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 und Dominic Meyer

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

Inhaltsverzeichnis

Abstract

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Zusammenfassung

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet

orci dignissim rutrum.

1 Stand der Technik

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

1.1 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].

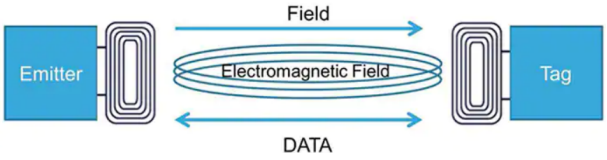

Abbildung 1: Teilnehmer der Kommunikation über nfc
Quelle: Proehl, 2021

1.1.1 Angriffsmöglichkeit auf nfc

Da diese Technologie neu ist [Tabet and Ayu, 2016], sie existiert seit 2006, sind Schwachstellen und Härtungsmaßnahmen 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 Integrität[1] nicht verletzt wird.

[1] Es ist Subjekten nicht möglich, die zu schützenden Daten unatorisiert 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 Engineering[2]. [Alrawais, 2020] hebt andere Schwachstellen hervor: *Eavesdropping*[3] je nachdem, wie viele Ressourcen investiert werden, kann ein Angreifer in der Lage sein, der Kommunikation zu lauschen; ddos[4], um die Authentifizierung und Verfügbarkeit der Kommunikation zu beeinträchtigen.

1.1.2 Gegenmaßnahmen für die Härtung von drahtlose Verbindung

Um die Risiken bei der Verwendung von nfc zu abzuschwächen, 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 authorisierten Geräten; Einsetzung von künstlicher Intelligenz (KI) für die Detektion von abweichendem Verhalten; Kontrolle gegen Social Engineering [5]

Kredit- und EC-Karten sollen auch als Zahlungsmittel bei unserem cba akzeptiert werden. In Bezug auf diese Zahlungsmittel, wird die Sicherheit im folgenden untersucht.

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

[3]Eavesdropping ist das unauthorisierte Mithören von einer Kummunikation [Wendzel, 2018].

[4]Bei solchen Angriffen wird die Verfügbarkeit des Dienstes verletzt, sodass die Kommunikation nicht mehr einwandfrei stattfinden kann [Wendzel, 2018].

[5]Beim 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]

1.2 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 Nutzenden. Im folgenden ist ein Beispiel von einer Smartcard für eine zahlende Karte zu sehen:

Abbildung 2: Eine Smartcard und deren eingebetete 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 traditionelen Magnetstreifenkarten, weil sie verschiedene Authentifizierungsmethoden ermöglichen auch ohne eine direkte Verbindung zur Bank [Tanembaum, 2009]. Im folgenden wird der Authentifizierungsprozess einer Smartcard 3 dargestellt.

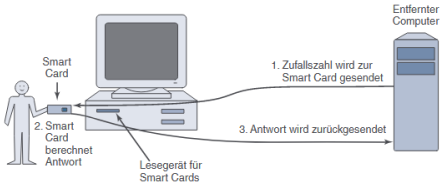

Abbildung 3: Authentifizierungsprozess von Smartcards
Quelle: Tanenbaum, 2009, S.755

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

1.2.1 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 [**?**]. 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.

1.2.2 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 [**?**]. 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 dar-

stellt [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.

1.3 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 Härtungsmaßnahmen 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.

2 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 Härtungsmaßnahmen von nfc und von Smartcards. Um an vertrauenswürdige und wissenschaftliche Informationen für die geplante wissenschaftliche Arbeit zu gelangen, werden wir folgende Dinge durchführen:

- Durchführung von Experimenten mit Smartcards und nfc
- Beobachtung von Angriffsmöglichkeiten
- Interview mit IT-Sicherheitsfirmen
- Literaturrecherche

Der IT-Bereich entwickelte seine eigenen Forschungsmethode auf Basis von anderen Fachrichtungen [**?**]. Aus diesem Grund müssen sowohl die Recherche als auch ihre Darstellung entsprechend angepasst werden, sodass die Recherche selbst und deren Ergebnisse verständlich präsentiert werden können. 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 konzipert werden, sodass sie der Richtlinien von [**?**] 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. Die folgende Abbildung soll den Rechercheweg der geplanten

wissenschaftlichen Arbeit verdeutlichen.

2.1 Durchführung von Experimenten

Hier bin ich mir nicht ganz sicher, ob wir schreiben, als ob wir die Experimenten schon ausgeführt haben oder wie wir es ausführen wollen.

Die Tests für die Objekte dieser Untersuchung sollen im Labor der Hochschule Worms durchgeführt werden. Dazu werden 5 Maschinen verwendet, die folgende Rollen übernahmen sollen: Server, Host und Angreifer und 2 Leerlauf-Maschine oder *Zombie-botnet* [6]. Der Host soll eine Anfrage an den Server schicken, die eine Simulation von einem Bezahlvorgang darstellen soll. Der Server soll unter normalen Umstände auf diese Anfrage antworten und unter einem Angriff keine Antwort geben. Dieses Verfahren findet sowohl bei Drahtlosen Verbindungen als auch bei Smartcards statt.

2.1.1 Angriff und Härtungsmaßnahme einer drahtlosen Server

Für dieses Experiment sollen folgende Angriffstechniken verwendet werden: ddos.

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

Der erste Angriff wird mithilfe des Tools nmap[7] durchgeführt werden. In diesem Angriff benutzt der Angreifer eine weitere Maschine, um sich selbst zu

[6] Leerlaufe, *idle* oder *Zombie-botnet* bezeichnen Maschine, die für Angriff verwendet werden. In den meisten Fälle sind die Nutzer dieser Maschine nicht bewusst, dass Angreifer ihre Maschine für diesen Zweck verwenden [**?**].

[7] nmap ist eine freie und Open Source Anwendung für die Entdeckung und Sicherheitsüberprüfung von Netzwerken [**?**].

verbergen und, um den Angriff zu verstärken. Der Angreifer schickt gespoofte[8] Pakete[9] an die zwei *Zombie* und diese schicken sehr viele kleine Pakete in sehr kürzem Abstand an das Server, um dessen Kapazität auszulasten, sodass er auf keine Anfragen mehr antworten kann [**?**]. Im folgenden gibt es eine Abbildung zu dieser Angriffstechnik:

2.1.2 Angriff und Härtungsmaßnahme von Smartcard

Ich würde nur das Beispiel von NFC geben und die anderen nur nach Bedarf hinzufügen, sonst werden wir hier viele Seite haben

Vllt sollten wir ein Diagramm von diesem Angriff darstellen.

2.2 Beobachtung von Angriffsmöglichkeiten

Hier können wir sagen, dass wir in einem Labor einige Angriffe durchgeführt haben. Wir beschreiben alle Elementen dieses Labor und was wir von diesem Experimenten erwarten. Auch die Quelle für solche Beobachtung.

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 überhaubt keine Antwort.

Seitens des Servers wurde das Tool Wireshark[10] verwendet, um die Ein- und

[8] Angreifer verwenden meistens legitimen Adresse von anderen Rechner, um die eigene Identität zu verbergen. In diesem Fall ist die eigene Adresse gefälscht [**?**].

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

[10] Wireshark ist eine Anwendung für die Analyse von Networkprotoklle. Es beschreibt ein- und ausgehende Pakete und dessen Bestandteile [**?**].

Ausgehenden Pakete zu beobachten und zu analysieren [**?**]. Unter normalen Umstände 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 aufezeichnet hat:

Wie [Yildirim and Varol, 2019] vorschlug, Um den Angriff zu verhindern, schlug [Yildirim and Varol, 2019] vor, den Server erneut zu konfigurieren, indem er nur Anfragen von registrierten Hosts akzeptiert. 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.

2.3 Interview mit IT-SicherheitsFirmen

Hier schreiben wir, dass wir Person x der Firma y nach dem ihrem Produkt bezüglich auf Sicherheit gefragt haben. Vllt. 9 Frage, 3 über das Produkt, 3 über Schwachstelle und 3 über Härtung. Wir brauchen auch am Anfang irgendwelche Zitation wie eine wissenschaftliche Interview aussehen sollte.

2.4 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 Quelle trugen zu der Suche nach vertrauenswürdiger Literatur bei:

- ScienceDirect

- Researchg Gate
- IEEE Xplore
- Google Scholar.

Diese Quellen ermöglichten eine allgemein theoretische Kenntnis über das Objekt dieser Untersuchung und dessen aktuellen Stand der Forschung.

Literaturverzeichnis

[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.

[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.

[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.

[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.

[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.

[Singh, 2020] Singh, N. K. (2020). Near-field Communication (NFC). *Information Technology and Libraries*, 39(2). https://doi.org/10.6017/ital.v39i2.11811.

[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.

[Wendzel, 2018] Wendzel, S. (2018). *IT-Sicherheit für TCP/IP- und IoT-*

Netzwerke. Springer Vieweg, Wiesbaden.

[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.