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

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 kontaktlos 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].

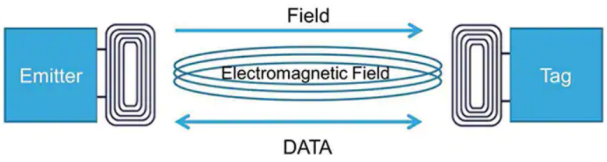

Abbildung 1: Teilnehmer der Kommunikation über NFC ([Proehl, 2021])

1.1.1 Angriffsmöglichkeit auf NFC

Da diese Technologie relativ 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.

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; *Denial-of-Service*[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, 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]

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

[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 Cyber-Security 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]

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

1.2 Anwendung von Smartcards und sicheres Bezahlen

Smartcards sind heutzutage sehr stark verbreitet, nicht nur für eine Zahlungsabwicklung, sondern auch für die Identifizierung. Viele Ausweise wie zum Beispiel 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
(eigene Quelle)

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.

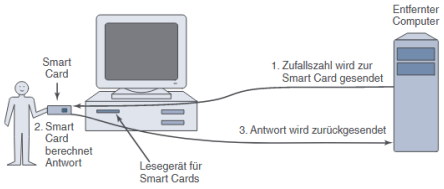

Abbildung 3: Authentifizierungsprozess von Smartcards
(Tanenbaum, 2009, S.755)

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 in keinem Fall eine 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, das heißt es werden keine Standardzellen oder ähnliches verwendet. 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 darstellt [Steffen, 2012]. Dazu wären asymmetrische Verschlüsselungsverfahren sinnvoller als symmetrische, da jede Karte bei asymmetrischer Verschlüsselung einen öffentlichen und privaten Schlüssel hat und nicht alle den selben 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 Schachstelle 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 umfangreicher, besonders weil auch Non-Native sie eher nutzen.

Aus den obigen genannten Gründen können wir sagen, dass Smartcards der bessere Einsatz für einen Click-and-Buy-Automat neben einem Campingplatz wäre, solange die Technologie von NFC noch nicht so weit erforscht ist und

in der Gesellschaft nicht so etabliert ist.

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.

[Proehl, 2021] Proehl, G. (2021). An Introduction to Near Field Communications. *Mouser Electronics*. https://www.mouser.de/applications/rfid-nfc-introduction/.

[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`.