[34] Diese Technologie wird mit PAN abgekürzt und bezieht sich auf die „Primary-Account-Number“.

Reversible Tokensysteme

Bei einem reversiblen Tokensystem gibt es die Möglichkeit, den eigentlichen Token wieder in die ursprünglichen PAN-Daten zurück zu konvertieren. Bei dem Token-Zurückführungsprozess können diese zu einem einzigen oder aber mehreren Token einer PAN-Transaktion zurückgeführt werden. Wenn es technisch möglich ist, einen oder mehrere Tokendaten zurück zu transformieren, spricht man von einem reversiblen Tokensystem. Diese Definition trifft auch dann zu, wenn das System eigentlich keine Rückkonvertierung vorsieht. [24, pp. 7 - 8]

Um ein solches System abzusichern, können z.B. kryptographische Verfahren eingesetzt werden:

- **Rückführbare kryptographische** Token sind mittels Kryptografie verschlüsselte PAN-Daten. Bei der Übertragung des Token werden die eigentlichen PAN-Daten somit auf keinem Gerät gespeichert.
- **Nicht rückführbare kryptographische** Token haben keinen direkten mathematischen Hintergrund und werden nur in Form eines einfachen Vergleichs in einer Datentabelle benutzt. Die einzig schützenswerte Information für derartige Tokenverarbeitung, ist die eigentliche Beziehung zwischen den PAN-Daten und dem Token. [24, pp. 7 - 8]

Graphische Darstellung der Tokenkonzepte

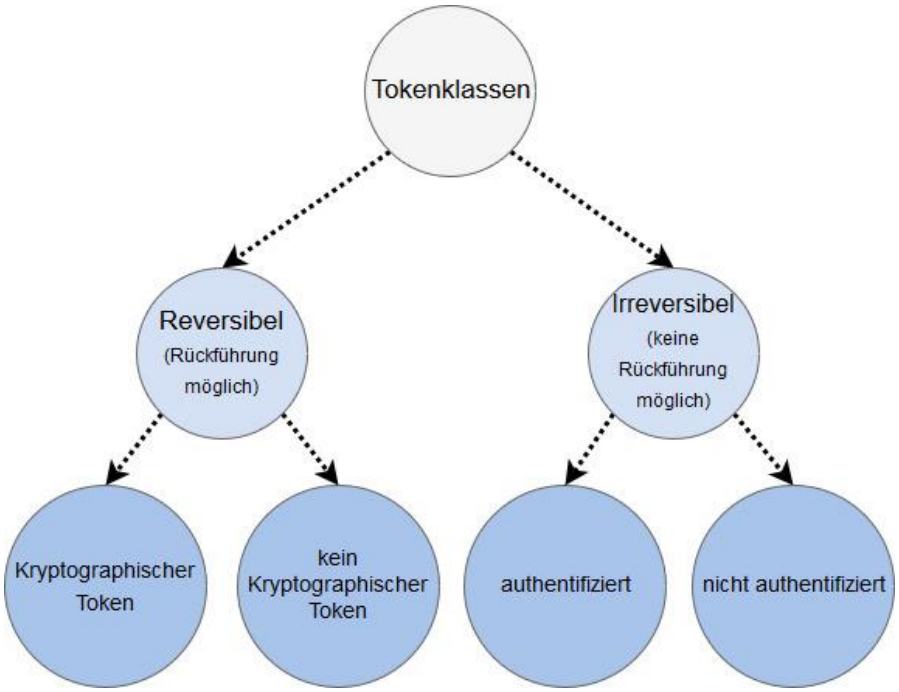

Abbildung 17 Tokensystem nach [24, p. 6]

Irreversible Tokenisierung - Fallbeispiel

In nachfolgendem generischen Fallbeispiel wird das Zahlungssystem mittels authentifizierbaren oder nicht authentifizierbaren Token betrieben.

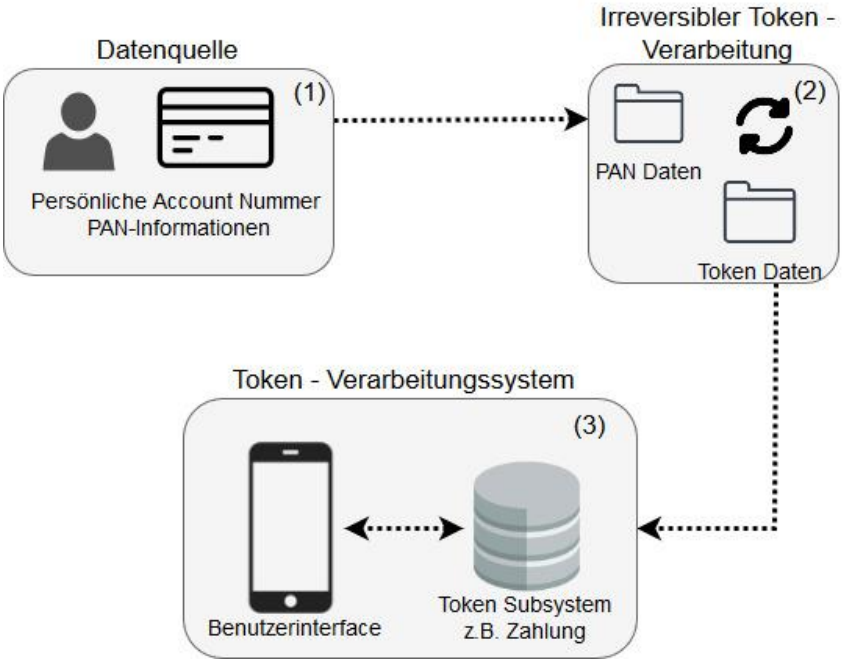

Abbildung 18 Irreversible Tokenisierung nach [24, p. 9]

- Im ersten Schritt werden die PAN-Source Daten an das Token-Generierungssystem transferiert. Dies sollte auf dem sichersten Weg mittels eines Secure-Channels geschehen, um ein mögliches Mitlauschen zu verhindern (1).
- In Schritt Nummer Zwei wird bei der Token-Verarbeitung ein entsprechender Token geformt. Dabei werden die eigentlichen PAN-Daten mittels eines mathematischen Verfahrens verschlüsselt und somit verbleiben keine ursprünglichen PAN-Daten am Gerät (2).
- Für den dritten und letzten Schritt wird der generierte Token an das Token-Verarbeitungssystem übertragen. Das Token-Subsystem, das auf den eigentlichen Businessprozess spezialisiert ist, beendet den Tokenprozess (3). [24, p. 9]

Irreversible Tokenisierung - Fallbeispiel an einem POS oder einem anderen Stand-A-Lone-Gerät

Am „Point-of-Sale“-Terminal wird der Token direkt am Gerät generiert und über das Verarbeitungssystem auf ein Smartphone übertragen. Als Übertragungsmedium findet hier beispielsweise die NFC-Schnittstelle Verwendung. Der übertragene Token kann nun auf dem Endgerät verarbeitet werden, um z.B. eine Zahlung durchzuführen [24, p. 10].

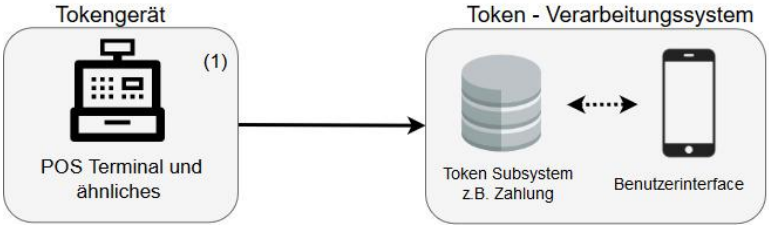

Abbildung 19 IR Token POS nach [24, p. 10]

Reversible Tokenisierung - Fallbeispiel

Die nachfolgende Abbildung 19Abbildung 20 ist die, eines generischen reversiblen Tokensystems. Die Datenquelle sendet über einen Secure-Channel die Informationen an das Token-Generierungssystem (1). Jenes wandelt die PAN-Daten mittels eines geeigneten kryptographischen Algorithmus um und speichert diese am Gerät (2). Nun beginnt ein Challenge-Respons-Verfahren über das Backend für die Überprüfung des Token (3). Je nach Aufbau des dahinterliegenden Businessprozesses kann der Token im Backend auch wieder zurück transformiert werden, um eine Zuordnung zu schaffen. [24, p. 11]

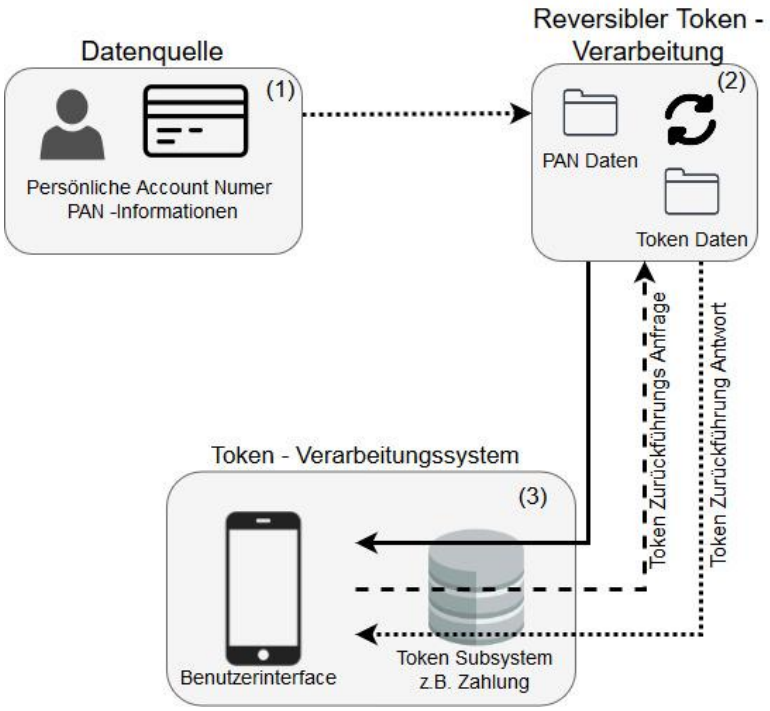

Abbildung 20 Reversible Token nach [24, p. 11]

ApplePay

ApplePay ist die Umsetzung eines mobilen Zahlungssystems der Firma Apple und stellt ein kontaktloses System dar, das auf diversen mobilen Apple-Geräten[35] implementiert ist. Das Grundkonzept beinhaltet, dass die Informationen der Kartenbesitzer/innen nicht an den Zahlungsempfänger übertragen werden. Der Kunde/Die Kundin bekommt damit die Möglichkeit eine Transaktion auf einem definierten Zahlungsterminal zu tätigen. Das Zahlungssystem von Apple setzt auf schon vorhandene Sicherheitskonzepte und Überprüfungen, um den eigentlichen Geldtransfer durchzuführen und wird in den nachfolgenden Kapiteln näher erläutert. Um das gesamte Konzept betrachten zu können, wird anschließend der Prozess gezeigt, wie ein Kunde/eine Kundin sein vorhandenes Zahlungsmittel zu Apples Ökosystem hinzufügt. [25, p. 10]

[35] Zu den unterstützen mobilen Geräten zählen: das iPhone SE sowie alle iPhones 6 und neuere Modelle. Im Bereich der Tablets die Geräte: iPad (6 Generation), iPad Pro, iPad (5 Generation), iPad Air 2, iPad mini 4, und iPad mini 3. Zusätzlich werden auch noch Apples Smartwatch ab der ersten Generation oder neuer in das Zahlungssystem eingebunden. [35]

ApplePay-Karten hinzufügen

Um eine Transaktion zu tätigen, muss in erster Instanz eine gültige Kreditkarte oder ein anderweitiges Zahlungsmedium hinzugefügt werden.

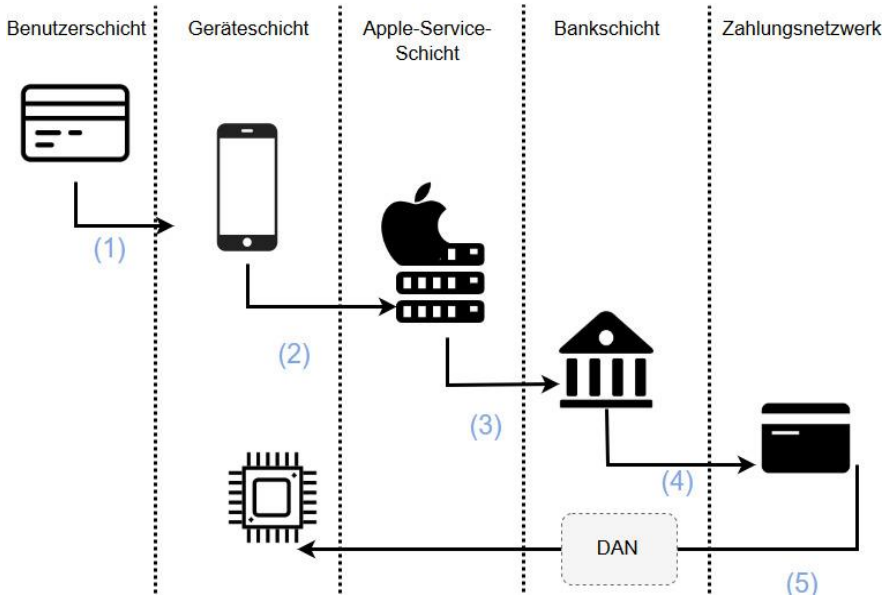

Abbildung 21 Apple-Zahlungsmittel hinzufügen nach [25, p. 10]

- 1. Der/Die Benutzer/in gibt zunächst manuell oder per Foto seine Zahlungsinformationen in die Verwaltungsapp ein.
- 2. Die gespeicherten Daten werden nun mittels einer sicheren Übertragung an das Backend von ApplePay übertragen. Diese Initialisierung enthält die Kontoinformationen, wie auch folgende spezifische Informationen:
    - iTunes/App Store Aktivitäten
    - Geräteinformationen (Rufnummer, Modelltyp, etc.)
    - Benutzerstandort mithilfe der eingebauten Sensoren, wie GPS oder per Handynetzzellen-Informationen
- 3. Apple überträgt die aufbereiteten Informationen an das Finanzinstitut, welches diese legitimiert und anhand einer Risikoeinschätzung entscheidet, ob es sich um eine gültige Anfrage handelt. Der Entscheidungsprozess beinhaltet eine technisch unterstützte Risikobewertung und stellt eine von vielen Risikoindikatoren zur Verfügung. Auf deren Basis trifft das Bankinstitut seine Entscheidung. Die technische Umsetzung dafür kann als „Missbrauchskontrolle“ gesehen werden.
- 4. Sobald die Karte vom Zahlungsinstitut akzeptiert wurde, erstellt der Mobilfunkprovider einen einzigartigen Token für den Kunden/die Kundin. Für die Generierung ist meist ein Drittanbieter zuständig, auch **T**oken-**S**ervice-**P**rovider[36] genannt.
- 5. In der letzten Phase wird vom TSO eine sogenannte **D**evice-**A**ccount-**N**umber[37] generiert, welche einzigartig und an Geräte und Zahlungsarten gebunden ist. Der DAN-Token, inklusive der benötigten kryptographischen Operationen zum Durchführen des Zahlungsvorganges, werden dann am Endgerät in der Secure-Enclave abgelegt.

Der hier gezeigte Prozess des „Hinzufügens einer Karte“ läuft in fünf gesonderten Schritten ab, die alle in der Software implementiert wurden. [25, pp. 10 - 11]

[36] Der Token-Service-Provider wird mit TSO abgekürzt.

[37] Die Device-Account-Number wird mit DAN abgekürzt.

ApplePay-Zahlung

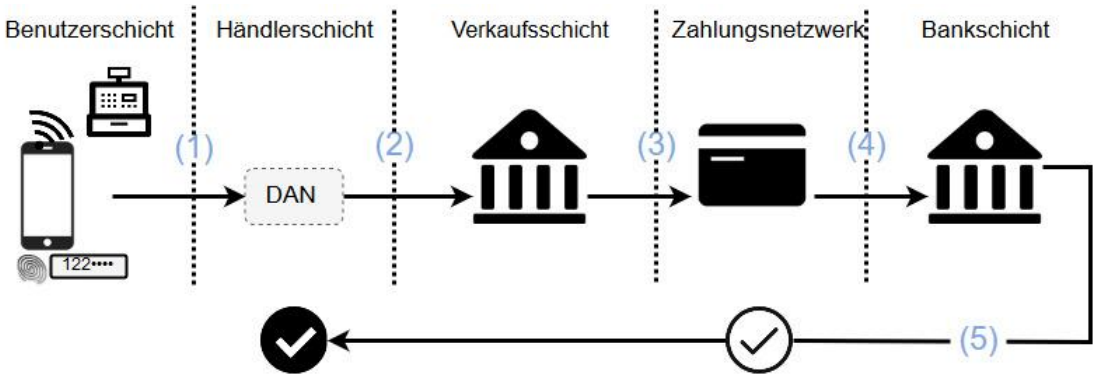

Abbildung 22 Apple-Zahlung nach [25, p. 11]

ApplePay-Zahlung Beschreibung

- 1. Wenn der/die Benutzer/in den Zahlungsvorgang starten will, hält er die NFC-Schnittstelle des Mobiltelefons in den gekennzeichneten Bereich am POS-Terminal. Um den/die Benutzer/in zu identifizieren stehen je nach Gerät der Fingerabdruck-Sensor[38] oder ein PIN zur Verfügung. Startet nun der Zahlungsvorgang, wird die DAN-Nummer übertragen.
- 2. Die Transaktion und die dazugehörigen Informationen werden vom Händler an die beauftragte Bank übermittelt.
- 3. Die Bank in der Verkaufsschicht kann den Token jedoch nicht zuordnen, und liest den Wert der **B**ank-**I**nformations-**N**ummer aus. Mit der Information zu welchem Bankinstitut die übermittelten Daten gehören, werden sie durch das Zahlungsnetzwerk an die Bank von dem Kunden/der Kundin übertragen.
- 4. Die Kundenbank erkennt die DAN-Informationen und konvertiert diese zurück in die eigentlichen verwertbaren Zahlungsinformationen.
- 5. Die Kundenbank entscheidet anhand der Risikobewertung über die Gültigkeit der Transaktion. Das Ergebnis wird nun zurück an den Händler übertragen, der die Zahlung abschließt. [25, pp. 11 - 12]

Kontrollen und Echtheitsprüfung des Users/der Userin und des Gerätes

Um den von dem/der User/in begonnen Zahlungsvorgang abzuschließen, muss noch die Echtheit dessen und des Gerätes überprüft werden. Der Vorgang wird nachfolgend beschrieben.

Der/Die User/in wird bei einem aktiven Zahlungsvorgang nach seinem definierten „Geheimnis“ gefragt. Dabei handelt es sich technisch um einen per Sensor eingelesenen Fingerabdruck, von Apple TouchID genannt, oder um einen vorher definierten PIN, beispielsweise im Falle einer Apple-Watch. Derartige Sicherheitsmaßnahmen sind für den Fall gedacht, sollte das Gerät unbeaufsichtigt zurückgelassen, abhandenkommen oder gestohlen werden. Der/Die Angreifer/in hat ohne Zugangsinformationen nur minimalen Aktionsspielraum bzw. geringe Missbrauchsmöglichkeiten. Im direkten Vergleich zu Bargeld oder Kreditkarten, bei denen sofort ein direkter monetärer Verlust besteht. [25, p. 12]

Die Geräte-Echtheit wird mittels der oben vorgestellten, eindeutigen Token bei jeder Transaktion sichergestellt. Jede auf diesem Weg abgehandelte Zahlung erzeugt bei ihrer Durchführung einen einzigartigen Wert. Dabei wird geprüft, ob die Zahlung von einem berechtigten Gerät kommt, wie in der oben dargestellten Abbildung 22 gezeigt. Der einzigartige Token und das eingesetzte Kryptogramm sorgen dafür, dass selbst wenn ein Token von einem/einer Angreifer/in abgefangen wird oder anderweitig abhandenkommt, dieser nicht weiterverwendet werden kann. Der Token ist vom Gerät selbst generiert und sollte er von einem anderen Gerät benutzt werden, stimmt dessen Abhängigkeit nicht mehr und ist somit unbrauchbar. Als zusätzliches Sicherheitsmerkmal gilt, dass der Zahlungsbetrag als eine Variable bei der Erzeugung in den Token einfließt. Das Abfangen jenes Token

[38] Diese Funktion wird in Apples Ökosystem auch TouchID genannt.

und der anschließende Missbrauch für eine andere Transaktion führen dazu, dass sich beispielsweise die Zahlungsbeträge unterscheiden und der Token folglich keine Gültigkeit mehr hat. [25, p. 12]

ApplePay Security-Kontrollen - Zusammenfassung

- Einsatz eines Tokensystems und Kryptographie
- Secure-Enclave-System mit Hardwarechip
- Daten werden verschlüsselt aus der Secure-Enclave an das Zahlungsservice übertragen
- Direkte Kommunikation zwischen POS und SE über die integrierte NFC-Funkschnittstelle
- Strikte Trennung zwischen Zahlungsverkehrs-Schicht und der User Anwendungs-Schicht [25, p. 12]

Google-Wallet /Google-Pay

Ursprünglich verfolgte Google mit seinem Google-Wallet eine ähnliche Strategie, es wurde ebenfalls ein SE-Element benutzt, um dort sensitive Zahlungsinformationen abzulegen und vor Angreifer/inne/n zu schützen. Mit der Einführung von HCE im Mai 2015 änderte Google die Strategie in Bezug auf mobile Zahlungen und wechselte auf einen softwarebasierten Ansatz bzw. in späterer Folge auf die vollständige Abwicklung in der „Cloud“. Der Ansatz sieht vor, dass alle Zahlungsinformationen in der Softwareumgebung gespeichert und verwaltet werden. Im Zuge dieser Veränderung wurden auch neue Services und APIs integriert und weitere Authentifizierungsmaßnahmen umgesetzt. [25, pp. 12 - 13]

Karten Hinzufügen bei Google-Wallet

Als ersten Schritt, um diese Zahlungsart anzuwenden, muss die Kredit- oder Debit-Karte bei Googles Zahlungsdienst registriert werden. Die Haftung bei der Zahlung liegt aber beim eigentlichen Bankinstitut. Google bietet diesem mehrere Identifikations-Optionen, um die Echtheit des Kunden/der Kundin zu überprüfen.

- **Email- & Brief-Verifikation** - Der Kunde/Die Kundin bekommt per Post oder per Email ein Schreiben mit einem Verifikationscode, der dann im Gerät eingetragen wird.
- **Telefon-Verifikation** - Der Kunde/Die Kundin kann sein Bankinstitut kontaktieren und bekommt von jener Stelle seinen Verifikationscode.
- **Per Banking-App** - Der Kunde/Die Kundin hat bereits die individuelle Bank-Applikation auf seinem Gerät installiert und loggt sich mit dieser ein. Je nach Userinterface kann der Kunde/die Kundin nun in der App die Verifikationsnummern abrufen.
- **Per Micro-Abbuchung** - Dabei erfolgt der Abzug eines minimalen Betrages auf dem Kundenkonto mit anschließender Rückbuchung nach einem kurzen Zeitraum. In der Buchungszeile des Betrages befindet sich ein Verifikationscode, mit dem der Besitz der Karte bestätigt wird.

Beim Karten-Initialisierungsvorgang wird die eigentliche Kartennummer an das Cloud-Backend von Google übertragen und gespeichert. Somit sind keine zahlungsrelevanten Informationen direkt am Gerät gespeichert, die in späterer Folge eine Angriffsfläche bieten könnten. [25, p. 13]

Zahlungsprozess

Wie schon erwähnt wurde bis 2015 das SE am Gerät selbst verwendet, welches alle zahlungsrelevanten Informationen von dem Kunden/der Kundin speichert. In Form eines Strategiewechsels nach 2015 wurde dieses Konzept verworfen und das Endgerät als potentiell unsicher eingestuft. Diesem Ansatz folgetragend war es nicht mehr ratsam, die sensiblen Informationen für den Zahlungsvorgang auf dem Endgerät abzulegen oder zu verwalten. [25, pp. 13 - 14]

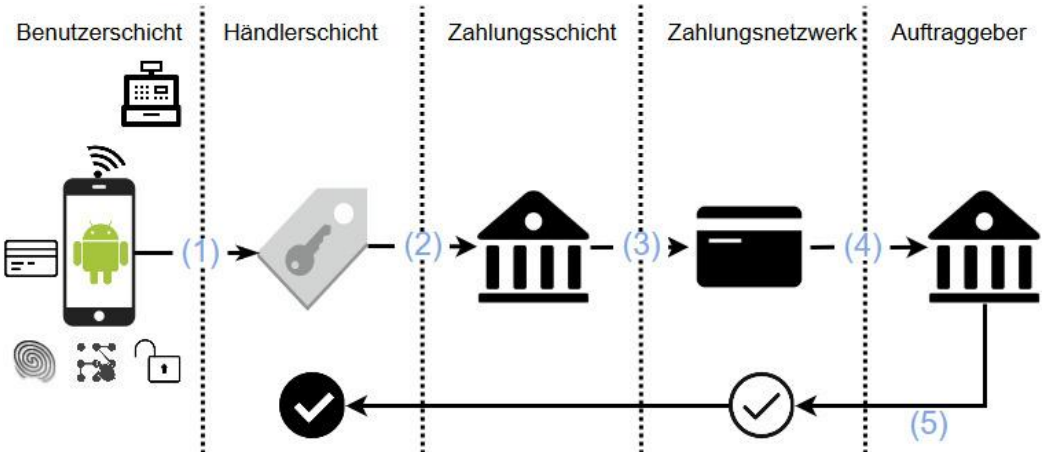

Abbildung 23 Google-Karte Hinzufügen [25, pp. 13 - 14]

- 1. Als Grundvoraussetzung für die Transaktion muss das Mobilgerät eine Internetverbindung aufweisen, um den Zahlungsdienst von Google zu erreichen. Die Server der Services stellen dem mobilen Gerät eine definierte Anzahl von Token zur Verfügung, die für den Geldtransfer eingesetzt werden können. Der Zahlungsvorgang beginnt mit der Auflage des Mobiltelefons mit aktiver NFC-Schnittstelle auf das NFC-POS. Über die HCE-Schnittstelle wird einer der abgerufenen Token für die angeforderte Zahlung benützt. Der NFC-Controller am Gerät stellt dabei, wie im Kapitel *NFC - technologische Gerätetypen (S. 24)* beschrieben, die Verbindung zwischen digitaler Geldbörse und dem POS-Terminal her. Während dieses Vorganges wird zusätzlich zum Token auch ein Kryptogramm übertragen.
- 2. Der/Die Verkäufer/in, sendet über den/die Käufer/in den eigentlichen Zahlungsauftrag an die abrechnende Bank.
- 3. Das zahlende Bankinstitut erhält nun den ausgesendeten Token und das Kryptogramm und leitet die gewonnenen Informationen über das eigentliche Transaktionsnetzwerk an das Bankinstitut weiter.
- 4. Das Netzwerk der Bankinstitution wandelt nun die empfangenen Token und Kryptogramme in die hinterlegten PAN-Informationen um und wartet auf die Genehmigung des Ausstellers.
- 5. Im letzten Schritt überprüft der Aussteller, ob die Transaktion gültig ist bzw. ob der Kunde/die Kundin genug Geld zur Verfügung hat, um diese auch durchzuführen. Besteht ein gültiger Vorgang, werden die Zahlungsinformationen an den Händler übertragen und die Zahlung ist vollständig. [25, pp. 13 - 14]

Echtheitsprüfung des Users/der Userin und des Gerätes

In jedem Fall findet vor der Tätigung einer Transaktion eine Überprüfung der Echtheit des Users/der Userin über die von Android bereitgestellten Funktionen statt. Android bietet je nach vorliegender Version und Gerätetyp die nachfolgenden Authentifizierungsmöglichkeiten:

- Fingerabdruck
- Pin-Code
- Passwort
- Sonstige biometrische Erkennung
- Muster-Code (Display Pattern)

Um die Echtheit des Gerätes festzustellen, werden vorab vom Google Server die benötigten Token an die entsprechenden Benutzer/innen und Ihre Geräte verteilt. Dies kann erst geschehen, wenn sich das Gerät in einem Netzwerk mit Internetverbindung befindet, z.B. über mobile Datenverbindungen oder per WLAN. Außerdem wird im Vorhinein eine Geräteeinschätzung vorgenommen, bei der eine Überprüfung über eine Modifikation des Gerätes erfolgt. Jener Mechanismus stellt sicher bzw. beugt vor, dass mithilfe von tiefgreifenden Systemmodifikationen eine Gefahr für eine Zahlung besteht. Sollte diese Überprüfung fehlschlagen, bietet das Gerät die beschriebene Zahlungsart grundsätzlich nicht mehr an [25, p. 15].

Mögliche zahlungsbeeinflussende Modifikationen sind:

- Bootloader
- Root
- Third-Party-Frameworks etc.

Ein ebenfalls zu betrachtender Hauptunterschied zur Zahlung mit Bargeld ist vor allem der Umgang bzw. die Awareness mit PINs oder ähnlichen Geheimnissen. Die Passwort- oder Geheimnisverwaltung im digitalen Umfeld werden von vielen Personen nicht ordnungsgemäß betrieben, alleine schon aufgrund ihrer Vielzahl von digitalen Identitäten. Wie der Alltag leider zeigt überträgt sich dieser legere Umgang auch auf den Smartphone-Sektor und führt uns zu typischen Passwort-Problemen, die auch schon aus dem klassischen Computerumfeld bekannt sind. Der sorglose Umgang oder sogar die Weitergabe sensibler Informationen stellen dabei eine große Bedrohung dar. Im direkten Vergleich dazu, werden die Pins der Bankkarten nicht so sorglos herausgegeben. [25, p. 15]

Google-Wallet – Security-by-Design-Kontrollen

Die grundsätzliche Annahme, dass jegliche Daten und Informationen auf einem Gerät kompromittiert sein könnten, ist heutzutage gar nicht so abwegig. Derzeit wendet Google in seinem Zahlungsmodell den HCE-Ansatz[39] an, bei dem jegliche sensitiven Informationen in der eigenen sicheren Cloud-Umgebung gespeichert werden.

- Einschränkung der Schlüsselverwendbarkeit
- Tokenisierung
- Authentifizierung via Betriebssystemschicht
- Risikoanalyse der Transaktion

Die technische Einschränkung der Schlüsselverwendbarkeit basiert auf dem System, welches durch eine kurze Schlüssellebensdauer versucht, Missbrauch unmöglich zu machen. Die Token verhindern, dass die eigentlichen Pan-Daten übertragen werden. Der Einsatz einer Pin-, Muster- oder Fingerabdruck-Verifizierung stellt die anschließende Gerätevalidierung dar. Als letzter Schritt werden eine Risikobewertung und eine Echtzeit-bewertung der Transaktion durchgeführt, um mögliche bösartige Muster oder manipulierte Informationen zu identifizieren. [25, p. 15]

Übersicht von generischen Angriffsvektoren in digitalen Zahlungssystemen und digitalen Wallet-Systemen

Die Sicherheit der bisher beschriebenen Zahlungssysteme ist stark von der sogenannten „Chain-of-Trust“ abhängig. Bei solchen Vertrauensketten müssen die einzelnen „Kettenglieder“ betrachtet werden, da der allgemein bekannte Grundsatz „Eine Kette ist nur so stark wie sein schwächstes Glied“ gilt. Die Kettenglieder stellen technische Elemente dar, die jeweils eine grundlegende spezifische Aufgabe erfüllen. Das zeigt sich exemplarisch an dem von Apple eingesetzten SE-Element. Bei der Betrachtung dieser unterschiedlichen Bestandteile sind besonders die Übergänge zwischen den einzelnen Elementen interessant. Jedes bietet jeweils eigene spezifische Angriffs- wie auch Verteidigungsmöglichkeiten. Nachfolgend wird ein generisches Bedrohungsmodell vorgestellt, dass mögliche POI[40] für einen/eine Angreifer/in hervorhebt. [25, p. 19]

[39] Wie die Geschichte zeigt, kann sich der hier vorgestellte HCE-Ansatz aber auch weiterentwickeln bzw. ganz verändern.

[40] Der Begriff POI beschreibt die Abkürzung zu „Points-Of-Interesting”.

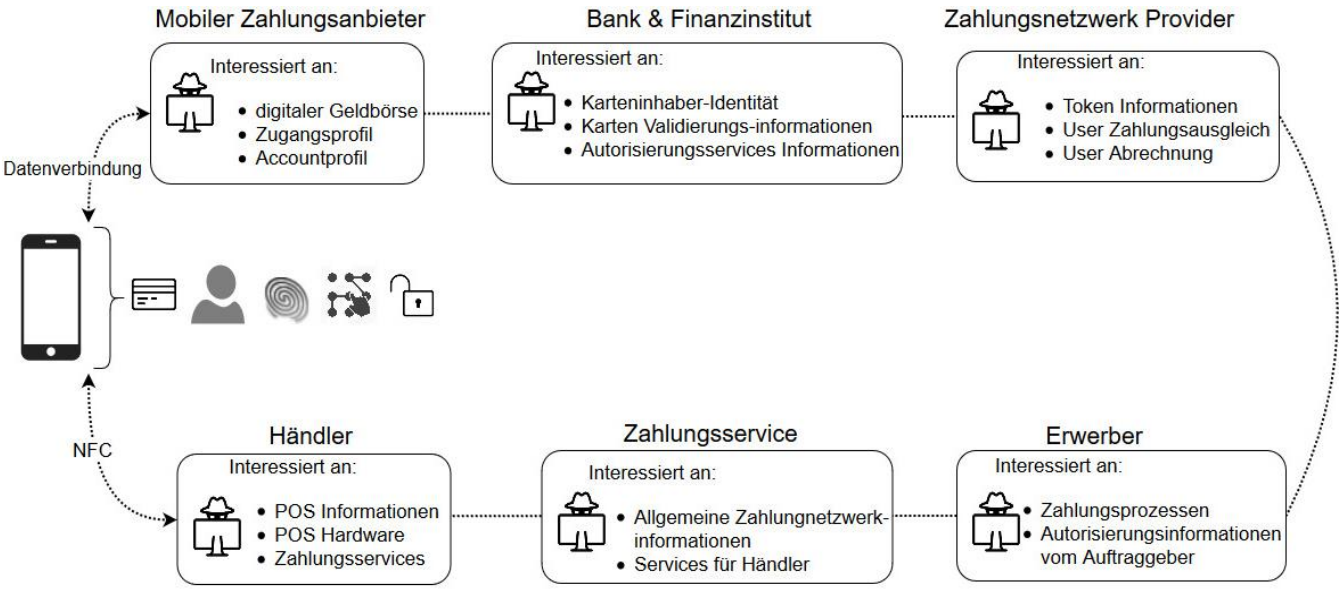

Abbildung 24 Generisches Angriffsmodell nach [25, p. 19]

Attacken auf Benutzerebene im Kontext von digitalen Transaktionen - Thread Model

Nachfolgend wird gezeigt, dass sich Übergriffe im Zahlungsumfeld nicht nur auf einer rein technischen Ebene abspielen, sondern auch direkt auf den/die Benutzer/in und sein kontextuales Umfeld abzielen. Viele dieser Attacken basieren auf sozialen Kompetenzdefiziten oder der Leichtgläubigkeit des Benutzers/der Benutzerin. Als Angriffsvektoren wurden die nachfolgenden Threads identifiziert:

- "Phishing" und "Social-Engineering"
- Einschleusen einer schadhaften Applikation
- Identitätsmissbrauch

Social-Engineering als generischer Thread im Kontext von mobilen Zahlungen

Definition von Social-Engineering

„Social-Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch "Aushorchen" zu erlangen. Beim Social-Engineering werden menschliche Eigenschaften wie z.B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln". [26]

Die Grenze zwischen einem rein privat und geschäftlich genutzten Gerät verschwimmt meist zusehens, vor allem wenn Firmen Konzepte wie „Bring-Your-Own-Device" anbieten. Das Smartphone hat in vielen Fällen eine große Anzahl an spezifischen Benutzerinformationen gespeichert. Diese reichen von PINs, Passwörtern, persönlichen, firmenbezogene bis hin zu finanztechnischen Informationen, die einen hohen Wert für Angreifer/innen besitzen. Besonders Firmendaten sind in solchen Fällen oft lohnenswerte Ziele. Auf einem mobilen Gerät[41] sind oft eMails, VPNs oder andere wichtige Zugänge zu Firmendiensten hinterlegt. Unter den passenden Voraussetzungen kann das mobile Gerät auch als „Sprungbrett" ins Firmennetzwerk dienen, um in späterer Folge einen Übergriff durchzuführen. Jene Informationen müssen keinen direkten Bezug zum

[41] Dabei handelt es sich **nicht** ausschließlich um Smartphones, sondern auch Geräte wie Tablets, Laptophybriden und so weiter.

eigentlichen Angriffsziel haben, jedoch ermöglichen sie eine Einschätzung des Zieles bzw. weiterer Schlussfolgerungen oder Zugangsmöglichkeiten zu anderen Services.

Die klassischen Angriffswege auf mobilen Geräten bei „Social-Engineering“ und „Phishing“ sind:

- Telefonanrufe
- SMS
- Emails
- Digitale Nachrichtendienste (WhatsApp, Signal, WeChat, etc.)
- Apps mit dubiosen Sicherheitsinformationen

Der/Die Angreifer/in hat darüber hinaus noch die Möglichkeit, zusätzliche öffentliche Informationen zu seinem Angriffsziel einzuholen, wofür oftmals folgende beliebte Methoden Anwendung finden:

- Die Person mittels einer Suchmaschine ausspähen.
- Recherche des sozialen Netzwerks über Dienste wie Facebook, Twitter, Xing, usw.
- Durchsuchen von persönlichen Webseiten wie Homepages oder Blogs.

Informationen, die durch solche Quellen gewonnen wurden, können meist dazu genutzt werden, weitere gezielte Attacken vorzubereiten, oder aber auch schon durchzuführen. Außerdem haben sensible Daten in ihrer Ursprungsform einen monetären Wert für den/die Angreifer/in. Diese können jene Daten gewinnbringend verkaufen, tauschen oder, wie schon erwähnt, für zusätzliche Vorbereitungen verwenden, z.B. Identitäts-diebstahl für anderwärtige Zahlungen. [25, pp. 19 - 20]

Einschleusen von schadhaften Applikationen als generischer Thread im Kontext von mobilen Zahlungen

Sollte es einem/einer Angreifer/in gelingen, eine schadhafte Applikation auf dem Zielgerät zu installieren, kann der Schaden noch größer sein. Klassische Verbreitungswege derartiger Übergriffe sind:

- Phishing
- Öffnen eines schadhaften Email-Anhanges
- URL Umleitungen
- Schadhafte Werbung
- Drive-by-Downloads
- Third-Party-Inhalte

Aber auch der Gebrauch von öffentlichen WLAN Netzwerken, wie in nachfolgend aufgezählten Umgebungen, bergen ein erhebliches Gefahrenpotenzial:

- U-Bahn
- Bahnhöfe und Züge oder Flughäfen
- Bars und Restaurants
- Cafés und Freizeitanlagen
- Mobile Hotspots in öffentlichen Bereichen

Eine Datenverbindung an derartigen öffentlichen Standorten sollten nur mit Vorsicht benutzt werden, da sie ein erhebliches Angriffspotential besitzen. Möglichkeiten dafür wären beispielsweise der Man-In-The-Middle- oder Spoofing-Angriff, um den User in eine Falle zu locken und eine dritte Applikation auf dem Zielgerät zu installieren oder Informationsgewinnung zu betreiben.

Diese Tatsache stellt für einen/eine User/in, der einen „unsicheren“ Umgang mit seinen Passwörtern pflegt, eine sehr große Gefahr dar, da mit großer Wahrscheinlichkeit User-Passwort-Kombination bei anderen Services wiederverwendet werden. Im Allgemeinen ist auch davon abzuraten, derartige unsichere Verbindungen für einen Zahlungsverkehr zu nutzen, was den User aber nicht daran hindert, es zu tun. [25, p. 20]

Mobilgeräte – mögliche Schnittstellen für mobile Angriffsszenarien

Mobile Geräte haben viele Kommunikationsschnittstellen und befinden sich meist in einer komplexen Systemumgebung. Um die Komplexität eines Smartphones und deren Schnittstelle verstehen zu können, dient die nachfolgende generische Abbildung. [27]

Übersicht mobiles Thread-Model

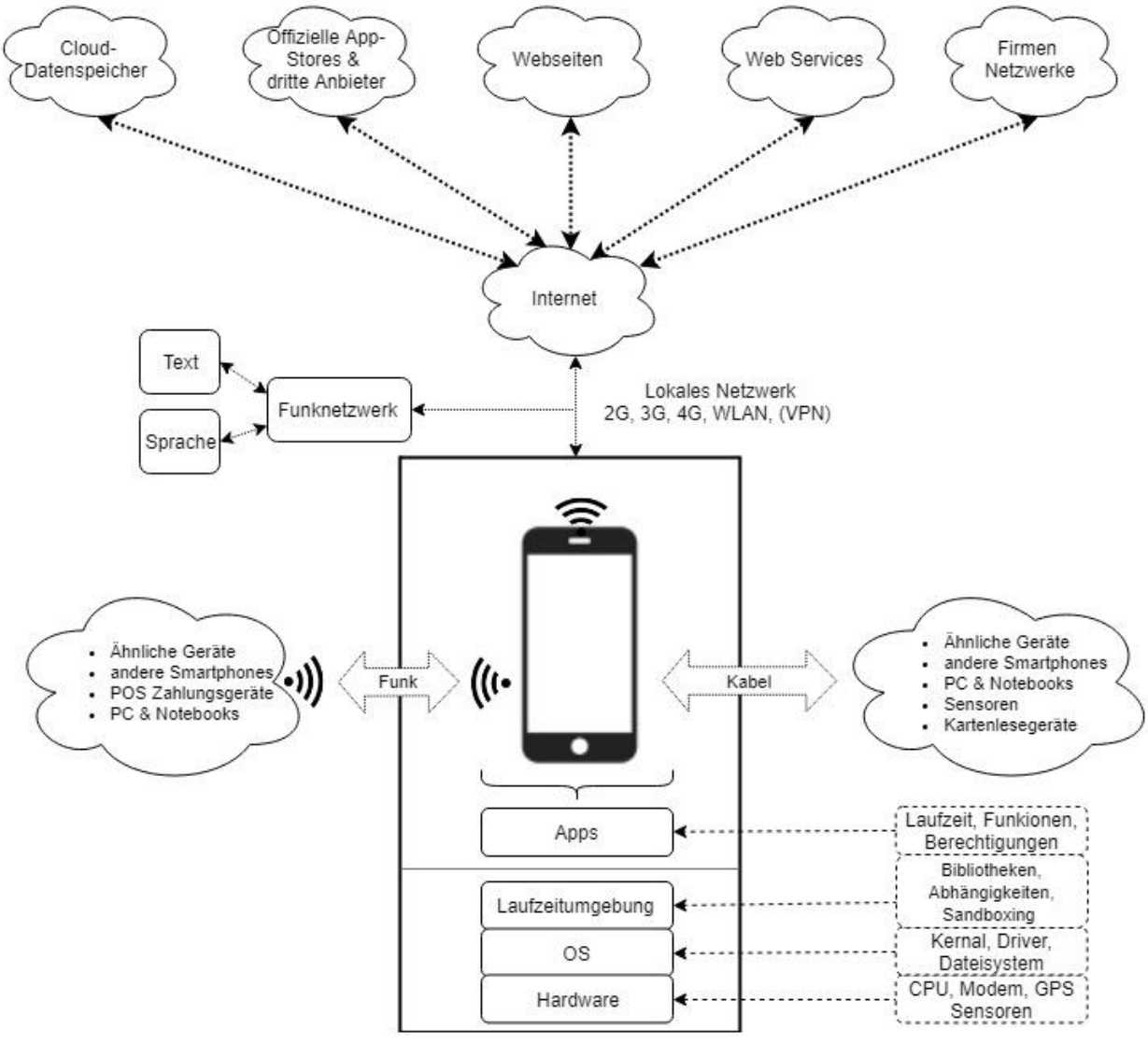

Abbildung 25 Mobile Threads nach [27]

Basierend auf der Statistik, der anhand der OWASP erhobenen Daten, haben sich seit 2016 die nachfolgenden kritischen Applikationsschwerpunkte herauskristallisiert. Diese können sowohl von einem Angreifer, wie auch von einem Developer herangezogen werden, um in der Applikation spezifische Probleme zu identifizieren. Je nach Blickwinkel können mit Hilfe einer derartigen Liste Bugs gesucht oder aber auch Schwachstellen gefunden werden. [28]

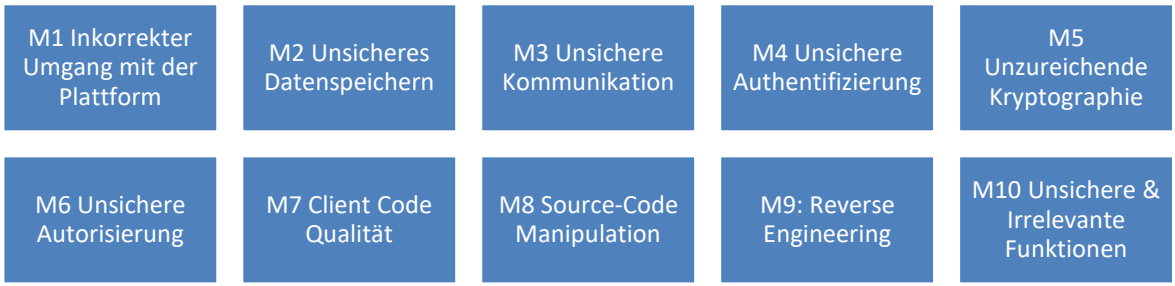

Abbildung 26 OWASP Top 10 2016 nach [28]

Physischer Zugriff auf ein mobiles Gerät

Abseits von Software-Schwachstellen existieren beim Smartphone noch weitere Problemstellungen, wie z.B. der Verlust des Gerätes. Sollte es einem/einer Angreifer/in gelingen sich einen physischen Zugriff auf das Gerät zu verschaffen, gibt es nur noch wenige Sicherheitsmechanismen, die diese Art von Zugriff verhindern können. Ein/e Angreifer/in versucht in erster Linie die physischen Sicherheitsmechanismen zu umgehen, um im späteren Verlauf Zugriff auf das Filesystem und dessen Daten zu bekommen. Überwindet der/die Angreifer/in auch die letzten Schutzfunktionen, kann er seinen Übergriff fortsetzen. Die dafür nötige Arbeit wird entweder manuell, mittels eines kommerziellen Tools oder mit Hilfe von Open-Source-Software gelöst. Je nach eingesetztem Tool können die Ergebnisse sehr unterschiedlich sein. [22, pp. 1 - 2]

Anmerkung zu biometrischen Zugriffsschutztechniken

Biometrische Merkmale auf mobilen Geräten sind im Alltag sehr nützlich und erfreuen sich einer breiten Akzeptanz. Das liegt hauptsächlich am universellen, bequemen und schnellen Einsatz dieser. Jedoch sieht die Kehrseite so aus, dass wir Menschen überall unwissentlich biometrische Informationen hinterlassen, beispielsweise Fingerabdrücke auf einem Glas oder anderen Oberflächen. Ein weiterer Faktor ist, wie Brotkrumen verteilte biometrische Merkmale können nicht geändert werden und somit keine Sicherheit mehr gewährleisten. Eine biometrische Authentifikation ist deshalb nur der Wissensnachweis und nicht der Willensnachweis.

Außerdem spielt bei vielen Geräten die korrekte Lebenderkennung eine große Rolle, welche sicherstellen soll, dass es sich dabei nicht um ein nachgemachtes biometrisches Merkmal handelt. Jedoch sollte das nicht verallgemeinert werden, da Sensoren gerätespezifisch abhängig von der jeweiligen Scan-Qualität verbaut sind. [29]

Malware-Installation auf mobilen Geräten

Die Installation von Malware geschieht meist ohne zusätzliches Eingreifen des Benutzers/der Benutzerin oder so versteckt, dass dieser getäuscht wird und eine Bestätigung für die Installation gibt. Die Malware kommt z.B. über einen „Drive-by-Download“ auf das Gerät und wartet dort, bis sie die Möglichkeit hat sich selbst auszuführen oder aber von dem/der Benutzer/in ausgeführt wird. Das Aggressivitätslevel einer solchen Schadsoftware reicht von geringem bis hin zu sehr aggressivem Verhalten und ist nicht zu vereinheitlichen. Es führen sowohl einfache Techniken, wie das schlichte Kopieren von Daten, als auch erweiterte Techniken, wie dem Rooten oder Jailbreaken, zum Ziel des/der Angreifer/in. Das Ergebnis ist eine anschließenden Komplettübernahme des Gerätes. Ein anderer Weg, wie derartige Malware auf das Endgerät gelangen kann, ist der App-Store (Android-Pay und Apple-App-Store), bei dem nur automatisierte Kontrollen auf missbräuchliches Verhalten einer App verwendet werden. Zudem existieren auch diverse App-Download-Portale und alternative App-Stores, bei denen die oben angesprochenen Maßnahmen gar nicht vorhanden sind. Die erwähnten Third-Party-App-Stores stellen für den/die Angreifer/in eine beliebte Quelle dar, „Copy-Cat-Apps[42]“ mit Malware zu

[42] Ist die Beschreibung einer App, die eine andere imitiert aber meist schadhafte Funktionen enthält.

verbreiten. Der App-Store bietet hier für den/die Angreifer/in einen zentralen Verteilungs- und Kontrollpunkt um Malwarekampanien zu starten. [25, p. 20]

Malware Angriffsklassen

- **Repacking** basiert auf dem Hinzufügen von schadhaftem Sourcecode in der Applikation. Dabei werden meistens regionale oder länderspezifische beliebte Anwendungen herausgesucht und um den schadhaften Sourcecode ergänzt. Dafür werden jene wieder in Sourcecode rückkonvertiert und anschließend um das schadhafte Codestück erweitert. Die neue manipulierte Applikation wird anschließend dem/der User/in über Plattformen wie Foren, Tauschbörsen und einschlägigen Markplätzen angeboten.
- Die **Update-Attacke** beschreibt ein Szenario, in dem die ursprüngliche App noch keinen eigentlichen Schadcode beinhaltet. Das Nachladen des Schadcodes geschieht dann folglich über ein Update der App selbst und wird während der Verwendung jener ausgeführt. Diese Methode hat aus Angreifersicht den Vorteil, dass ein statischer Malewarescanner bei einer App-Überprüfung den eigentlichen Schadcode schwieriger erkennt.
- Der **Drive-by-Download** im Appkontext ist schon aus vielen anderen Bereichen der klassischen IT bekannt, so auch im mobilen Bereich. Für derartige Übergriffe werden aber nicht nur Schwachstellen im Browser oder ähnlichen Funktionen ausgenutzt. Sondern auch Formen eines Social-Engineering-Angriffes. Es wird versucht den/die User/in zu verleiten, eine App aus einer nicht gesicherten Quelle zu installieren. Das geschieht beispielsweise durch In-App-Werbung, die auf eine nachgebaute schadhafte Anwendung verweist.
- Im mobilen Umfeld gibt es noch vielfältigere Möglichkeiten Malware zu verbreiten, jedoch lassen sich diese nicht eindeutig einer übergeordneten Kategorie zuordnen. Sie beinhalten oft Angriffsmuster aus verschiedensten Bereichen. [30, pp. 97 - 100]

Die Kosten, die auf Grund solcher Manipulationen entstehen, versuchen die infizierten Apps in vielen Fällen zu verheimlichen. Dabei werden oft sogenannte „Premiumdienste“ für die Zahlung angewählt oder „abonniert“, es handelt sich dabei meist um kostenpflichtige Mehrwertnummern, die sich über die ganze Welt verteilen. Wie diese Kostenfunktion in der App integriert ist, ist abhängig von der eingesetzten Malware und reicht von hardcodierten SMS-Sendungen bis zum dynamischen Anwählen der oben genannten Dienste. [30, pp. 101 - 103]

Attacken über einen Sprachassistenten

Spracherkennungssysteme erreichen zunehmend die breite Masse und stehen als Funktion mit unterschiedlichen Ausprägungen auf den einigen mobilen Geräten zur Verfügung. So entwickelten sich auch neue Angriffsmethoden rund um derartige Interaktionsmöglichkeiten, welche auf spezielle Gegebenheiten ausgerichtet sind. Das Grundprinzip dieser Übergriffe basiert darauf, dass das menschliche Ohr nur einen gewissen Frequenzbereich akustisch wahrnimmt und in Informationen umwandelt. Im direkten Vergleich dazu kann ein digitales Mikrofon, wie es in Smartphones oder anderen mobilen Geräten Einsatz findet, ein breiteres Frequenzspektrum wahrnehmen. Die digitalen Subsysteme so eines Sprachassistenten bestehen aus Tonaufnahme, Sprachverarbeitung und Kommandoausführung. Jedes Element bietet eine eigene Angriffsfläche, die die Möglichkeit einer zielführenden Attacke beinhaltet. Daraus lässt sich schließen, dass ein/e Angreifer/in digital hörbare Befehle an ein Smartphone weitergeben kann, ohne dass es von seinem/seiner menschlichen Benutzer/in wahrgenommen wird. In einem „Proof-of-Concept“, wie der „Dolphin-Attacke“, können über für Menschen nicht hörbare Töne, präparierte Webseiten geöffnet oder Hardwareschnittstellen aktiviert werden, wie z.B. NFC. Durch die zusätzliche Modifikation dieses Konzeptes, wäre es durchaus denkbar, dass über einen solchen Eingriff eine Zahlung, ein Kauf, eine Überweisung oder sonstige Interaktionen mit mobilen Zahlungen ausgelöst werden.

Je nach Ziel des Angreifers/der Angreiferin können daraus neue Angriffsszenarien gebaut werden, die aus der Userperspektive alle technischen Sicherheitszonen überwindet. Auf technischer Ebene wirken derartige Übergriffe legitim und benutzen die regulären und vorgesehenen Schritte, um die Transaktion durchzuführen. [31, pp. 103 - 105]

Aufbau eines generischen Audioangriffes

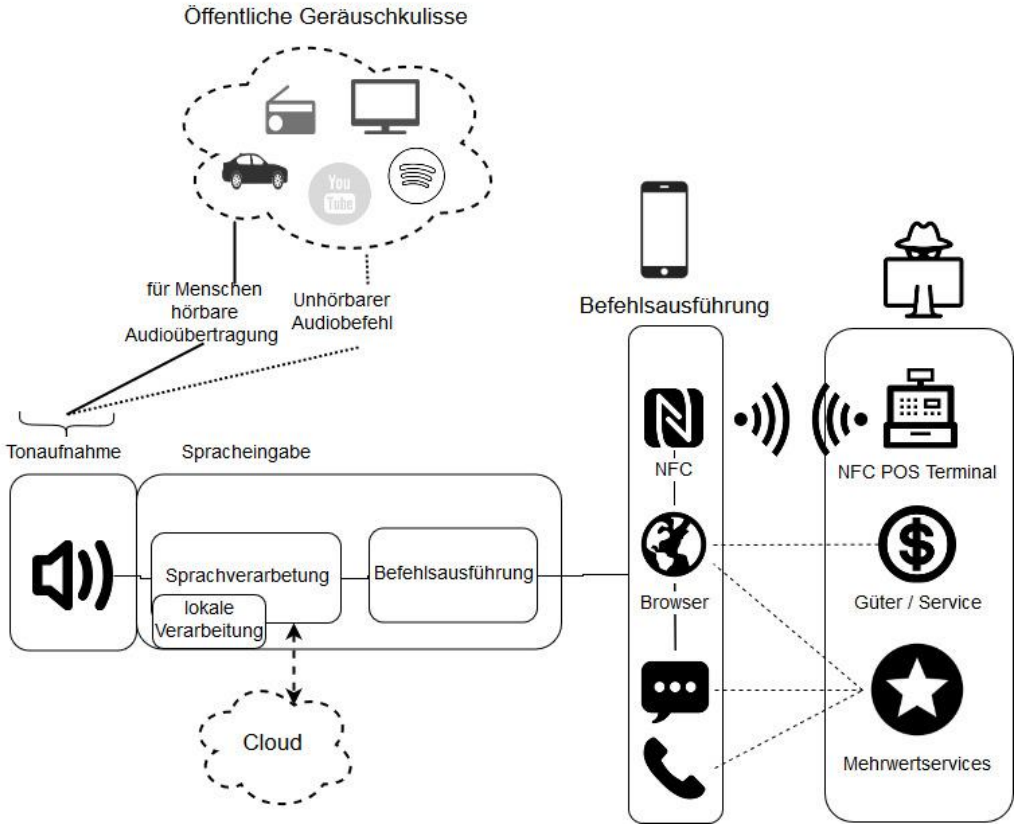

Abbildung 27 Angriff Sprachassistent nach [31, p. 104]

Angriffsmodelle für digitale Zahlung- und Geldbörsen-Apps

Bei mobilen Anwendungen handelt es sich immer um ein Stück Software, das in unterschiedlichsten Formen in das jeweilige mobile Ökosystem eingebettet ist. Die Integration kann hierbei von einer „Stand-A-Lone“ Applikation bis hin zu einer im OS verankerten Funktion reichen. [25, p. 20]

Reverse-Engineering der Applikation

Abhängig vom vorhandenen Ökosystem, ist immer eine Möglichkeit des Reverse-Engineerings (Rückführung der ausführbaren Binärdatei in den Source-Code) gegeben. Das vorhandene OS ist dabei die maßgebliche Instanz für das App-Format. Je nach vorliegender App, kann durch diese Technik ein/e Angreifer/in ein technisches Verständnis für die Software aufbauen. Je nach konzeptionellem Aufbau der Software können auch hartcodierte Passwörter, Security-Token, sensible Kundeninformationen oder andere programmspezifische Sicherheitslücken aufgedeckt werden, die einen digitalen Betrug ermöglichen. [25, p. 20]

Gezielte App-Manipulation

Angreifer/innen haben auch die Möglichkeit, gezielt Inhalte oder Teile einer App zu manipulieren. Dafür ist die Ergänzung der App durch individuellen Schadcode notwendig. Die ausgewählte Anwendung muss dafür in Source-Code umgewandelt werden, dann werden die gewünschten Codeelemente hinzugefügt. Im letzten Schritt wird der App-Source-Code wieder zu einer lauffähigen Applikation gepackt und in einen beliebigen App-Store hochgeladen. Solche Schadcodes können beispielsweise die gesammelten Informationen, wie Username

und Passwort, Kreditkarten und andere Zahlungsoptionen abgreifen und an einen Server senden, der unter der Kontrolle des Angreifers/der Angreiferin steht.

Die Vielzahl an App-Stores und die sich darin befindlichen Anwendungen, stellen für den/die Endbenutzer/in einen erschwerenden Faktor dar, die legitime Herstellerapplikation zu erkennen, herunterzuladen, zu installieren und anschließend zu benutzen. [25, p. 21]

Installation von Rootkits und Ähnlichem

Sollte es einem/einer Angreifer/in gelingen ein Rootkit auf dem Gerät einzuschleusen, ist die Möglichkeit einer Manipulation noch höher. Im Allgemeinen ist mittels einer solchen Technik der Zugriff auf alle Fileebenen, die vom Betriebssystem gemanagt werden, möglich. Der Eingriff in das System ist so tiefgehend, dass die Manipulation der API-Calls realisierbar ist, bevor diese das Serverbackend der Applikation erreichen. Das ermöglicht, z.B. das Verändern eines Zahlungsbetrages, einer Zahlungsadresse und anderen Datenfeldern, die für ordnungsgemäße Transaktionen benötigt werden. [25, p. 21]

Mobile Betriebssystem-Berechtigungen

Ein zusätzlicher Sicherheitsmechanismus von modernen mobilen Betriebssystemen ist die erweiterte Verwaltung der Softwareberechtigungen. Das kann je nach Betriebssystem und Hersteller eine im OS integrierte Funktion oder durch eine vom Drittanbieter bereitgestellte Software sein. Die Berechtigungen werden meist per App verteilt, weswegen eine starke Individualisierung jener erreicht wird. Sollte von dem/der Benutzer/in ein zu restriktives Berechtigungsschema gewählt werden, das für eine App benötigt wird, führt das meist zu einem instabilen Verhalten oder gar zu einer nicht ausführbaren Software. Sollten die Berechtigungen zu offen vergeben werden, besteht die Möglichkeit eines Datenübergriffs. [25, p. 21]

Angriffsmodelle für die digitale Zahlung beim Händler

Der Händler hat in den wenigsten Fällen Einfluss auf das Sicherheitskonzept eines Zahlungsservices. Er wird von diesem nur mit einem Point-of-Sale-Terminal ausgestattet, um den Zahlungsvorgang durchzuführen. Jene POS-Systeme sind meist Stand-A-Lone-Geräte, die entweder direkt oder indirekt mit dem Internet verbunden sind. Je nachdem wie der Hersteller sein Zahlungssystem designt hat, können auch die Anforderung an ein Terminal stark differenzieren. Eine Zertifizierung nach dem Zahlungsverkehrs-Standard „PCI-DSS“ setzt solche Datenverbindungen voraus, damit für das POS-Terminal nachfolgende Funktionen gegeben sind:

- Zentrales Management
- Monitorring
- Updatefunktion
- Zeitsynchronisation [32, pp. 1 - 4]

Geldfluss-Diagramm an einem POS-Terminal

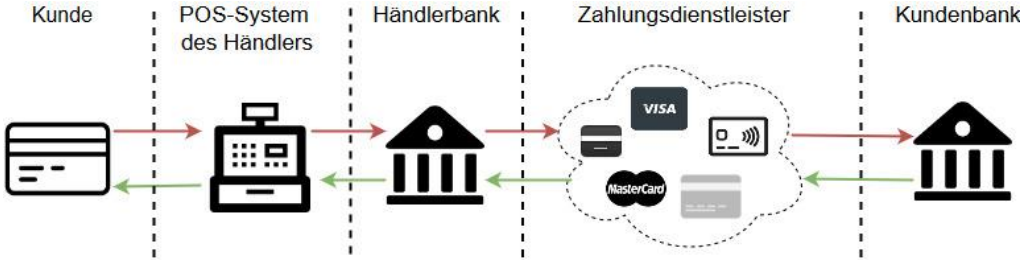

Abbildung 28 Geldfluss POS nach [32, p. 4]

- 1. Zuerst wählt der Kunde/die Kundin eine Karte für die Transaktion aus, die Zahlungsdaten werden im POS-System angenommen.
- 2. Diese (und der Token) werden anschließend an die Händlerbank übertragen.
- 3. Die Händlerbank überträgt nun den Zahlungsvorgang an das Zahlungsinstitut (z.B. MasterCard).
- 4. Dieses gibt die Transaktion an die Kundenbank weiter.
- 5. Die Kundenbank überprüft im letzten Schritt, ob die Zahlungsanfrage legitim ist (Karte ist nicht gestohlen, der/die Kunde/Kundin hat ausreichend Geldmittel etc.).
- 6. Die Kundenbank erstellt nun eine Autorisierungsnummer und sendet diese zurück an das Zahlungsinstitut.
- 7. Dieses sendet dieselbe Nummer an die Händlerbank, welche den angefangenen Zahlungsvorgang mit einer schriftlichen Bestätigung abschließt (Kassenbeleg/Zahlungsbeleg).

Je nachdem wie das Zahlungssystem architektonisch und technisch konzipiert wurde, existieren weitere technische Gegebenheiten für die gezielte Manipulation. Jedoch lassen sich vier Datenmanipulationsszenarien basierend auf diesem generischen Zahlungsvorgang erörtern:

- 1. Datenmanipulation im Arbeitsspeicher des Gerätes
- 2. Datenmanipulation bei der Ablage (temporär oder permanent)
- 3. Datenmanipulation auf dem Übertragungsweg
- 4. Die letzte Manipulationsmöglichkeit besteht direkt in der POS-Software, welche durch einen vorangegangenen Hackingangriff auf die POS-Terminal-Firma geschehen sein kann oder aber durch einen/eine Insider/in. [32, pp. 4 - 5]

Die derzeitig beschriebenen Funktionen eines POS-Terminal haben auch sehr starke Ähnlichkeit zu anderen Systemen wie:

- Kiosksysteme
- Ticketsysteme
- Hotelkarten
- Büroarbeitskarten
- Prepay-Zahlungskarten-Systeme

Jedoch unterscheiden sie sich jeweils in der Bedrohungslage und der Missbrauchswahrscheinlichkeit. Da die Abwicklung über die POS-Systeme im Allgemeinen immer eine Art von Zahlungsverkehr durchführt, stellen diese für Angreifer/innen ein lohnenswertes Ziel dar. Das geht sogar so weit, dass spezielle Schadsoftware für Zahlungs-POS entwickelt wurden. Die ersten Fälle derartiger Malware wurde um das Jahr 2010 bekannt und es werden im Jahresrhythmus neue Malwarevarianten solcher Art entdeckt. Viele POS-Geräte unterscheiden sich nicht von klassischen Arbeitsplatzstationen, daher bieten sie auch die dementsprechend identische oder größere Angriffsfläche. Ein POS-System kann demnach auch von schon geläufiger Malware infiziert werden, beispielsweise ein Verschlüsselungstrojaner, Keylogger, Cryptominer oder Ähnlichem. [33, pp. 1 - 4]

Angriffsmodelle für Hardwareschwachstellen

Abseits von Software Schwachstellen haben die Sicherheitslücken „Spectre“ und „Meltdown“ klar und deutlich gezeigt, dass auch Hardware von falschen designerischen Entscheidungen oder fehlerhaften Implementierungen betroffen sein kann und sich somit auf die Sicherheit auswirkten. Im Fall von „Spectre“ und „Meltdown“, waren die eingesetzten unsicheren Funktionen schon seit Jahrzehnten in den verschiedensten CPU Typen integriert und in Verwendung. Dabei war die Bandbreite von betroffenen Geräten sehr hoch und in den unterschiedlichsten Bereichen zu finden, so auch im Zahlungsverkehr.

Hardware-Sicherheitslücken können das Grundkonzept von Vertraulichkeit, Verfügbarkeit und Integrität beeinträchtigen. Solche tiefgreifenden Fehlfunktionen betreffen in der Regel auch die Thematik rund um den Zahlungsverkehr.

Hardware-Attacken auf das SE-Element

Mithilfe der Angriffsvektoren von „Spectre“ und „Meltdown“ besteht die theoretische Möglichkeit, Zugriff auf Daten im SE-Element zu erlangen. Damit können die vorhandenen Sicherheitsmechanismen, die sich bei Apple beispielsweise rund um das SE aufbauen, durchbrochen werden. Das betrifft nicht nur Smartphones, auch andere Plattformen, die ähnliche CPUs oder „System-on-a-Chip“[43]-Hardware benutzt haben, sind betroffen. In wie weit derzeit praktische Auswirkungen auf den Zahlungsverkehr verzeichnet werden können, ist nur schwer einzuschätzen. Es zeigt sich, dass es trotz aller Sicherheitszonen und Abstraktionsschichten immer wieder zu Sicherheitslücken auf Hardwareebene kommt.

Im Vergleich zu Softwareschwachstellen ist es jedoch schwieriger, Hardwarelücken zu finden und auch auszunutzen. In manchen Fällen wird auch spezielles Equipment benötigt, um die Hardwareschnittstellen der diversen Chips abzugreifen. Die Beschaffung und die Kosten für die genannte Spezialhardware ist dabei auch ein entscheidender Punkt. Oft stehen einem/einer Angreifer/in nicht die benötigten Mittel zur Verfügung, um derartige Schwachstellen zu identifizieren. Bekannt gewordene Schwachstellen auf Hardwareebene stellen jedoch eine große Bedrohung für Zahlensysteme dar, soweit es auch die passenden Exploits und Angriffsmuster dafür gibt. Sollte ein Schadcode einer solchen Hardwarelücke den „Massenmarkt“ erreichen, bevor es eine Korrektur des Herstellers gibt, kann mit finanziellen Einbüßen gerechnet werden. Ein ebenfalls großes Problem bei Hardware basierten Sicherheitslücken ist, dass die im Feld oder bei Kund/inn/en eingesetzten betroffenen Geräte ebenfalls ein Update oder gar einen Austausch benötigen. Sollten diese Geräte nicht über eine zentral gemanagte Schnittstelle verwaltet werden, stellt die Behebung der Sicherheitslücken ein ebenso großes logistisches Problem dar, das mit hohen Kosten gekoppelt ist. [34]

[43] SOC beschreibt ein minimales Computersystem, das eine geringe Bauform aufweist und auf einige wenige Aufgaben spezialisiert ist.

Fazit

Diese Masterarbeit befasst sich mit den modernen Anforderungen an digitalen Zahlungssysteme, die auf Grund ihrer Flexibilität und Modularität entstehen. Einer der wesentlichen zahlungsrelevanten Aspekte ist, dass alle drei Seiten, Endverbraucher/innen, Verkäufer/innen und Zahlungsanbieter, sicher sein müssen, damit die Transaktion im vorhergesehen Rahmen funktioniert. Der „vorhergesehene“ Rahmen liegt dabei ganz individuell auf dem jeweiligen Fokus des Zahlungsanbieters. Dieser stellt die grundlegenden Mechanismen zur Verfügung, die der/die Endverbraucher/in benutzt. Solche Konzepte sind aber bei weitem nicht perfekt und bieten aufgrund der schon dargestellten Flexibilität eine Vielzahl an möglichen Angriffsflächen. Die Angriffsmöglichkeiten sind sehr vielfältig und reichen von einfachen technischen Attacken wie Serviceunterbrechung, bis hin zu Übergriffen auf die eigentlichen Businessprozesse. Je nach Definition des Angriffsszenarios muss die Serviceanbieterseite mit unterschiedlichen Verteidigungsstrategien kontern. Der Serviceanbieter muss mit Attacken auf verschiedensten Ebenen rechnen und sollte im Vorfeld ganz klare Vorstellungen und Richtlinien zu seinem Zahlungsökosystem definieren, um diese im Vorfeld abzufedern. Je nach Strategie kommen bei der Sicherung des eigenen Ökosystems unterschiedliche Kernelemente zum Einsatz wie z.B. Cloud basiertes Computing oder die Ablage von zahlungsrelevanten Daten in einem eigenen geschützten Hardwarebereich. Aber auch andere Abstraktionsebenen, die auf Seite des Betriebssystems zur Verfügung gestellt werden, kommen zum Einsatz. Das Endgerät des Kunden/der Kundin hat daher einen maßgeblichen Einfluss auf das gesamte Zahlungskonstrukt. Die Entscheidungen des Anbieters können selbst entwickelte oder als sicher definierte Hardware darstellen, z.B. die Bankkarte oder aber eine Plattform die grundsätzlich unter dem Einflussbereich des Kunden/der Kundin steht, beispielweise das Smartphone oder die Smartwatch. Sollte es sich um das zweite Szenario handeln, die Verwendung von smarten Geräten, hat man viele bekannte Risiken und Angriffsmodelle aus der klassischen IT.

Außerdem kommen noch neue Funktionen hinzu, die dem/der Benutzer/in eine noch einfachere Interaktion mit dem Gerät bieten soll, die ausgenutzt werden können. Die ständige Anpassung an neue Gegebenheiten ist jedoch auch eine große Stärke solcher modularen Zahlungsansätze. Für den/die Benutzer/in sind die derzeit am Markt verbreitetsten Vertreter Google-Wallet und Apple-Pay eine gute Wahl. Sie bieten trotz unterschiedlicher Implementierungen ein sicheres und durchdachtes Grundkonzept. Das gewährleistet ihnen einen sicheren Geldtransfer auf technischer Ebene, ohne Einbußen an der gewünschten Flexibilität und Interaktionsmöglichkeit. Die weitere Integration in den Alltag, um eine möglichst breite Kundenbasis anzusprechen, stellt die nächste große Hürde für den regionalen oder globalen Durchbruch dar. Wie schnell sich eine solche neuartige Zahlungsmethode durchsetzt, ist von vielen weiteren Faktoren abhängig, die nicht von einer der vorgestellten Parteien beeinflusst werden können. Derzeit ist der Markt auch noch weit von der kompletten Abschaffung des Bargeldes entfernt.

Jedoch kann mit Spannung beobachtet werden, wie sich das Themengebiet der digitalen Zahlung anhand der vorliegenden Gegebenheiten in den nächsten Jahren entwickeln wird.

Was uns aber die vorgestellten Thesen und Angriffsmodelle deutlich zeigen, ist, dass es immer Schwachstellen geben kann, die beispielsweise in der Designphase nicht berücksichtigt wurden. Jedoch ist es entscheidend mit welcher Strategie und mit welchen Mitteln der Systemanbieter auf das neue Problem reagiert.

Literaturverzeichnis

[1] R. Contius und R. Martignoni, „Mobile Payment im Spannungsfeld von Ungewissheit und Notwendigkeit," BFS Finance, München, 2003.

[2] T. Trütsch , „Die Presse Online," Universität St. Gallen, 15 02 2016. [Online]. Available: https://diepresse.com/home/wirtschaft/oekonomenstimme/4926181/Wird-das-Bargeld-bestehen-bleiben. [Zugriff am 9 August 2018].

[3] OeNB, „Banknotenumlauf," OeNB, 2 8 2018. [Online]. Available: https://www.oenb.at/isaweb/report.do;jsessionid=7C824925A8F38541671072793E7D58AA?report=5.1.1 . [Zugriff am 9 August 2018].

[4] V. f. Konsumenteninformation, „Konsument.at," Verein für Konsumenteninformation, 05 04 2017. [Online]. Available: https://www.konsument.at/quick052017?pn=1. [Zugriff am 9 August 2018].

[5] „Paylife.at," Paylife, [Online]. Available: https://www.paylife.at/de/home/service/faq/quick-einstellung.html. [Zugriff am 9 August 2018].

[6] M. N. P. Jiménez, „ijsser.org," International Journal of Social Science and Economic Research, 2016. [Online]. Available: ijsser.org/uploads/ijsser_01__66.pdf. [Zugriff am 9 August 2018].

[7] E. Kazan und J. Damsgaard, „A Framework For Analyzing Digital Payment As A Multi-Sided Platform: A Study Of Three European NFC Solutions," Copenhagen Business School, 2013. [Online]. Available: https://www.researchgate.net/publication/256989677_A_Framework_For_Analyzing_Digital_Payment_As_A_Multi-Sided_Platform_A_Study_Of_Three_European_NFC_Solutions_2013_ECIS_2013_Proceedings_Paper_155?enrichId=rgreq-ca747e86e64e7d60edb44531f0328376-XXX&enrichS. [Zugriff am 9 August 2018].

[8] Y. Wang, C. Hahn und K. Sutrave, „Mobile Payment Security, Threats, and Challenges," Gainesville, 2016.

[9] T. Zefferer, Technologiebeobachtung "Konzepte und Umsetzungen NFC-Basierten Zahlungssystemen", Österreich, 2012.

[10] LSaranzaya, *NFC Tag Structure.PNG,* Attribution-ShareAlike 4.0 International CC BY-SA 4.0, 2016.

[11] E. Haselsteiner, Security in Near Field Communication (NFC) Workshop on RFID Security, Österreich: Semiconductors, Philips, 2006.

[12] „www.nfc-forum.org," [Online]. Available: https://nfc-forum.org/what-is-nfc/what-it-does/. [Zugriff am 9 August 2018].

[13] A. Serruya, „The Extent of Biohacking and Its Security Implications," Tufts University, Medford, The Extent of Biohacking and Its Security Implications.

[14] M. Maxim und D. Pollino, Wireless Security, McGraw-Hill, 2002.

[15] Church, Liam ; Moloney, Maria, „State of the Art for Near Field Communication: security and privacy within the field," Escher Group Ltd, Ireland, 2013.

[16] R. Michael , J. Langer und J. Scharinger, „Applying Relay Attacks to Google Wallet," NFC Research Lab Hagenberg, Zurich, 2013.

[17] I. Gurulian, C. Shepherd, K. Markantonakis, R. N. Akram und K. Mayes, „When Theory and Reality Collide: Demystifying the Effectiveness of Ambient Sensing for NFC-based Proximity Detection by Applying Relay Attack Data," Information Security Group, Smart Card Centre, Royal Holloway, University of London, 2016.

[18] M. Hansen, M. Hansen, M. Häuser, K. Janneck, H. Krasemann, M. Meints, S. Meissner, M. Raguse, M. Rost und J. Schallaböck, „Verkettung digitaler Identitäten," Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein, Kiel, 2007.

[19] A. Tobin und D. Reed, „The Inevitable Rise of Self-Sovereign Identity," Sovrin Foundation, 2017.

[20] E. Buchmann, „Datenschutz und Privatheit in vernetzten Informationssystemen," Karlsruhe Institute of Technology, Baden-Württemberg, 2011.

[21] J. Weber, „Identity Fraud Study Javelin Strategy & Research," Javelin, 6 Feb 2018. [Online]. Available: https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin. [Zugriff am 9 August 2018].

[22] D. Andersson, „A survey on contactless payment," Blekinge Institute of Technology, Karlskrona, 2016.

[23] „Bankomatkarte-mobil.at," PSA Payment Services Austria GmbH, [Online]. Available: https://www.bankomatkarte-mobil.at/faq-fragen-rund-um-das-android-smartphone-und-die-nfc-sim-karte/#toggle-id-6. [Zugriff am 9 August 2018].

[24] PCI Security Standards Council, „Tokenization Product Security Guidelines," PCI Security Standards Council, 2015.

[25] European Union Agency For Network and Information, „Security of Mobile Payments and Digital Wallets," European Union Agency For Network and Information, 2016.

[26] BSI - Bundesamt für Sicherheit in der Informationstechnik, „Bundesamt für Sicherheit in der Informationstechnik," 2011. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html. [Zugriff am 9 August 2018].

[27] OWASP Mobile Security Project - Mobile Threat Model, „Open Web Application Security Project - OWASP," 2013. [Online]. Available: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Mobile_Threat_Model/Releases/Current. [Zugriff am 9 August 2018].

[28] OWASP Mobile Security Project, „Open Web Application Security Project - OWASP," 2016. [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks. [Zugriff am 18 Juli 2018].

[29] Kaspersky Lab, „Mobile Fingerabdrucksensoren: sicher oder unsicher?," 2016. [Online]. Available: https://www.kaspersky.de/blog/fingerprints-sensors-security/6785/. [Zugriff am 9 August 2018].

[30] Y. Zhou und X. Jiang, „Dissecting Android Malware: Characterization and Evolution," IEEE Symposium, North Carolina, 2012.

[31] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang und W. Xu, „DolphinAttack: Inaudible Voice Commands," Zhejiang, 2017.

[32] R. J. Rodriguez, „Evolution and Characterization of Point-of-Sale RAM Scraping Malware," in *Journal of Computer Virology and Hacking Techniques*, Zaragoza, Spain, Springer, 2016.

[33] Kaspersky Enterprise Cybersecurity, „Point of Sale als Angriffsfläche: Bedrohungen für POS-Systeme," 2017. [Online]. Available: https://media.kaspersky.com/de/business-security/enterprise/KESS_POS_Threats_Whitepaper_DE.pdf. [Zugriff am 09 August 2018].

[34] G. Bouffard und D. El-Baze, „SoC, why should we care about Fault Injection Attacks ?," ANSSI, Paris, 2018.

[35] Apple, „https://support.apple.com/," Apple, 26 April 2018. [Online]. Available: https://support.apple.com/en-us/HT208531. [Zugriff am 07 Juni 2018].

[36] I. Muslukhov, „Survey: Data Protection in Smartphones Against Physical," The University of British Columbia Department of Electrical and Computer Engineering, British Columbia, 2015.