8-2023

Attacks On Near Field Communication Devices

Enow Ehabe

Attacks On Near Field Communication Devices

by

Enow-Nkongho Ehabe

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the degree of

Master of Science

in Information Assurance

August 2023

Starred Paper Committee:
Herath Susantha, Chairperson
Wang Jieyu
Farra Hazem

Abstract

For some years, Near Field Communication (NFC) has been a popularly known technology characterized by its short-distance wireless communication, mainly used in providing different agreeable services such as payment with mobile phones in stores, Electronic Identification, Transportation Electronic Ticketing, Patient Monitoring, and Healthcare. The ability to quickly connect devices offers a level of secure communication. That notwithstanding, looking deeply at NFC and its security level, identifying threats leading to attacks that can alter the user's confidentiality and data privacy becomes obvious. This paper summarizes some of these attacks, emphasizing four main attack vectors, bringing out a taxonomy of these attack vectors on NFC, and presenting security issues alongside privacy threats within the application environment.

Acknowledgments

In presenting this study, I would like to acknowledge the assistance of several persons for their support and influence during my journey through this process. First, I would like to thank my Supervisor, Dr. Herath, Susantha, for his help, advice, and knowledge which guided me throughout the research. To Dr. Abu Hussein Abdullah, Dr. Wang Jieyu, and Dr. Farra Hazem, thank you for the positive feedback to ensure my research is completed in time.

Also, to everyone who significantly influenced my career achievement and encouraged me to study and improve.

Finally, I thank to my mother and family for their unconditional love, prayers, and sacrifice. My family has always encouraged me to be a goal-getter and think for myself. Exceptional gratitude goes to my wife for her understanding and for encouraging me to finish my master's paper.

Table of Contents

Chapter Page

List Of Tables

List Of Figures

Figure Page

Figure Page

Chapter I: Introduction

Near Field Communication NFC is a technology based on short-range wireless technology for the transfer of information. With its high capacity to quickly build a contact process between two devices, it will take less time for one device to identify with the other and build a communication channel.

NFC comes with different advantages for communication, but various types of threats exist when transactions occur or when NFC makes contact. For example, when using unencrypted data in a transaction through a secure and safe channel before the transaction, the data will be vulnerable, giving opportunities to expose confidential information to others. These and many more are common vulnerabilities that can lead to attacks on NFC, and the following sections of this study look at these vulnerabilities. Based on NFC's short distance and short time transmission process, it still poses many threats that result in NFC attacks that can lead to data theft or privacy disclosure.

The subsequent sections of this study throw more light on why this technology is essential, the problems faced by the technology, and how these problems can be solved, looking at what others have done to try to find solutions to these problems. Finally, our conclusions and suggestions are proposals for feature works concerning attacks on NFCs.

Problem Statement

NFC is the set of standards used by mobile devices since around the mid-2000s to establish radio communication between these devices when brought together within a close range or is touched together.

However, NFC is still vulnerable to eavesdropping, data modification, and relay attacks. When carried out, these attacks can compromise the user's sensitive data transmitted with the

NFC. The NFC technology being exploited in sensitive areas such as the financial and healthcare sectors, with the possibility of compromised sensitive data, becomes a call for concern on security and privacy issues that have not been thoroughly investigated. Knowing the kind of attacks and attack vectors used on this technology will go a long way toward improving the technology's security level.

Nature and Significance of the Problem

A wider population has gained familiarity with NFC and is using NFC regularly. During 2010-2018 new NFC activations increased by 71% from 2010-2018 and 63% increase in NFC interactions. Thus, Bering about a total growth of 82% in NFC reached within the same time frame ("Security Risks of Near Field Communication Technology," n.d.).

With this growth, looking at a broader scale, it is estimated that they will be 1.6 billion NFC- enabled devices by 2024, with a market value of $47 billion by that same year.

Among 3.4 billion active smartphones today, there are more than 2 billion NFC-enabled devices, most phones. This gives access to 20%+ of the world's population to NFC.

An increase in the number of NFC users leads to a rise in possible NFC attack victims. Some of these attacks are because of vulnerabilities on the devices, like in the Protectimus SLIM NFC 70 10.01 devices which can allow a time traveler attack whereby the attacker can predict TOTP passwords in certain situations. Also, when configuring the NFC modules on specific devices, the possibility of failing to distinguish individual devices because of an insecure default value can lead to local execution of privileges with no additional execution privileges needed.

In 2021, a security researcher Rodriguez triggered a basic "buffer overflow" by using a custom app to send an Application Protocol Data Unit (APDU) ("Security Risks of Near Field Communication Technology", n.d.).

NFC In Contactless Payments

Contactless payment is a quick and suitable way to complete payments. Despite the usefulness of contactless payments, most standard undersized enterprises in the United States have hesitated to embrace this "contactless" payment technique.

Nevertheless, the COVID-19 pandemic has altered all that. Companies have had to upgrade their credit card processing solutions for these businesses to operate and not compromise the security of their employees and customers.

Contactless payments and the different types.

Before getting to the statistics, it is worth getting acquainted with what contactless payments are all about contactless payments. Investopedia defines contactless payments as a secure way for consumers to make payments for products or services utilizing a debit card, credit card, or smart card. They are other types of payment devices that use (RFID) and (NFC) technology. Consumers can complete payments by maintaining a payment card or smartphone near the POS (point of sale) terminal. POS terminals are compatible with contactless payment solutions for enterprises like diners, sports and fitness centers, beauty parlors, and supermarkets. This way, the shopping process becomes more suitable and safe for their customers. Contactless payments, for a better understanding, are separated into two general classes:

Mobile Wallets

Mobile wallets are arguably the most prevalent and well-known form of contactless payment, with an evaluated 150 million Americans declaring they have utilized the method at least once. Samsung, Google, and Apple have mobile applications for their digital wallets. Most Apple devices have the Apple Wallet app preinstalled on them. Most iPhone or iWatch users can complete their payments using this app. Android and Apple device users can download the

Google Pay application. However, the preinstalled Apple Wallet is more suitable for most Apple users. Just like the other two mobile wallet options, Samsung Pay works similarly. Users only need to provide their card details once they have the app installed, and the user can start making payments.

Figure 1

NFC Mobile Wallet [2]

Embedded Contactless Technology

Credit cards with contactless features have integrated chips that emit short-range radio waves. When consumers 'tap and go' or 'tap to pay' with them at an NFC-enabled point-of-sale system, payment information is shared - no physical contact is required. The downside is that they do not require a PIN or signature, so if they are lost or stolen, someone else could purchase with them at any store accepting contactless payments. To combat this, card issuers have set a transaction limit of $250 for all contactless credit cards and put anti-fraud policies in place. This means customers are protected even if their card is missing.(“US Contactless Payment Statistics 2022,” n.d.)

Figure 2

Embedded Contactless Payment [2]

US trends and key facts about contactless payments.

A study conducted by Mastercard during the pandemic revealed that 46% of respondents now store their contactless payment cards on top of their wallets. Remarkably, more than half of those aged 35 and younger have adopted this change in their buying habits. Moreover, 82% of people surveyed consider contactless payments more secure and up to 10 times faster than other methods, and this swiftness enables consumers to enter conveniently and exit stores quickly. As life returns to regular, contactless payments will remain widespread, with about three-quarters of the participants indicating that they will continue using them after the pandemic("What Is A Contactless Credit Card? – Forbes Advisor," n.d.).

In the US, contactless payments are most used to buy necessary items such as groceries. CNBC reported that a whopping 85% of grocery store transactions are made with contactless

methods. Similarly, pharmacies (39%), retailers (38%), and restaurants (36%) have all seen a surge in contactless payments ("What Is A Contactless Credit Card?" – Forbes Advisor, n.d.).

The transportation industry has been slow to adopt contactless transactions, with only about 9% of transactions being contactless. However, this was likely caused by mandatory quarantines and the transition to remote work.

Why contactless payments are rapidly adopted

The advantages of Contactless payment are undeniable when compared to traditional payments. It is no wonder consumers and retailers are quickly embracing contactless payment solutions! Some of these benefits include:

Transaction Speed

When RFID-free embedded chips were introduced, they were touted to be faster and more secure than card swiping. Unfortunately, these chips experience wear and tear over time, making them hard to read. This requires the acquirer to insert the card, wait for a refusal request, remove it, and reinsert it. If the chip is unreadable, multiple attempts may be made before the device allows swiping. Nevertheless, contactless chips and mobile wallets offer quicker payment solutions than traditional methods. A consumer can quickly complete a purchase by hovering their payment method near an NFC device – in only a few seconds(“US Contactless Payment Statistics 2022,” n.d.).

Figure 3

NFC Speedy Transaction [2]

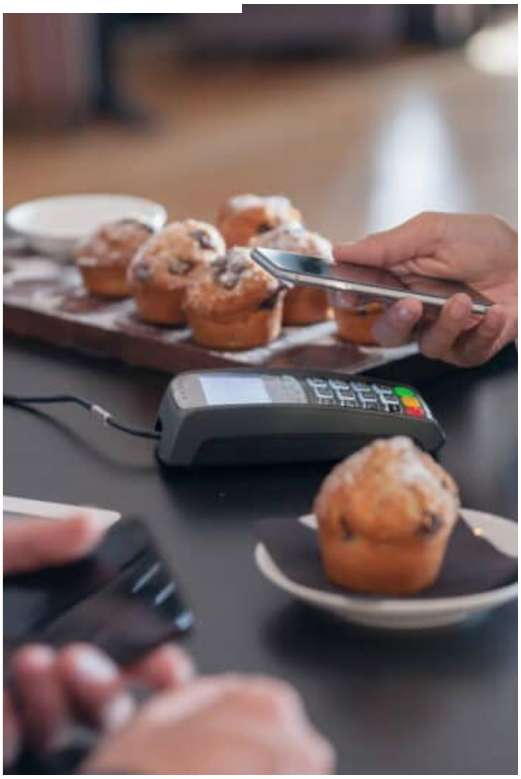
Reduced physical contact

Due to the pandemic, contactless payment options are a great benefit as they require no physical contact. Without it, customers would have to swipe or insert their card into the terminal and use the keyboard, which can spread germs and bacteria. Cleaning POS terminals is tricky, too -retailers need to be cautious, as oversaturating them could damage components. Cash payments are even worse since currency can easily transmit disease, changing hands an average of 55 times a year and some viruses staying on surfaces for up to three days(“US Contactless Payment Statistics 2022,” n.d.).

Consumers can eliminate the need to interact with store surfaces using contactless payment solutions. They must wave their mobile device or card near the NFC component and the purchase is complete.

Figure 4

Reduced Physical Contact with NFC [2]



Durability

Magnetic tapes and EMV chips can deteriorate quickly due to their frequent use for payments. Insertion and removal of cards from one's wallet may cause damage to them over time. On the other hand, contactless chips have higher longevity, often lasting for years without requiring a replacement. Moreover, mobile wallets are even more durable, especially when the phone is kept in a shockproof case.

Figure 5

Durable Contactless Payment Card [2]

Easy use for travelers

Travel restrictions during and after the pandemic have made contactless payment solutions more appealing. Before the pandemic, the US hesitated to implement this technology; however, Europe had already begun moving away from PIN or chip-based POS systems to utilize NFC solutions.

Figure 6

Contactless Payment Card Used in Travelling [2]

Adult American percentage who uses contactless payments

Almost half of adult Americans use contactless payment, including mobile wallets and tap-and-go credit cards. To accommodate this, many retailers are upgrading their payment processing technology to allow contactless payments.

By the end of 2020, around 58% of merchants could process payments from digital wallets and contactless cards. Plus, more retailers were expected to join in by 2021 due to increased consumer demand for contactless payments ("US Contactless Payment Statistics 2022," n.d.).

Percentage of banks that issue contactless-enabled credit cards

No exact percentage of credit cards supporting contactless payments has been published, but all major players have implemented the technology in their latest releases. Chase and Capital One have been offering contactless cards for some time now.

Most of the major banks are providing contactless payments on their credit cards

- American Express offers them on all cards,
- Bank of America includes it in all newly released ones,

- Capital One began offering them in 2017,
- Chase has made all cards issued or renewed since mid-2019 contactless,
- Citi has some of its cards like the Double Cash Card with contactless functionality,
- Discover makes available contactless cards to its customers on request, and
- Wells Fargo has included such technology in all new releases (“US Contactless Payment Statistics 2022,” n.d.).

Percentage of banks that issue contactless enabled credit cards

Recently, the American Bankers Association extensively examined the "contactless economy." Their research revealed that in 2019, only 11% of debit cards facilitated contactless payments (“US Contactless Payment Statistics 2022,” n.d.).

Only about 29% of issuing banks currently offer contactless cards to their customers. Another 62% anticipate to begin issuing contactless cards within the next 1-3 years, whereas the remaining 9% have no plans to do so (“US Contactless Payment Statistics 2022,” n.d.).

In 2020, 66% of issuing banks offered contactless cards, while 25% planned to start issuing them within 1-3 years. The remaining 9% had not decided on contactless cards (“US Contactless Payment Statistics 2022,” n.d.).

According to the ABA's analysis, up to 87% of debit cards should be contactless by the end of 2022. According to Ed Gross of the ABA, "Banks will receive more money on the increasing revenue line as more contactless debit cards are used on small denomination notes grows (“US Contactless Payment Statistics 2022,” n.d.).

This revenue source is the critical driver behind how quickly debit cards with contactless payment functionality are being adopted by many issuing banks.

How the use of contactless payments was impacted by COVID-19

Even while banks have begun issuing contactless payment cards in large quantities thanks to the potential to leverage the "contactless economy," the epidemic is probably why such an "economy" even exists today.

The pandemic's challenges have made consumers and retailers reevaluate their interactions. Since there is less physical touch between users of public locations while using contactless payments, shopping has been considered safer (“US Contactless Payment Statistics 2022,” n.d.).

Only a small portion of American adults used contactless payments before to COVID-19. 2020 that number climbed by tens of millions, and 101.2 million were predicted to exist in 2021. This is no doubt that the coronavirus pandemic has had a direct impact on the quick adoption of contactless payments (“US Contactless Payment Statistics 2022,” n.d.).

The statistics speak for themselves, as can be seen. The use of contactless payments has completely changed how customers shop.

In the coming years, mobile wallets will become crucial to buying. Businesses must ensure they are prepared to process this form of payment considering this fact. Therefore, it is crucial to thoroughly understand the attacks involving this technology to provide its secure operation.

Differences between RFID, NFC, and Bluetooth Technologies

Table 1

Differences between RFID, NFC, and Bluetooth Technologies

	RFID	NFC	Bluetooth
Network	A distributed application	Two Near Field Communication (NFC)-	Bluetooth is a short-range radio wireless

	architecture called point-to-point (P2P) computing or networking aids in dividing workloads or tasks among peers. An innovative distributed system is the P2P-based RFID network.	enabled devices are needed for point-to-point (P2P), which requires baud rates of 106 kbps (NFC-A), 212 kbps (NFC-F), or 424 kbps (NFC-F). The transceiver that starts polling and starts the communication is the initiator. The target is the transceiver that is initially listening to receive.	communication Wireless Personal Area Network (WPAN) technology that simplifies connections between computing and electronic devices.
Communication	RFID technology only allows for one-way communicatio n. The tag (whether active or inactive) provides data to the reader. The reader itself can scan the data but	Each device can simultaneously serve as a reader and a tag for near-field communication. Hence, making them capable of unidirectional and bidirectional communication.	Bidirectional

	does not store any information.		
Security	Hardware and protocol level	Hardware and protocol level	Protocol level
Range	Active tags release a signal to transmit data stored on their microchips. Active RFID systems typically range to 100 m and operate in a very high frequency band (UHF).	A connection between two devices using Near Field Communication (NFC) typically needs to be made within 4 cm of each other. Small data payloads can be shared through NFC between two Android smartphones or between an NFC tag and an Android device.	The distance of the Bluetooth connection is approximately 10 meters. Nevertheless, the highest communication range varies based on the electromagnetic environment or the obstructions (people, metal, walls, Etc.).
Frequency	The ultra-high frequency range includes frequencies from 300 to 1000MHz, but only two frequency ranges, 433MHz and 860–960MHz are used in	NFC primary purpose is to serve as a key for accessing content and services such as cashless payments, ticketing and access control. It's operating frequency range is centered on 13.56MHz	Bluetooth technology operates in the 2.4 GHz ISM band (2400 to 2483.5 MHz) for a good balance of range and speed. Moreover, the 2.4GHz band is available worldwide, making it the standard for low-power wireless networking.

	RFID applications. The 433MHz frequency is used for active beacons while the 860–960MHz frequency is used mainly for passive and semi-passive beacons.		
Bit rate	The RFID bit rate varies with its frequency	NFC's main purpose is to serve as a key for accessing content and services such as cashless payments, ticketing and access control. It's operating frequency range is centered on 13.56MHz, offers a data transmission rate of up to 424 kbit/s.	Using frequency shift coding, the transmission speed of traditional Bluetooth is about 1Mbps. The data transfer rate increased to 24 Mbit/s with Bluetooth Low Energy (BLE). Since the transmission speed is higher than traditional Bluetooth, BLE reduces power consumption and is important in IoT applications.
Setup time	Assuming you've already assessed your	NFC has a set time of approximately <0.1s	Bluetooth has an approximate set p time of <6 s.

	facility's environmental conditions and identified the right RFID tag (or multiple tag options for different asset types), this can be set up in a day or two.		
Power consumption	with most RFID readers, the minimum transmission power varies between 0 or 10 dBm and their maximum transmission power varies between 30 and 33 dBm.	In sleep mode, NFC chips consume only 3 to 5 mA. With the power saving mode enabled, the power consumption is even lower (5 microamps). Compared to Bluetooth, NFC is a more energy-efficient data transmission standard.	One watt is the recommended amount of power for conventional Bluetooth designs. That is a significant number in terms of wireless IoT applications. ZigBee and Bluetooth LE both operate at 10 to 100 milliwatts (mW), which is 10 to 100 times less power than what conventional Bluetooth advises.
Continuous sampling	No continuous sample	Provides continuous sampling	Provides continuous sampling
Cost	The passive tags of RFID systems can sometimes	NFC tag costs vary but typically range from $0.10 to $1.00.	They generally cost about $5 or higher.

	be very inexpensive, costing from about $0.10 to $1.50 per tag, making that one of its main benefits.		

Comparing NFC and other payment methods

NFC and EMV (Europay Master-card and Visa)

- EMV is a payment technology centered around smart cards, while NFC technology is a payment processing method that paves the way for contactless transactions.
- EMV chips can also be incorporated into bracelets and watches.
- The ability of EMV chips to securely store information is one of their most important properties.
- Dynamic authentication assigns a unique value to each new transaction made with a single EMV chip.
- While EMV smart cards need to be inserted into a card reader, NFC payments enable tap-and-pay functionality.
- Simply swipe your NFC card or smartphone over the device to process payments. EMV and NFC payments provide secure payment processing.
- Entrepreneurs use these technologies to offer their customers the latest and secure hassle-free payments.

NFC and MST

- MST technology can simulate a magnetic field like the signal from a traditional credit card.
- The terminal thinks you kept the card and didn't hang up.
- The range is close to NFC - up to 7 centimeters.
- For Samsung Pay, MST or NFC can be used for secure contactless transactions.
- The main difference is that around 90% of all merchants can accept MST, making Samsung Pay the most widely used mobile payment service on the market.

The Objective of the Study

The study aims to identify the main problems of NFC. The various methods and techniques used by attackers to compromise NFC-enabled systems and devices will be comprehensively explored to identify the most common attack vectors and come out with a taxonomy that presents a summarized version of the findings from this study.

Study Questions

The main study questions are given below.

a) How vulnerable are NFC-enabled systems to attacks, and what are the most common attack vectors?
b) Can existing countermeasures effectively mitigate the risks associated with NFC attacks, or are new approaches needed?
c) What are the potential consequences of a successful NFC attack, and how can organizations best prepare to prevent and respond to such incidents?

d) How effective are different security technologies (such as encryption, access control, or biometric authentication) at preventing NFC attacks, and what are the trade-offs between security and usability?

e) How do cultural, social, and economic factors affect the likelihood and impact of NFC attacks in different regions or industries?

Having these answers will go a long way to help identify the types of attacks that are carried out on NFCs.

Definition of Terms

Near Field Communication: Near field communication, abbreviated NFC, is a contactless, wireless technology for sending information or making payments ("Security Risks of Near Field Communication Technology", n.d.).

Eavesdropping: An eavesdropping attack, also known as a sniffing or snooping attack, is a theft of information as it is transmitted over a network by a computer, smartphone, or another connected device ("What Is an Eavesdropping Attack?", n.d.).

Application Protocol Data Unit (APDU): A part of the Open Systems Interconnection Reference model application layer used for communication between two separate device applications. In the context of smart cards, an APDU is the communication unit between a smart card reader and a smart card (National Institute of Standards and Technology, n.d.)

TOTP: Time-based one-time authentication password.

Summary

This chapter emphasizes a little background knowledge on what NFC is all about, looking at the problems faced by this technology and why it’s essential to pay attention to them.

In the next chapter, a different look will be taken at the works others have done concerning some of these problems faced by NFC.

Chapter II

Background And Review Of Literature

Introduction

The NFC technology has been around for some time now. As millions of users use it to carry out daily activities, different problems keep arising for the technology, and many researchers have investigated these problems in different ways. In this chapter, some of the work done by some of these researchers will be looked at to understand better what has been done so far, what needs to be done, and how to do it to make this technology more secured and reliable for everyday use.

Background Related to the Problem

The increasing number of released NFC applications raised a call for concern about its security issues.

It has since had global interoperability, making NFC usable in multiple areas based on its different communication protocols and data-exchanging formats. Some of these areas that can benefit from this technology are:

- Payment with mobile devices (smartphones and tablets)
- Electronic identification
- Transportation electronic ticketing
- Credit cards integration in mobile devices
- Data transfer between devices (media players, mobile phones, digital cameras)
- transferring data between wireless devices using a peer-to-peer connection.
- Pairing devices
- Patient monitoring and healthcare

Figure 7

NFC Applications [1]

Most of these areas can be integrated into a single device, facilitating, and increasing the user's experience in different environments. In addition, the short communication distance between terminals increases security using this technology. Many security researchers have attempted the analysis of vulnerabilities and attacks on NFC technologies.

Literature Related to the Problem

Near field communication (NFC) is highly adopted in different technologies and applications due to its short-range frequencies, making it suitable for token-based security access control. However, the small size of NFC tags, plain text content and an unprotected communication channel between the tag-reader and database makes NFC vulnerable to attacks such as man-in-the-middle, DOS, and many more attacks.

Singh (2018) stated in their work on NFC technology and security vulnerabilities and countermeasures that NFC attacks have led to the leakage of critical user data, which could seriously impact any organization adopting NFC applications. They also looked at NFC

vulnerabilities causing both security and privacy attack (Singh, 2018). By paying special attention to attacks such as DOS and data corruption, existing risk management models are evaluated using Analytical Hierarchy Process (AHP). They also presented best practices for mitigating these attacks (Porter, 2021).

Cavdar and Tomur (2015) looked at the practical relay attack on mobile devices using card emulator mode. Although NFC originated from Radio Frequency Identification (RFID) technology, security needs, requirements, and solutions differ in use and application solutions. The security precautions in the RFID technology of the communication layer cannot prevent the relay attack in the application layer. Their study conducted a relay attack to show how possible it can occur by using only mobile phones for relaying credentials instead of RFID-based smartcards in access control applications. The relay attack is also facilitated with the help of the Host Card Emulator (HCE) mode. This study explained the conceptual description of the proposed relay attack, the development and operational logic of mobile applications based on the card emulation mode, and the description of the server software and web services (Cavdar & Tomur, 2015).

In his article on NFC vulnerabilities and defenses (2014), Naveed Ashraf Chattha pointed out the top relevant concerns about NFC technology, which shows that the technology is vulnerable (Chattha, 2014b). Some of the vulnerabilities listed in the document are:

Eavesdropping: NFC communication occurs in wireless mode, which is very susceptible to eavesdropping. It is a core threat in wireless communications that requires additional resources to stop such incidents (Chattha, 2014b; "What Is an Eavesdropping Attack?", n.d.).

Data corruption: Data transmitted via the NFC interface can be modified by an attacker if he can intercept it. Data corruption can be viewed as a denial of service if the attacker changes the data to an unknown format (Chattha, 2014b).

Data change: To move from data corruption to data change, the attacker changes the actual data with valid but incorrect data (Chattha, 2014b).

Data insertion: An attacker can insert false and unwanted data in messages into the data while it is exchanged between two devices (Chattha, 2014b).

ManinMiddle attack: In a ManinMiddle attack, a third party deceives the two legitimate parties into the other honest party and thus directs the communication between the two parties through the third party (Chattha, 2014b).

Literature Related to the Methodology

Using taxonomy to clarify security issues and attacks on NFC goes a long way to providing a clear understanding and shedding light on security issues on NFC. Ron Bitton et al., in their article on mobile users' security awareness Taxonomy, present a hierarchical taxonomy for security awareness explicitly designed for mobile device users. Their taxonomy defines a set of measurable criteria classified according to different areas of technological interest and in the context of psychological dimensions. The applicability of the proposed taxonomy is demonstrated by introducing an expert-based procedure to derive mobile security awareness models for different classes of attacks. Each type aggregates social engineering attacks that exploit similar human vulnerabilities. Each model reflects the contribution of each criterion to the mitigation of the corresponding class of attack (Bitton et al., 2018).

A summary of more work that has been done concerning the problems faced with NFC and its base RFID technology is shown below with for the Article title, the research problem, major

findings of the research, the further research studies, source of the material, and finally the goal of the research.

I. **Title of article:** NFC Technology: Assessment Effective of Security towards Protecting NFC Devices & Service (Albattah et al., 2020).

Research Problem: Near Field Communication (NFC) has become an important feature of our daily life. This technology

has offered an easy way for data exchange and information transfer with NFC tags to be integrated into most technologies used. It can be read with a mobile device that supports NFC technology. Wave Credit card or phone at checkout overwhelms you with pleasant feelings. However, some risks are mainly related to unencrypted data transmissions, unsecured hardware, software, or communications.

Major findings: The study discovered that using a secure channel is the best defense against data modification, relay attacks, eavesdropping, and data collection. It also discovered numerous other ways to defend against attacks, including using RF checkboxes and encrypted data. (Albattah et al., 2020)

Further Studies: Looking at potential attacks on NFC and implementing scientific mechanisms against these attacks.

Source of Material: Albattah, A., Alghofaili, Y., & Elkhediri, S. (2020).

Goal: The main purpose of this article aims to provide a general overview and comparison of NFC technology with RFID. In addition, it has reviewed various types of attacks and finally tried to find some scientific mechanisms that can help increase security in NFC performance and ensure information security on NFC technology.

II. **Title of article:** Security of NFC Banking Transactions: Overview on Attacks and Solutions (Chabbi et al., 2022)

Research Problem: The usage of this NFC technology causes security difficulties, notably for contactless transactions - NFC with an automatic teller machine (ATM) or point of sale (PoS) Device.

Major findings: An introduction to the NFC technology world overview. After that, a presentation on the most well-known NFC device attacks and NFC communication during NFC banking transactions will take place.

Further Studies: Look at the advantages and limitations of the proposed main solutions for the protection of Bank transactions with NFC.

Source of Material: Samir Chabbi, Nour El Madhoun, Lazhar Khamer. (2022)

Goal: In this article, Gold would first like to present the most well-known attacks on NFC banking, followed by an overview of the main ones Recently, solutions were proposed to secure NFC banking transactions.

III. **Title of article:** Security in Near Field Communication (NFC) (Haselsteiner & Breitfuß, n.d.-a)

Research Problem: Looking at the security of NFC in various applications.

Major findings: Comprehensive analysis of security issues related to NFC is provided in this article. It is not limited to a specific NFC application but uses a systematic approach to analyze different security aspects whenever NFC is used. presented typical use cases for NFC interfaces. A list of threats has been compiled and addressed.

Further Studies: Employ key agreement techniques to provide a standard secure route without authentication.

Source of Material: Ernst Haselsteiner and Klemens Breitfuß

Goal: To clear up many misconceptions about security and NFC in different applications.

IV. **Title of article:** NFC - Possibilities and Risks (Trottmann, 2013).

Research Problem: NFC provides an easy way to share information with NFC tags that can be embedded and readable anywhere NFC-enabled mobile device in your pocket. However, some risks are mainly related to unencrypted data transfers, fledgling software libraries vulnerabilities, or theft.

Major findings: NFC has already been integrated into contemporary smartphones, devices, and operating systems and will continue to be. Touching two NFC devices together enabled payment services, broadband connection establishment, information sharing, and identity verification.

Further Studies:

Source of Material: Lehrstuhl Netzarchitekturen and Netzdienste.

Goal: To provide an overview of how NFC technology works with some of its present and potential applications and what threats and vulnerabilities arise with its simplicity.

V. **Title of article:** Security Issues in Near Field Communications (NFC) (Alrawais, 2020)

Research Problem: Near Field Communication technology cannot protect against most studied attacks, such as eavesdropping or data modification, offer no protection. Establishing a secure channel between NFC devices mitigate many security risks.

Major findings: This article discusses possible solutions to mitigate these security threats after reviewing related documents. Also attacks Evaluation of countermeasures in terms of practicality and cost were further investigated.

Further Studies: Future work on Near-filed communications could focus on developing reliable near-filed communications operations. In addition, other security-related attacks require further investigation, such as: Examples include NFC session hijacking, cloning attacks, counterattacks, and NFC skimming attacks that read an NFC device in a person's pocket. In addition, using near-filed communications in a payment system raises several privacy issues that require further investigation and analysis.

Source of Material: Arwa Alrawais (2020)

Goal: This article analyzes NFC vulnerabilities and uses different types of security attacks.

VI. **Title of article:** Issues in NFC as a Form of Contactless Communication: A Comprehensive Survey (Ghosh et al., 2015).

Research Problem: Know the security issues available in all respected internal branches that are constantly trying to increase the number of users of this NFC technology.

Major findings: the problems present in the current technology of big industries like Apple, Google, PayPal were found and came up with new ideas to solve them. Also, analyze the NFC business ecosystem and current/future market trends. In other words, this holistic review leading to the innovative design of NFC ensures that knowledge in the field advances alongside future research directions.

Further Studies: looking forward to developing an NFC system enabling contactless card-to-card transactions. Also: comparison of NFC vulnerabilities applications on different services. Development of design principles and methodology for building specific applications such as an intelligent environment. Developing user interface templates for various areas of application. Economic Outcomes of NFC Development.

Identification and demanding barriers and problems to getting initiated with new NFC applications. Exposure to medical, psychological, and relationship issues in NFC customizations. Potential NFC apps based on pear-to-pear. Impact of NFC technology on different organizations, companies, and business models. Biometric security in NFC applications. Health monitoring with NFC for economical use.

Source of Material: Shirsha Ghosh, Joyeeta Goswami, Abhishek Kumar, and Alak Majumder (2015)

Goal: Offer an in-depth NFC investigation and discuss it based on their point of view.

VII. **Title of article:** Qualitative Assessment on Effectiveness of Security Approaches towards Safeguarding NFC Devices & Services (Anusha & Shastrimat, 2018).

Research Problem: Research is being done to strengthen the security system, but no standard protocol or security framework has yet been reported to ensure maximum resiliency.

Major findings: It's pretty evident that using strong cryptographic rules can lead to potential encryption, which is good for security but may not provide better communication performance for many streaming applications in the future.

Further Studies: The next research phase will focus on using some lightweight cryptographic approaches, such as B. the never-before-tested hummingbird to secure NFC communication. As the hummingbird unlocks the potential of stream and block ciphers, there is a good chance of minimizing any form of computational complexity associated with the cryptographic algorithm in NFC.

Source of Material: Anusha R., Veena Devi Shastrimat V.

Goal: The main goal of this article is to provide a comprehensive overview of the effectiveness of existing research approaches in formulating a research trend and research gap.

VIII. **Title of article:** NFC Technology: Current and Future Trends in India (Dhar & Dasgupta, 2014)

Research Problem: NFC is in its infancy, especially in India, largely due to the lack of a proper ecosystem. However, implementation is incremental, and several solution providers are working to make the technology available.

Major findings: An overview of NFC technology and its present and potential future in India is given in this article.

Further Studies: It proposed a healthcare system that could manage medical records effectively between patients, physicians, and other staff members with the help of NFC.

Source of Material: Sudipta Dhar, Aniruddha Dasgupta

Goal: This article aims to provide an overview of NFC technology, discuss its adoption worldwide and then focus on the current trends and applications of NFC technology in India. Therefore, existing NFC applications and some possible future situations are analyzed. In addition, current security issues, challenges and conflicts are discussed.

IX. **Title of article:** Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens (Hancke, 2011).

Research Problem: Near-field communication electronic passports and credit cards are just two safe applications that use HF RFID technology. These gadgets' radio communication interfaces are open to eavesdropping and skimming attacks. Although

these attacks are a known danger to RFID devices, few articles specify a potential experimental setup or valuable outcomes.

Major findings: Briefly describe the radio capabilities of the well-liked HF-RFID and give valuable results of eavesdropping tests using ISO 14443 and ISO 15693 tokens. It also demonstrates how an attacker may create a low-cost eavesdropping device utilizing parts that are easily accessible and reference designs. The outcomes of the skimming tests performed against ISO 14443 tokens are then provided.

Further Studies: Improved data recovery techniques should be developed, as well as tests to see how different drive designs affect eavesdropping distance. Listening distances are achievable, for instance, when chatting passively and actively on NFC-enabled mobile devices. Consider utilizing E-field antennas to listen in on reader-token communications or if data is unintentionally being communicated in other frequency bands.

Source of Material: Gerhard P. Hancke

Goal: Looking into eavesdropping and skimming attacks of RFID, reviewing previous work, and explaining why the feasibility of practical attacks is still a relevant and emerging research topic.

X. **Title of article:** A Platform for RFID Security and Privacy Administration (Rieback et al., n.d.).

Research Problem: RFID automation's unimaginable avalanche of new uses will eliminate wires, grocery store cashiers, credit cards, and pocket cards. Supporters of RFID applaud its business uses for supply chain and real-time resource management. RFID-based passports control residential, commercial, and international crossings;

drivers have embraced RFID-based retail systems like EZ-Pass, FastPass, IPass, PayPass, and SpeedPass. RFID-based personal "health" applications are also becoming more prevalent, from "smart" dishwashers to kid-friendly interactive toys to senior care at home.

Major findings: The systems platform offers granular control of RFID-based verification, key management, access control, authentication operations, and the automated and coordinated usage of RFID security methods. Experience has demonstrated that active mobile devices are an excellent tool for controlling RFID tag security in several applications, including protecting inexpensive tags that cannot control your use. It also prototyped the RFID Guardian using commercially available components.

Further Studies: This article not only offers a solution to a current practical problem but also gives an insight into how systems management might look in the future world of ubiquitous computing.

Source of Material: Melanie R. Rieback, Georgi N., Gaydadjiev Bruno Crispo, Rutger F. H. Hofman, and Andrew S. Tanenbaum

Goal: This article is intended to provide a glimpse of what system administration might look like in the future when laypersons are faced with the need to manage small computer systems that they know nothing about.

Summary

Looking at how much work has been carried out by different researchers on these problems and attacks on NFCs, shows the importance of this technology and how important it is to find long-lasting solutions to these problems. Form the different articles studied, the research

emphasis is not only on NFC but also on related technologies, which helps in the proper functioning of the NFC technology. The next chapter will focus on how to come up with the solution to most of the problems encountered in these studies.

Chapter III: Methodology

Introduction

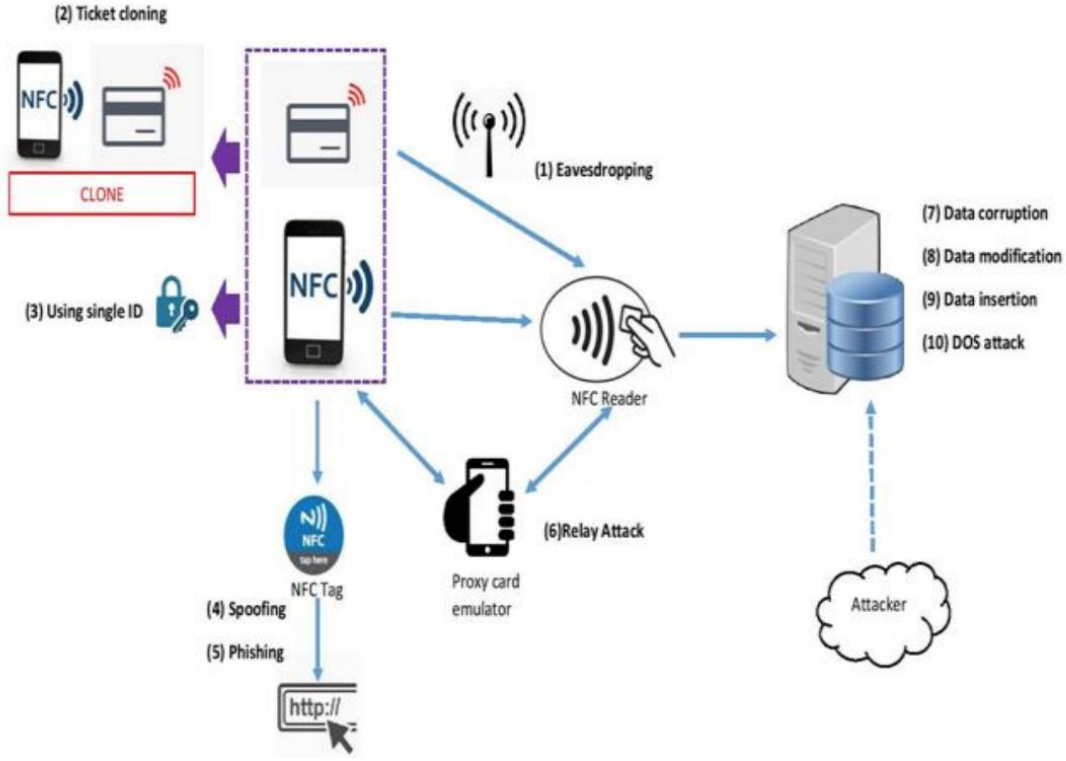
It is essential to note that every problem has its cause and trying to solve a problem without understanding its cause makes the process tedious and complicated. This chapter focuses on these root causes of attacks on NFC to better understand their origin.

Design of the Study

The physical nature of sensors on NFC and the mechanism of an operation whose communication channel is not secure can lead to or facilitate the occurrence of security attacks in NFC. Below, the figure illustrates the attack that can occur on NFC in general, emphasizing the different levels on which different kinds of attacks occur. For example, it can be seen from the figure below that the data corruption, modification, insertion, and DOS attacks, can happen on the technology’s sever level.

Figure 8

Attacks on NFC [1]



Data Collection

The data collected and analyzed in this study came from a controlled environment using Qualitics online survey tool. A comprehensive survey has been created using Qualitics to understand the basic behavioral activities of some random NFC users. This aimed to understand the root causes of NFC attacks by looking at the origin of the attack vectors. This survey was shared online on social media platforms to reach a wider population quickly. Their responses collected raw data on these NFC 'users' initial and primary routine activities. The results were then analyzed to come out with and identify some primary attack vectors and their origins.

Tools and Techniques

For conducting surveys, assessments, and other data-gathering tasks, Qualtrics is an accessible online survey platform for both novice and experienced users. This research suite allows anyone, regardless of expertise level, to construct surveys, submit surveys, and evaluate replies online, at any time and from any location. For this paper, the Qualtrics survey tool is used for the following reasons:

- It's free
- No software installation is required
- User-friendly point-and-click interface. The process is quick and easy, and the results are available immediately.
- Surveys with graphics, complex branching, and randomization can be created by anyone.
- 85 and more question types.
- Many question and survey templates to choose from.
- Tools for all types of users, basic and advanced users, and surveys.
- Can upload graphics and media to surveys.
- Publishing on the internet helps to reach a larger audience.
- Multiple polls can be published simultaneously and in 48 different languages.
- Respondents can stop taking the survey midway through and continue where they left off.
- Integrated reporting tools for dynamic data Direct data exporting to SPSS, CSV, PDF, Word, Excel, and PowerPoint is possible.
- Real-Time Collaboration Feature, both CSULB and non-CSULB users can shear with one another.
- Availability of Qualtrics free online training webinars

- Qualtrics staff offer live support.

Summary

The approach to the study has been presented in this chapter. The study followed the quantitative research method that involved a comprehensive survey. The survey was to gather primary usage and configuration information from random NFC users to understand the origin of some common attack vectors and then identify the origin of the common attacks NFC. The survey provides accurate life information from day-to-day NFC users, which can be used to understand NFC attacks from an attack vector perspective.

Chapter IV: Data Presentation and Analysis

Having previously examined several security measures against NFC attacks, random NFC user's daily routines are analyzed to discover and comprehend which routines best ensure that end users' data is protected, safe, and private and which encourages attacks against NFC. A survey with over 50 randomly selected participants was done to gather additional quantitative information on the efficiency of different security practices in assuring and comprehending NFC users. The following questions were posed to the participants.

1. How old are you?
2. How do you describe yourself?
3. Do they use contactless card payments?
4. Do you know about NFC?
5. Have you used NFC?
6. What did you use it to do?
7. Did you configure the security setting yourself?
8. Did a technician configure the security settings?
9. Did they use default security settings?
10. Do you double-check an NFC reader when using your NFC device with it?
11. Have you ever had any security issues with NFC?
12. Do you store their NFC card/securely?

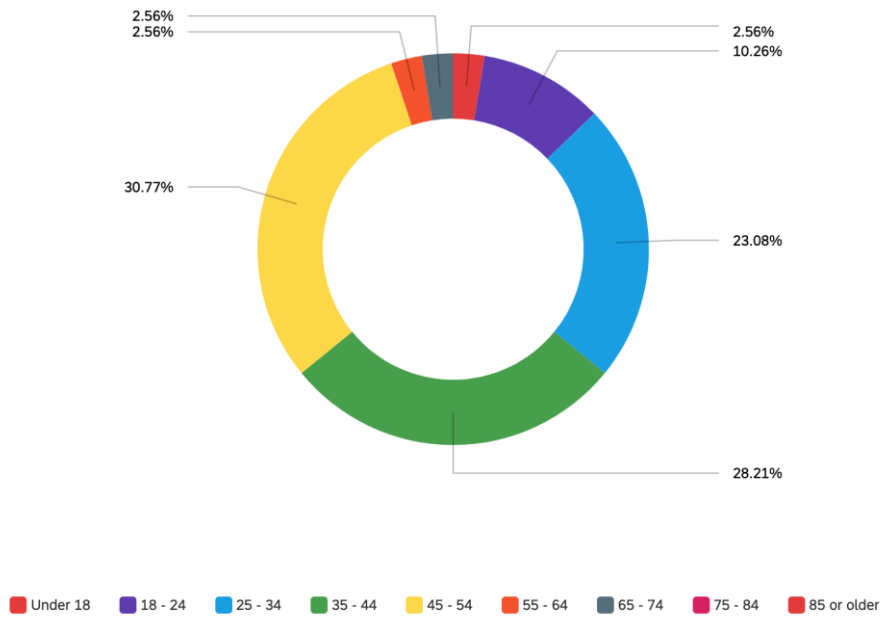
To gain more replies from end users and to keep their attention throughout the survey, this survey's 12 questions with clear answers were purposefully reduced to a minimum. This allowed for accurate data to be collected for analysis and trustworthy results to be generated. Also, all

technical terms and procedures contained in the survey were explained to participants as they took it to ensure that the results were correct.

I. Survey responds to question 1 are discussed below

Figure 9

Survey Responds for Question 1

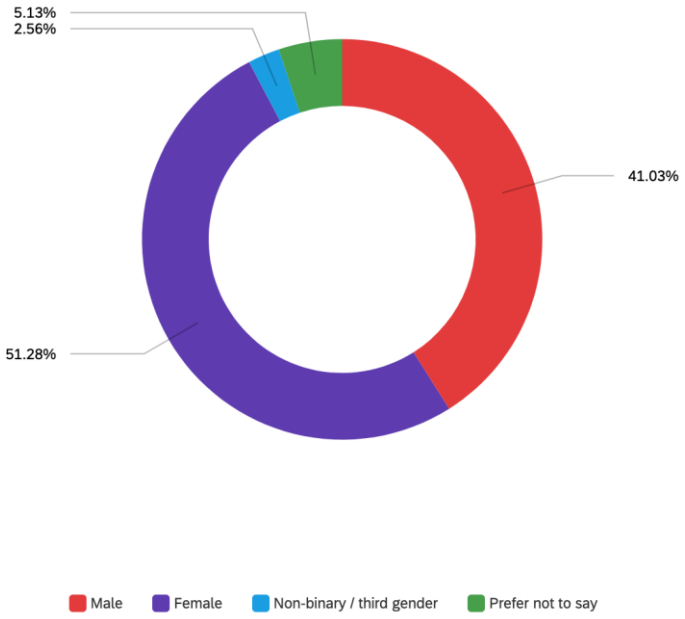


From the above results in Fig 9, the question asked the participants their age, and 2.56% of the participants were under 18, 2.56% between 55 – 64, 2.56% were 65 – 74, 10.26% were 18 – 24, 23.08% were 25 – 34, 28.21% were 32 – 44, and the majority age group was 45 – 54 years with a percentage of 30.77%. The survey did not focus only on a specific age group; all age groups were represented.

II. Survey responds to Question 2

Figure 10

Survey Responds for Question 2

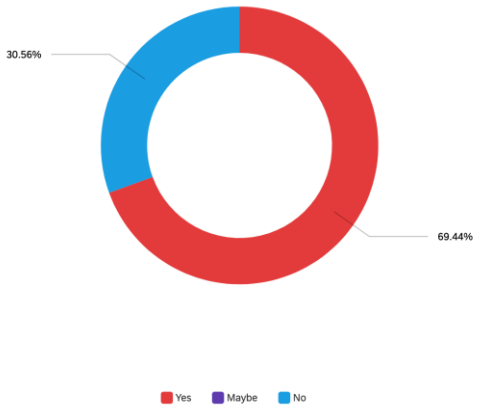


Also, the results seen in the above Fig10, show the gender distribution of the different participants.

III. Survey responds to Question 3

Figure 11

Survey Responds for Question 3

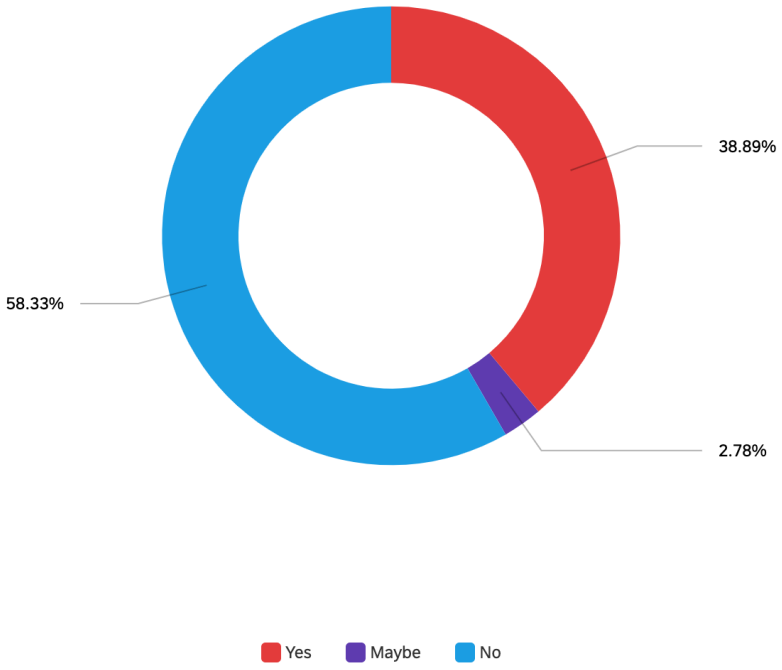


The above result of question 3 finds out amongst the participants who use contactless card payments. This is to understand the number of participants who use and know about contactless payment methods in general. According to the results, 69.44% of the participants use contactless card payments, and it's noted that most contactless cards have an NFC baseline technology.

IV. Survey responds to Question 4

Figure 12

Survey Responds for Question 4

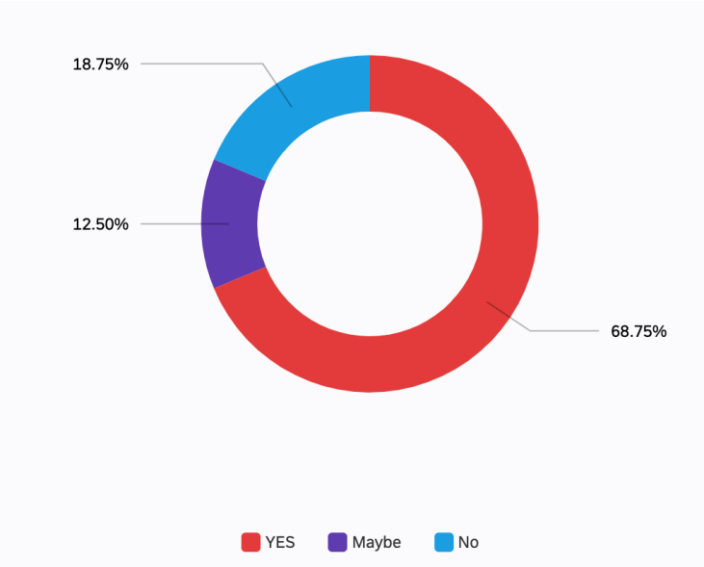


The results of question 4 show that 38.89% of participants who use contactless payment know about NFC and 58.33% don't know about NFC, and 2.78% are unsure if they know about NFC or not.

V. Survey responds to Question 5

Figure 13

Survey Responds for Question 4

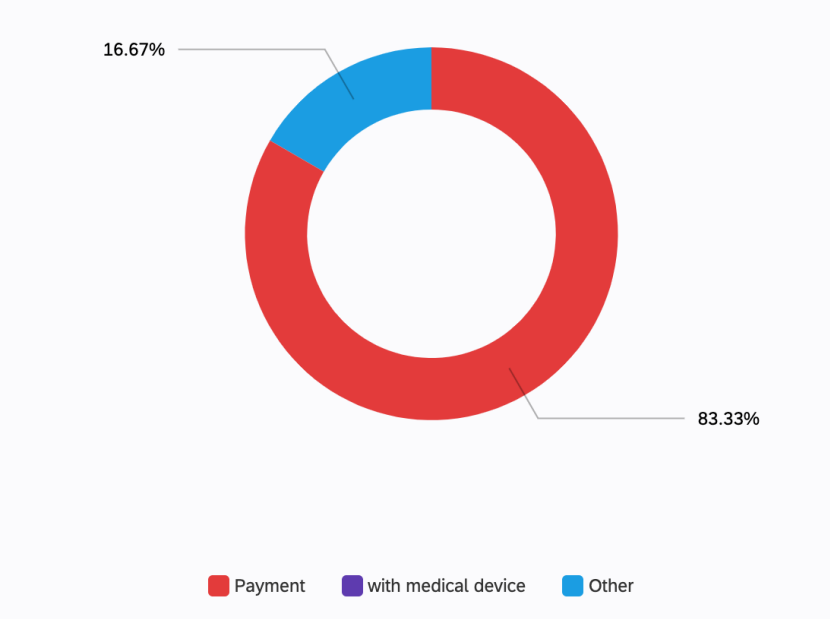


With respect to the percentage of participants who know about NFC, 68.75% of them use NFC, 18.75 % do not use NFC, and 12.50% don't know if they use it or not. From this result, it can be noticed that those who don't know if they use NFC or not will not be able to take the necessary needed security measures if they use the technology in their daily life and this can lead to misuse and subsequent loss of data through an attack on their NFC device or card.

VI. Survey responds to Question 6

Figure 14

Survey Responds for Question 5

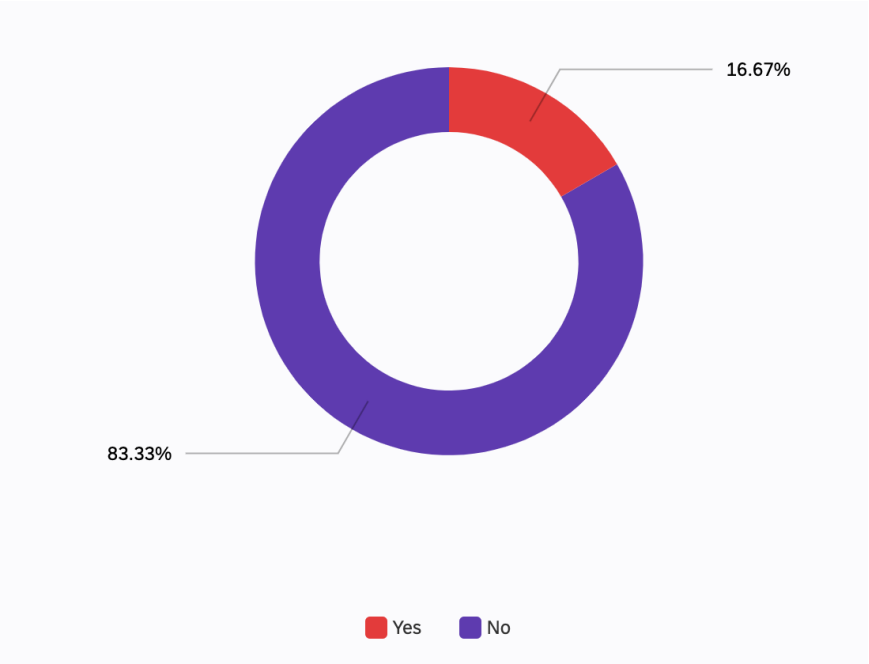


To know what the NFC users use it for mostly, the question of what they use it for was asked, and the above results in Fig14 were obtained. From the results, it can be observed that 83.33% of the participants use NFC for financial transactions, which always contain very sensitive data that must be protected from the wrong hands. The remaining 16.67% use NFC for other purposes.

VII. Survey responds to Question 7

Figure 15

Survey Responds for Question 7

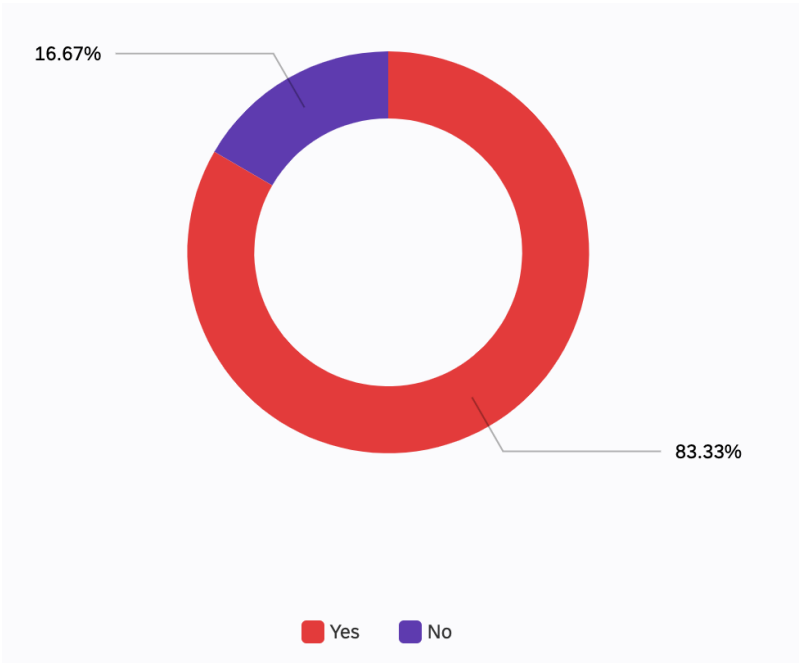


The seventh question of this survey was to find out if those who use NFC did the security configurations themselves or by someone else. The results show that the user did not do 83.33% of the security configurations and 16.67% of the users did their configurations by themselves. This brings a call for concern since when carrying out security configurations, some major technical factors need to be considered to ensure the secured functioning of their NFC. That brings us to the next question to know if the security configurations were done by somebody knowledgeable enough to ensure it is done properly.

VIII. Survey responds to Question 8

Figure 16

Survey Responds for Question 8

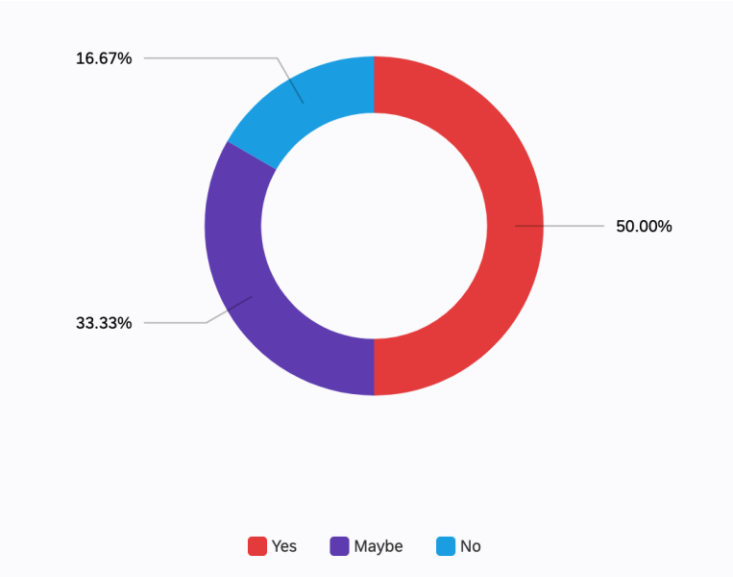


As seen in question 7 above, they did not do most of the user's security configurations. This leads to question 8 to determine if the person who did the security configurations was a technician or lay person. The percentages of the question 7 results are the same as in question 8. A knowledgeable person must do the security configurations so that the possibility of an attack on the user's NFC can be significantly reduced, making it more secure.

IX. Survey responds to Question 9

Figure 17

Survey Responds for Question 9

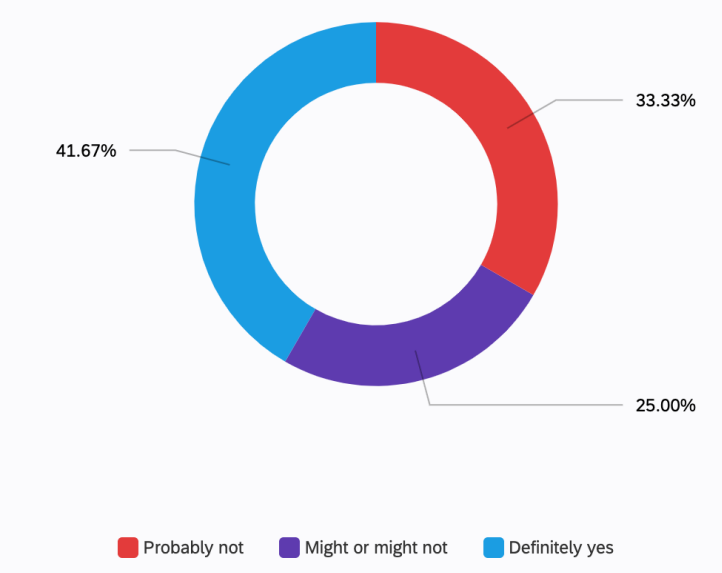


The above results are for question 9, which finds out if the security setting used were the default settings or personalized settings were used, and we see that 50.00% of the participants used default settings. This can be a serious call for concern because these default settings can harbor known NFC vulnerabilities, which can act as an attack vector for an NFC attack. The other 33.33% did not realize, while 16.67% did not use default security settings.

X. Survey responds to Question 10

Figure 18

Survey Responds for Question 10

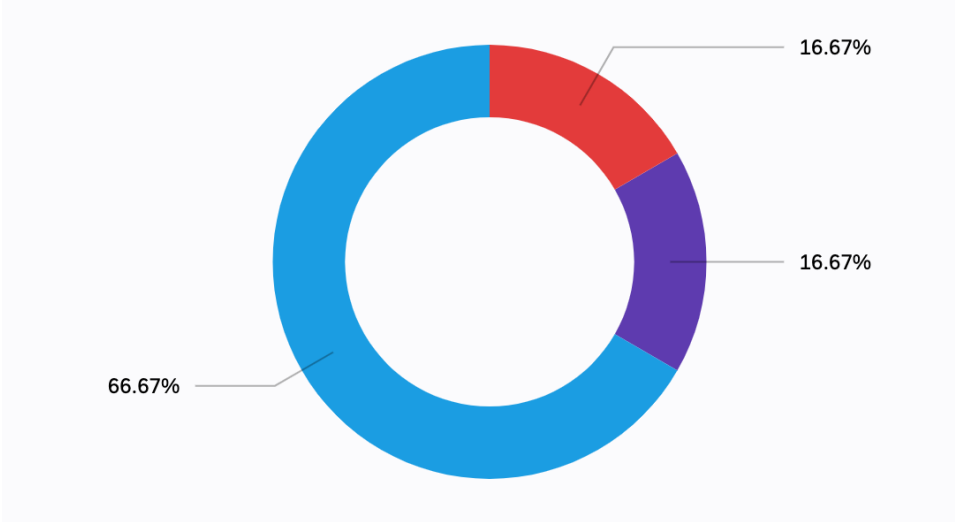


Question 10 of the survey aims to determine if users double-check the NFC readers before using their NFC device. Here it is seen from the results that 33.33% of users don't double-check these NFC readers before they use them, which can lead to a breach of confidential data if the reader has got a fraudulent installation on it.

XI. Survey responds to Question 11

Figure 19

Survey Responds for Question 11

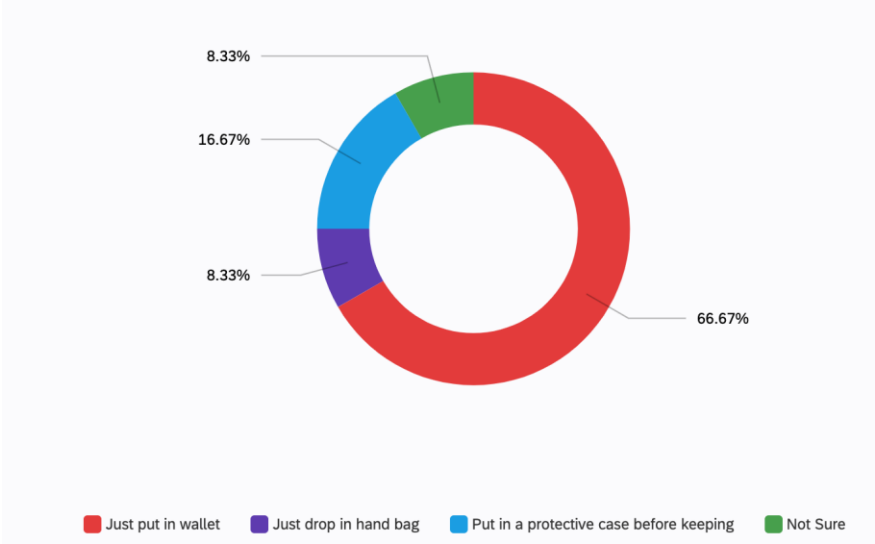


Knowing if these users have ever had security and privacy issues with their NFC is a primordial factor in bringing out the importance of the survey. The results show that 66.67% of the participants who use NFC have never had security and privacy issues with their NFC and 16.67% have been victims of security and privacy issues, and 16.67% don't know if they have been victims or not.

XII. Survey responds for question 12

Figure 20

Survey Responds for Question 12

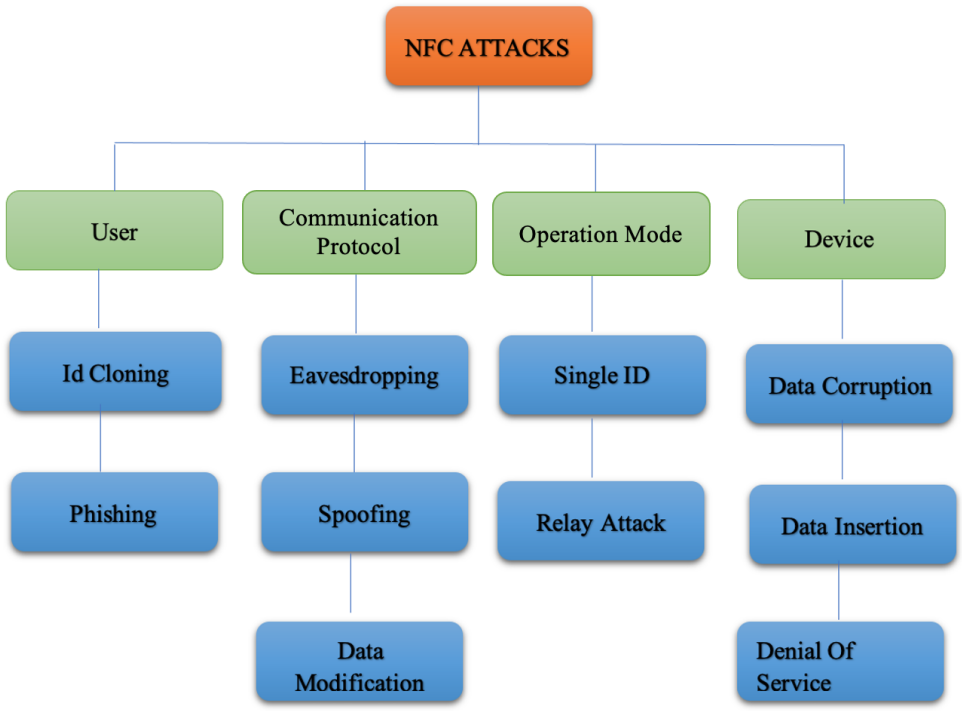


How the users keep their NFC devices is very important to, which gives the reason for question 12. The level of security with which the NFC device or card is kept goes a long way in preventing an attack on the NFC device. The results shows that 66.67% of participants who use NFC just put their cards in their wallets, making them very vulnerable to attacks. 8.33% drop it in their handbag, 16.67% put protective cases before keeping preventing an attack on it, and the other 8.33% are unsure if they are keeping the NFC cards or devices as secured as they should.

Looking at the different responds gotten from the comprehensive survey on NFC users, a hierarchical taxonomy for the different types of attacks on NFC devices is designed explicitly concerning other attack vectors that influence the occurrence of these attacks on NFC, such as the user's activities, the connection between the devices, protocol, and the type of device used. These attacks are briefly explained and described in how they can be carried out on NFC devices.

Figure 21

Taxonomy of NFC Attack Vectors



User

Regarding users, note that it is not necessarily the owner of the NFC device. It also includes the stakeholders of the NFC transaction and their permissions concerning the given NFC transaction. The owner of the NFC device must be able to approve the NFC transactions and ensure it has maximum security to protect it should it be lost or tampered with. Also, the

merchant, the receiver of the NFC payment, should be able to validate the transaction details. They should not obtain sensitive information about the owner's card or device, and the merchant should not adjust the transaction details.

Id Cloning: NFC is known to be helpful in payment systems and ticketing services, for example, e-tickets. Cloning a ticket from NFC can be possible if, before verification, it is copied and shared with others (Chen et al., 2014). Once the ticket has been verified, anyone with the clone can use it as a new ticket to carry out the same activities as the original ticket. This can go on until the ticket is expired. This cloning can occur in two different ways depending on the design of the ticket system. The other way the cloning can be done is by the user's multiplication and shearing of an already verified e-ticket for others to use. The main objective of this cloning is to make the ticket available and share it until it expires. In a nutshell, the type of cloning (pre-validation cloning or post-validation cloning) (Ceipidor et al., 2013), the owner has a role to play in facilitating the attack, knowingly or unknowingly, during ticket validation.

Phishing: For a phishing attack to occur on NFC, the user's phone is used to read an NFC, which an attacker has altered to mislead the user. The user is then redirected to the site that the attack wants instead of the original internet site of the NFC tag (Madlmayr et al., 2008). This site will let users enter their personally identifiable information and the data sent to the attackers.

Communication and protocol modes

For the proper functioning of the NFC technology, some main standards and operation modes are needed to organize the base communication protocols. Looking at these standards briefly to understand how they facilitate the functioning of the NFC, they are

- The ISO/IEC 18092 Standard is the current standard for NFC technology (Noh & Choi, 2013). The developers of this standard, SONY Corporation, Nokia Corporation, and NXP

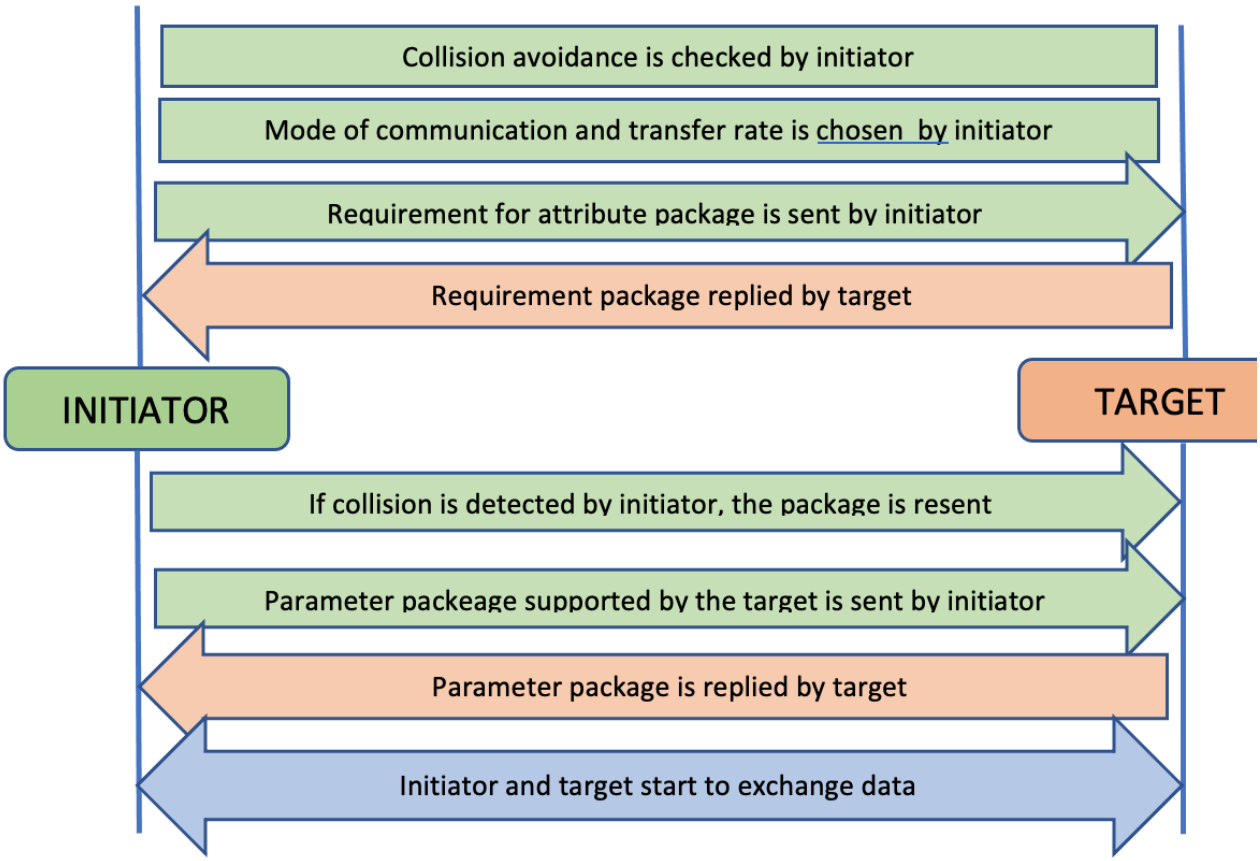
Semiconductors, submitted a draft to the Electronic Computer Manufacturers Association (ECMA) for examination and validation. When the ECMA confirmed the standard, it was sent to the International Standard Organization for reexamining and publishing. This standard identifies if an NFC device is the target or the initiator during the NFC communication process. The communication is then divided into two modes: the active or the passive mode. An effective contact distance of under 15 centimeters is also stated.

The communication mode, either active or passive, is chosen by the initiator before each contact starts. Once it is selected, the mode cannot be changed until the end of the communication. A transfer speed of 106 Kbits/second, 212kbits/second, or 424kbits/second is decided after the initiator and target are fully coordinated.

The protocol of the NFC communication mode is shown in the figure below. To avoid a collision, the initiator, before contact with the target, broadcasts a signal to the external radio field to make sure the field exists or to detect anyone if that field does not exist by activating the target with its own generated radio field. The initiator then chooses which mode to use for communication with the target. If the active mode is chosen, the target can communicate with the initiator using their radio field. As soon as the target learns about the initiator's message, it activates its radio field to reply to the initiator. But if the initiator selects the passive mode, a temporary transfer rate will be used for communication. The package for attribute requirement is sent to the target, and the target replies to the request, but its own frequency field is not activated. The initiator's frequency field will determine the power of the target. Once the initiator receives the response, the transfer rate is adjusted with respect to the target's required speed.

Figure 22

NFC Communication Mode



- ISO/IEC 14443 Standard: the transmission protocol and the communication standard between the mobile phone's emulated card and the reader are defined with this standard.

The frequency on which the wireless activities mainly operate is on 13.56MHz. The two main transmissions of NFC are the NFC-A and the NFC-B (Chen et al., 2019; Enzinger, 2009). However, the third technology, known as NFC-F, was developed by the SONY Corporation. In

addition, the Japanese Industrial Standard (JIS) X6319-4 provides the technology for air interface, which is now part of the ISO/IEC 18092 standard.

For different types of tags in NFC can be seen in the table below, with the differences between each of the tags. For example, the users can determine the read or write function in type1 and type 2 tags while the type 3 and type 4 can be read and re-writable or read-only.

Table 2

Types of NFC Tags

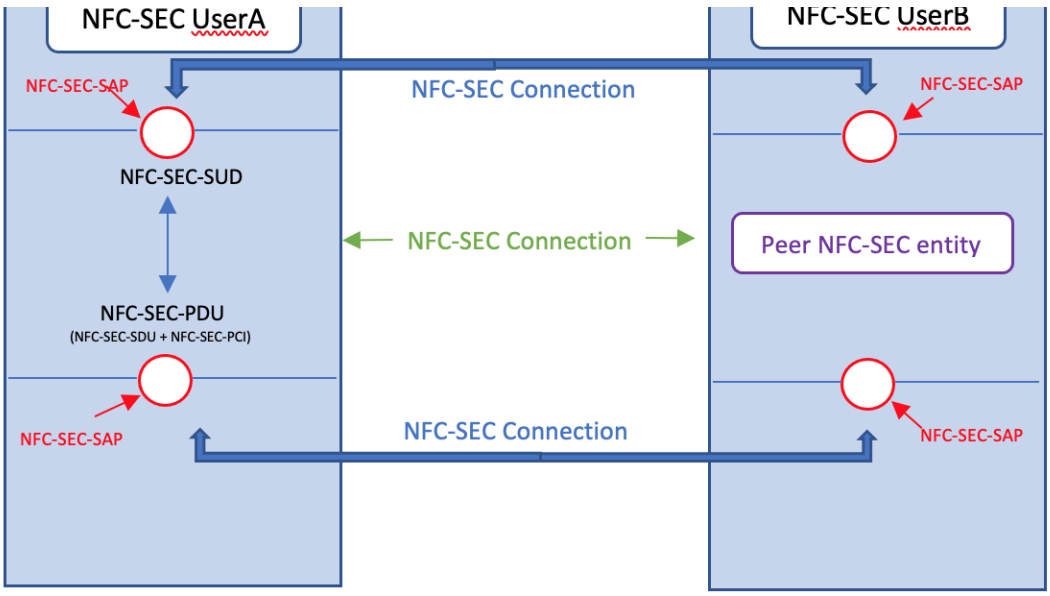
Tag	Type1	Type2	Type3	Type4
Standards	ISO/IEC 14443A	ISO/IEC 14443A	JIS-X 6319-4	ISO/IEC 14443A/B
Capabilities	Read and re-write	Read and re-write	read-only or already configured to be writable	read-only or already configured to be writable
Memory	96 Bytes. Expandable to 2 Kbytes	48 Bytes. Expandable to 2 Kbytes	1Mbyte per service	Variable. Max: 32 KB per service
Data Rate	106 kbits/S	106 kbits/S	212 Kbits/S 424 Kbits/S	106 kbits/S

- ECMA 385 and ECMA 386 standard: The Shared Secret Service (SSE) and the Secure Channel Service are the key services covered by this standard (SCH) (Isaivani & Kannadhasan, 2014; Kortvedt & Mjølsnes, 2009). To design the model of the ECMA 385 structure, the OSI Reference was referred to for the design. The system is divided into three layers, as seen in the figure below. The three layers are NFC-SEC User, NFC-SEC, and NFC (Zhao, 2017).

This NFC-SEC protocol's primary purpose is to protect against eavesdropping and data modulation by attackers. The NFC-SEC-SAP (Service Accessing Point) invokes the requested service so that an NFC userA's phone can contact another NFC userB's phone. The NFC-SEC-SDU (Service Data Unit) then recorded the user's request. A combination of NFC-SEC-SDU and NFC-SEC-PCI (Protocol Control Information) becomes NFC-SEC-PDU (Protocol Data Unit). It then builds an NFC connection with the NFC-SEC-SAP of the NFC-SEC userB via the NFC-SEC-SAP of the userA. It motivates the coordination of shared secret values for communication. This is the Secure Channel service (SCH) in the ECMA 386 standard

Figure 23

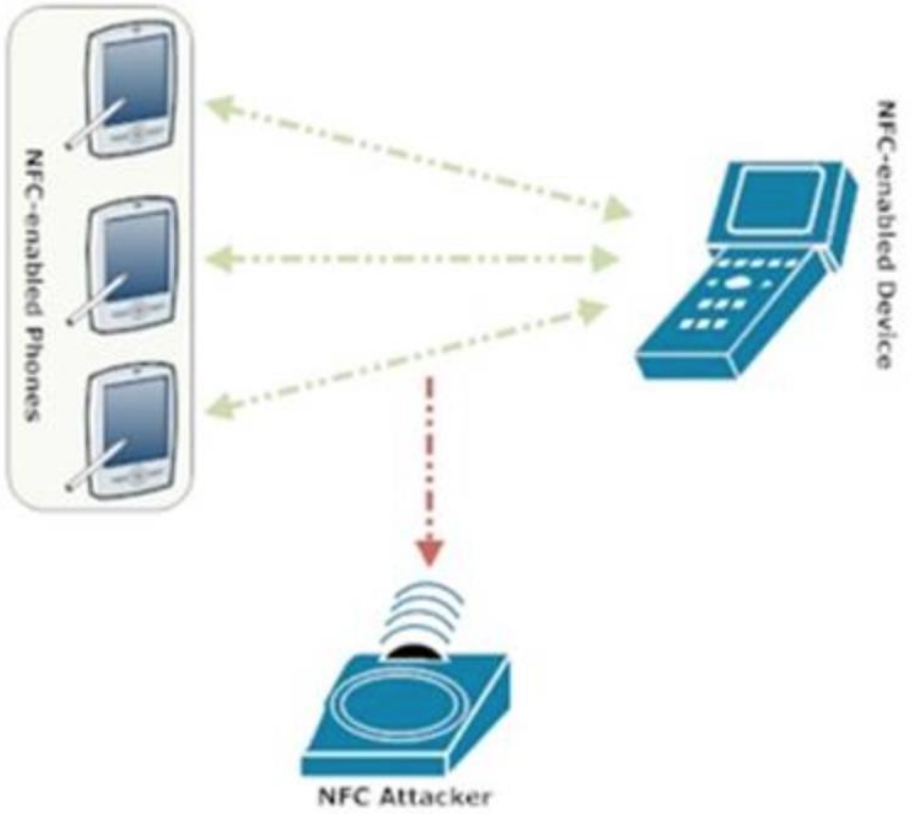
Model For the Ecma 385 Protocol



Eavesdropping: With NFCs, communication between devices is carried out with the help of wireless communication. This communication is vulnerable to attacks and allows attackers to eavesdrop on the NFC within their reach using antennas that are bigger and more powerful than the receiving mobile device (Chattha, 2014a). Eavesdropping can occur in any NFC operation mode, either card emulation mode or peer-to-peer mode (Chen et al., 2014). When the NFC function is not used on a device, the attacker can read the data in card emulation mode. If data in peer-to-peer mode is transmitted without secure protection, the communication suffers the risk of eavesdropping by an attacker.

Figure 24

Eavesdropping attack [8]



Data Modification: While transmitting data via NFC devices, the data can be manipulated and changed by an attacker from correct to incorrect data (Haselsteiner & Breitfuß, n.d.-b). During data transmission between the NFC devices, the devices could receive the manipulated data. For this vulnerability to be perfectly exploited, the attack must have an excellent knowledge of wireless and radio communication on which the amplitude modulation is transmitted.

Spoofing: The tag content can be spoofed for a spoofing attack to take palace on NFC. This is achieved by providing false information like a fake domain name or email (Coskun et al., 2015). URI smart poster spoofing facilitates attacks on a web browser, URLs and telephony URIs, to name a few (Madlmayr et al., 2008).

Operation Mode

- Peer-to-Peer Mode: The NFC function must be turned on for both devices before an initiator contacts the target. Their distance should be within the communication distance range, so the NFC function establishes a connection of less than one second when the initiator touches the target. When this process is completed, data will be transmitted through Bluetooth technology. The complicated process of target search and very long connection time can be resolved using of NFC technology, which makes its use advantageous in the transferring and exchanging information between devices. This mode is highly supported by the ISO/IEC 18092 standard (Noh & Choi, 2013).

- Card Emulated Mode: The two main ways to accomplish the card emulated mode are by using software for the secured chip emulation, which is not common, or using the smart card chip embedded in the mobile phone. This embedded smart card chip is the main way a card emulation is achieved (Roland et al., 2012). The user's confidential information is stored on the

emulated card, which can be used for payment or to verify the user's identification. The related specifications of this mode are defined by the ISO/IEC 14443 standard.

- Reader/Writer Mode: NFC tags that store information in the NFC Exchange Format (NDEF) are read by NFC devices. The smart cards and tags data storing formats are defined by the NDEF, which can be applied in different areas, such as a patient wearing an NFC tag on their hand in the hospital in the form of a bracelet. The patient's heartbeat rate, temperature, and blood pressure are stored on this bracelet. An NFC reader is used by the health personnel to read these values from the patient's bracelet, which are then automatically transmitted to the hospital's information station for doctors to control the patient's current physical status. This mode is also supported by the ISO/IEC 14443 standard.

The table below illustrates a blend of the standards and operating modes.

Table 3

NFC Standards and Operating Modes

Operation mode	**Peer-to-Peer**	**Card Emulated**	**Reader/Writer**
Standards	ISO/IEC 18092	ISO/IEC 14443	ISO/IEC 14443
Advantages	They have a low connection speed of less than 0.1 seconds.	On one phone, many digital value cards are combined.	In the dark, tag information may be read and contacted right away.
Disadvantages	Has a low transaction speed of 424kb/s, lower than Bluetooth's 2.1MB/s	When phone is off, or haw low battery card content can still be read by others.	The production of active tags is more costly than QR-code.

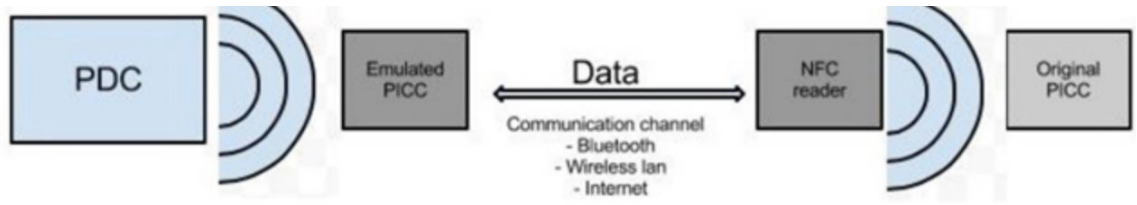
Uses	Can be used to share business cards, share information.	Mobile payment, Check-in systems, user identification and e-passport.	Guide in museum, tokens for transportation,

Single ID: Before data communication, all smart cart cards will need to have a unique ID to avoid a collision. Other devices not gaining the authentication can simulate this ID (Madlmayr et al., 2008). When this happens, it does not become a risk only to the card owning the ID but also to applications on which the card is dependent. The copied unique ID can be used without the victim's permission in different applicable situations.

Relay Attack: The commands of the Application Protocol Data Unit are used to obtain this attack. The Application Protocol Data Unit commands used by the attacking application are obtained from the network socket (Roland et al., 2012). A request is invoked to the secured chip. When a reply consisting of confidential information is made by the secure element of the application, the data is then sent to a different place by Wi-Fi or Bluetooth for transaction or identification.

Figure 25

Relay Attack on NFC [1]



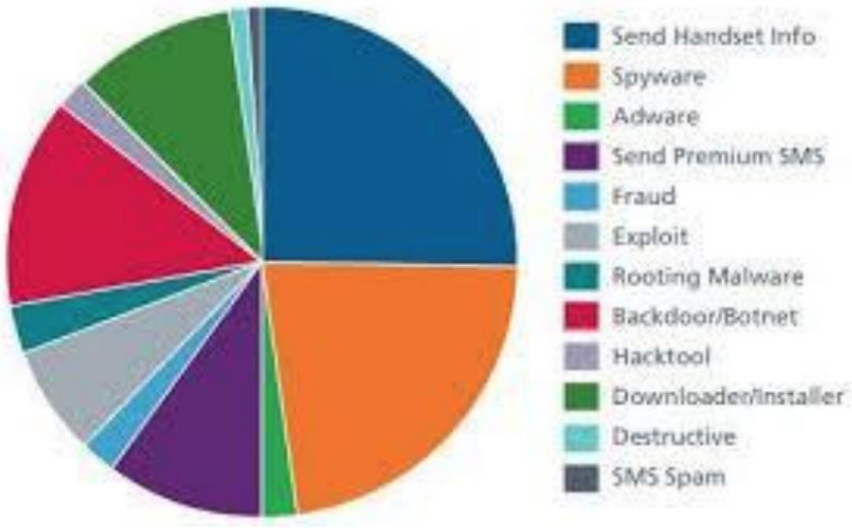
Device

Mobile devices are popular because of their unique level of convenience, flexibility, and portability. The ease with which smartphones transfer data and communicate with other electronic devices supports most of the technologies developed for wireless communication, including NFC. They do this by establishing Radio Communication with these similar devices by touching or bringing them together. They then communicated by inductive coupling, that is, by letting the sharing of power and data over a very small distance by loosely coupled inductive circuits (Kavya et al., 2014).

NFC's reliable security on devices not vulnerable to privacy protection is relatively low. In addition, the protocols used by NFC provide very few safeguards for data sniffing and modification. Because the most used application of NFC is contactless payment, securing and the properly using of the devices on which this technology works has become a big call for concern (Monteiro et al., 2012).

Figure 26

Security Concerns on NFC Devices



Data corruption: When an attacker modifies data transmitted through an NFC interface, the data is said to have been corrupted (Haselsteiner & Breitfuß, n.d.-b), (Chattha, 2014a). When the attacker changes the data to a format that cannot be recognized, it can be considered a denial of service. This can disturb the communication between the user and the receiver. The NFC tag becomes useless when stored data becomes corrupted, and the data needs to be retrieved again by the device. Malicious software running on a smartphone can perform data corruption.

Data Insertion: During data exchange, an attacker can insert unwanted data in the form of messages to NFC devices (Haselsteiner & Breitfuß, n.d.-b); Chattha, 2014a). Before the legitimate device establishes communication, the attacker must have responded to the device. When both the legitimate and the spoofed devices transmit data at the same time, the received data is going to be corrupted.

Denial of Service: when an NFC-secured chip and malicious application in a mobile phone are flooded with continuous incoming access requests, a DOS attack occurs (Madlmayr et al., 2008), (Chen et al., 2014). Until the massive incoming request messages are stopped, the function which provides access to the secure chip will stay locked, and all the application installation processes will be stopped. When this happens, transactions via the secured chip will not. Be able to go through, and hence it losses its function. A DOS can also occur when an empty tag is used t touch an NFC device (Chattha, 2014b). This empty tag touch can cause a flooding error message, affecting the NFC device or its services, and changing its status to suspended.

Chapter V: Results, Conclusion, and Recommendations

As seen are the above descriptions of security issues on NFC technology in this paper, using the attack vector taxonomy, many other security issues can still be noticed in NFC technology. For instance, secure elements of the Card Emulated Mode make available functions used in writing and reading data. They are also made up of some measures for protecting the access of information by non-authorized users. Therefore, the protocol, which manages the secure chip security and helps with the ability to distinguish and judge users' authorizations, needs to look at and highly enhanced.

In their environment of use, NFC mobile phones can not predict who will contact them, so security keys can't be generated before the transaction. The focus of the identification is more on the reader or writer mode.

This paper lists four main attack vectors which were investigated concerning the different attacks they facilitate. The strength of these attack vectors to reduce the attack occurrence and increase security on the NFC technology should be a serious concern.

Generally, the need for more robust authentication mechanisms and secure communication protocols to protect NFC-enabled devices from malicious attacks must be emphasized. The importance of user awareness and education to prevent social engineering attacks that exploit the vulnerabilities of NFC technology is an essential factor that also needs to be looked at in the feature.

This paper involved a comprehensive literature review on NFC technology and its security vulnerabilities. While coming out with the paper, several articles and experiments to simulate various attacks on NFC-enabled devices were investigated. Several problems were

encountered during the research, which hindered the study's progress. The main problems encountered include:

1. Limited access to NFC-enabled devices: While conducting the research, obtaining access to a wide range of NFC-enabled devices for the experiments took much work. This limited the scope of the research and made it challenging to analyze the security threats posed by NFC technology comprehensively.

2. Complexity of NFC technology: The complexity of NFC technology made it challenging to understand the intricacies of how the technology operates and how attackers can exploit it. This complexity also made developing effective countermeasures to mitigate security threats challenging.

3. Lack of standardization: The lack of standardization in NFC technology made it challenging to develop a universal set of protocols and countermeasures that can be applied across different devices and platforms.

4. Ethical considerations: The research was carried out considering the ethical implications of experiments, particularly concerning infringing on the privacy of individuals and organizations. This made conducting experiments that simulated real-world attacks on NFC-enabled devices challenging.

Despite the challenges encountered during the research, the study provided valuable insights into the security threats posed by NFC technology. The problems encountered during the research highlight the need for further studies to address the challenges associated with NFC technology and enhance its security.

In terms of future work, this paper shows that subsequent research is needed to develop effective countermeasures against emerging attacks on NFC technology. Future research should

focus on improving the security of NFC-enabled devices, particularly in authentication and communication protocols. Also, further studies should be conducted to evaluate the effectiveness of the proposed countermeasures in real-world scenarios.

Overall, the paper provides valuable insights into the security threats posed by NFC technology and offers several recommendations for improving the security of these devices. The discoveries made in this study apply to researchers, practitioners, and policymakers involved in developing and deploying NFC-enabled devices.

References

Albattah, A., Alghofaili, Y., & Elkhediri, S. (2020). NFC Technology: Assessment Effective of Security towards Protecting NFC Devices & Services. *2020 International Conference on Computing and Information Technology* (ICCIT-1441), 1–5. https://doi.org/10.1109/ICCIT-144147971.2020.9213758

Alrawais, A. (2020). Security Issues in Near Field Communications (NFC). *International Journal of Advanced Computer Science and Applications, 11*(11). https://doi.org/10.14569/IJACSA.2020.0111176

Anusha, R., & Shastrimat V, V. D. (2018). Qualitative Assessment on Effectiveness of Security Approaches towards Safeguarding NFC Devices & Services. *International Journal of Electrical and Computer Engineering (IJECE), 8*(2), 1214. https://doi.org/10.11591/ijece.v8i2.pp1214-1221

Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., & Shabtai, A. (2018). Taxonomy of mobile users' security awareness. *Computers & Security, 73*, 266–293. https://doi.org/10.1016/j.cose.2017.10.015

Cavdar, D., & Tomur, E. (2015). A practical NFC relay attack on mobile devices using card emulation mode. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics* (MIPRO), 1308–1312. https://doi.org/10.1109/MIPRO.2015.7160477

Ceipidor, U. B., Medaglia, C. M., Marino, A., Morena, M., Sposato, S., Moroni, A., Di Rollo, P., & Morgia, M. L. (2013). Mobile ticketing with NFC management for transport companies. Problems and solutions. *2013 5th International Workshop on Near Field Communication (NFC)*, 1–6. https://doi.org/10.1109/NFC.2013.6482446

Chabbi, S., Madhoun, N. E., & Khamer, L. (2022). Security of NFC Banking Transactions: Overview on Attacks and Solutions. *2022 6th Cyber Security in Networking Conference (CSNet)*, 1–5. https://doi.org/10.1109/CSNet56116.2022.9955600

Chattha, N. A. (2014a). NFC — Vulnerabilities and defense. *2014 Conference on Information Assurance and Cyber Security (CIACS)*, 35–38. https://doi.org/10.1109/CIACS.2014.6861328

Chattha, N. A. (2014b). NFC — Vulnerabilities and defense. *2014 Conference on Information Assurance and Cyber Security (CIACS)*, 35–38. https://doi.org/10.1109/CIACS.2014.6861328

Chen, C. H., Lin, I. C., & Yang, C. C. (2014). NFC Attacks Analysis and Survey. 2*014 Eighth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 458–462. https://doi.org/10.1109/IMIS.2014.66

Chen, I.-F., Peng, C.-M., & Yan, Z.-D. (2019). A simple NFC parameters measurement method based on ISO/IEC 14443 standard. 2*019 IEEE International Conference on RFID Technology and Applications* (RFID-TA), 33–36. https://doi.org/10.1109/RFID-TA.2019.8892221

Coskun, V., Ozdenizci, B., & Ok, K. (2015). The Survey on Near Field Communication. *Sensors*, *15*(6), Article 6. https://doi.org/10.3390/s150613348

Dhar, S., & Dasgupta, A. (2014). NFC technology: Current and future trends in India. *2014 International Conference on Contemporary Computing and Informatics* (IC3I), 639–644. https://doi.org/10.1109/IC3I.2014.7019680

Enzinger, H. (2009). *Very High Data Rate Test Platform for Contactless Smartcard Systems* (Publication No RG.2.1.3532.3920) [Master's thesis, University of Applied Sciences Kapfenberg]. https://doi.org/10.13140/RG.2.1.3532.3920

Ghosh, S., Goswami, J., Kumar, A., & Majumder, A. (2015). Issues in NFC as a form of contactless communication: A comprehensive survey. *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 252. https://doi.org/10.1109/ICSTM.2015.7225422

Hancke, G. P. (2011). Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *Journal of Computer Security*, *19*(2), 259–288. https://doi.org/10.3233/JCS-2010-0407

Haselsteiner, E., & Breitfuß, K. (n.d.-a). *Security in Near Field Communication (NFC)*.

Haselsteiner, E., & Breitfuß, K. (n.d.-b). *Security in Near Field Communication (NFC)*, 12.

Isaivani, M., & Kannadhasan, S. (2014). *A Proposal of Privacy Retaining Security Protocol in Near Field Communication Technology*, 6.

Kavya, S., Pavithra, K., Rajaram, S., Vahini, M., & Harini, N. (2014). Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones. *International Journal of Scientific & Technology Research*, *3*(6), 4.

Kortvedt, H. S., & Mjølsnes, S. F. (2009). Eavesdropping Near Field Communication. *The Norwegian Information Security Conference*, 13.

Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). NFC Devices: Security and Privacy. *2008 Third International Conference on Availability, Reliability and Security*, 642–647. https://doi.org/10.1109/ARES.2008.105

Monteiro, D. M., Rodrigues, J. J. P. C., & Lloret, J. (2012). A secure NFC application for credit transfer among mobile phones. *2012 International Conference on Computer, Information and Telecommunication Systems (CITS)*, 1–5. https://doi.org/10.1109/CITS.2012.6220369

National Institute of Standards and Technology. (n.d.). *Application Protocol Data Unit—Glossary. CSRC*. Retrieved November 11, 2021, from https://csrc.nist.gov/glossary/term/application_protocol_data_unit

Noh, S.-K., & Choi, D.-Y. (2013). Standard technical analysis, trend and future of NFC. *Smart Media Journal, 2*(3), 10–16.

Porter, J. (2021, June 28). *Security researcher sounds alarm over ATM NFC reader vulnerabilities.* The Verge. https://www.theverge.com/2021/6/28/22553646/atm-point-of-sale-nfc-readers-hack-security-vulnerability-jackpotting

Rieback, M. R., Gaydadjiev, G. N., Crispo, B., Hofman, R. F. H., & Tanenbaum, A. S. (n.d.). *A Platform for RFID Security and Privacy Administration*.

Roland, M., Langer, J., & Scharinger, J. (2012). Practical Attack Scenarios on Secure Element-Enabled Mobile Devices. *2012 4th International Workshop on Near Field Communication*, 19–24. https://doi.org/10.1109/NFC.2012.10

Security Risks of Near Field Communication Technology. (n.d.). NFC. Retrieved November 11, 2021, from http://nearfieldcommunication.org/nfc-security-risks.html

Singh, M. M. (2018). Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures. *International Journal of Engineering*.

Trottmann, U. (2013). *NFC - Possibilities and Risks.*

US Contactless Payment Statistics 2022. (n.d.). Finical. Retrieved March 13, 2023, from https://finicalholdings.com/us-contactless-payment-statistics/

What Is A Contactless Credit Card? (n.d.). Forbes Advisor. Retrieved March 13, 2023, from https://www.forbes.com/advisor/credit-cards/contactless-credit-cards/

What Is an Eavesdropping Attack? (n.d.). Investopedia. Retrieved November 11, 2021, from https://www.investopedia.com/terms/e/eavesdropping-attack.asp

Zhao, H. (2017). *The Effect of Financial Incentives on NFC Mobile Payment Adoption* (Publication No. 201712) [Doctorate dissertation, University of Georgia]. getd.libs.uga.edu.