*Vulnerabilities of Near-Field Communication (NFC) Technology*

MIDN 1/C McKenzie Eshleman

Cyber Science

United States Naval Academy

Annapolis, USA

MIDN 1/C Ben McLellan

Cyber Science

United States Naval Academy

Annapolis, USA

MIDN 1/C Caitlynn Stringer

Cyber Science

United States Naval Academy

Annapolis, USA

MIDN 1/C Jon Robinson

Cyber Science

United States Naval Academy

Annapolis, USA

Advisors:

Professor William Casey

CDR Trisha Snyder (Ret.), USN

***Abstract* — Near Field Communication, also commonly referred to as NFC, is a consumer-oriented short range wireless technology that has recently experienced a sharp rise in usage due to its integration into smartphones and contactless payment cards. This research paper dives into the cybersecurity aspects of NFC and the four most common vulnerabilities that are currently threatening Near Field Communication and classify which vulnerability is the most critical. The four threats focused within the research paper are: Tag Duplication, Replay Attacks, Man in the Middle, and Denial of Service. The major findings that were discovered was how simple all four of these attacks can be conducted and relatively inexpensive. Our research will provide suggestions to help combat these threats.**

***Keywords — Near Field Communication (NFC), Vulnerabilities, Tag Duplication, Replay Attacks, Man in the Middle, Denial of Service***

1. BACKGROUND

Near Field Communication (NFC), a short range method of data communication, has seen a recent spike in usage with its recent integration with smartphones. Many new smartphones have the capability to enable NFC, thus retrieve information in a single touch. NFC tags can be used in a variety of applications, to include smart posters, product identification, access control, and contactless payment. The integration of these tags is typically secured by the use of digital signatures, however, these signatures do not always guarantee the legitimacy of these tags. This is where the research group has gained a focal area. There are various attack methods that can be deployed against NFC technology. Our research group’s primary areas of focus are Tag Duplication, Replay Attacks, Man in the Middle Attacks, and Denial of Service Attacks.

1. WHAT IS NFC?

Near Field Communication is a wireless technology that operates less than 4cm [1]. NFC is a basic evolution of RFID (Radio Frequency Identification), which has been implemented in technology for years. Examples of RFID-enabled technology include key cards used for accessing private spaces and tracking devices. NFC technology has recently dominated society due to its affordability, NFC operates using tags The main purpose of this technology is its compatibility with contactless smart cards at the 13.56MHz frequency band. The link between a tag and reader is established by a single touch, making it convenient for users. NFC devices can act as both a card and a reader. These functions allow for NFC-enabled mobile devices used as contactless readers that interact with a variety of contactless “smart objects.” NFC has become a standard medium of data transfer for these devices due to its simplicity and accessibility on almost all modern smartphones. NFC technology is rapidly on the rise due to its backing by the NFC Forum, a collection of hundreds of software companies such as Apple, Android, and Google who aim to certify the integration of NFC technology into devices that are commonly used in our daily lives. NFC devices play a large role in the advancement of the Internet of Things in modern society, and many of these devices are portable, being worn and used for the real-time exchanging of information. While this means of data sharing is trusted and widely accepted, it is possible that an NFC-enabled mobile device could be used as a contactless attack platform, and general awareness of these attacks should be spread in order to bolster defenses in these systems.

*Applications of NFC*

NFC tags contain information necessary for data to be transmitted between the tag itself and an NFC-enabled device. Initially, NFC tags were read-only, meaning information could only be read from the tag onto the device. However, recently updated NFC specifications allow both tags and NFC-enabled devices to read and write information onto the device or tag it is communicating with. Near Field Communication has brought many advantages to modern day technology, one of them being the integration into mobile devices and enhances their capabilities. The major advantage of NFC being integrated into mobile devices is the ability to both read and write data to and from NFC tags. In addition NFC can be used for access control to allow entry into secure spaces. There are three major applications that NFC can provide:

* **Reader/Writer Mode:** Enables NFC devices to read/write data from/to NFC compatible tags [2].
* **Card Emulation Mode:** In this mode NFC enabled devices act as an emulated card and external NFC readers read the data that resides in NFC enabled devices [2].
* **Peer-to-Peer Mode:** In the peer-to-peer mode, two devices can exchange data at the link-level. This mode is standardized on the ISO/IEC 18092 standard, and allows data speed up to 424 Kbit/sec [2].

NFC technology has many applications and prototypes that have been developed for academia and industry. A popular modern example of the integration of NFC technology into everyday lives is the use of mobile phones to complete monetary transactions in place of physical credit and debit cards, otherwise known as contactless pay.

VULNERABILITIES AND ATTACK METHODS

The vulnerabilities our research discusses include: tag duplication, replay attacks, man in the middle, and denial of service. Our attacks will then be theorized by the research conclusions we as a group have found to be feasible. Emphasis on gaining proper understanding of these vulnerabilities and spreading awareness is essential to thwarting those with malicious intent. Common motivations for carrying out NFC attacks include fraud being relatively simple to carry out and difficult to trace, NFC implementation in almost every electronic device in society, and most importantly, a lack of knowledge on how this technology works and how vulnerable NFC actually is.

1. *TAG DUPLICATION*

One of the most common forms of replicable attacks with respect to NFC technology is tag duplication. NFC tags on sensitive pieces of technology are dangerously prone to basic cloning techniques, some of which are credit cards, identification cards, supply chain equipment, and digitally stored medical records [3]. NFC tags act and operate as containers for data that was meant to be shared and easily read, and can also act as readers. For these reasons, the reality of an NFC device to be used as a tag duplication attack platform is extremely feasible. When a smartphone or device is configured to engage in an NFC data transfer, said device emulates a passive NFC tag, which is then able to interact with the device’s memory and the applications associated with it.

Within the scope of tag duplication attacks, there are two main attacks on NFC devices that are rather prominent, which are skimming and cloning attacks. Tag duplication is carried out via reading a UID (unique identification) number from the NFC tag. The purpose of this UID number is to serve as a unique identifier for a specific device, which would prevent cloned data from working properly on another device. Surprisingly, however, retrieving a UID from a source tag is extremely easy to do since most passive NFC tags are designed to provide their UID once data transfer is initiated with a reader. This is a great security flaw in NFC tags and should not be taken lightly.

The process is rather straightforward for cloning a tag and duplicating it. First, the tag UID is simply read from the source tag wishing to be duplicated. Next, if the tag that is being used for the reading also holds writing capabilities, the UID from the source tag will then be available on the clone tag, which can then be written onto a new device tag. Tools for duplication methods such as this are widely available in places such as your mobile phone’s app store and on the internet for significantly cheap prices.

Skimming depends on the frequency the tags operate on and the NFC communication protocol being used. When conducting a skimming attack on vulnerable devices, tag duplication can be carried out from a distance further than the typical 4cm range seen in NFC devices. With the use of a contactless reading terminal equipped with an antenna, the range of tag duplication is increased. Although these terminals are portable they are seldomly standalone. The skimming terminal needs to be connected to a host. This host provides power and the coded software needed to skim the device, duplicating the tag. Taking this limiting factor of range and extending it poses a larger challenge for the NFC Forum and creates easier targets for those wishing to duplicate tags and use them for malicious purposes.

However, operating at a higher frequency may be an integral part of defending these vulnerable tags. When an NFC tag uses a higher frequency, bit transfer rate also increases as frequency increases. The data on the chip is then encrypted more efficiently since the sheer volume of data being passed to an encryption algorithm is much greater, resulting in a more secure device. Typical NFC tags which store identification codes are extremely vulnerable since it is difficult to keep track of which serial numbers are unique to a single device, and very few protocols exist with access to an accurate database that would alert the user to a duplicated NFC tag UID number.

1. *REPLAY ATTACKS*

This paper introduces new authentication techniques for NFC communication that provides mutual authentication. The mutual authentication will be between connecting devices. Mutual Authentication is a security property that prevents replay and man-in-the-middle attacks. The proposed protocols deploy limited-use offline session key generation and distribution techniques to enhance security and importantly make our protocol lightweight [4]. A replay attack can be best described as an adversary broadcasting a previously captured tag authentication response to a tag reader in order to impersonate an unsuspecting victim’s device and utilize their stolen information to the attacker’s own benefit.

The most common method by which this authentication data is retrieved is by planting a device between the tag and the reader that harvests this information for later use. Real world examples of replay attacks include gaining access to a secure space by replaying the NFC signal of a person’s access card who has legitimate authorization, or broadcasting stolen credit card chip information to a terminal when making a purchase.

This attack method is difficult to defend against and highly successful because most NFC enabled interfaces implement cloud services when validating transactions. With access to widely available applications and the correct hardware, an attacker with decent technical knowledge and the drive to steal information can carry out a replay attack with relative ease.

Another benefit to choosing a replay attack over other methods is low probability of detection. An adversary captures traffic and uses it at a later time, meaning the replay could take place days after the initial compromise of information or months into the future, and little evidence can point toward who was responsible for the compromise or where it took place. No modification of the captured information is necessary to carry out this attack either since traffic and authentication requests are simply paused upon retrieval and resumed later on, decreasing the odds of the adversary being caught even further.

Another enticing aspect of replay attacks is the lack of physical access to the card needed to carry it out. Wireless antennas used for capturing this traffic are inexpensive and small in size. To capture the seriousness of replay attacks, an attacker could fit a low range antenna in their pocket, activate it, and stand in line near you at a store and capture your transactional data if you choose to pay via an NFC enabled device. Devices used to execute replay attacks are capable of storing multiple information broadcasts at a given time, which widens the scope of who is seriously impacted by this attack significantly.

1. MAN IN THE MIDDLE

The man-in-the-middle attack is defined as a cyberattack in which an individual with malicious intent inserts themselves between two connections. The attacker relays and has the option to change the integrity of the messages that are intercepted. This attack directly affects each pillar of the cyber security CIANA pillars: Confidentiality, Integrity, Availability, Non-Repudiation, and Authentication.

A more common use for Man in the Middle Attacks as they relate to NFC technologies is the ability to eavesdrop on information stored on these devices and to possibly clone and or alter the data stored. It could be used to gain access to spaces, gain the trust of a victim, or used in tandem with several other forms of attack. This can be quite straightforward in many circumstances; for example, an attacker within the reception range of an unencrypted [Wi-Fi access point](https://en.wikipedia.org/wiki/Wireless_access_point) could insert themselves as man-in-the-middle. The attack only succeeds when the attacker impersonates each endpoint well enough to meet their expectations of a secure connection. Most mitigation techniques involve encryption to provide for better security and authentication, however as we have seen several NFC technologies are not encrypted.

1. *DENIAL OF SERVICE*

The most basic denial of service attack relies primarily on brute force. To flood the target with an overwhelming influx of packets, inundating its bandwidth, or diminish the target's system resources. This method relies on the capability to provide a large enough number of packets to overwhelm the system. One of the most common methods to achieve this is through botnets.

Application layer attacks focus mainly on disrupting a specific and targeted purpose. This will apply to our research as we are studying the use of NFC technology and their vulnerabilities at a more individual level. These attacks typically require less resources to carry out but can commonly be combined with network level attacks. Attackers can use nonrepudiation fooling techniques to make traffic appear normal and to create a lesser likelihood of detection.

We may attempt to create a "scrubbing center" to divert all traffic directed towards a victim through various methods, including: updating the victim's IP address in DNS systems, tunneling methods, digital cross-connects, etc.or even direct circuits, which separates "bad" traffic and only sends good legitimate traffic to the victim server. This would require a central posture and access to the internet facilities required to carry out such filters. It is important to note that DDOS attacks are extremely efficient against several firewalls and as a result can become more enticing to attack high value targets as a result. This is even more of a reason that this threat is imperatively researched and well defended against.

1. DEMONSTRATION

The demonstration that our research group focused on is a simple “do it yourself” NFC cloner. Instead of simply purchasing a RFID cloner, our group used items that were less expensive than the actual device. The main components to build these cloner included:

* MBED Microcontroller
* ACR122U RFID Adapter
* 5.6mAh Power Bank
* 16x2 LCD Display

1. *RESULTS OF OUR DEMO*

With the required materials that we used for our demonstration, we first began with relearning the components of the MBED and the Nucleo microcontrollers. Once comfortable with the basic programming, our group then began implementing ways for our LCD screen to function properly. Once the display was functional we then added our RFID scanner to the breadboard and began making it function properly. Once the RFID scanner was connected we then needed to begin creating the program to have the NFC copy the initial card being scanned and then clone it to the next card using the reader. The program can work one of two ways, it can maliciously clone data from the RFID scanner onto the next card scanned. Or it can take a previous card's data and clone it onto the next card scanned. This demonstrates how simple it is to clone NFC data from two different cards. This means that if implemented, the NFC tag could be used on a popular reader, for example, access control, and can be used to deploy malicious code to any card that scans into that specific reader. This demonstration proves just how vulnerable NFC can be and how easy it is to impact many individuals.

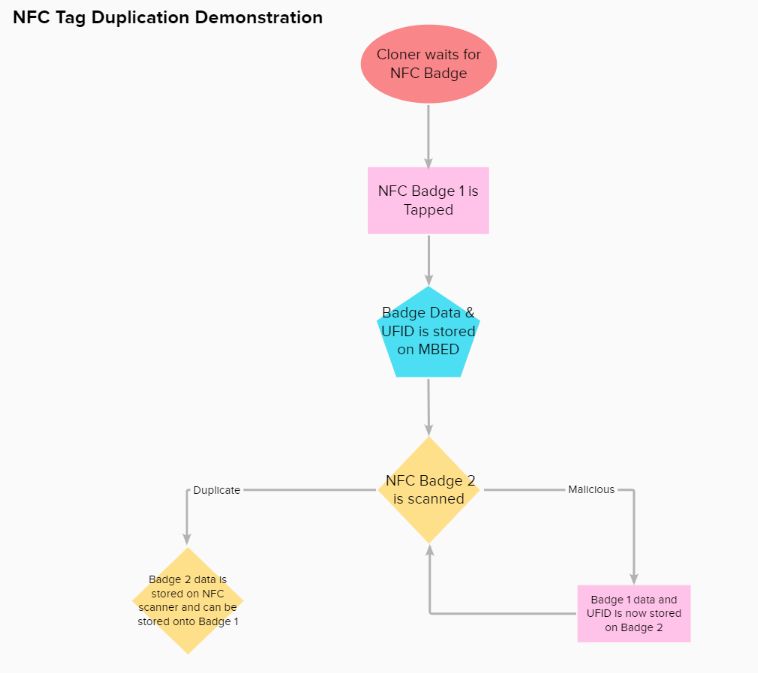


Fig. 1. Flow chart for two ways the demonstration can be conducted.

1. *OUR FINDINGS*

In our demo we found that with an aftermarket RFID scanner, one could collect the information of one card and add it to another. Essentially, we found that we could reenact a tag duplication attack. The aftermarket RFID scanner was simply connected to a computer out of the box and the instructions in the manual were followed. We downloaded drivers for the scanner to be compatible with the computer and downloaded a program that was compatible with the reader. Once the program was pulled up and connected to the scanner we were able to scan a card and collect the information on it to be placed on another. The same results were found with the Nucleo microcontrollers, Arduino software, LCD screens, card reader and cards. Although, the process was slightly more tedious. The microcontroller required programming code to be compatible with the other components. Additionally, the components required soldering and electronic wirework. Both the aftermarket RFID scanner and the “homemade” NFC reader that we developed can show a multitude of information that is being stored on the NFC tag. This shows just how important proper security measures need to be put into practice in order to protect this personal data. With this NFC terminal that we developed we could further develop the software to conduct a tag duplication attack, as described in figure 1.

VI. CONCLUSION

1. *QUALITATIVE RESULTS*

TABLE I. RANKING SYSTEM FOR VULNERABILITIES

|  | Tag Duplication | Replay Attacks | Man in the Middle | Denial of Service |
| --- | --- | --- | --- | --- |
| Cost | 6 | 8 | 9 | 8 |
| Ease | 8 | 9 | 5 | 5 |
| Effectiveness | 4 | 7 | 7 | 8 |
| No. People Affected | 1 | 4 | 2 | 9 |
| Total | 19 | 28 | 23 | 30 |

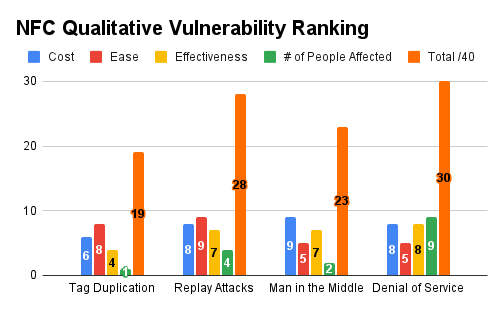


Fig. 2. Qualitative Vulnerability Rankings

In terms of the rankings for tag duplication it is given an overall score of nineteen out of forty points. Beginning with the cost of tag duplication, as seen with our demonstration, the material needed is relatively inexpensive, considering a sophisticated attack platform. There are also aftermarket NFC tag duplicators that cost from a range of three hundred to seven hundred dollars. With this information we gave the cost a score of six, this is based on being a relatively more expensive attack compared to the other vulnerabilities. For the ease of the attack it was given a score of an eight. This score was given because duplicating a tag is inexpensive and relatively easy to conduct. A nefarious actor could simply walk past someone and scan their tag to get all the data that is being stored on the tag. For effectiveness it was given a score of four. This is due to the fact that although the tag will be duplicated, the tag will still work properly. The information on the tag can also be retrieved or a card can be canceled if duplicated. For the number of people that are affected from this type of attack platform is a score of one. This is because a tag duplication attack can only affect a single person per attack, thus this is why it is given a low score. With the combination of the scores tag duplication is given a nineteen out of fourty, which is a 47.5% overall effectiveness of the vulnerability.

For replay attacks the cost score was an eight, this is because the only material needed for the vulnerability is an antenna which is relatively inexpensive. For ease of the attack, it was given a score of nine. This score was given because the attacker does not need to physically access the device, the antenna only needs to be in range to relay to the reader. For effectiveness replay attacks was given a score of seven. This is because multiple cards can be scanned and it is hard to detect when the attack has occured. For the number of people that can be affected, it was given a score of four. Although a replay attack can compromise multiple cards, it can only do so one at a time. With the combination of the scores replay attacks was given a score of twenty-eight out of fourty, which is a 70% overall effectiveness of the vulnerability.

For Man in the Middle, beginning with the cost of the attack it is given a score of nine. This is because to perform a basic MITM attack a malicious card is the only piece of equipment required. Since blank NFC cards are so inexpensive and can be programmed through applications on smartphones it was given this high score. For the ease of the attack it was given a score of five, this is because there needs to be an active terminal and also a passive card. Although this can be done, it is a harder attack to execute. For the effectiveness of the attack it was given a score of a seven. This score was given because the attack itself is hard to recognize, much like a replay attack. Both the card and the reader can not detect when a MITM attack is occuring making the attack very effective. For the number of people that can be affected per attack the score given was a two. This is because the attack platform can only affect one card at a time, thus giving it such a low score. For the overall score of the attack it was given a twenty three out of fourty. Giving a score of 57.5% overall effectiveness of a Man in the Middle vulnerability.

In terms of ranking for a Denial of Service attack it was given a score of eight for the cost of the attack. This is because the attack only requires malicious software, rather than purchasing any hardware. For the ease of the attack DoS was given a score of five, this average score was given because this vulnerability requires the knowledge of creating the malicious code or software. It also requires the ability for the code to be able to manipulate the NFC reader. For the effectiveness of the attack it was given a score of eight. This score was given because there are many different methods to conduct a DoS attack on NFC making this attack very effective. For the overall number of people for this attack it was given a score of nine. This score was given because a DoS attack can cause many NFC tags from properly connecting to various applications or websites. For the overall score of a Denial of Service attack it was given a thirty out of fourty, giving an overall effectiveness score of 75%.

Based on the data discussed above, we conclude that a Denial of Service Attack has the highest overall ranking for the most detrimental NFC attack. Although any four of these vulnerabilities will be effective in disrupting the service of Near Field Communication, Denial of Service attacks are the main vulnerability that needs to be addressed and focused on.

1. *SUGGESTIONS TO IMPROVE*

For specific ways to improve the chance of being a victim of these vulnerabilities our group suggests the following. First is to utilize a RFID Wallet, these kinds of wallets have a protective metal shield that will not allow for antennas to reach your RFID enabled cards being stored in your wallet. With a RFID wallet, it can help prevent a Tag Duplication, Man in the Middle, and Replay attacks.

The next suggestion that our group provides is the frequent checking of your NFC enabled card balances. Often when a Tag Duplication or a Replay Attack occurs they go unnoticed. By checking your balance frequently an attack will be caught earlier and action can be taken before it is too detrimental to your finances. This leads to our last recommendation.

Our last recommendation is the overall awareness, while this may be a given. Often these NFC vulnerabilities are caused by a lack of awareness. A user should inspect where they are inputting their cards and verify that there are no antennas that will scan your cards data. By checking where you are using an NFC tag, and ensuring that you are the only user accessing your data will help ensure that you do not fall victim to one of these four NFC vulnerabilities.

1. *OVERALL CONCLUSION*

As a result of our research and demonstrations, we have been able to study four different NFC vulnerabilities and categorize them on five different qualitative vulnerabilities: cost, ease, effectiveness, number of people affected, and overall effectiveness. Our research and demonstration is just a foundation for future research into the further exploitation of technology that is an integral part of society. We hope to have provided a better understanding of the dangers that plague society everyday in order to provide a more educated society. Just by improving awareness, many individuals can better protect themselves by taking a few of the suggestions provided by our research.

ACKNOWLEDGMENT

Our Capstone group would like to thank Josh Datko for his expertise in our project, as well as Professor Anthony Melaragno, USNA Cyber Science Department and our Capstone Advisors Professor William Casey, USNA Cyber Science Department, and CDR (Ret.) Trisha Snyder, USN.

REFERENCES

[1] Saeed, Muhammad Qasim, and Colin D. Walter. "Off-line nfc tag authentication." 2012 International Conference for Internet Technology and Secured Transactions. IEEE, 2012.

[2] Ecma International, Near Field Communication - White Paper, 2005, Ecma/TC32-TG19/2005/012, Available:

<http://www.ecma-international.org/>

[3] Kamaludin, Hazalila. “Clone Tag Detection in Distributed RFID Systems.” PlosOne.Org, 22 Mar. 2018, journals.plos.org/plosone/article?id=10.1371/journal.pone.0193951.

[4] Thammarat, Chalee, et al. "A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys." 2015 International conference on information networking (ICOIN). IEEE, 2015

[5] Francis, L., Hancke, G., Mayes, K. and Markantonakis, K., 2010. On the security issues of NFC enabled mobile phones. International Journal of Internet Technology and Secured Transactions, 2(3/4), p.336.

[6] Lehtonen, Mikko & Ostojic, Daniel & Ilic, Alexander & Michahelles, Florian. (2009). Securing RFID Systems by Detecting Tag Cloning. 5538. 291-308. 10.1007/978-3-642-01516-8\_20.

[7] Tesoriero, Ricardo, and Jose A. Gallud 2018. "Software Architecture and Framework to Develop NFC-Based Applications" Sensors 18, no. 8: 2654.

[8] Zanata Omayr. “How I Finally managed to clone a NFC TAG.” Medium, Medium, 20 Dec. 2018,

[9] A, Jeremie. “The DIY Portable NFC Cloner.” Medium, Medium, 25 Mar. 2019,

[10] Kassim, Jafar, and Yurii Maslyiak. SOFTWARE FOR OBJECT IDENTIFICATION USING NFC TECHNOLOGY. West Ukrainian National University, <http://dspace.wunu.edu.ua/bitstream/316497/39130/1/4.pdf>

[11] Saeed, D, Iqbal, R, Sherazi, HHR, Khan, UG. Evaluating Near-Field Communication tag security for identity theft prevention. Internet Technology Letters. 2019; 2:e123. https://doi.org/10.1002/itl2.123.

[12] Kamaludin, Hazalila. “Clone Tag Detection in Distributed RFID Systems.” PlosOne.Org, 22 Mar. 2018, journals.plos.org/plosone/article?id=10.1371/journal.pone.0193951.

[13] Thammarat, Chalee, et al. "A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys." 2015 International conference on information networking (ICOIN). IEEE, 2015.

[14] Lu, He-Jun, and Dui Liu. "An improved NFC device authentication protocol." Plos one 16.8 (2021): e0256367.

[15] Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (n.d.). “Classification of RFID Attacks.” 86.

[16] Dafalla, Yousif & Liu, Bo & Hahn, Dalton & Wu, Hongyu & Ahmadi, Reza & Bardas, Alexandru. (2020). “Prosumer Nanogrids: A Cybersecurity Assessment.” IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.3009611.

[17] Akter. (2020). Man-in-the-Middle Attack on Contactless Payment over NFC Communications: Design, Implementation, Experiments and Detection. IEEE Transactions on Dependable and Secure Computing., 1–1.

[18] Dreyer, Julian, Marten Fischer, and Ralf Tönjes. "NFC Key Exchange-A light-weight approach to authentic Public Key Exchange for IoT devices." 2021 IEEE 7th World Forum on Internet of Things (WF-IoT). IEEE, 2021.

[19] F. Fahrianto, M. F. Lubis and A. Fiade, "Denial-of-service attack possibilities on NFC technology," 2016 4th International Conference on Cyber and IT Service Management, 2016, pp. 1-5, doi: 10.1109/CITSM.2016.7577582.