

Hochschule Worms
Fachbereich Informatik
Studiengang Angewandte Informatik B.Sc.

**Gewährleistung von sicherem digitalen Bezahlen bei
einem Click-and-Buy-Automat**

Exposé für Wissenschaftliches Arbeiten

Bruno Macedo da Silva	Dominic Meyer
676839	676839
inf3645@hs-worms.de	inf3644@hs-wrosm.de
Bebelstraße 22 Z18	Im Langreh 6
67549 Worms	55294 Bodenheim

Betreuer	Michael Derek Werle-Rutter
Bearbeitungszeitraum:	Wintersemester 2021/2022
Abgabedatum:	8.Februar 2022

Inhaltsverzeichnis

Abkürzungsverzeichnis	5
1 Einführung	6
2 Forschungsziele	9
2.1 IT-Sicherheitsziel: Verfügbarkeit	9
2.2 User-Experience	10
2.3 IT-Sicherheitsziel: Vertraulichkeit	11
3 Stand der Forschung	13
3.1 Chancen und Risiken vom bargeldlosen Bezahlen	13
3.2 IT-Schutzziele vom bargeldlosen Zahlungsverfahren	15
4 Stand der Technik	19
4.1 Drahtlose Verbindungen und Sicherheit bei Bezahlungen	19
4.1.1 Angriffsmöglichkeit auf NFC	19
4.1.2 Gegenmaßnahmen für die Härtung von drahtlose Ver- bindung	20
4.2 Anwendung von Smartcards und sicheres Bezahlen	21
4.2.1 Angriffsmöglichkeit auf Smartcards	22
4.2.2 Gegenmaßnahmen für die Härtung von Smartcards	22
4.3 Fazit	23
5 Forschungsplan	24
5.1 Interview mit Click-and-Buy-Automat Firma	25
5.2 Durchführung von Experimenten	27
5.2.1 Angriffe und Härtungsmaßnahmen eines drahtlosen Ser- vers	28
5.2.2 Erwartete Beobachtung von Angriffsmöglichkeiten auf einen drahtlosen Servers	29

5.2.3	Angriff und Härungsmaßnahme von Smartcard	30
5.2.4	Erwartete Beobachtung von Angriffsmöglichkeiten von Smartcard	30
5.3	Literaturrecherche	31
6	Praktische Relevanz	32
	Literaturverzeichnis	34

Abbildungsverzeichnis

1	Neuzulassungen von Caravans und Reisemobilen (2013-2020)	
	Quelle: Graefe, 2021c	6
2	Forschungsfrage	
	Quelle: eigene Darstellung	8
3	Altergruppe von Campingurlauber*innen im Jahr 2019	
	Quelle: Graefe, 2019	11
4	Bargeldlose Zahlung über die Deutsche Bundesbank	
	Quelle: Bundesbank, 2009, S.52	14
5	Sicherheitseigenschaften von digitalen Zahlungsmethode	
	Quelle: Hassan et al. 2020, S8	15
6	Abbildung des Zahlungsverfahrens	
	Quelle: Isaac and Zeadally, 2012	16
7	Nachrichtenflussaustausch	
	Quelle: Isaac and Zeadally, 2012	17
8	Teilnehmer der Kommunikation über NFC	
	Quelle: Proehl, 2021	19
9	Eine Smartcard und deren eingebettete Mikrochip	
	Quelle: eigene Darstellung	21
10	Authentifizierungsprozess von Smartcards	
	Quelle: Tanenbaum, 2009, S.755	21
11	Forschungsdiagramm	
	Quelle: eigene Darstellung	25
12	Ein Beispiel von Distributed-Denial-of-Service (DDoS) mit mehreren Leerlauf-Maschinen	
	Quelle: Durcekova et al., 2012	29
13	Ausgabe von Wireshark	
	Quelle: Wireshark, 2021	30

Abkürzungsverzeichnis

CBA Click-and-Buy-Automat.

DDoS Distributed-Denial-of-Service.

EHI Handelsforschungsinstituts.

NFC Near Field Communication.

Nmap Network Mapper.

PIN Persönliche Identifikationsnummer.

TCP/IP Transmission Control Protocol/Internet Protocol.

UML Unified Modeling Language.

1 Einführung

Seit einigen Jahren entscheiden sich immer mehr Menschen Urlaub auf einem Campingplatz zu machen [Graefe, 2021a]. Der Gedanke an Menschenmassen und Fallen für Touristen schreckt die Leute von den typischen Touristenzielen ab. Zudem ist der Kontakt zu der Natur für viele ein wichtiger Teil in einem Urlaub. In den letzten anderthalb Jahren stieg die Anzahl von Campingplatzbesuchern rasant [Graefe, 2021c]. Die Corona-Pandemie drängte die Leute dazu, Urlaubsmöglichkeiten zu suchen, bei denen das Risiko von einer Infektion niedrig sei und wo genug Abstand gehalten werden könne [Graefe, 2021b]. Da viele Hotels und andere Ferieneinrichtungen geschlossen waren, blieb vielen Leuten, besonders Familien, nichts anderes übrig, als die Ferien etwas anders zu organisieren und gestalten

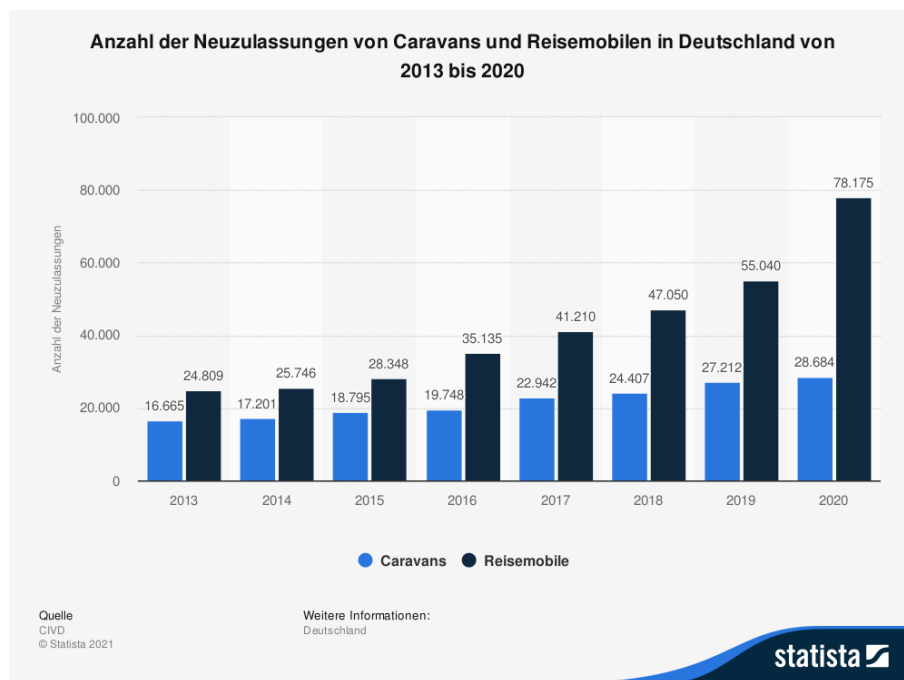


Abbildung 1: Neuzulassungen von Caravans und Reisemobilen (2013-2020)

Quelle: Graefe, 2021c

Die traditionelle Idee von Campingplätzen, bei der Jugendliche oder Familien weit entfernt von der Gesellschaft sind, ist heute eine andere. Heute wollen Urlauber auf den Kontakt mit der Natur möglichst nicht verzichten, wodurch Campingplätze immer voller werden. Aus diesem Grund wäre es sinnvoll, die Möglichkeiten zur Grundversorgung zu erweitern, ohne direkt einen neuen Supermarkt bauen zu müssen. In dieser Hinsicht kann die Einrichtung eines elektronischen Click-and-Buy-Automat (CBA)¹, der mit einem Automaten zu vergleichen ist, eine wesentliche Rolle spielen, um einen Campingplatz und die Gegend drum herum zu modernisieren, die Möglichkeiten zur Grundversorgung zu erweitern und ihn attraktiver für Reisende und die Leute auf dem Land zu machen.

Da die Errichtung eines solch Automaten aus verschiedene Bestandteilen besteht, wie die Verkabelung für den Netzwerkzugang, der physischer Aufbau für den Automat und die Software für den Kundenzugang, konzentrieren wir uns hier auf mögliche Zahlungsverfahren für unseren Automaten. Die Sicherheit der digitalen Zahlungsmethoden stellt eine der wichtigsten Herausforderung für die Entwicklung eines solchen Systems dar. Vernachlässigungen in diesem Bereich führen auf der einen Seite zu unberechenbarem Vertrauensverlust seitens der potenziellen Nutzenden und auf der anderen Seite zu finanziellen und moralischen Schäden der direkten Stakeholder. Die geplante Wissenschaftliche Arbeit soll folgende Frage behandeln: Wie kann sicheres bargeldloses Bezahlen

¹Die Waren werden online bezahlt und zu einem gewünschten Zeitpunkt können sie abgeholt werden [Ghosh and C., 2014].

in einem CBA gewährleistet werden?

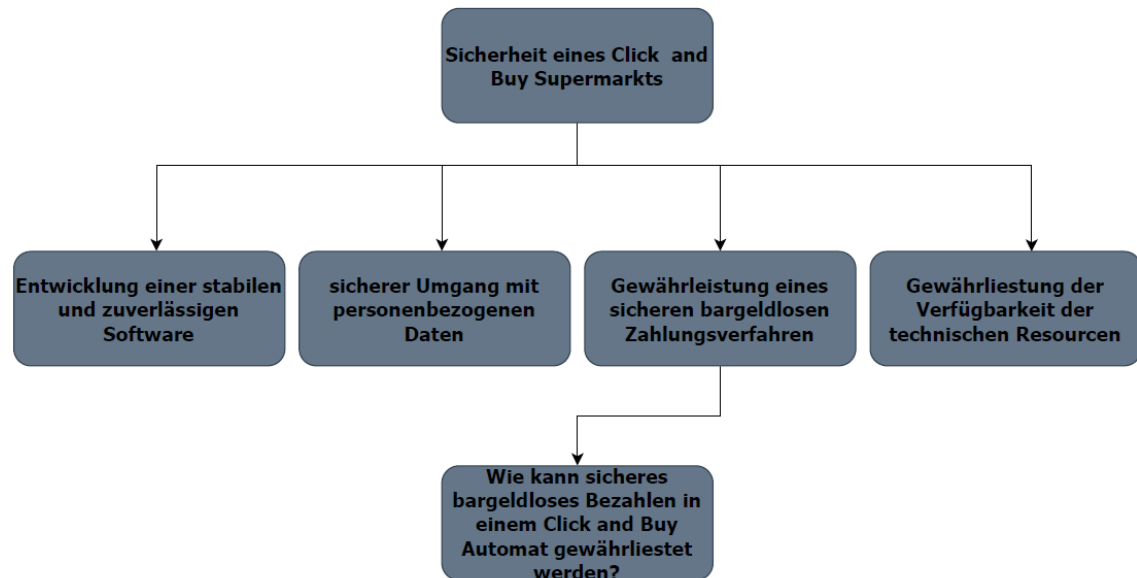


Abbildung 2: Forschungsfrage

Quelle: eigene Darstellung

2 Forschungsziele

In der geplanten Wissenschaftlichen Arbeit, soll ein Konzept für ein sicheres Zahlungsverfahren für einen CBA neben einem Campingplatz entwickelt werden. Solch ein Konzept kann dazu beitragen, dass Campingplätze und die Gegend modernisiert werden und noch mehr Touristen angelockt werden. Bevor das Projekt jedoch umgesetzt werden kann, müssen noch wichtige Dinge beleuchtet werden.

Der Zugang zum Netzwerk über das Glasfaser sollte immer gewährleistet werden, eine stabile Software, die den Qualitätsstandards entspricht, ein sicherer Umgang mit Kundendaten, der sich an spezifischen und internationalen Richtlinien² orientiert, ein benutzerfreundliches System, das sich an verschiedenen Kundentypen, wie Alters- und Bildungsgruppe anpasst und letztlich ein kryptographisches Verfahren³ für das bargeldlose Bezahlen, das die Vertraulichkeit sicherstellt.

2.1 IT-Sicherheitsziel: Verfügbarkeit

Um die Verfügbarkeit des Netzwerkzugangs für den CBA zu gewährleisten, muss zum einen geprüft werden, ob die bereits vorhandenen Leitungen ausreichen, um dieses Projekt umsetzen zu können. Die Vernetzung soll so aufgebaut sein, dass es auch in Regionen einwandfrei funktioniert, wo die Infrastruktur nicht so ausgeprägt ist, wie in der Stadt.

Die Software muss zudem so entwickelt werden, sodass diese eine geringe Ausfallquote aufweist, denn der Automat soll rund um die Uhr betriebsbereit sein, um das Ziel der Verfügbarkeit des Systems nicht zu verletzen [Wendzel, 2018].

²Es gibt Regeln, die aussagen, was mit personenbezogenen Daten passieren darf und was nicht [Datenschutz, 2021].

³Mit Hilfe kryptographischer Verfahren, wie Verschlüsselung, sollen Daten vor unbefugtem Zugriff geschützt und sicher ausgetauscht werden [Luber and Schmitz, 2017].

2.2 User-Experience

Zudem soll das System so entwickelt werden, sodass auch Digital Non-Natives⁴, die Möglichkeit [Wang et al., 2013] haben das System einfach bedienen zu können. Die Kunden sollten also nicht von Informationen überladen werden, sondern es sollte einfache Ein- und Ausgaben geben. Eine Umfrage aus dem Jahr 2019 [Graefe, 2019] zeigt, dass sich besonderes ältere Menschen [Graefe, 2019] für solch eine Urlaubsmöglichkeit entscheiden. Das spielt für den Erfolg des Konzeptes eine entscheidende Rolle, dass auch sie mit dem Automat umgehen können. Deshalb sollten die Bedürfnisse und Einschränkungen dieser Altersgruppe besonders berücksichtigt werden, um ihr Vertrauen zu gewinnen [Lübbecke, 2018] und hauptsächlich gegen Social-Engineering⁵ Angriffe zu schützen. Die Auswahl der Tests trägt dazu bei, dass die Zufriedenheit und die Akzeptanz gewährleistet wird, sodass jeder potenziellen Endnutzer das System bedienen kann [Sommerville, 2010].

⁴Bezeichnet eine Person, die in der Kindheit ohne Informationstechnologien und ohne dem Internet aufgewachsen ist und eine Welt mit digitalen Medien nicht kennt [Siepermann, 2018].

⁵Beim Social-Engineering nutzt der Täter den “Faktor Mensch” als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.[Bundesamt für Sicherheit in der Informationstechnik, 2020]

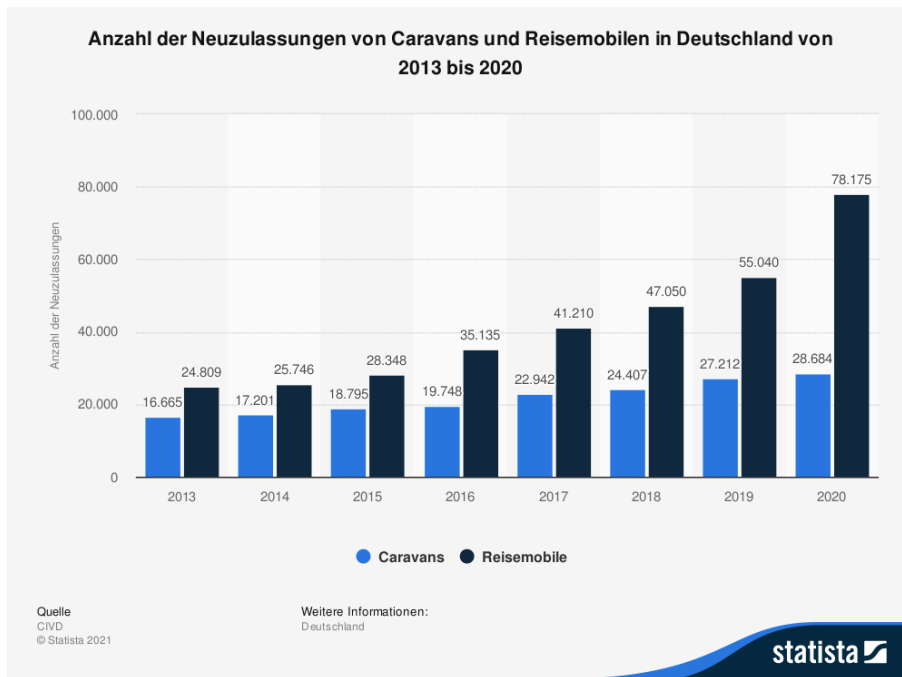


Abbildung 3: Altergruppe von Campingurlaubern im Jahr 2019

Quelle: Graefe, 2019

Außerdem spielt die Sicherheit bei den bargeldlosen Zahlungsvorgängen eine große Rolle und sollte deshalb höchste Priorität haben. Verschiedene aktuelle Beispiele von Cyberangriffen zeigen, dass der Umgang mit solchen Daten, kritisch zu sehen ist [Bundeskriminalamt, 2020].

2.3 IT-Sicherheitsziel: Vertraulichkeit

Es wird oft von Situationen in den Medien berichtet, bei denen Kunden ihr Geld verloren haben oder dessen personenbezogenen Daten missbraucht wurden. In seltenen Fällen sogar von der eigenen Regierung, weil das System nicht ausreichend gegen Angriffe geschützt wurde. In dieser Hinsicht sollten bei der Entwicklung spezifische und klare Richtlinien berücksichtigt werden, sodass der sichere Umgang mit personenbezogenen Daten gewährleistet ist

[Riebe et al., 2020]. Um diese Vertraulichkeitsverletzung zu vermeiden, spielt die Konzipierung von sicheren bargeldlosen Zahlungsmethoden eine wesentliche Rolle in diesem Artikel.

3 Stand der Forschung

In dem Transmission Control Protocol/Internet Protocol (TCP/IP)⁶ ist die Sicherheit ein sehr umfangreiches Thema, das sehr viele Facetten besitzt.

Das Thema beschäftigt sich mit physikalischen Komponenten, wie zum Beispiel der Verkabelung und Antennen oder auch mit abstrakten, wie logische Adressierung oder Übertragung von Signalen. Die meisten Elemente, die zum Oberbegriff Netzwerk gehören, spielen eine wesentliche Rolle für die Gewährleistung der Netzwerkschutzziele⁷. Im folgenden Abschnitt konzentrieren wir uns auf die Gewährleistung von Netzwerkschutzzielen bei bargeldlosen Zahlungsverfahren. Zu Beginn geben wir eine kurze Einleitung über die Entwicklung von bargeldlosen Zahlungsmethoden in Deutschland.

3.1 Chancen und Risiken vom bargeldlosen Bezahlen

Die zunehmende Tendenz in Deutschland von bargeldloser Bezahlung erfordert neuen Umgang mit den eingegebenen Daten. Eine Studie von 2009 der Deutschen Bundesbank zeigte den rasanten Anstieg von bargeldloser Bezahlung in der Bundesrepublik seit der Einführung von solchen Zahlungsmethoden [Bundesbank, 2009].

⁶Die TCP/IPProtokollfamilie bezieht sich auf die Aufteilung der verschiedenen Ebenen der Diensten und Regel, die in der Netzkommunikation existieren [Wendzel, 2018].

⁷Die Netzwerkschutzziele oder IT-Schutzziele sind internationalen Zielen, die in dem Netzbereich erreicht werden sollen. Diese Ziele sind Vertraulichkeit, Integrität und Authentizität.

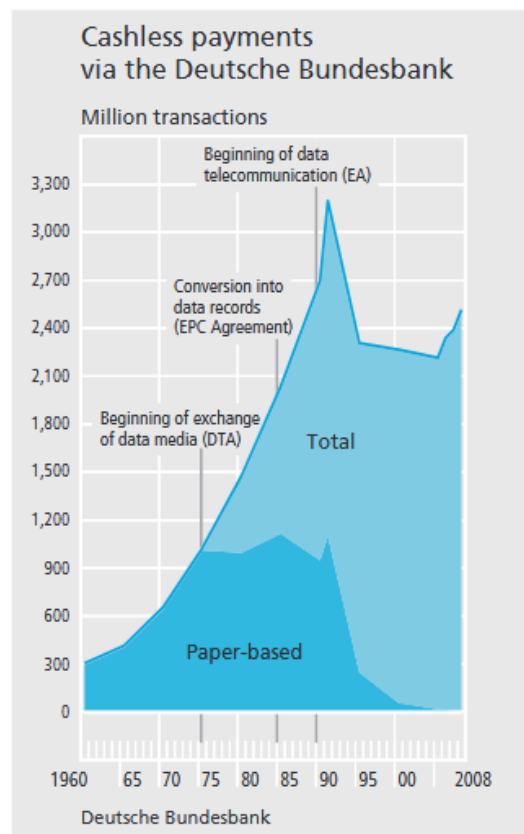


Abbildung 4: Bargeldlose Zahlung über die Deutsche Bundesbank

Quelle: Bundesbank, 2009, S.52

Laut einer Statistik des Handelsforschungsinstituts (EHI) von 2019 bezahlen 48,6% der deutschen ihre Waren mit Karte, wohingegen nur noch 46,9% der deutschen den klassischen Weg über Bargeld gehen [Seibel, 2019]. Auch das kontaktlose Bezahlen, bei dem kleine Beträge nicht einmal mit einer Persönliche Identifikationsnummer (PIN) bestätigt werden müssen, nimmt immer weiter zu. Doch gerade bei dieser Variante ist es sehr einfach im Namen eines anderen zu bezahlen, was eine Sicherheitsrisiko darstellt. Diese Tendenz wurde auch von [Dahlberg et al., 2008] in seiner Studie beobachtet, bei der er die meist verbreiteten Zahlungsarten in verschiedenen Regionen dieser Welt vergleicht.

Immer wenn mit Karte bezahlt wird, gehen die Kunden davon aus, dass die Zahlungsabwicklung sicher ist. Wie sicher ist das bargeldlose Zahlen heutzutage wirklich?

3.2 IT-Schutzziele vom bargeldlosen Zahlungsverfahren

Vertraulichkeit ist die erste und wichtigste Voraussetzung, das ein solches Zahlungssystem erfüllen muss, um neue potenzielle Kunden zu gewinnen. Unter dem Begriff Vertraulichkeit verstehen wir, dass es keine unautorisierte Informationsgewinnung gibt [Wendzel, 2018]. In dieser Hinsicht sollte ein CBA so konzipiert werden, dass er einen sicheren Umgang mit den Kundendaten anbietet. Die Interaktion zwischen einem Kunden und systemkritischen Mechanismen wurde von [Hassan et al., 2020] so dargestellt:

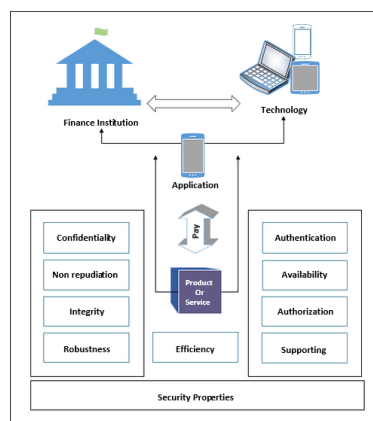


Abbildung 5: Sicherheitseigenschaften von digitalen Zahlungsmethode
Quelle: Hassan et al. 2020, S8

[Isaac and Zeadally, 2012] beschreibt didaktisch ein Zahlungsverfahren, dass die Vertraulichkeit gewährleisten kann. Dieses findet in verschiedenen 2 getrennten Schritten statt.

Im ersten Schritt sendet der Nutzer seinen Namen. Es wird da einen einen Sitzungsschlüssel generiert und eine Anfrage für die Transaktion wird gesendet.

Diese Anfrage wird daraufhin an den Händler geschickt, der diese wiederum bearbeitet. Nachdem das abgeschlossen wurde, sendet der Händler seine Antwort an das Bezahlgerät, das wiederum die Antwort an den Nutzer weiterleitet.

Im zweiten Schritt wird die Bezahl Anfrage an das Bezahlgerät gesendet, die unter anderem den Preis und die Uhrzeit enthält. Das Bezahlgerät leitet die empfangene Nachricht an den Händler weiter. Dieser empfängt die Daten und prüft auf Aktualität der Daten. Wenn dieser Test erfolgreich ist, wird wieder eine Nachricht an das Bezahlgerät geschickt. Dieses schickt die Daten dann wiederum an die Bank, welche überprüft, ob das Geld von dem Konto abgebucht werden kann. Wenn das geprüft wurde, wird eine Nachricht an das Bezahlgerät gesendet, in der steht, dass das Geld abgebucht wurde.

Besonders wichtig ist, dass bei jeder Kommunikation die Daten kryptographisch verschlüsselt werden, sodass es einem potenziellen Angreifer nicht möglich ist, Daten zu ändern oder zu entschlüsseln. In den folgenden Abbildungen wird das oben beschriebene Verfahren dargestellt:

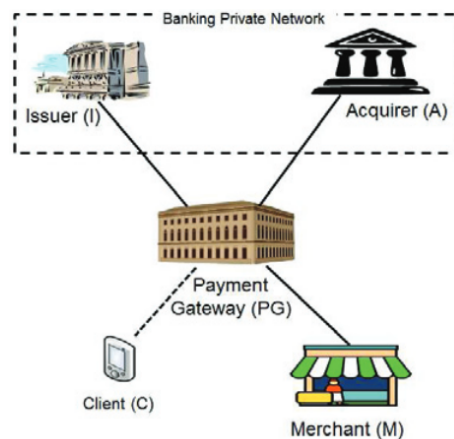


Abbildung 6: Abbildung des Zahlungsverfahrens

Quelle: Isaac and Zeadally, 2012

Das folgende Sequenzdiagramm⁸ stellt den Nachrichtenaustausch zwischen den Elementen dieser Zahlungsmethode dar:

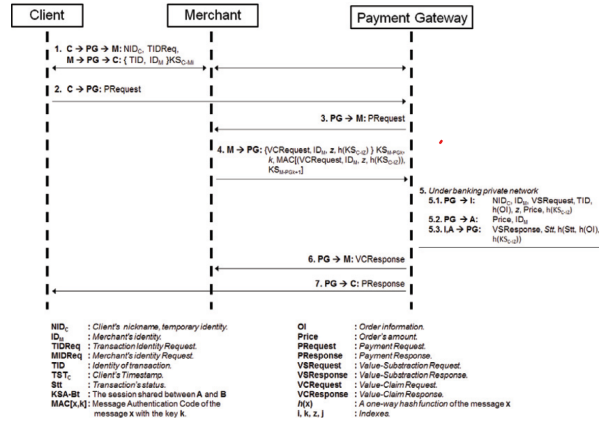


Abbildung 7: Nachrichtenaustausch

Quelle: Isaac and Zeadally, 2012

Zudem sollten die weiteren Schutzziele der IT-Sicherheit: Integrität und Authentizität berücksichtigt werden, sodass das Zahlungssystem einwandfrei und sicher funktioniert [Me, 2003]. Eine Zahlungsmethode, bei der alle Voraussetzungen erfüllt werden, kann in der Lage sein, das Vertrauen und die Akzeptanz von den Nutzenden zu bekommen [Hassan et al., 2020]. Besonders im deutschen Markt, spielen die oben genannten Schutzziele eine wesentliche Rolle für die Akzeptanz von neuen unbekannten Systemen [Khodawandi et al., 2003].

Da wir hier von einem dynamischen und breiten Bereich reden, bei dem es sehr schnell zu Änderungen kommen kann, besonders bei den Angriffstechniken, müssen die dazu gehörigen Technologien stets weiterentwickelt und angepasst werden [Yildirim and Varol, 2019], um Vertraulichkeitsverlust seitens der Kunden zu vermeiden. Da die Vertraulichkeit noch nicht zu 100 Prozent

⁸Ein Sequenzdiagramm ist ein Verhaltensdiagramm, welches eine Interaktion im Sinne der Unified Modeling Language (UML) grafisch darstellt [Sommerville, 2010].

gewähleistet werden kann, verweigern viele Kunden das bargeldlose Bezahlen. Aber wird es jemals eine 100 prozentige Sicherheit geben?

Viele Studien befassen sich mit den verschiedenen Aspekten der Sicherheit bei bargeldlosen Zahlungsmethoden. Da die Literatur dieses Forschungsfeldes sehr umfangreich ist und da dieses Thema sehr Vielfältig ist [Me, 2003], sollen hier zwei dieser Technologien in Bezug auf Angriffstechniken und Gegenmaßnahmen genauer betrachtet werden: drahtlose Verbindungen mit Near Field Communication (NFC)⁹ und Smartcards¹⁰.

⁹Near Field Communication (NFC) ist eine auf Radio Frequenz basierte Technologie, die der kabellose Austausch von Nachrichten in kürzer Distanz, zwischen vier und zehn cm, zwischen elektronischen Gerät, wie Handys, Computer, ermöglicht [Singh, 2020].

¹⁰Der Begriff Smartcards bezeichnet eine Plastikkarte mit einem eingebauten Chip, der ein eigenes Betriebssystem, einen Mikroprozessor und minimale Funktionalitäten besitzt [Farrell, 1996].

4 Stand der Technik

Für die Bezahlungsmethoden werden hier zwei verschiedene Arten von Zahlungsverfahren analysiert und deren Vorteile in Bezug auf Sicherheit und Härungsmaßnahmen dargestellt: drahtlose Zahlung mit und Smartcards.

4.1 Drahtlose Verbindungen und Sicherheit bei Bezahlungen

Viele digitale Zahlungen finden über NFC statt. Diese Technologie ermöglicht ein Zahlungs- und Identifizierungsverfahren, indem ein passives Gerät oder auch Tag genannt mit einem aktiven Gerät, auch Ermitter genannt, kommuniziert. In dieser Situation will das passive Gerät eine Autorisierung initiieren, während das aktive Gerät für die Erlaubnis zuständig ist [Singh, 2020].

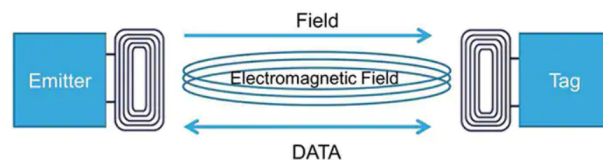


Abbildung 8: Teilnehmer der Kommunikation über NFC

Quelle: Proehl, 2021

4.1.1 Angriffsmöglichkeit auf NFC

Da diese Technologie neu ist [Tabet and Ayu, 2016], sie existiert seit 2006, sind Schwachstellen und Härungsmaßnahmen nicht in ihrer Vollständigkeit bekannt. Drahtlose Verbindungen sind auch für ihre Schattenseite bekannt [Yildirim and Varol, 2019]. Maßnahmen zu entwickeln, die sich an verschiedene Systeme anpassen, kosten Zeit und Investitionen von Banken und Sicherheitsfirmen. Für jeden möglichen Angriffe müssten Gegenmaßnahmen existieren, sodass das Schutzziel der Integrität¹¹ nicht verletzt wird.

¹¹Es ist Subjekten nicht möglich, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren [Wendzel, 2018].

Bekannte Angriffe für kabellose Verbindungen können auch bei NFC verwendet werden[Yildirim and Varol, 2019], wie die Erstellung und das Hinzufügen von Dateien in einem Opfersystem mit umfangreichen Privilegien; die Konzipierung von schwachen digitalen Zertifikaten oder auch die Verwendung von Reverse Engineering¹². [Alrawais, 2020] hebt andere Schwachstellen hervor: *Eavesdropping*¹³ je nachdem, wie viele Ressourcen investiert werden, kann ein Angreifer in der Lage sein, der Kommunikation zu lauschen; Distributed-Denial-of-Service (DDoS)¹⁴, um die Authentifizierung und Verfügbarkeit der Kommunikation zu beeinträchtigen.

4.1.2 Gegenmaßnahmen für die Härtung von drahtlose Verbindung

Um die Risiken bei der Verwendung von NFC zu abschwächen, schlägt [Yildirim and Varol, 2019] einige Sicherheitsmechanismen vor, die sich eher auf allgemeine drahtlose Verbindungen beziehen und die auch für NFC verwendet werden können: Nutzung von modernen kryptographischen Standards für die Validierung von Zertifikaten; Verwendung von Zwei-Faktor- Authentifizierung; Erstellung von schwer zu erratenden Passwörtern; Registrierung von autorisierten Geräten; Einsetzung von künstlicher Intelligenz (KI) für die Detektion von abweichendem Verhalten; Kontrolle gegen Social Engineering

15

Kredit- und EC-Karten sollen auch als Zahlungsmittel bei unserem CBA ak-

¹²Reverse Engineering ist ein Prozess von der Identifizierung von Bestandteilen eines Systems und von die Wiederherstellung dieser in einem anderen Format [Chikofsky and Cross, 1990]. Im Bereich der Cybersicherheit wird Reverse Engineering verwendet, um Schwachstellen von Systemen zu entdecken, sodass diese gegen Hardware und Software ausgenutzt werden können [Matthies et al., 2015].

¹³Eavesdropping ist das unautorisierte Mithören von einer Kommunikation [Wendzel, 2018].

¹⁴Bei solchen Angriffen wird die Verfügbarkeit des Dienstes verletzt, sodass die Kommunikation nicht mehr einwandfrei funktioniert [Wendzel, 2018]. In diesem Fall findet dieser Angriff mithilfe vieler Quellen statt, die von dem Angreifer ferngesteuert sind.

¹⁵Beim Social Engineering nutzt der Täter den "Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus, um seine kriminelle Absicht zu verwirklichen.[Bundesamt für Sicherheit in der Informationstechnik, 2020]

zeptiert werden. In Bezug auf diese Zahlungsmittel, wird die Sicherheit im folgenden untersucht.

4.2 Anwendung von Smartcards und sicheres Bezahlen

Smartcards sind heutzutage stark verbreitet für eine Zahlungsabwicklung und auch für die Identifizierung. Viele Ausweise, wie der Reisepass und die Krankenkassenkarte, verwenden diese Technologie zur Authentifizierung des Nutzens. Im folgenden ist ein Beispiel von einer Smartcard für eine zahlende Karte zu sehen:

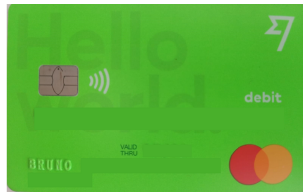


Abbildung 9: Eine Smartcard und deren eingebettete Mikrochip

Quelle: eigene Darstellung

Die Smartcard wurde vor mehr als 40 Jahren erfunden und ihr Ziel ist die Sicherheit von Kartenzahlungen und allgemeine Authentifizierungsverfahren zu erhöhen [Farrell, 1996]. Sie unterscheiden sich von traditionellen Magnetstreifenkarten, weil sie verschiedene Authentifizierungsmethoden ermöglichen auch ohne eine direkte Verbindung zur Bank [Tanenbaum, 2009]. Im folgenden wird der Authentifizierungsprozess einer Smartcard 10 dargestellt.

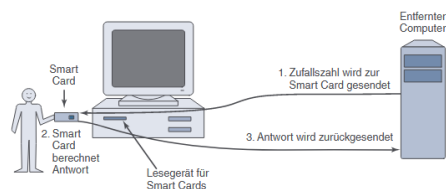


Abbildung 10: Authentifizierungsprozess von Smartcards

Quelle: Tanenbaum, 2009, S.755

Die meisten Angriffe bei Smartcards geschehen laut [Steffen, 2012] auf Hardwareebene. Er beschreibt folgende Techniken für Angriffe: Protokollanalyse, bei schwacher Konzipierung oder mangelnder Verschlüsselung ermöglichen Zugang zum Klartext; Hardware Reverse Engineering: Verständnis über die Algorithmen oder Extrahieren des Schlüssels

4.2.1 Angriffsmöglichkeit auf Smartcards

Smartcards sind auf Hardwareebene extrem sicher. [Steffen, 2012] bezeichnet sie auch als ein in Hardware gegossener Tresor für Informationen. Wenn eine Smartcard für das Bezahlen verwendet wird, ist kein Backend-System nötig, denn alle wichtigen Informationen wie das Guthaben sind direkt auf der Karte gespeichert. Aus diesem Grund können keine Daten abgefangen werden, die auf dem Weg vom Lesegerät zum Backend-System sind, was den Bezahlprozess deutlich sicherer macht [Rankl and Effing, 2002]. Zudem muss jede Kommunikation vom Lesegerät initiiert werden, die Karte selber startet also keine Kommunikation. Da die wichtigsten Daten direkt auf der Karte gespeichert sind, muss ein Angriff auf die Hardware initiiert werden, um an relevante Informationen zu gelangen. Eine weitere Möglichkeit wäre, die Schwachstellen eines bestimmten Protokolls, das für die Kommunikation verwendet wird auszunutzen.

4.2.2 Gegenmaßnahmen für die Härtung von Smartcards

Um einen Angriff auf die Hardware möglichst zu vermeiden, ist es sinnvoll den Chip nicht rekonstruierbar zu machen, d.h. dass keine Standardzellen oder ähnliches verwendet werden. Zusätzlich spielt die Verschlüsselung der Daten eine große Rolle und erhöht die Sicherheit enorm [Rohr et al., 2010]. Außerdem können Mechanismen in die Smartcard eingebaut werden, die permanent die Spannung oder Frequenz überprüfen und sobald etwas nicht dem

Normalzustand entspricht, wird der Chip ausgeschaltet, sodass kein Lesegerät mit der Karte kommunizieren kann. Letztlich ist es wichtig, dass jede Karte individuell ist, sodass ein erfolgreicher Angriff kein Sicherheitsrisiko für andere Karten darstellt [Steffen, 2012]. Dazu wären asymmetrische Verschlüsselungsverfahren sinnvoller als symmetrische, da jede Karte bei asymmetrischer Verschlüsselung einen öffentlichen und privaten Schlüssel hat und somit alle einen unterschiedlichen Schlüssel haben.

4.3 Fazit

NFC ist eine Technologie die viele Vorteile bietet. Sie ermöglicht in nur einem Gerät die Anwendung verschiedener Aktivitäten, wie Zahlung, Identifizierung und Authentifizierung, ohne dass ein Nutzer unterschiedliche Karten bei sich haben muss. Die Nachteile beziehen sich auf die Neuigkeit dieser Technologie, die mehr Forschung verlangt, damit deren Schwachstellen weiter erforscht werden [Alrawais, 2020]. Die Technologie der Smartcards ist bereits breit erforscht, sodass sowohl Schwachstellen, als auch Härungsmaßnahmen bekannt sind. Die Akzeptanz und die Verwendung von Smartcards sind auch größer, da besonders Non-Natives eher auf Smartcards zurückgreifen.

Aus den obigen genannten Gründen können wir sagen, dass Smartcards der bessere Einsatz für einen CBA neben einem Campingplatz wäre, solange die Technologie von NFC noch nicht so weit erforscht ist und in der Gesellschaft nicht so etabliert ist.

5 Forschungsplan

Das Thema Netzwerksicherheit beinhaltet viele Forschungsrichtungen, die zu umfangreich für eine einfache Recherche sind. Aus diesem Grund und aus Knappheit von Platz, konzentrieren wir uns in der geplanten wissenschaftlichen Arbeit auf zwei spezifische Aspekte dieses Themas, und zwar auf Schwachstellen und auf Härtingsmaßnahmen von NFC und von Smartcards. Die verwendeten Methoden dieser Untersuchung sollen sowohl quantitative als auch qualitative Daten hervorheben [Lazar et al., 2009], die dabei helfen sollen, die Sicherheitsmaßnahmen von Zahlungsverfahren, festzulegen und zu implementieren. Um an vertrauenswürdige und wissenschaftliche Informationen für die geplante wissenschaftliche Arbeit zu gelangen, verwenden wir die unten beschriebenen Methoden:

- Interview mit einer Firma, die Click-and-Buy-Automat (CBA) herstellt
- Durchführung von Experimenten mit Smartcards und NFC
- Beobachtung von Angriffsmöglichkeiten
- Literaturrecherche

Der IT-Bereich entwickelte seine eigenen Forschungsmethoden auf Basis von anderen Fachrichtungen [Hevner and Chatterjee, 2010a]. Aus diesem Grund müssen sowohl die Recherche als auch ihre Darstellung entsprechend angepasst werden, sodass die Forschung selbst und deren Ergebnisse verständlich präsentiert werden können [Lazar et al., 2009]. Da Forschung und ihre Methoden nicht in Stein gemeißelt sind, spielen Flexibilität und Vielfältigkeit der Quellen eine wichtige Rolle für die Entwicklung einer erfolgreichen und glaubwürdigen Untersuchung.

Jedes Element der geplanten wissenschaftlichen Arbeit soll so konzipiert werden, sodass sie der Richtlinien von [Demeyer, 2011] für die Entwicklung von

Forschungen im IT-Bereich entsprechen. Die verwendeten Methoden sollen eine theoretische und praktische Abbildung des Objekts dieser Untersuchung zeigen, um ihre Anwendung direkt in der realen Welt darzustellen. Im folgenden werden die diversen Methoden der geplanten wissenschaftlichen Arbeit ausführlich beschrieben. Zudem soll die folgende Abbildung den Recherche-
weg der geplanten wissenschaftlichen Arbeit verdeutlichen.

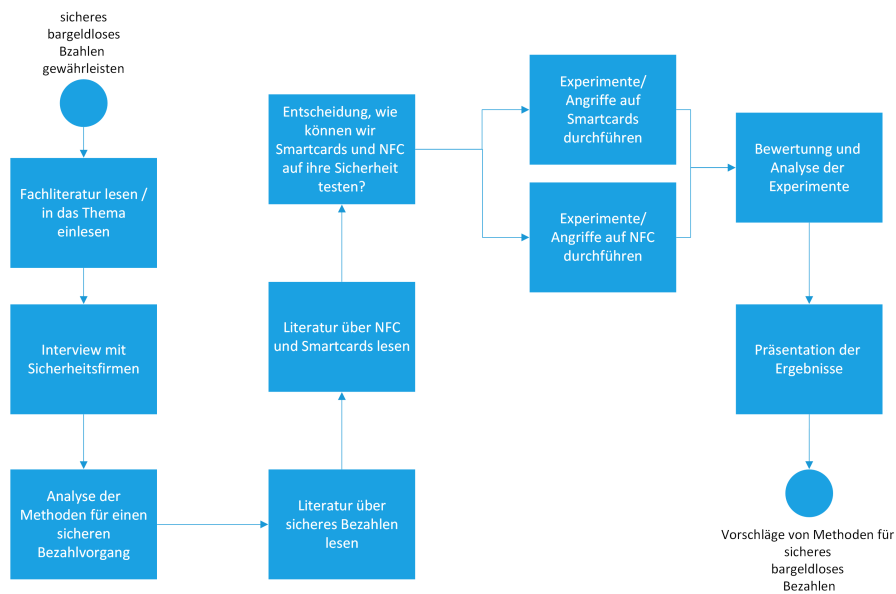


Abbildung 11: Forschungsdiagramm

Quelle: eigene Darstellung

5.1 Interview mit Click-and-Buy-Automat Firma

Die Sicherheit eines Bezahlsystems steht im Mittelpunkt jeder Firma, die Click-and-Buy-Automat (CBA) entwickeln. Für diese Recherche wollen wir Interviews mit IT-Sicherheitsfirmen führen [Lindner, 2013]. Dazu haben wir zwei in Deutschland sitzende Firmen rausgesucht, die diese Art von Geschäft schon anbieten: "REWE digital" und "myenso". In diesem Fall werden wir mit Firmen arbeiten, die zwar einen ähnlichen Dienst anbieten, aber verschiedene

Einsätze haben. Während die Firma erste ein großes Unternehmen ist und mehr als 300.000 Mitarbeiter hat [REWE Digital, 2021], ist das zweite Unternehmen, das weniger als 100 Mitarbeiter beschäftigt [myenso, 2021], etwas kleiner und auch neuer.

“REWE digital” gehört der REWE Group und ist dafür zuständig, die Marke zu digitalisieren. Die Firma hat sich in verschiedenen Bereichen der Digitalisierung entwickelt, wie Liefer- und Abholservice, oder auch Mobile Anwendung. “myenso” will ein neues Konzept vom Einkauf anbieten, indem die Kunden mehr Entscheidungen selber treffen können. Im Vergleich zu größeren Ketten will “myenso” Kunden in Orten erreichen, wo es weniger Einkaufsmöglichkeiten gibt oder die Mehrheit der Bürger kein Interesse an großen Ketten haben.

Für die Interviews stellen wir sowohl quantitative als auch qualitative Fragen. Aus dem quantitativen Fragenkatalog wollen wir messbare Daten hervorheben [Recker, 2013], die den Umgang der Firma mit Sicherheit in Zahlungsverfahren beschreibt: Anzahl von Click-and-Buy-Automat (CBA) und von Mitarbeitern, die sich nur mit digitalen Sicherheitsverfahren beschäftigen; und Beschreibung möglicher Angriffe. Aus der qualitativen Fragensammlung wollen wir uns mit Verfahren und Mechanismen beschäftigen, die die Firma verwendet, um die Sicherheit ihres Zahlungsverfahrens zu gewährleisten. Sowohl die Entwicklung von Zahlungsmethoden bei den Produkten als auch der aktuelle technische Stand der Zahlungsverfahren sollen in dieser Umfrage gedeckt sein. Für die qualitative Datenerhebung werden Methoden von Fokusgruppen¹⁶ verwendet, um die wichtigsten Anforderungen in Bezug auf Sicherheit von Zahlungsverfahren aufzudecken, zu analysieren und zu bewerten. Die gezielten und auch gleichzeitig offenen Fragen sollen dem Befragten die Möglichkeit bieten [Fern, 2001], sich über die existierenden Schwachstellen

¹⁶Fokusgruppe aus dem Englischen “focus group” bezeichnet eine Art von qualitativen Diskussionen, wo die Teilnehmer mithilfe eines Moderators ein Thema besprechen [Przyborski and Riegler, 2010].

des angebotenen Dienstes zu äußern und auch über verwendete oder in Naher Zukunft verwendete Sicherheitsmaßnahmen.

Die unteren Quellen und deren Themen:

- [Rupp and SOPHISTen, 2020]: Requirements-Engineering und -Management: Das Handbuch für Anforderungen in jeder Situation **Dieses Buch MUSS irgendwo zitiert werden. Es wird von Frau Heinemann in ihrem Unterricht verwendet**
- [Ebert, 2008]: Systematisches Requirements Engineering und Management - Anforderungen ermitteln, spezifizieren, analysieren und verwalten
- [Morgan, 1998]: he Focus Group Guidebook - **Über dieses Thema habe ich schon geschrieben.**
- [Flick, 2011]: Triangulation: Eine Einführung
- [Alber et al., 2017]: Biografieforschung als Praxis der Triangulation
- [Lazar et al., 2009]: Scientific Research in Information Systems - A Beginner's Guide

5.2 Durchführung von Experimenten

Die Tests für die Objekte dieser Untersuchung sollen im Labor der Hochschule Worms durchgeführt werden [Lindner, 2013]. Dazu werden 5 Maschinen verwendet, die folgende Rollen übernehmen sollen: Server, Host, Angreifer und zwei Leerlauf-Maschine oder auch *Zombie-botnet*¹⁷. Der Host soll eine Anfrage an den Server schicken, die eine Simulation von einem Bezahlvorgang

¹⁷Leerlaufe, *idle* oder *Zombie-botnet* bezeichnen Maschine, die für Angriff verwendet werden. In den meisten Fällen sind die Nutzer dieser Maschine nicht bewusst, dass Angreifer ihre Maschine für diesen Zweck verwenden [Geng and Whinston, 2000].

darstellen soll. Der Server soll unter normalen Umstände auf diese Anfrage antworten und wenn er es als Angriff detektiert, keine Antwort geben. Dieses Verfahren findet sowohl bei drahtlosen Verbindungen als auch bei Smartcards statt.

5.2.1 Angriffe und Härtingsmaßnahmen eines drahtlosen Servers

Für dieses Experiment sollen folgende Angriffstechniken verwendet werden: Distributed-Denial-of-Service (DDoS).

Im erstem Experiment wird der Host eine normale Anfrage an den Server schicken. Dieser wird ohne zusätzliche Sicherheitsmechanismen, wie Authentifizierung, Überprüfung der Anzahl von Verbindungen oder Anfragen nach Zertifikaten konfiguriert.

Der erste Angriff soll mithilfe des Tools Network Mapper (Nmap)¹⁸ durchgeführt werden. In diesem Angriff benutzt der Angreifer eine weitere Maschine, um sich selbst zu verbergen und um den Angriff zu verstärken. Der Angreifer schickt gespoofte¹⁹ Pakete²⁰ an die zwei *Zombies* und diese schicken sehr viele kleine Pakete in sehr kurzen Abständen an den Server, um dessen Kapazität auszureizen, sodass er auf keine Anfragen mehr antworten kann [Vanitha et al., 2017]. Im folgenden gibt es eine Abbildung zu dieser Angriffstechnik:

¹⁸Nmap ist eine freie und Open Source Anwendung für die Entdeckung und Sicherheitsüberprüfung von Netzwerken [Nmap.Org, 2021].

¹⁹Angreifer verwenden meistens legitimen Adresse von anderen Rechner, um die eigene Identität zu verbergen. In diesem Fall ist die eigene Adresse gefälscht [IONOS, 2020].

²⁰Pakete sind im Netzwerk die Einkapselung von Metainformationen, wie Quell- und Zieladresse Protokolltyp und Größe die Nutzdaten, wie Text, Videos oder Bilder [Wendzel, 2018].

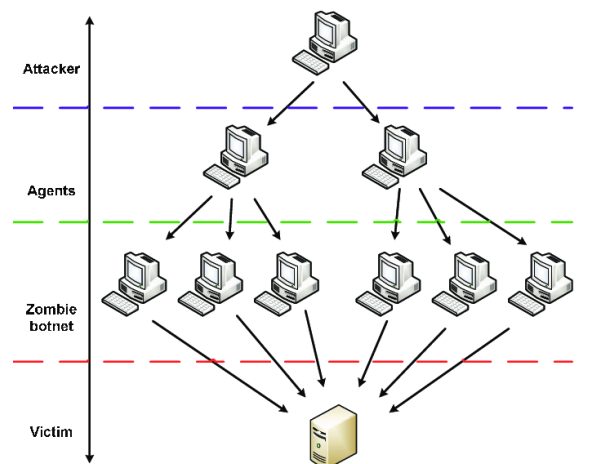


Abbildung 12: Ein Beispiel von Distributed-Denial-of-Service (DDoS) mit mehreren Leerlaufe-Maschinen

Quelle: Durcekova et al., 2012

5.2.2 Erwartete Beobachtung von Angriffsmöglichkeiten auf einen drahtlosen Servers

Vor dem Angriff konnte der Host normal mit dem Server kommunizieren, also Anfragen schicken und er hat eine Antwort bekommen. Während des Angriffes war die Kommunikation mit dem Server entweder sehr langsam oder sogar unterbrochen. In diesem Fall bekam der Host selten eine Antwort auf seine Anfrage. In einigen Momenten gab es überhaupt keine Antwort.

Seitens des Servers wurde das Tool Wireshark²¹ verwendet, um die Ein- und Ausgehenden Pakete zu beobachten und zu analysieren [Banerjee et al., 2010]. Unter normalen Umständen kamen die Pakete in einem angemessenen Zeitabstand. Während des Angriffes bekam der Server viele kleine Pakete ohne nützlichen Inhalt und in sehr kurzem Zeitabstand. Im folgenden gibt es eine Abbildung, wie Wireshark die Kommunikation aufgezeichnet hat:

²¹Wireshark ist eine Anwendung für die Analyse von Networkprotokolle. Es beschreibt ein- und ausgehende Pakete und dessen Bestandteile [Wireshark, 2021].

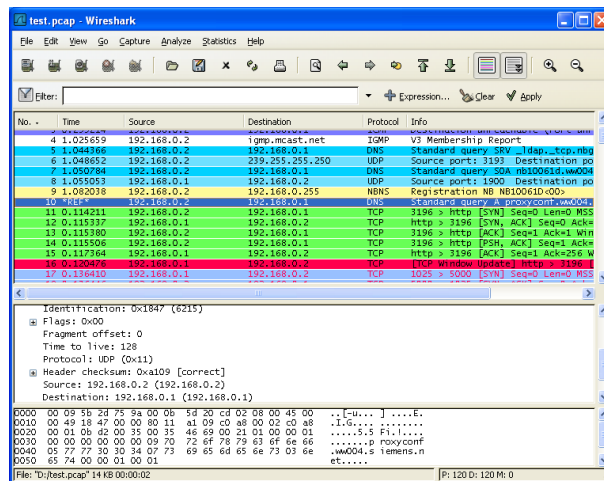


Abbildung 13: Ausgabe von Wireshark

Quelle: Wireshark, 2021

Um den Angriff zu verhindern, schlug [Yildirim and Varol, 2019] vor, den Server erneut zu konfigurieren, indem er nur Anfragen von registrierten Hosts akzeptiert **Zero Trust Modell, Beleg, Fussnote und kurze Erklärung**. Nach dieser Anpassung konnte sich der Angreifer nicht mehr mit dem Server verbinden, da er kein registrierter Nutzer war. In der Aufzeichnung on Wireshark wurden nicht angemeldete Pakete direkt verworfen.

5.2.3 Angriff und Härungsmaßnahme von Smartcard

Das will Dominic sehr gern schreiben.

5.2.4 Erwartete Beobachtung von Angriffsmöglichkeiten von Smartcard

Das will Dominic sehr gern schreiben.

5.3 Literaturrecherche

Die Literatur bezüglich Netzwerksicherheit, bargeldlose Zahlungsverfahren und Vending Machines, ist in den letzten 20 Jahren deutlich umfangreicher geworden. Da diese Begriffe viele und nahezu unendlich Konzepte decken, gehen wir hier auf spezifische Aspekte dieser Begriffe ein und zwar auf die Sicherheit von drahtlosen Zahlungsmethode und von Smartcards.

Folgende Quellen trugen zu der Suche nach vertrauenswürdiger Literatur bei:

- ScienceDirect
- Researchg Gate
- IEEE Xplore
- Google Scholar.

6 Praktische Relevanz

Die Entwicklung jedes Systems setzt die Akzeptanz von den Stakeholdern²² voraus. Um dieses Ziel zu erreichen, müssen einige Schritte befolgt werden: Welche Wünsche haben die Stakeholder?; Hervorhebung der Anforderungen des zu entwickelnden Systems; Tests des zu gestalteten Produkts; Implementierung des Systems oder der Anwendung; Weiterentwicklung des Systems [Rupp and SOPHISTen, 2020]. Alle diese Schritte ermöglichen die Erzeugung eines potenziellen akzeptierten Systems, das von Kunden genutzt werden kann.

Relevant für Kunde weil Firma weil IT weil Sozial weil

Diese geplante wissenschaftliche Arbeit soll vor allem Menschen nutzen, die in eher abgelegenen Orten wohnen und somit meistens von großen Supermarktketten vernachlässigt werden. Da der Automat 24 Stunden und 7 Tage in der Woche offen sein soll, können potenzielle Kunden auch mitten in der Nacht oder am Sonntag ihre Einkauf am Click-and-Buy-Automat (CBA) tätigen, ohne für die übersteuerten Preise von der Tankstelle bezahlen zu müssen.

Dadurch, dass der Automat rund um die Uhr funktioniert, ist es auch für die Lieferanten einfacher einen Termin für die Auslieferung der Waren zu finden. Denn es ist im Prinzip egal, wann die Ware eintrifft. Die Hauptsache ist, dass die Waren im Click-and-Buy-Automat (CBA) möglichst immer verfügbar sind.

Der eigentlich wichtigste Punkt ist die Sicherheit beim Bezahlvorgang, bei der es in der geplanten wissenschaftlichen Arbeit hauptsächlich geht. Das Ziel von der Entwicklung eines sicheren Zahlungsverfahrens ist, dass die Kunden sich also keine Sorgen um die Sicherheit bei bargeldloser Bezahlung machen

²²Eine Person oder Gruppe, die Interesse für das Projekt haben oder auch die Auftraggeber [Sharp et al., 1999].

müssen, da die Methoden für die Bezahlung auf dem neusten technischen Stand sind.

Die Akzeptanz, die durch ein solches Verfahren entsteht, kann sogar auch dazu beitragen, Digital Non-Natives als potenzielle Kunden zu gewinnen. Außerdem kann dieses Projekt andere Firmen dazu bringen, mehr in die Forschung für die Sicherheit bei bargeldloser Bezahlung zu investieren.

Literaturverzeichnis

- [Alber et al., 2017] Alber, I., Griese, B., and Schiebel, M. (2017). *Biografie-forschung als Praxis der Triangulation*. Springer Fachmedien Wiesbaden. <https://books.google.de/books?id=AgFeswEACAAJ>.
- [Alrawais, 2020] Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). *International Journal of Advanced Computer Science and Applications*, 11(11). <http://dx.doi.org/10.14569/IJACSA.2020.0111176>.
- [Aquilina and Saliba, 2019] Aquilina, Y. and Saliba, M. A. (2019). An automated supermarket checkout system utilizing a SCARA robot: preliminary prototype development. *Procedia Manufacturing*, 38:1558–1565. 29th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM 2019), June 24-28, 2019, Limerick, Ireland, Beyond Industry 4.0: Industrial Advances, Engineering Education and Intelligent Manufacturing.
- [Banerjee et al., 2010] Banerjee, U., Ashutosh, V., and Mukul, S. (2010). Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection. *International Journal of Computer Applications*, 6. <http://dx.doi.org/10.5120/1092-1427>.
- [Bankar, 2019] Bankar, S. (2019). Automated Supermarket Run System. *Journal of Advanced Research in Embedded System*, 6(3 and 4). <https://thejournalshouse.com/index.php/ADR-Journal-Embedded-Systems/article/view/223>.
- [Bremser et al., 2019] Bremser, C., Piller, G., and Rothlauf, F. (2019). How Smart Cities Explore New Technologies. In Pankowska, M. and Sandkuhl, K., editors, *Perspectives in Business Informatics Research - 18th International Conference, BIR 2019, Katowice, Poland, September 23-25, 2019, Proceedings, series=Lecture Notes in Business Information Processing*, volume 365, pages 1–15. Springer. https://doi.org/10.1007/978-3-030-31143-8_1.
- [Bundesamt für Sicherheit in der Informationstechnik, 2020] Bundesamt für Sicherheit in der Informationstechnik (2020). Social Engineering – der Mensch als Schwachstelle. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html.
- [Bundesbank, 2009] Bundesbank, D. (2009). Cashless payments in Germany and the role of the Deutsche Bundesbank: Developments and key trends over the past 50 years. *Deutsche Bundesbank Eurosystem - Monthly Report*.

- [Bundeskriminalamt, 2020] Bundeskriminalamt (2020). Cybercrime Bundeslagebild 2020. <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2020.html;jsessionid=1A921B916A930B1DEB3130BCF4399153.live291?nn=28110>.
- [Chikofsky and Cross, 1990] Chikofsky, E. and Cross, J. (1990). Reverse engineering and design recovery: a taxonomy. *IEEE Software*, 7(1):13–17. <https://ieeexplore.ieee.org/abstract/document/43044>.
- [Dahlberg et al., 2008] Dahlberg, T., Mallat, N., Ondrus, J., and Zmijewska, A. (2008). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, 7(2):165–181. <https://doi.org/10.1016/j.elerap.2007.02.001>.
- [Datenschutz, 2021] Datenschutz (2021). Datenschutz im Internet: Privatsphäre als höchstes Gut bewahren. *Datenschutz.org*. <https://www.datenschutz.org/datenschutz-im-internet/>.
- [Demeyer, 2011] Demeyer, S. (2011). Research methods in computer science. In *2011 27th IEEE International Conference on Software Maintenance (ICSM)*, page 600. <http://dx.doi.org/10.1109/ICSM.2011.6080841>.
- [Dijaya et al., 2019] Dijaya, R., Suprayitno, E., and Wicaksono, A. (2019). Integrated Point of Sales and Snack Vending Machine based on Internet of Things for Self Service Scale Micro Enterprises. *Journal of Physics: Conference Series*, 1179:012098. <http://dx.doi.org/10.1088/1742-6596/1179/1/012098>.
- [Dullien, 2018] Dullien, T. (2018). Maschinelles Lernen und künstliche Intelligenz in der Informationssicherheit. *Datenschutz und Datensicherheit - DuD*, 42(10):618–622. <https://doi.org/10.1007/978-3-7089-1162-3-1012-3>.
- [Durcekova et al., 2012] Durcekova, V., Schwartz, L., and Shahmehri, N. (2012). Sophisticated Denial of Service Attacks Aimed at Application Layer. In *2012 ELEKTRO*, pages 55–60. <http://dx.doi.org/10.1109/ELEKTRO.2012.6225571>.
- [Ebert, 2008] Ebert, C. (2008). *Systematisches Requirements Engineering und Management - Anforderungen ermitteln, spezifizieren, analysieren und verwalten (2. Aufl.)*. dpunkt Verlag.
- [Farrell, 1996] Farrell, J. (1996). Smartcards become an international technology. In *Proceedings 13th TRON Project International Symposium /TEPS '96*, pages 134–140. <https://doi.org/10.1109/TRON.1996.566204>.

- [Fern, 2001] Fern, E. F. (2001). *Advanced Focus Group Research*. SAGE Publications Inc, New Delhi.
- [Flick, 2011] Flick, U. (2011). *Triangulation: Eine Einführung*. Qualitative Sozialforschung. VS Verlag für Sozialwissenschaften. <https://books.google.de/books?id=XMt8vwEACAAJ>.
- [Geng and Whinston, 2000] Geng, X. and Whinston, A. (2000). Defeating distributed denial of service attacks. *IT Professional*, 2(4):36–42. <https://doi.org/10.1109/6294.869381>.
- [Ghosh and C., 2014] Ghosh, P. and C., C. (2014). E-commerce: ‘click and buy’ – an easy way of shopping (with respect to indian market). *International Journal of Innovative Research & Development*, 3:416–431. <http://52.172.159.94/index.php/ijird/article/viewFile/58573/45795>.
- [Gomm et al., 1997] Gomm, G. R., Paul, G. R. G., and Paul, S. (1997). Cash alternative transaction system. <https://www.freepatentsonline.com/5650761.html>.
- [Graefe, 2019] Graefe, L. (2019). Altersverteilung von deutschen Campingurlaubern im Jahr 2019. <https://de.statista.com/statistik/daten/studie/1044777/umfrage/altersverteilung-der-deutschen-campingurlauber/>.
- [Graefe, 2021a] Graefe, L. (2021a). Anzahl der Neuzulassungen von Caravans und Reisemobilen in Deutschland von 2013 bis 2020. <https://de.statista.com/statistik/daten/studie/662102/umfrage/neuzulassungen-von-caravans-und-reisemobile-in-deutschland/>.
- [Graefe, 2021b] Graefe, L. (2021b). Anzahl der Übernachtungen von Gästen in Beherbergungsstätten in Deutschland von September 2019 bis September 2021. <https://de.statista.com/statistik/daten/studie/73548/umfrage/uebernachtungen-in-beherbergungsstaetten-und-auf-campingplaetzen/>.
- [Graefe, 2021c] Graefe, L. (2021c). Übernachtungen in Beherbergungsstätten in Deutschland bis September 2021. <https://de.statista.com/statistik/daten/studie/73548/umfrage/uebernachtungen-in-beherbergungsstaetten-und-auf-campingplaetzen/>.
- [Hassan et al., 2020] Hassan, M. A., Shukur, Z., Hasan, M. K., and Al-Khaleefa, A. S. (2020). A Review on Electronic Payments Security. *Symmetry*, 12:22. <http://dx.doi.org/10.3390/sym12081344>.
- [Henze et al., 2017] Henze, M., Hiller, J., Hummen, R., Matzutt, R., Wehrle,

- K., and Ziegeldorf, J. H. (2017). *Network Security and Privacy for Cyber-Physical Systems*, chapter 2, pages 25–56. John Wiley and Sons Ltd. <https://doi.org/10.1002/9781119226079.ch2>.
- [Hevner and Chatterjee, 2010a] Hevner, A. and Chatterjee, S. (2010a). *Design Science Research in Information Systems*, pages 9–22. Springer US, Boston, MA. https://doi.org/10.1007/978-1-4419-5653-8_2
- [Hevner and Chatterjee, 2010b] Hevner, A. and Chatterjee, S. (2010b). *Design Science Research in Information Systems*, pages 9–22. Springer US, Boston, MA. https://doi.org/10.1007/978-1-4419-5653-8_2.
- [Hiroyuki, 2004] Hiroyuki, U. (2004). Lowering elderly Japanese users resistance towards computers by using touchscreen technology. *Universal Access in the Information Society*, 3(3-4):276–288. <https://www.proquest.com/scholarly-journals/lowering-elderly-japanese-users-resistance/docview/201543463/se-2?accountid=15921>.
- [IONOS, 2020] IONOS (2020). IP-Spoofing: So einfach manipulieren Angreifer Datenpakete. <https://www.ionos.de/digitalguide/server/sicherheit/ip-spoofing-grundlagen-und-gegenmassnahmen/>. Accessed: 2021-12-14.
- [Iqbal et al., 2012] Iqbal, Q., Whitman, L. E., and Malzahn, D. (2012). Reducing Customer Wait Time at a Fast Food Restaurant on Campus. *Journal of Foodservice Business Research*, 15(4):319–334. <https://doi.org/10.1080/15378020.2012.706176>.
- [Isaac and Zeadally, 2012] Isaac, J. T. and Zeadally, S. (2012). An anonymous secure payment protocol in a payment gateway centric model. <https://doi.org/10.1016/j.procs.2012.06.097>.
- [Isaac and Zeadally, 2014] Isaac, J. T. and Zeadally, S. (2014). Design, implementation, and performance analysis of a secure payment protocol in a payment gateway centric model. *Computing*, 96:587–611. <https://doi.org/10.1007/s00607-013-0306-4>.
- [Itako, 2004] Itako, E. (2004). Automatic vending machine and sales method thereof. <https://www.freepatentsonline.com/6754559.html>.
- [Jadhav et al., 2018] Jadhav, S., Pawar, N., Kharade, N., and Lengare, P. S. (2018). Automatic Vending Machine. *International Journal of Innovative Science and Research Technology (IJISRT)*, 3:376–378. <https://www.ijis>

rt.com/automatic-vending-machine.

- [Kavitha, 2018] Kavitha, D. (2018). Modern shopping cart with automatic billing system using load sensor. *International Journal of Engineering and Technology*, 7(2.33). <https://www.sciencepubco.com/index.php/ijet/article/view/14846>.
- [Keller et al., 2017] Keller, J., Gabriele, and Wendzel, S. S. (2017). Ant Colony-Inspired Parallel Algorithm to Improve Cryptographic Pseudo Random Number Generators. In *IEEE Symposium on Security and Privacy Workshops*, pages 17–22.
- [Khodawandi et al., 2003] Khodawandi, D., Pousttchi, K., and Wiedemann, D. G. (2003). Akzeptanz mobiler Bezahlverfahren in Deutschland. In *Mobile Commerce - Anwendungen und Perspektiven, Proceedings zum 3. Workshop Mobile Commerce*, pages 42–57, Bonn. Gesellschaft für Informatik e.V.
- [Kwon et al., 2020] Kwon, H., Nam, H., Lee, S., Hahn, C., and Hur, J. (2020). (In-)Security of Cookies in HTTPS: Cookie Theft by Removing Cookie Flags. *IEEE Transactions on Information Forensics and Security*, 15:1204–1215. <https://ieeexplore.ieee.org/document/8820079/authors#authors>.
- [Langdon et al., 2013] Langdon, P., Clarkson, J., and Robinson, P. (2013). Designing inclusive interactions. *Universal Access in the Information Society*, 12:233–235. <https://doi.org/10.1007/s10209-013-0289-0>.
- [Lauzi, 2017] Lauzi, M. (2017). Smart-City: Die Stadt der Zukunft. *VDI Rheingau Regional Magazin*, 2:12–18.
- [Lazar et al., 2009] Lazar, J., Feng, J. H., and Hochheiser, H. (2009). *Research Methods in Human-Computer Interaction*. Wiley & Sons Ltd, West Sussex.
- [Lindner, 2013] Lindner, D. (2013). *Forschungsdesigns der Wirtschaftsinformatik*. Springer Gabler, Wiesbaden, Wiesbaden. <https://link.springer.com/book/10.1007%2F978-3-658-31140-7>.
- [Luber and Schmitz, 2017] Luber, S. and Schmitz, P. (2017). Was ist Kryptographie? *Security Insider*. <https://www.security-insider.de/was-ist-kryptographie-a-642288/>.
- [Lübbecke, 2018] Lübbecke, H. (2018). Akzeptanz und Übernahme von Informatikprodukten durch Ältere. *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)*, 4:31–34. <https://www.fiff.de/publikationen/fiff-kommunikation/fk-2018/fk-2018-4/fk-2018-4-content/fk-4-18-p31.pdf>.

- [Matthies et al., 2015] Matthies, C., Pirl, L., Azodi, A., and Meinel, C. (2015). Beat your mom at solitaire — a review of reverse engineering techniques and countermeasures. In *2015 6th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pages 1094–1097. <https://ieeexplore.ieee.org/document/7339242>.
- [Me, 2003] Me, G. (2003). Payment security in mobile environment. In *ACS/IEEE International Conference on Computer Systems and Applications, 2003. Book of Abstracts.*, pages 34–. <http://dx.doi.org/10.1109/AICCSA.2003.1227468>.
- [Morgan, 1998] Morgan, D. (1998). *The Focus Group Guidebook*. SAGE Knowledge. <https://sk.sagepub.com/books/the-focus-group-guidebook>.
- [myenso, 2021] myenso (2021). Die Idee von myEnso. <https://www.myenso.de/content/idee>. Accessed: 2021-12-17.
- [Nießner, 2017] Nießner, M. (2017). *Innovative Technik im Zahlungsverkehr. Ein kompakter Überblick über traditionelle und moderne Zahlungsverfahren*. GRIN Verlag, Norderstedt, 1 edition.
- [Nmap.Org, 2021] Nmap.Org (2021). Nmap: the Network Mapper - Free Security Scanner. <https://nmap.org/>. Accessed: 2021-12-10.
- [Opiela and Garey, 2010] Opiela, M. S. and Garey, R. E. (2010). Electronic postal money order method and system. <https://www.freepatentsonline.com/7849015.html>.
- [Patil et al., 2020] Patil, A. B., Mahajan, G., Phale, V., and Mane, S. (2020). Vending Machine with Cash and Cashless Payment Support. *International Journal in IT and Engineering*, 07:341–348.
- [Proehl, 2021] Proehl, G. (2021). An Introduction to Near Field Communications. *Mouser Electronics*. <https://www.mouser.de/applications/rfid-nfc-introduction/>.
- [Przyborski and Riegler, 2010] Przyborski, A. and Riegler, J. (2010). *Gruppendiskussion und Fokusgruppe*, pages 436–448. VS Verlag für Sozialwissenschaften, Wiesbaden. https://doi.org/10.1007/978-3-531-92052-8_31.
- [Rankl and Effing, 2002] Rankl, W. and Effing, W. (2002). *Handbuch der Chipkarten - Aufbau, Funktionsweise, Einsatz von Smart Cards (4. Aufl.)*.,. Hanser.

- [Recker, 2013] Recker, J. (2013). *Scientific Research in Information Systems - A Beginner's Guide*. Springer, Berlin, Heidelberg, Heidelberg. <https://doi.org/10.1007/978-3-642-30048-6>.
- [Renaudin et al., 2004] Renaudin, M., Bouesse, F., Proust, P., Tual, J., Sourgen, L., and Germain, F. (2004). High security smartcards. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, volume 1, pages 228–232 Vol.1. <http://dx.doi.org/10.1109/DATE.2004.1268853>.
- [REWE Digital, 2021] REWE Digital (2021). Über uns: REFE digital. <https://www.rewe-digital.com/ueber-uns.html>. Accessed: 2021-12-17.
- [Riebe et al., 2020] Riebe, T., Haunschild, J., Divo, F., Lang, M., Roitburd, G., Franken, J., and Reuter, C. (2020). Die vorratsdatenspeicherung in europa. *Datenschutz und Datensicherheit - DuD*, 44:316–321. http://www.peasec.de/paper/2020/2020_Riebeetal_VDSinEuropa_DuD.pdf.
- [Rihaczek, 2013] Rihaczek, K. (2013). Datenschutz & Computer. *Datenschutz und Datensicherheit*, 37(9):561. <https://doi.org/10.1007/s11623-013-0236-5>.
- [Rohr et al., 2010] Rohr, A., Nohl, K., and Plötz, H. (2010). Establishing Security Best Practices in Access Control. <https://www.readkong.com/page/establishing-security-best-practices-in-access-control-2712189>. Accessed: 2021-12-10.
- [Rupp and SOPHISTen, 2020] Rupp, C. and SOPHISTen (2020). *Requirements-Engineering und -Management: Das Handbuch für Anforderungen in jeder Situation*. Carl Hanser Verlag GmbH & Co. KG, München, 7 edition.
- [Schaeffler, 2008] Schaeffler, J. (2008). *Digital Signage: Software, Networks, Advertising, and Displays a Primer for Understanding the Business*. Focal Press, Burlington.
- [Seibel, 2019] Seibel, K. (2019). Die deutsche Liebe zum Bargeld verblasst – wegen nur einer Karte. *Die Welt*. <https://www.welt.de/wirtschaft/article193063435/Zahlungsmittel-Karte-schlaegt-in-Deutschland-erstmals-Bargeld.html>.
- [Semenov et al., 2017] Semenov, V. P., Chernokulsky, V. V., and Razmochayeva, N. V. (2017). The cashless payment device for vending machines — Import substitution in the sphere of vending. In *2017 International Conference Quality Management, Transport and Information Security, Information Technologies (IT QM IS)*, pages 798–801.

- [Sharp et al., 1999] Sharp, H., Finkelstein, A., and Galal, G. (1999). Stakeholder identification in the requirements engineering process. In *Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99*, pages 387–391. <https://doi.org/10.1109/DEXA.1999.795198>.
- [Shen et al., 2019] Shen, L., Qiu, C., Wu, X., Han, C., and Hu, L. (2019). Design of removable vending machine and research on the key implementation technology. *The Journal of Engineering*, 2019(13):402–405. <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/joe.2018.9021>.
- [Sibanda et al., 2020] Sibanda, V., Munetsi, L., Mpofu, K., Murena, E., and Trimble, J. (2020). Design of a high-tech vending machine. *Procedia CIRP*, 91:678–683. <https://www.sciencedirect.com/science/article/pii/S2212827120308829>.
- [Siepermann, 2018] Siepermann, M. (2018). Gabler wirtschaftslexikon: Stichwort: Digital native. <https://wirtschaftslexikon.gabler.de/definition/digital-native-54496>.
- [Singh, 2020] Singh, N. K. (2020). Near-field Communication (NFC). *Information Technology and Libraries*, 39(2). <https://doi.org/10.6017/ital.v39i2.11811>.
- [Sommerville, 2010] Sommerville, I. (2010). *Software Engineering*. Pearson, Boston, 9 edition.
- [Steffen, 2012] Steffen, A. (2012). Sicherheit Smartcard-basierter Zugangskontrollsysteme. Master’s thesis, Ruhr-Universität Bochum, Universitätsstraße 150, 44801 Bochum. <https://www.emsec.ruhr-uni-bochum.de/media/attachments/files/2012/04/Master-Arbeit-public.pdf>.
- [Tabet and Ayu, 2016] Tabet, N. E. and Ayu, M. A. (2016). Analysing the security of nfc based payment systems. In *2016 International Conference on Informatics and Computing (ICIC)*, pages 169–174. <http://dx.doi.org/10.1109/IAC.2016.7905710>.
- [Tanembaum, 2009] Tanembaum, A. S. (2009). *Moderne Betriebssysteme*. Pearson, München.
- [Vanitha et al., 2017] Vanitha, K., UMA, S. V., and Mahidhar, S. (2017). Distributed denial of service: Attack techniques and mitigation. In *2017 International Conference on Circuits, Controls, and Communications (CCUBE)*, pages 226–231.
- [Wang et al., 2013] Wang, Q. E., Myers, M. D., and Sundaram, D. (2013).

- Digital Natives und Digital Immigrants. *Wirtschaftsinformatik*, 55(6):409–420. <https://link.springer.com/article/10.1007/s11576-013-0390-2#citeas>.
- [Wendzel, 2018] Wendzel, S. (2018). *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Springer Vieweg, Wiesbaden.
- [Wendzel et al., 2021] Wendzel, S., Mazurczyk, W., Caviglione, L., and (Eds.), A. H. (2021). Emerging Topics in Defending Networked Systems. *Special Issue at Future Generation Computer Systems (FGCS)*.
- [Wendzel and Plötner, 2007] Wendzel, S. and Plötner, J. (2007). *Praxisbuch Netzwerk-Sicherheit: Risikoanalyse, Methoden und Umsetzung; für Unix-Linux und Windows; VPN, WLAN, Intrusion Detection, Disaster Recovery, Kryptologie*. Galileo Computing, Bonn.
- [Wendzel et al., 2017] Wendzel, S., Tonejc, J., Kaur, J., and Kobekova, A. (2017). *Cyber Security of Smart Buildings*, chapter 16, pages 327–351. John Wiley & Sons, Ltd. <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119226079.ch16>.
- [Wireshark, 2021] Wireshark (2021). About Wireshark. <https://www.wireshark.org/>. Accessed: 2021-12-10.
- [Woehe and Kurz, 2021] Woehe, J. M. and Kurz, E. (2021). *Krisen in Digitalprojekten erfolgreich managen*. Hanser, München.
- [Yildirim and Varol, 2019] Yildirim, N. and Varol, A. (2019). A Research on Security Vulnerabilities in Online and Mobile Banking Systems. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–5. <http://dx.doi.org/10.3390/sym12081344>.