A Survey on NFC Security

Nithyashree Rangaprasad
Department of Computer Science
Purdue University
West Lafayette, USA
E-Mail:nrangapr@purdue.edu

ABSTRACT

The NFC (Near Field Communication) is one of the latest and most popular short-distance wireless communication technology which validates two-way interaction between electronic devices and provides ease of connection with a single touch. There are many applications in NFC including, medicine and healthcare, smart ticketing, smart tags, e-wallets, etc. With its vast applicability, also comes the security concerns associated with the collection and processing of the data. In this survey project, we also encountered many papers that either explained the working and technology behind NFC or the attacks and defenses in detail. Our goal is two folds. To give a detailed overview of NFC technology, including the working principle, transmission details, protocols, and standards. And, to explain in detail the security threats and existing defenses related to the NFC application, in specific to give a comprehensive view of the attacks and defenses around mobile-based NFC applications in Healthcare and Finance.

1 INTRODUCTION

Near-field communication (NFC) is a short-range wireless technology that enables devices to communicate when brought within close proximity. NFC has many advantages for communication, including its convenience and ease of use. However, there are also several security threats associated with NFC. One of the biggest threats to NFC security is the potential for data theft. Unencrypted data, when transmitted using NFC technology can be interpreted by any attacker. This is a concern for users using NFC to make payments or exchange sensitive information. Another threat to NFC security is the potential for privacy violations. NFC can be used to track users' movements and activities. This information can then target users with advertising or invade their privacy in other ways. Despite the security threats, NFC is a valuable technology that can be used for a variety of purposes. By taking steps to protect their devices and data, users can help to mitigate the risks associated with NFC.

1.1 Organization.

The remainder of this paper is organized as follows: Section II explains the background of NFC. Section III explains the existing healthcare applications and finances that use NFC technology. Section IV discusses various attacks in NFC with respective various modes of operation. Section V analyzes and categorizes various CVEs related to NFC. Section VI discusses possible defenses for the existing attacks. Finally, we discuss the limitation, suggest new ideas for future works, and summarize with the conclusion in Section VII and Section VIII

2 BACKGROUND AND ARCHITECTURE

In this section, we are covering the basic protocols that are used in NFC, the different modes of operations, and communications.

2.1 NFC Standards and Protocols:

ISO/IEC 18092 Standardl. ISO/IEC 18092 is the standard used for Near Field Communication (NFC). It specifies the interface and protocol for simple wireless communication between close coupled devices. These Near Field Communication (NFC) devices communicate with bit rates of 106, 212, and 424 kbit/s [11].

ISO/IEC 14443 Standard. ISO/IEC 14443 is the standard used for contactless integrated circuits (IC) cards. It specifies the air interface and protocol for communication between a reader and an IC card. The standard is divided into three parts: Part 1: defines the air interface and protocol for communication between a reader and an IC card. Part 2: defines the physical characteristics of the IC card. Part 3: defines the test methods for IC cards. It uses 13.56MHz for wireless frequency operations. NFC-A and NFC-B are two different transmission systems [9] [10]. The third technology of ISO/IEC 14443, known as "NFC-F,". It was developed by the SONY Corporation. It uses the FiliCa contactless IC card transfer standard. Prior to becoming a part of the ISO/IEC 18092 standard, air interface technology was a component of the Japanese Industrial Standard (JIS) X 6319-4[9][10].

ECMA 385 and ECMA 386 Standardsl. ECMA-385 specifies the NFC-SEC secure channel and shared secret services for NFCIP-1. The secure channel provides confidentiality, integrity, and authentication for NFCIP-1 communications. The shared secret services provide a way for NFCIP-1 devices to establish shared secrets that can be used for authentication and encryption. The NFC-SEC secure channel is based on the TLS protocol. The shared secret services in ECMA-385 provide a way for NFCIP-1 devices to establish shared secrets that can be used for authentication and encryption. The shared secret services use the Diffie-Hellman key exchange protocol to establish shared secrets between NFCIP-1 devices [5]. ECMA-386 specifies the cryptographic mechanisms for PID 01. PID 01 is a profile for NFCIP-1 that uses Elliptic Curve Diffie-Hellman (ECDH) and the Advanced Encryption Standard (AES). ECDH is used for key agreement, and AES is used for data encryption and

Conference'17, July 2017, Washington, DC, USA
© 2023 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

integrity. ECDH is a cryptographic protocol that allows two parties to establish a shared secret without exchanging any secret information over an insecure channel. ECDH is used in ECMA-386 for key agreements.

2.2 NFC Modes of Communication:

Under ISO/IEC 18092 Standard, there are 3 modes of communication:

1) Active – Active
2) Active – Passive
3) Passive – Active.

NFC technology has two types of devices. The initiator device, that initiates the communication and controls the data exchanges, and the target device, that responds to the initiator device.
Active mode: In this mode, both the initiator and the target device generate radio frequency (RF) signals. The initiator device creates a strong RF field that powers the target device. The target device then responds by generating its own RF signal.
Passive mode: In this mode, only the initiator device generates an RF signal. The target device does not generate its own RF signal. Instead, it responds to the initiator device's RF signal by modulating the load on the initiator device's signal. This modulation is what allows the target device to communicate with the initiator device.
Apart from the above, NFC uses two types of coding mechanisms (Manchester and Miller coding) to transfer data.

2.3 NFC Modes of Operation:

Peer-to-peer mode In this mode, two NFC-enabled devices exchange data with each other. When one device initiates a connection, the other device responds and the two devices establish a connection within 1 second. Data is then transferred between the devices via Bluetooth. This mode is useful for exchanging information between two devices, such as contacts, files, or photos.

Card emulation mode This mode allows an NFC-enabled device to act as a contactless smart card. This can be used for making payments, accessing buildings, or verifying identity. In this mode, the NFC-enabled device stores the user's confidential information, such as a credit card number or a security code.

Reader/writer mode This mode allows an NFC-enabled device to read data from an NFC tag. NFC tags are small, passive devices that can be used to store data, such as a website URL, a contact card, or a loyalty card number. Reader/writer mode is used to read data from NFC tags that are attached to objects, such as posters or products. For example, when paramedics want to get the vital signs of the patient, he/she can read the data from the NFC tag. This can be shared with the doctor before the patient arrives at the hospital. This gives the doctor a head start with patient care.

3 NFC IN HEALTHCARE AND FINANCE:

In recent years, NFC usage has increased tremendously in various industries, including healthcare and finance. The ability to communicate securely and conveniently between devices makes NFC an ideal technology for applications such as patient monitoring, medical records management, payment transactions, and more. In this paper, we will explore more on various use cases in healthcare and finance, especially the applications that can be maintained and monitored using a mobile application.

3.1 Using NFC in Healthcare:

The healthcare industry is increasingly turning to technology solutions to improve patient care and outcomes. With many wireless technologies in place, it is preferable to use NFC for short-distance communication which ensures security and faster data transfer. [4]. It provides a convenient and secure way to transfer data such as patient information, medicines prescribed, X-rays, and other scan images between devices like computers, iPad, etc [25]. In this paper, our scope is limited to applications used in basic healthcare which are discussed in the flowing subsections:
1) Monitoring applications: Since the boom of smartwatches, we have been using various sensors to collect and analyze various information such as SPo2 levels, Heart rate, sleep intervals, etc. A heart rate monitor is one such important healthcare application that is important in many diagnostics. NFC technology can be used in this case to collect the data and directly send it over to the healthcare provider [17] [22].
2) Tracking applications: With the huge amount of data that is being collected, it is also important for monitoring the data for any anomalies. Some applications like prescription monitoring can be automated and monitored using NFC. Also, we have seen how it is tiring for recording the blood pressure level, and SP02 level every time we visit the doctor. These data which are obtained from the sensors in smartwatches or medical devices can directly be transferred to the patient portal using NFC technology [19].

3.2 Using NFC in Finance:

Finance especially contactless and wireless payments and transactions are also getting increasingly popular with the introduction of NFC as it enables a user to make a swift and safe payment just using their mobile phones [4]. In the following subsection, we will explain more about two of the many applications of payments:
1) E-wallets: People used cash or cards for payments in earlier days. With the improvement in wireless technology, mainly with NFC, the traditional smart card services from banks are moved to NFC. A smartphone can simulate a credit card using e-wallet applications such as Google Pay or Apple Pay. Typically, a hardware Secure Element (SE) or host card emulator (HCE) is used to provide this emulation. The SE mobile payment solution uses a highly secure, tamper-resistant chip that encrypts and stores credit card data locally on a device [12].
2) Transport payments and Loyalty cards: The scope of NFC is not restricted to payments and health care. It can also be extended to be used in transportation management and loyalty points management. For example, we have seen people signup for monthly metro cards or in case of cashback points that can be redeemed in our favorite food places. These points and ticket details can be read/written using NFC tags [12][1].

4 ANALYSIS OF SECURITY ATTACKS

With this huge applicability, there are also security concerns that we need to consider. The data that is transmitted or collected are very sensitive in both the payment and healthcare services and there are many attacks that can exploit the user to reveal sensitive information. In this section, we will be looking at various attacks in detail.

Denial of Service attacks In this attack, the attacker floods the secure chip with multiple access requests which exhaust the capacity and result in denial of access. In essence, a DoS attack attempts to make the computer resources unavailable. This is done by sending a large number of requests to the website, or by sending requests that are very large or very complex. These types of attacks result in the loss of trust between the client and the service which results in financial loss [2]. To explain further, we consider a scenario where a user with a mobile phone is trying to get some information from the NFC tag through touch (Reader/writer mode). If the actions result in a crash and reboot loop for the mobile, then this will result in the user losing trust in the service. Mulliner et al implemented the above attack using a simple sticky paper tag with a malformed NDEF message which what placed on top of the original tag to disrupt the service [15].

Mehmet et al presented that in one of the protocols that are used to monitor the patient's medication and other information if the reader sends continuous transmission can keep the tags busy and since a reader cannot wait indefinitely, it will try to restart a new session which in turn has the potential to disrupt the drug administration [18].

Eavesdropping With any wireless communication, there is a risk of eavesdropping by the attacker to obtain sensitive information from the user. NFC is also susceptible to eavesdropping attacks. Eavesdropping can happen in card emulation mode and peer-to-peer mode of NFC operation mode [2]. Eavesdropping is possible in both card emulation and peer-to-peer modes of NFC operation. In card emulation mode, an attacker can read the data content of an NFC device if the device is not in use. In peer-to-peer mode, an attacker can eavesdrop on communications between two NFC devices if the data is not transmitted securely.

Peer-to-Peer (P2P) Mode: Madlmayr et al [13] demonstrated that P2P mode is vulnerable to eavesdropping attacks. P2P mode is a data link without security protection which allows an attacker to intercept and read the data that is transmitted between two devices. He also showed that unencrypted communication in P2P is prone to eavesdropping attacks[2].An attacker can use a jammer to disrupt the communication between two devices or to steal the data that is being exchanged.In other words, a jammer emits radio waves at the same frequency as the devices that are communicating. This causes the devices to lose communication with each other or receive corrupted data. In some cases, the attacker may be able to use the jammer to intercept the data that is being exchanged and steal it.

Card-Emulated Mode: Alzahrani et al. [4] stated that irrespective of the phone not in use, an NFC-enabled mobile phone the content of the NFC card is still vulnerable to attackers due to its short-range wireless technology. This means the close proximity of the attacker i.e. placing their phone close to the card aids them in reading the card details. This could include personal information such as credit card numbers, loyalty card numbers, or even medical records.

Fuzzing It is a software testing technique that is used for finding vulnerabilities in software that has no source code available by feeding invalid, unexpected, or random data to a program to identify potential bugs. Mulliner et al have presented that fuzzing can be used in NFC/NDEF tags, to find vulnerabilities in the tag's firmware or the software that reads the tag. A fuzzer generates a series of invalid or unexpected data and writes it to the tag which is then read by a phone or other device until we find some crashes like reboot. This process is repeated until the fuzzer's output has no effect on the tag or the device. Mulliner et al demonstrated two length values, the phone crashes, and resets. It also means that the GUI system crashes as the user was not able to enter a PIN.

Replay Attacks A relay attack is a type of man-in-the-middle attack in which the attacker intercepts and relays communication between two devices. In this type of attack, it is easy to bypass any application layer security protocol as the attacker can circumvent authentication by simply relaying a challenge to a legitimate token which in turn provides the correct response that the attacker must send to the verifier. This also requires no previous knowledge as the attacker acts as a relaying party between a reader and the receiver. Francis et al demonstrated the same through an experiment as shown in Figure 1 in which the attacker needs 2 devices (token and reader) that are connected via a suitable channel to relay information. There is also a proxy reader and proxy token to communicate with the real token and real reader respectively. As mentioned above the proxy devices relays the information to and fro such that the reader cannot distinguish between the real and the proxy which in turn results in the attacker getting the access [12].

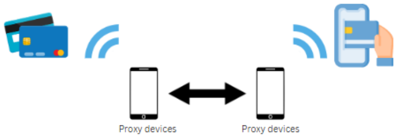


Figure 1: Replay Attacks in NFC

Identity Authentication Authentication is important in ensuring that the device communicates with the authorized one. Authentication plays a major role in defending against the Man in the middle attacks. But if a phone or an NFC device connects without checking the identification of the target, this can be potentially exploited by attackers. Verdult et al demonstrated the above in the NDEF pairing attack. In this experiment, the attacker has replaced the original tag with a malicious NFC-emulating device in the poster. When a phone is turned on, it scans for Bluetooth devices that are in range. If the phone finds this malicious tag that has the same matching

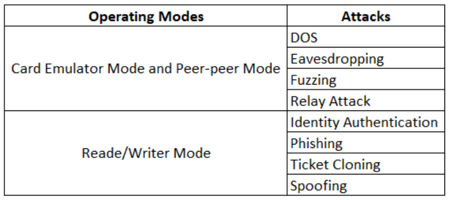
PIN code and MAC address, it will turn on the Bluetooth function so that the two devices can communicate with each other which in turn helps the attacker to send malicious files to the victim's phone [24].

This type of attack is much more dangerous as it does not require the client's authorization for the action to complete which gives the attacker complete control over the victim's devices.

Phishing attacks It is easy to trick users into malicious websites using phishing attacks. With NFC, an attacker can redirect the user to websites where we can tricker users into revealing sensitive information like login credentials or passwords, or card number [13].

Ticket Cloning With the smart cards used in transportation [1], The NFC tags in the cards can also be misused to generate duplicates. One of the scenarios is the cloning of tickets to other users before the verification process so that the transportation industries are tricked to believe that these duplicates are new tickets when scanned repeatedly [2]. One more problem is that this type of cloning attack also has a risk of misusing the identity of a victim user.

Spoofing Attack Mulliner et al have demonstrated that in the case of a smart poster, an attacker can insert some special data like space or tab or newline. In such cases, the victim fails to notice the changes in the message of the NFC tag. This can be used to manipulate the user to visit a new URL that is managed by the attacker to obtain identification information from the victim. The same also can be used to trick the user into sending a message to a premium number which in turn will result in significant financial loss.



Operating Modes	Attacks
Card Emulator Mode and Peer-peer Mode	DOS
	Eavesdropping
	Fuzzing
	Relay Attack
Reade/Writer Mode	Identity Authentication
	Phishing
	Ticket Cloning
	Spoofing

Figure 2: Table showing various attacks and in various operation modes

5 ANALYSIS OF THE CVES IN NFC

CVE (Common Vulnerabilities and Exposures) lists publicly known cybersecurity vulnerabilities. CVEs are used by security professionals to communicate about vulnerabilities and to track the status of remediation efforts. In this section, top eight CVEs will be introduced detailed [16].

CVE-2019-2114 – Bypass User Interaction This vulnerability is found in the Android version which is 8.0 or above. This allows the attacker to bypass user interaction requirements and install any malicious application that the user sends. The cause of the vulnerability is the default permission setting which allows application installation without user interactions. In close proximity to the victim's device, the attacker installs any application into the victim's phone using the NFC tap. This vulnerability was patched by Google in Android version 10 in October 2019.

CVE-2018-9585 – Arbitrary code execution This vulnerability was found in the NFC service of Android devices running Android 7.0, 7.1.1, 7.1.2, 8.0, 8.1, and 9. It is caused by a missing bounds check. An attacker can use this vulnerability to execute arbitrary code on the device with no additional privileges needed. It was patched by Google on January 2019

CVE-2017-15322 - Insufficient input validation This vulnerability was found in some of the Huawei smartphones with the software BGO-L03C158B003CUSTC158D001 and BGO-L03C331B009CUSTC331D001. The cause of this vulnerability is insufficient input validation which allows the attacker to launch a denial-of-service attack by sending specially crafted NFC messages to the target device. The patch for this vulnerability was released in 2017 by Huawei and the updated versions are not susceptible to this vulnerability.

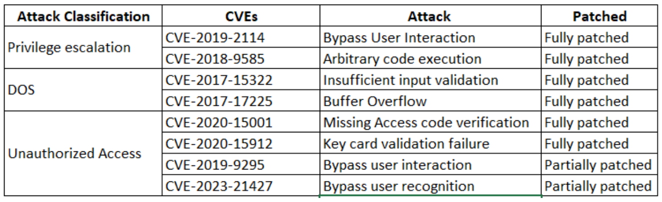
CVE-2017-17225 – Buffer Overflow This vulnerability is found in Huawei Mate 9 Pro mobile phones with the previous versions of LON-AL00B 8.0.0.340a(C00). It is a buffer overflow attack that allows the attacker to execute arbitrary code on the target device which can result in data medication (system compromise or data theft) and Denial-of-service. It was patched by Huawei on February 2018.

CVE-2020-15001 – Missing Access code verification The vulnerability is found in the Yubico YubiKey 5 NFC device which allows the attacker with physical access to the device to use a tool such as NFC tools to send a specially crafted NFC message to the device. The message would contain a command to read the OTPs and passwords from the device. This is caused by a missing access code check which allows the bypass of user access code verification. This was patched by Yubico on July 2020.

CVE-2020-15912 – Key card validation failure This vulnerability was found in Tesla Model 3. This vulnerability is the result of incorrect NFC authentication. This allows an attacker mimic the signal from a legitimate key card using a attack/proxy device. Once the attacker has opened the car door, they could then steal the car or its contents. This vulnerability was patched by Tesla on January 2020.

CVE-2019-9295 - Bypass user interaction This vulnerability is found in the Android tags applications which allow an attacker to bypass user interaction requirements and read NFC tags. This is caused by a missing permission check in the Tags app. This allows an attacker to create a malicious NFC tag that contains a specially crafted payload. When the user scans this malicious tag, the Tags app will read the payload without waiting for the user to confirm the action. The payload could contain malicious code that could be executed on the device. Google released patches to tackle this vulnerability but this is still present in many mobiles and users are still prone to this attack. One feasible solution could be to refrain from using public NFC readers.

CVE-2023-21427 – Bypass user recognition This vulnerability is found in the Samsung NfcTile app which allows an attacker to use NFC without user recognition. This is the result of improper access control vulnerability. In this, the NFC tile app does not validate the user's identity properly which in turn is exploited by creating a malicious NFC tag that contains a specially crafted payload. When the user scans the malicious tag, the NfcTile app will allow the attacker to use NFC without requiring the user to confirm the action. The payload could contain malicious code that could be executed on the device. Samsung released the patch on February 2023 however, there are many mobiles that are yet to be updated with this above patch.



Attack Classification	CVEs	Attack	Patched
Privilege escalation	CVE-2019-2114	Bypass User Interaction	Fully patched
	CVE-2018-9585	Arbitrary code execution	Fully patched
DOS	CVE-2017-15322	Insufficient input validation	Fully patched
	CVE-2017-17225	Buffer Overflow	Fully patched
Unauthorized Access	CVE-2020-15001	Missing Access code verification	Fully patched
	CVE-2020-15912	Key card validation failure	Fully patched
	CVE-2019-9295	Bypass user interaction	Partially patched
	CVE-2023-21427	Bypass user recognition	Partially patched

Figure 3: Table showing various CVEs and its classification

6 ANALYSIS OF DEFENSES IN NFC

NFC is an extension of RFID. It also includes encrypted transmissions to meet the confidentiality requirement. This architectural advantage allows several security methods that have been developed for RFID and encrypted transmission to be modified to suit NFC. These modified methods can be applied to protect signal safety, data transmission, and device tags. In this section, we will discuss various NFC security protection methods that have been proposed[26].

Encryption Protocols Confidentiality plays a major role in establishing a secure channel in any form of wireless communication. It is achieved by encrypting the channel/data. The same concept can be applied in NFC to tackle attacks like eavesdropping, DoS, Data corruption, etc. There are several protocols that can be used to establish a secure channel in NFC. One such protocol is Diffie-Hellman (DH), which can be based on RSA or Elliptic Curves Cryptography (ECC). DH allows two parties to exchange secret keys without revealing them to each other. These secret keys can then be used to encrypt data, ensuring confidentiality, integrity, and authenticity.[8] [21]. In the following parts, we will be comparing and studying various secure channel implementations:
Chalee Thammarat et al showed various existing NFC defenses against Dos and MitM.

1) An authentication protocol, involving 3 parties (mobile, authentication device, and authentication center), can deploy symmetric and, asymmetric cryptography including hash functions. However, the shortcoming of this protocol is that there are no multiple authentication mechanisms and other security properties, like recipient authentication, message authentication, etc.

2) A mutual authentication protocol between an NFC-enable device and POS (Point of Sales which also involves 3 parties: a sales station providing an NFC device, an NFC Phone, and an authentication server. However, the two shortcomings of this protocol are: there is no message integrity. The session keys are static parameters. This makes the protocol a target for brute-force attacks. As an improvement, the following protocols were proposed to tackle the shortcomings of the previously mentioned protocols.

• NFCAuthv1 provides authentication between an NFC device and an authentication server.

• NFCAuthv2 provides authentication between an NFC device and an authentication server through a POS (Point-of-Sale)

The advantage of the above 2 protocols: They contain only symmetric cryptographic operations, MAC (Message Authentication Code), and a hash function which makes them lightweight. It also improves from the previous shortcoming with mutual authentication where the sender's identity is verified. Additionally, by using a limited-use session key generation and distribution method, the sender and receiver share the same key. This ensures that encryption and decryption of the messages are done only by those parties that share the same key [23].
W. Chen et al proposes a secure protocol to support mobile payments. This is built upon the existing GSM and NFC components which take advantage of the identity/authentication services provided by the MO and SIM to build an NFC payment service. The four major steps in the implementation are Initial setup, Price checking, Triple authentication, and transaction execution. The main advantage of this system is that it is scalable, just like a GSM system. It also inherits the same authentication and encryption parameters. This makes it easier to implement and integrate the system. In other words, the system is easy to use and set up because it is based on a well-known and established technology. This means that there is no need to develop new protocols or procedures, which can save time and money [3].

Replay attack countermeasures It is important to implement feasible and usable countermeasures against attacks. And Francis et al propose some possible solutions against the Replay attack. One of the solutions proposed was timing the response so that the device can distinguish between the attacker and the normal user. However, in the real-world setup, this can be complicated as there are many other factors that will affect the response timing and it is difficult to separate them from attacks. The next proposed solution is to use a distance bounding protocol. This protocol determines an upper bound for the physical distance between two communicating parties based on the Round-Trip-Time (RTT) of cryptographic challenge-response pairs. To explain more, the protocol sends a challenge to the other party and measures how long it takes for the other party to respond. This time is then used to calculate an upper bound on the distance between the two parties. This method is effective because it is difficult for an attacker to fake a short RTT. But the caveat is that this method requires special communication channels that can provide a secure and accurate distance estimate. It is also important to note that conventional RF channels are inadequate for the implementation of secure distance bounding. The last proposed solution was to use the location metrics as they are reliable, accurate, and an effective countermeasure against relay attacks, e.g. location information could be simply appended to a transaction that is then signed by the legitimate sender. This can stop any attacker from using a proxy device [6].

Secure E-Ticket We encountered the ticket cloning attacks in the previous section. This involved creating multiple duplicates of the same tickets by an attacker to bypass the checking. Gudymenko et al propose a protocol to tackle the ticket cloning attack. In this experiment, the e-ticket consists of 1) user public keys and 2) a vending machine's signature over the hash of the attributes. There are 3 protocols to implement the proposed mechanism. 1) the vending machine protocol to purchase the ticket and 2) the stamping protocol to verify the purchased ticket. 3) the checking protocol to check the authenticity of the e-ticket. Each protocol has a series of steps like certificate verification, hashing, and signature verification to ensure that no foul play is found in the ticket verification and purchase [7].

7 LIMITATIONS AND FUTURE WORK

NFC is a growing technology with a lot of potential for research and improvements. In this paper, we detailed various attacks, defenses, and some well-known CVEs that are there in NFC however, there are some limitations that would improve the working of NFC, and these limitations are detailed in the following part:

Physical and Hardware Limitations NFC is a short-range transfer protocol. Its main advantage is speed and security. The physical and hardware constraints are one of the major limitations of NFC. This makes other technologies like Bluetooth have an upper hand in terms of the scope. Hence one of the future scopes would be to expand the scope with respect to the physical contraints with better security.

Targeted attacks Roland et al demonstrated a cloning attack on contactless EMV payment cards where even with the defenses and improved protocol in place, it was possible to downgrade the protocol to a vulnerable protocol like Mag-Stripe mode protocol and launch this type of attack to steal the credit card information. This shows that even with the discussed prevention in place, it was possible to launch targeted attacks on the applications that use NFC [20]. This shows the lack of centralized defense.

Lack of centralised Defenses We also observed that irrespective of the defenses and patches that exist, the attacks are not completely eliminated as many other factors like Vulnerabilities in supporting technology or incomplete patch updates in the Mobiles, still presented a huge risk for attacks. We also observed that the defenses were proposed for a particular attack or technology that had that specific vulnerability. And we believe research focusing on providing a centralized defense is the future approach to tackling existing and future attacks.

Increasing the scope in Healthcare In the previous sections, the scope was confined to applications that were used in normal medical care. Morak et al proposed a telemonitoring concept that can use NFC-enabled mobile phones and sensor devices to collect and transmit data to a central server in the intensive care units [14]. This allows for the remote monitoring of elderly patients with chronic diseases and easy data transportation and improved analysis. Such improvements and scope advancements are some of the areas that we need more research on as the type of data that is being handled is sensitive and critical.
Also, the future direction with respect to healthcare would be to experiment more on the security issues with that application that uses NFC and research to increase defenses for the attacks that are still prevalent.

8 CONCLUSION

This paper has found that there are a number of security vulnerabilities in mobile applications that use NFC. However, we still need more research to find vulnerabilities in healthcare applications that uses NFC. In an uncontrolled environment, NFC devices cannot determine if the other device they are communicating with is malicious or safe. They also cannot generate security keys before the transaction begins. This is why it is important to focus on identification in Reader/Writer Mode. This paper surveys eight security issues in NFC, as well as some well-known CVEs. It is important to strengthen defenses against attacks from other phones in NFC communication. In healthcare applications that use NFC, a limited amount of research exist covering basic implementation and common attacks but a detailed experiment and testing will be required to identify potential bugs/vulnerability. This will help in making it robust against any attacks as these applications deal with very sensitive pieces of information like patient details and medication details.

REFERENCES

[1] Alessandra Basili, Walter Liguori, and Federica Palumbo. 2014. NFC smart tourist card: Combining mobile and contactless technologies towards a smart tourist experience. In *2014 IEEE 23rd International WETICE Conference*. IEEE, 249–254.

[2] Cheng Hao Chen, Iuon Chang Lin, and Chou Chen Yang. 2014. NFC attacks analysis and survey. In *2014 eighth international conference on innovative mobile and internet services in ubiquitous computing*. IEEE, 458–462.

[3] W Chen, GP Hancke, KE Mayes, Y Lien, and J-H Chiu. 2010. NFC mobile transactions and authentication based on GSM network. In *2010 Second International Workshop on Near Field Communication*. IEEE, 83–89.

[4] Vedat Coskun, Busra Ozdenizci, and Kerem Ok. 2015. The survey on near field communication. *Sensors* 15, 6 (2015), 13348–13405.

[5] ECMA. *NFC-SEC-01:NFC-SEC Cryptography Standard using ECDH and AES (2rd Edition, 2010)*. Standard ECMA 386. ECMA, Geneva, CH.

[6] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. 2011. Practical relay attack on contactless transactions by using NFC mobile phones. *Cryptology ePrint Archive* (2011).

[7] Ivan Gudymenko, Felipe Sousa, and Stefan Köpsell. 2014. A simple and secure e-ticketing system for intelligent public transportation based on NFC. In *Proceedings of the First International Conference on IoT in Urban Space*. 19–24.

[8] Ernst Haselsteiner and Klemens Breitfuß. 2006. Security in near field communication (NFC). In *Workshop on RFID security*, Vol. 517. sn, 517.

[9] ISO Central Secretary. *Identification cards — Contactless integrated circuit(s) cards - Proximity cards — Part 3: Initialization and anticollision (2008)*. Standard ISO/IEC 14443-3. International Organization for Standardization, Geneva, CH.

[10] ISO Central Secretary. *Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol (2008)*. Standard ISO/IEC 14443-4:2008. International Organization for Standardization, Geneva, CH.

[11] ISO Central Secretary. *Information technology — Telecommunications and information exchange between systems — Near Field*. Standard ISO/IEC 18092:2013. International Organization for Standardization, Geneva, CH.

[12] Ratinder Kaur, Yan Li, Junaid Iqbal, Hugo Gonzalez, and Natalia Stakhanova. 2018. A security assessment of HCE-NFC enabled E-wallet banking android apps. In *2018 IEEE 42nd Annual Computer Software and Applications Conference*

(COMPSAC), Vol. 2. IEEE, 492–497.

[13] Gerald Madlmayr, Josef Langer, Christian Kantner, and Josef Scharinger. 2008. NFC devices: Security and privacy. In *2008 Third International Conference on Availability, Reliability and Security*. IEEE, 642–647.

[14] Jürgen Morak, Hannes Kumpusch, Dieter Hayn, Robert Modre-Osprian, and Günter Schreier. 2011. Design and evaluation of a telemonitoring concept based on NFC-enabled mobile phones and sensor devices. *IEEE transactions on information technology in biomedicine* 16, 1 (2011), 17–23.

[15] Collin Mulliner. 2009. Vulnerability analysis and attacks on NFC-enabled mobile phones. In *2009 International Conference on Availability, Reliability and Security*. IEEE, 695–700.

[16] NIST. *NIST National Vulnerability Databse(NVD) CVEs: CVE-2019-2114, CVE-2017-15322, CVE-2017-17225 , CVE-2018-9585 , CVE-2020-15001 , CVE-2020-15912 ,CVE-2019-9295, CVE-2023-21427*. Standard NVD. NIST. https://nvd.nist.gov/vuln/detail

[17] Charl A Opperman and Gerhard P Hancke. 2011. A generic NFC-enabled measurement system for remote monitoring and control of client-side equipment. In *2011 Third International Workshop on Near Field Communication*. IEEE, 44–49.

[18] Mehmet Hilal Özcanhan, Gökhan Dalkılıç, and Semih Utku. 2014. Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of medical systems* 38 (2014), 1–15.

[19] M Paksuniemi, Hannu Sorvoja, Esko Alasaarela, and R Myllyla. 2006. Wireless sensor and data transmission needs and technologies for patient monitoring in the operating room and intensive care unit. In *2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*. IEEE, 5182–5185.

[20] Michael Roland and Josef Langer. 2013. Cloning Credit Cards: A Combined Pre-play and Downgrade Attack on {EMV} Contactless. In *7th {USENIX} Workshop on Offensive Technologies ({WOOT} 13)*.

[21] Manmeet Mahinderjit Singh, KAAK Adzman, and Rohail Hassan. 2018. Near Field Communication (NFC) technology security vulnerabilities and countermeasures. *International Journal of Engineering & Technology* 7, 4.31 (2018), 298–305.

[22] Esko Strommer, Jouni Kaartinen, Juha Parkka, Arto Ylisaukko-Oja, and Ilkka Korhonen. 2006. Application of near field communication for health monitoring in daily life. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 3246–3249.

[23] Chalee Thammarat, Roongroj Chokngamwong, Chian Techapanupreeda, and Supakorn Kungpisdan. 2015. A secure lightweight protocol for NFC communications with mutual authentication based on limited-use of session keys. In *2015 International conference on information networking (ICOIN)*. IEEE, 133–138.

[24] Roel Verdult and François Kooman. 2011. Practical attacks on NFC enabled cell phones. In *2011 Third international workshop on near field communication*. IEEE, 77–82.

[25] M Vergara, P Díaz-Hellín, J Fontecha, R Hervás, C Sánchez-Barba, C Fuentes, and José Bravo. 2010. Mobile prescription: An NFC-based proposal for AAL. In *2010 Second International Workshop on Near Field Communication*. IEEE, 27–32.

[26] Zining Wang. 2018. Information security vulnerabilities of NFC technology and improvement programs. In *Proceedings of the 1st International Conference on Information Science and Systems*. 196–199.