Can You Get into the Middle of Near Field Communication?

Sajeda Akter*, Tusher Chakraborty†, Taslim Arefin Khan‡, Sriram Chellappan§, A. B. M. Alim Al Islam¶
*†‡¶Department of CSE, Bangladesh University of Engineering and Technology, Bangladesh
§Department of CSE, University of South Florida, USA
Email: *sajeda24@yahoo.com, †tusherchakraborty@matholympiad.org.bd, ‡arefin612@gmail.com,
§sriramc@usf.edu, ¶alim_razi@cse.buet.ac.bd

***Abstract*—A recent development emanating from the widely used RFID technology is Near Field Communication (NFC). Basically, NFC is a popular short range (<10cm) wireless communication technology with applications in areas sensitive to security and privacy concerns including contact-less payment. Since NFC communications require very close proximity between two communicating devices (for example a smartcard and a reader), it is generally believed that Man-in-the-Middle (MITM) attacks are practically infeasible here. On the contrary to this general belief, in this paper, we successfully establish MITM attacks in NFC communications between a passive tag and an active reader. We present physical fundamentals of the attack, our engineering design, and results of our successful implementation. We also present practical impacts of the attack from the perspective of how a malicious user can leverage our MITM attack to compromise integrity of contact-less payment transactions. Finally, we present insights to combat the MITM attack in NFC communications towards the end of the paper.**

***Keywords*—NFC, Contactless payment, Attacks, Security.**

I. Introduction

Since the past decade, RFID based technologies have been gaining immense popularity with applications in Logistics, Supply Chain Management, Mobility Tracking, Access Control, etc. Within the broad realm of RFIDs, a particular technology is Near Field Communication (NFC). Briefly, NFC technologies enable two electronic devices (one of them typically portable like a smartphone or a credit card) to establish communication with each other through bringing both devices in very close proximity (within <10cm of each other). NFC devices can be of two types, namely active and passive, based on whether or not the devices own a power supply. An active device generally possesses a chip connected with a copper-wire coil. When this device is powered on, the coil generates a magnetic field to establish communications. A passive NFC device, on the other hand, does not have its own power supply. When a passive device comes close enough to an active device, due to electromagnetic induction, the coil of the passive device gets powered allowing communication as shown in Figure 1.

Applications of NFC Technologies: The most critical applications of NFC technologies today are in contactless payment systems generally used in smart debitcards or creditcards. These typically follow the Active-Passive model, where the active device is a reader (used by the merchant), while the passive device is the smartcard (presented by the user). They alternatively communicate in half-duplex mode following established protocols. Other applications such as sharing contacts, photos, videos, or files between NFC devices are also there, where both devices (e.g., smartphones) are active and can communicate in full duplex mode. Needless to say, the contactless payment applications (and even others sometimes) are highly security sensitive, with incentives for adversaries to compromise their operations.

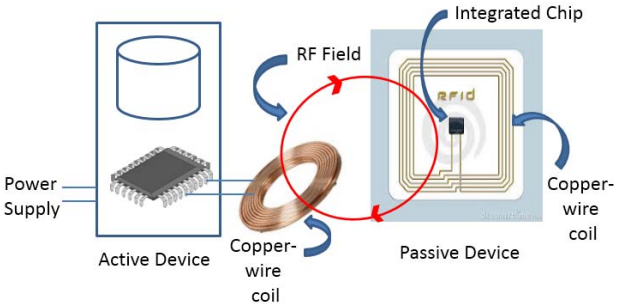


Figure 1: Working mechanism of NFC devices

The Security Perspective of NFC Technologies: As of today, it is generally believed that with NFC technologies, since the communications are held in close proximity between devices, the feasibility of unintentional data transfers is low. Nevertheless, to combat attacks, the notion of a Secure Element (essentially a chip) to enable a secure memory and execution environment is integrated within NFC devices. The secure element is a dynamic environment wherein application code and application data can be securely stored and administered, while enabling secure execution of applications. The secure element resides in highly secure crypto chips that also provide functions to encrypt, decrypt, and sign data packets.

While existing designs do provide a high degree of confidentiality and integrity for NFC communications, one potentially dangerous attack that has not been considered yet in this realm is Man-in-the-Middle Attack. It is generally assumed that Man-in-the-Middle (MITM) attacks are infeasible with NFC communications due to inductive coupling fundamentals, an illustration of which is presented in Figure 2. To demonstrate further, let Alice (an active server) and Bob (a passive tag) be two legitimate entities that are engaging in an NFC communication in close proximity. They can do so, since there exists an RF field generated by Alice. Let Eve be an adversary attempting to launch an MITM attack. In the above scenario,

DOI 10.1109/LCN.2017.39

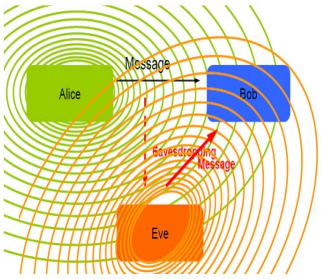


Figure 2: Alignment of two RF fields

for Eve to launch a successful MITM attack, its RF field needs to be perfectly aligned with that of Alice and Bob (to avoid RF disturbances), which is considered infeasible considering the already close proximity of Alice and Bob (less than 10cm). Such a situation will likely prevent Eve from becoming a Man-in-the-Middle with NFC communications [1], [2].

Our Contributions: In this paper, for the first time, we demonstrate the practical feasibility of MITM attacks over NFC communications between an active NFC device and a passive NFC device (in the context of smartcard payments), while still bounded by the physical constraints of Figure 2. To elaborate briefly, the adversary NFC device that we design from the ground up has an embedded reader, writer, and a passive tag, and when integrated together, becomes an *MITM card*.

What is unique about our work is the following. Rather than focusing on an external adversary trying to get into the middle at run time (which is physically very challenging to do considering inductive coupling fundamental presented above), we explore the intriguing possibility of placing an adversary device in between an original card and a reader at any flextime. In this paper, we consider a scenario where the user possess two cards, and interchangeably uses them with malicious intent. One of the cards is the one that is ideally accepted at a terminal, and is called *original card*. The other one called *MITM card* is one that is a clone of another valid card issued by a bank, however, whose details are exposed (possibly via skimming) by the user. In ideal case, this card should be rejected by the terminal. We will elaborate this in section III (D). Here, the attack we present is one where the user carefully places the *MITM card* between the communications of an *original card* (also belonging to the user) and the reader, and then use this scenario to compromise the integrity of contact-less payment[1]. To the best of our knowledge, this possibility of an MITM attack has never been explored before, which is the core novelty of our work in this paper. To do so, we perform careful engineering designs leveraging fundamentals of wireless communications. While the proof-of-concept of MITM we demonstrate in this paper is of a larger dimension, once the smartcard is programmed, the size can be shrunk to be comparable to that of a regular smartcard, which is typically 85.6mm $\times$ 53.98mm $\times$ 0.76mm (defined by ISO 7816). Thus, our design is pragmatic.

To the best of our knowledge, ours is the first work to demonstrate the practical feasibility of true MITM attacks with NFC communications, and then demonstrate the impact to compromise financial transactions generally performed today. We believe our paper exposes an important new vulnerability in this realm. Therefore, towards the end of this paper, we also provide insights on how to combat such attacks.

[1]However, it is not mandatory that the adversary must be insider. An outsider may keep the attack module in the wallet or similar belonging to an innocent user.

II. Related Work and Our Novelty

We now present briefly an overview of important work related to security of NFC devices and their communications, while also highlighting the novelty of our work in this paper.

a. The differences of our proposed MITM attack from Replay Attacks: Our proposed attack may resemble the well known "Replay Attack" (also called the "Relay and Ghost attack" or "Mafia Attack") [6], however, there are clear differences. The Replay Attack is one where the reader is typically malicious and it simply replays the contents of a benign tag (e.g., a smartcard) to a malicious entity to enable a fake transaction through compromising the *original card*. As we elaborate below, such attacks can be mitigated using dynamically changing crypto solutions, or location based approaches that attempt to physically tie a card and a reader at a particular location for approving a transaction [6], [10]. On the contrary, our MITM attack will enable an attacker module to be physically present in the same environment to collude with the *original card*. It is thus equipped with the ability to read all communications between the reader and the *original card* from start to finish (see Figure 3). Solutions proposed to combat Replay Attacks are not effective for our MITM attack proposed in this paper.

b. Crypto based solutions: Many attacks over NFC can be mitigated using crypto based solutions as in [1], where it is shown that eavesdropping, data corruption, data modification, and data insertion can be mitigated by establishing a secure channel between the devices with a shared secret key. In most solutions proposed today [1], [2], [3], dynamically changing session keys are recommended to secure the channel between sender and receiver. The work in [3] also shows how a combination of AES encryption [4] and Deffie-Hellman key exchange [5] scheme can be used to prevent data modification, and eavesdropping over NFC. In [1], more innovative approaches were proposed for NFC specific key agreement mechanism. The idea is to synchronize the bits, amplitudes, as well as phases of RF signals randomly generated by two devices. Once they are synchronized, the devices communicate with exactly the same amplitude and phases as secret keys. However, these techniques are also not effective against our MITM attack due to collusion between the *original card* and the malicious *MITM card*.

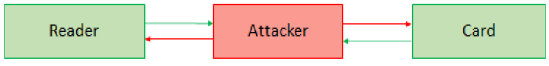
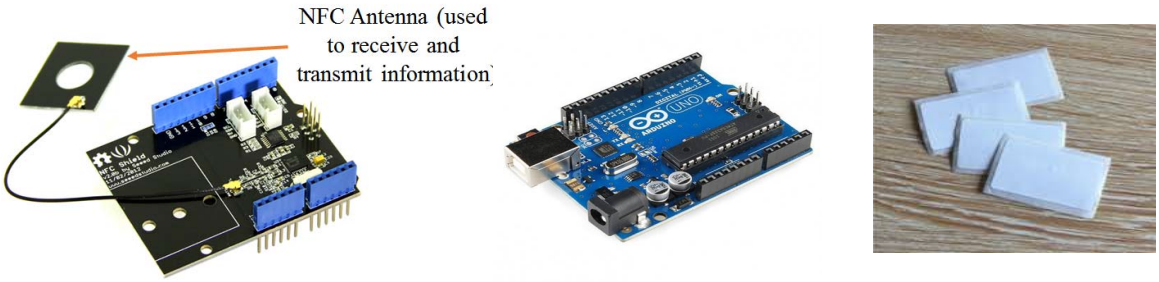


Figure 3: Man-in-the-middle (MITM) attack over NFC



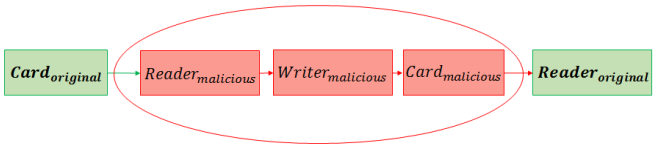
(a) NFC shield (b) Arduino uno board (c) MiFare Classic 1K tag

Figure 4: Device Specification

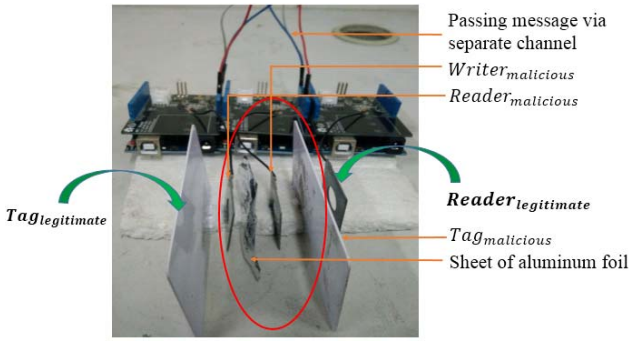
c. Location centric approaches: Another security scheme for NFC communications is called Tap-Tap and Pay [10], where the user of a valid card will tap the reader a specific number of times. Then, the accelerometer responses of the card and the reader are sent in real-time to a server along with the time stamps, wherein the server will determine if they are correlated. If so, then the transaction is approved, and it is rejected otherwise. This can mitigate replay attacks. Additionally, a study [6] proposes that a card should be unlocked only when it is in an appropriate (pre-specified) location. These approaches also will not work for defending against our attack, since the *original card* and *MITM card* in our attack are co-located next to each other and colluding as well.

d. Approaches leveraging physical unclonability of a tag: This is an interesting approach that leverages unclonability of components of electronic circuitry during fabrication. Briefly, a physically unclonable function (PUF) is a physical entity that is embodied in a physical electronic microstructure that is easy to evaluate, however, hard to predict or clone. In this respect a PUF is the hardware analog of a one-way function [15]. Approaches leveraging PUFs have been used for challenge-response based authentication and also dynamic key generation and sharing in RFID/ NFC based communications. The standard approach is where the more secure and power enabled reader has prior knowledge about the unique properties of the tag that are then challenged and verified at run-time [16]. However, PUF based designs are complex to implement, and furthermore, since the *original card* is co-located with the *MITM card* and colluding, the complexity of challenge-response mechanisms may introduce significant hardware design, and latency issues during verification that could impose constraints on practicality of PUF based designs for NFC devices.

e. The Significance and Novelty of Our Attack: Our work in this paper is important because MITM attacks have simply not been investigated in NFC communications because they are considered unlikely in practice [1], [2], [3]. Furthermore, existing solutions proposed for other security vulnerabilities in the NFC literature that were highlighted above are ineffective against our proposed MITM attack. State-of-the-art crypto solutions will not work simply because the *MITM card* is present and listening to all communications between the *original card* (with which the *MITM card* colludes) and the reader from start to finish. Location based approaches obviously fail because the malicious tag is physically close to the original tag and the reader. PUF based approaches are very challenging similar to reasons mentioned above, since the malicious tag is privy to all communication and keys between the original tag and the reader. The significance and novelty of our work in this paper is demonstrating the practical feasibility of MITM attacks over NFC, leveraging the attack



(a) High-level view



(b) Real setup

```
Scan a NFC tag

NFC Tag - Mifare Classic
UID 05 26 2D 7B

NDEF Message 1 record, 11 bytes
  NDEF Record
    TNF 0x1 Well Known
    Type Length 0x1 1
    Payload Length 0x7 7
    Type 55 U
    Payload hello
    Record is 11 bytes
```

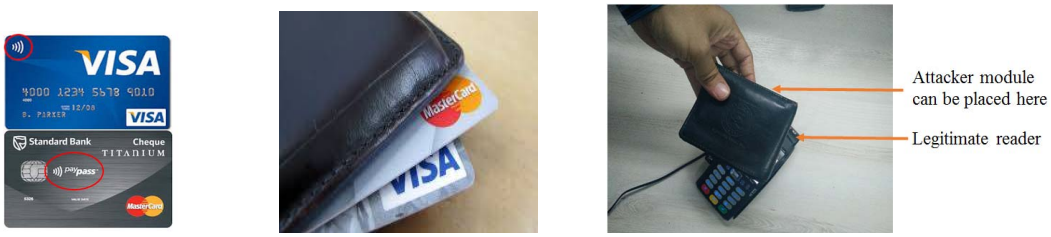
```
Scan a NFC tag

NFC Tag - Mifare Classic
UID 95 D4 2A 7B

NDEF Message 1 record, 105 bytes
  NDEF Record
    TNF 0x1 Well Known
    Type Length 0x1 1
    Payload Length 0x65 101
    Type 55 U
    Payload ifmmp
    Record is 11 bytes
```

(c) Screenshots of a legitimate transmission and a transmission under demo attack

Figure 5: Experimental setup and demonstration of MITM



(a) NFC-enabled payment cards from different parties

(b) Multiple cards usually kept in a wallet

(c) Holding wallet in front of a PoS machine while making a payment

Figure 6: The feasibility of our MITM attack module being invisible in a Wallet

to compromise contact-less payment protocols in manner that existing approaches cannot defend against.

III. Our Proposed Man-In-The-Middle Attack Over NFC Communications

We now present our MITM attack over NFC communications. First, we present the formal attack model. Then, we present the underlying physical fundamentals of our MITM attack over NFC communications. Subsequently, we present how our MITM attack can compromise the fidelity of a financial transaction when executed between two entities using a state-of-the-art protocol for contactless payments.

A. The Formal Attack Model

Our proposed attack model is one where the user/ owner of an NFC-enabled smartcard is malicious. The malicious user (also known as adversary) possesses two smartcards, one called as the *original card*, and the other one called as the *MITM card*. It is important to note that the *MITM card* is one that is a clone of another valid card issued by a bank, however, whose details are exposed (possibly via skimming) by the user. The reader/ server is assumed to be benign. The goal of the adversary is to conduct NFC-enabled communications with the reader using the *original card* and the *MITM card* interchangeably during a single transaction with the motivation to fool the reader (e.g., a merchant).

To do so, two things must happen. First, the adversary must first be able to emplace an *MITM card* in between the *original card* and the reader throughout the communication between them, wherein the *MITM card* must be able to read all communication between the *original card* and the reader, while also being able to physically communicate with both parties. This is an engineering challenge. Second, the adversary must be able to exploit a vulnerability in existing contact-less payment protocols by intelligently manipulating which smartcard (between the *original card* and *MITM card*) communicates with the reader and when, so that the reader is victimized. This is an algorithmic challenge. In the following, we address both in detail.

B. The Physical Fundamentals of Our MITM Attack

There are three critical components (shown in Figure 4) in our design of the MITM attack module. The first is NFC shield with antenna (Figure 4(a)) to transmit and receive information. In our set-up, we use three NFC shields (v2.1) [11] as active devices, whose maximum effective communication range is 5cm over a frequency of 13.56MHz. Second is Arduino Uno boards [12] containing ATmega328 microcontroller (Figure 4(b)), which is used to make the shields programmable. The last component is the passive card. For this, we use MiFare Classic 1K cards (Figure 4(c)). Figure 5(a) shows the schematic view of our MITM attack where the *MITM card* (that is embedded with a reader, and a writer) resides between the *original card* and the reader. Figure 5(b) shows the detailed implementation set-up.

To make the NFC shield operational, we stack the NFC shield on an Arduino development board and connect the board to a computer using a USB cable. The NFC shield can act as a reader or a writer depending on the instructions enabled in it. In both cases, when an NFC-enabled card is held in-front of the antenna of a NFC shield, it can detect and communicate with the card. Here, the *MITM card* is placed in between the $Reader_{original}$ and $Card_{original}$. A sheet of aluminium foil is used to isolate $Reader_{malicious}$ and $Writer_{malicious}$ to avoid collision between their radio signals. They are connected via a separate channel (for example, wire in our case) to pass information. In our experiment, three active and two passive devices are placed in passive-active-active-passive-active manner where the devices act as card-reader-writer-card-reader mode.

We now refer back to Figure 5(a) to illustrate how the MITM attack works in our set-up. In the absence of the MITM attack, two-way communication is normal between the *original card* and the reader. Under attack, $Reader_{malicious}$, $Writer_{malicious}$, and $Card_{malicious}$ combinedly act as the MITM attacker. Here, $Reader_{malicious}$ reads any message from $Card_{original}$, modifies it (if needed), and sends the modified message to the $Writer_{malicious}$. Then, $Writer_{malicious}$ writes the information in $Card_{malicious}$. Once writing has been completed, $Writer_{malicious}$ needs to release the channel so that $Reader_{original}$ gets the channel free and can read $Card_{malicious}$. Therefore, when the original reader $Reader_{original}$ wants to read $Card_{original}$, it actually reads the attacker's card $Card_{malicious}$ which may contain a modified message. Here, since attacker is in the middle of the original reader and original card, he/ she can decide when and which message will be passed to the original reader. Such messages can be anything from payment details, challenge-responses, personal details etc. Note that as long as the attacker

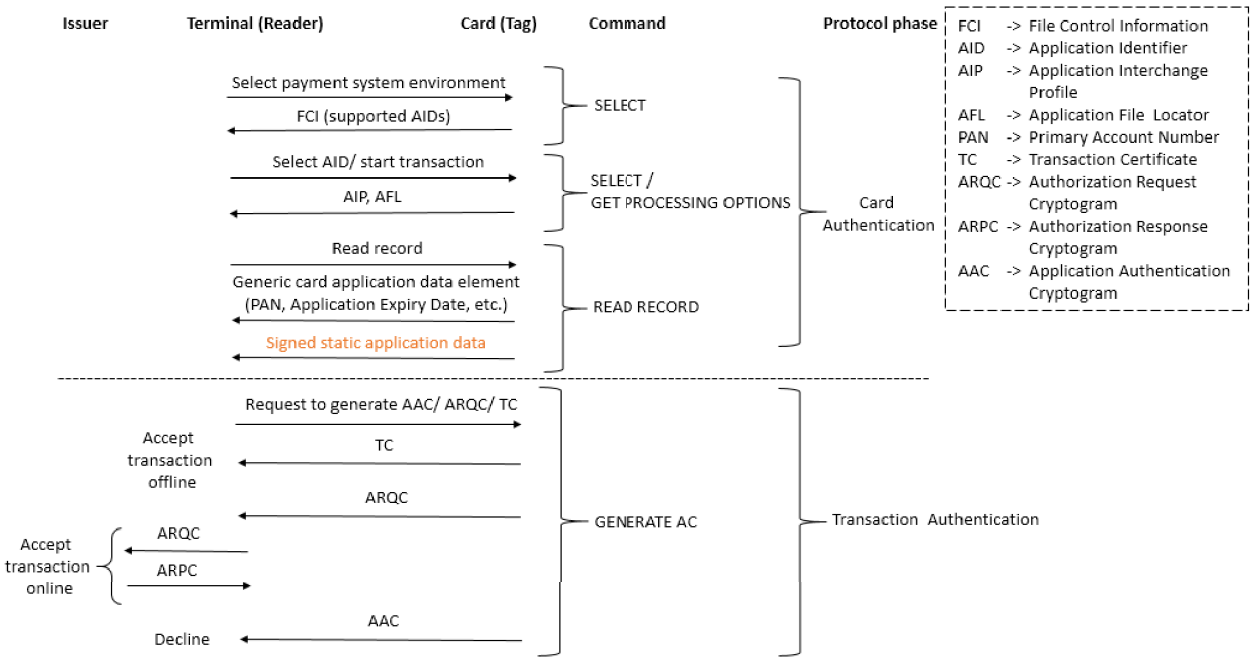


Figure 7: Complete mechanism of contact-less payment protocol [27], [28]

keeps the channel busy, $Reader_{original}$ cannot detect the presence of any card. Therefore, the attacker can control the channel smartly to ensure that $Reader_{original}$ cannot figure out any channel switch during communication. To clarify, Figure 5(c) shows a screenshots of demo attack. Here, for simplicity, we just increment the ASCII value of each character of the original message under transmission through the attacker module. Therefore, the original reader receives the message "ifmmp" (red marked) when the original tag sends message "hello" (green marked). The left side of figure 5(c) shows a legitimate transmission, whereas the right side shows a transmission under attack.

An important consideration here is the physical form-factor of our proposed design. We believe that our proposed MITM attacker module can be easily designed in the form of a regular commercial smartcard with state-of-the-art engineering designs. As such, the entire attacker module can be easily emplaced in a wallet adjacent to another card. This is because, the NFC shield with arduino board in our design presented above is used for programming only. Once programmed, the NFC shield can be replaced with the microcontroller and the antenna. The dimension of the antenna is 30.48mm $\times$ 27.94mm $\times$ 0.5mm. Thus when integrated with a tag, the resulting dimensions of the MITM module is comparable to typical smartcards, which is 85.6mm $\times$ 53.98mm $\times$ 0.76mm (defined by ISO 7816). Thus, it is possible to accommodate the entire attacker module within 2mm to 3mm width, which makes our MITM attacker practically invisible in a wallet.

C. Details on Contact-less Payment Protocol

We are ready to present discussions on how the above attack setup can be practically leveraged by a malicious user to fool a merchant in the domain of contactless payment. Before, we do that, we present in Figure 6, an illustration of how the smartcards that employ NFC technologies look like. With our implementation presented above, we can see that it is simple to invisibly emplace the *MITM card* between the *original card* and the reader. How the presence of these two cards creates an attack scenario is presented next.

Contact-less payment protocol [23] is based on the traditional contact EMV transaction protocols [24], [25] with few exceptions. Briefly, EMV (Europay, MasterCard, and Visa) is a technical standard for smart payment cards, payment terminals and automated teller machines that accept them. EMV cards are smartcards (also called chip cards or IC cards) that store data on integrated circuits in addition to magnetic stripes (for backward compatibility). Clearly, a critical goal of the protocol is to ensure secure communication between the terminal and the card consuming minimal amount of time.

The current EMV protocol can be split into three phases [26]: 1. Card authentication, 2. Cardholder verification, and 3. Transaction authorization. Contact-less transaction skips the second phase since offline Personal Identification Number (PIN) is typically not supported here due to the security vulnerabilities in terms of eavesdropping to extract the PIN. Besides, it is practically difficult to ask card holders to enter a PIN while holding a card in-front of the terminal [28]. While selecting transaction instances, a PIN could be made mandatory, for the most part it is not, and therefore, in general, only two phases (Card Authentication and Transaction Authorization) are involved in contact-less payment system. Figure 7 depicts the complete mechanism of the contact-less payment protocol. We briefly elaborate the phases next.

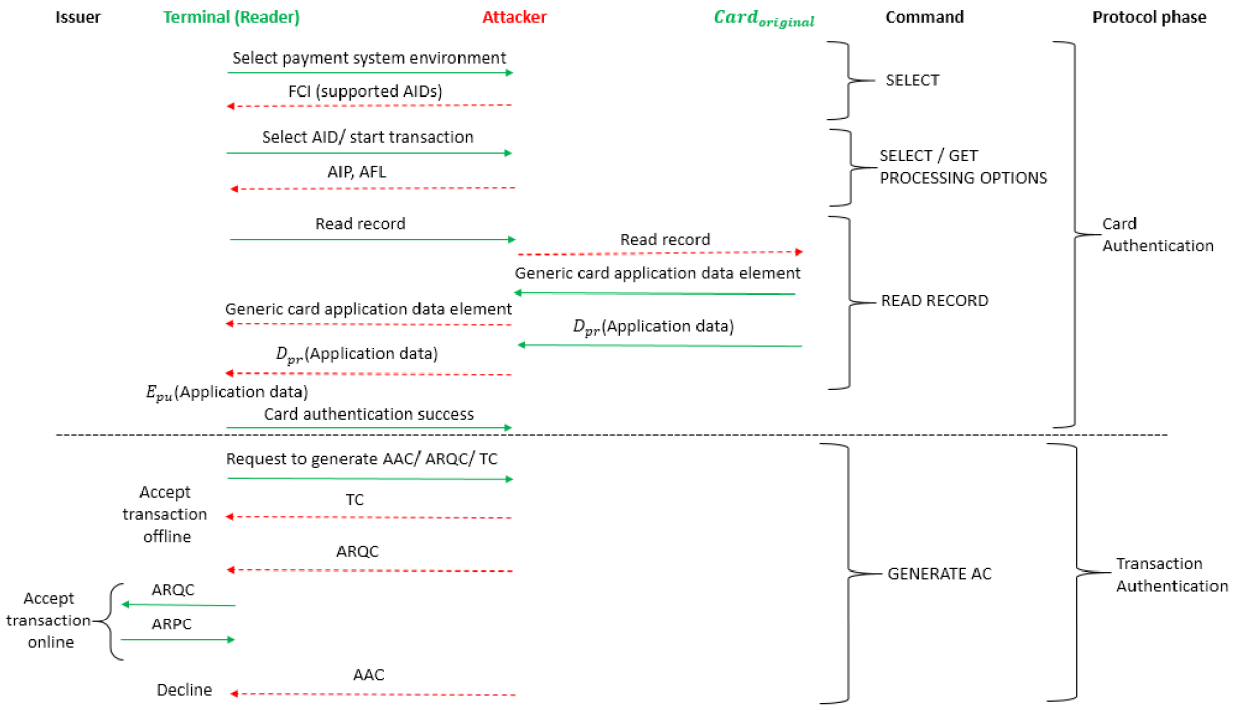


Figure 8: Attacker in between card and terminal perform card authentication using *original card* information, then transaction authorization using a fake card

1) Card Authentication: Both terminal (reader) and card (tag) may support multiple sensitive applications such as Payment System Environment (PSE) [27], Proximity System Environment (PPSE) [28], Debit/ Credit card, etc., each of which has different mechanisms to authenticate the card. To do so, the terminal is allowed to select an efficient payment environment using SELECT command. The card responds with the File Control Information (FCI) containing the list of supported applications (AIDs). Then the terminal selects an AID and starts a transaction using GET PROCESSING OPTIONS command. Subsequently, the terminal asks for a generic card application data element using READ RECORD command. With this step, the terminal will validate whether or not the corresponding card is approved for transaction. Note that in contact-less payment, Static Data Authentication (SDA) is typically performed, wherein the card sends over signed static application data for verification, which is verified by the terminal via public key authentication of the cryptogram to detect unauthorized cards or tampering. Cards identified as unauthorized in this step are rejected for payment. Otherwise, the terminal performs the next steps identified below.

2) Transaction Authorization: If a card is validated, then the terminal asks the card to generate a cryptographic MAC in addition to transaction related details such as amount, date, currency, etc., using GENERATE AC command. Here, the terminal may request the card to generate TC, ARQC, or AAC (explained in Figure 7), which are essentially digital signatures of the financial transaction, generated via secret card keys and session keys. Here, the card responds with TC if it allows offline transaction, returns ARQC if it forces the transaction to be online or returns AAC if it rejects the transaction. Typically, ARQC is preferred by the terminal since any fraud can be detected at run-time. Once the ARQC is received from the card, the terminal sends the ARQC to the issuer bank of the card. The issuer, then, verifies the transaction, approves the card if it was indeed issued by the bank, and sends an ARPC to the terminal. These steps also ensure two aspects:

- The financial message (amount, currency, date, etc.) is originated from the source that it claims to be from, and
- Content of the message is not altered.

A critical fact to observe here is that the check for validity of a card to be processed by a particular terminal happens only in the Card Authentication Phase via checking digital signatures generated by the card. Once the terminal decides that a card is validated, then in the next phase of Transaction Authorization, the issuer bank of the card will only validate if the card whose details are supplied by the terminal was indeed issued by the bank (along with financial details to verify integrity). In this phase, no checks are performed if the card is actually authentic for transaction in the particular terminal. The absence of redundancy in checking simplifies the overall protocol, and speeds up transactions, which is vital for contact-less payment. However, this fact is precisely what our MITM attacker will exploit as we present below.

D. Attack Model over the Payment Protocol

We now present details on how the presence of the MITM can compromise the above protocol. Usually, banks provide

terminals (readers) to merchants, and they allow all their issuing cards with the right BINs[2] to be processed in their terminals for free. However, when a bank is willing to accept cards issued by other banks (Visa, MasterCard, UnionPay, American Express, etc.) in their terminal, then the bank that supplies the terminal is called acquirer and the acquirer bank should have an agreement with the bank that issued the card. Different charge or commission may be fixed for different card types during these agreements. If any fraud occurs with a card, the issuer bank (of any card) should not ignore the liability owing to the agreement. If the issuer bank denies to take the liability, the acquirer bank normally declines the card during Card Authentication phase.

Figure 8 depicts a way how the MITM attack can be incorporated with contact-less payment protocol. Let a malicious user owns two cards. One of them will be accepted by the terminal (i.e., the *original card*). The other card is the *MITM card*, and is the clone of another valid card legally issued by a bank. Note that the *MITM card* has been engineered by the malicious user using our designs presented in this paper, and via skimming details of the valid card [7]. Note also that the valid card that was cloned as the *MITM card* is one that is not authorized for use at a particular terminal. In this context, we present a practical attack.

Let, the terminal initiate communication with the user. This is through the *MITM card* because it is an MITM between the *original card* and the terminal. Here, the payment environment is selected by the *MITM card*. When the terminal asks for generic card application data, the *MITM card* simply relays the request to the *original card*, receives a response, and relays it to the terminal. Since this data comes from the *original card*, the card authentication phase is successful using the right keys. Since the attacker just relays the messages, he/ she does not need to uncover any messages.

Once card authentication is completed, the *MITM card* does not need to communicate with the *original card*. In this phase, since *MITM card* directly communicates with the terminal, it can respond with TC to perform offline transaction. If the terminal does not support offline transaction, attacker needs to respond with its ARQC to the terminal. The terminal then sends this cryptogram to the corresponding payment card association (e.g., Visa, MasterCard, American Express, UnionPay etc.) which does not apply any verification, however, rather just sends the cryptogram to the bank that issued the card for verifying transaction details. Since this was a card that was issued by a bank, the terminal receives a successful ARPC from the issuer bank (see Figure 8) for a successful transaction, which is then executed.

[2]Bank Identification Number (BIN) refers to first four to six digits of a card that indicates a specific card type of a specific Bank.

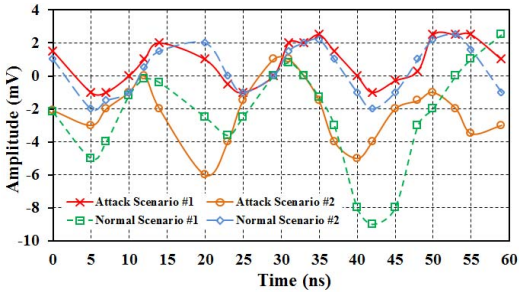
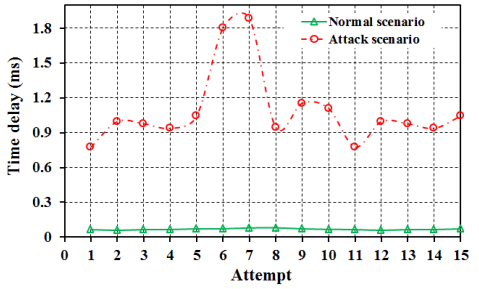
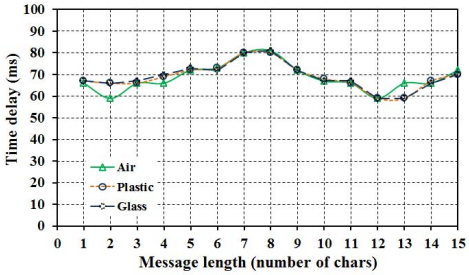


Figure 9: Changes in signal amplitude



(a) Time variation between normal and attack scenario



(b) Time delay for different communication medium between card and reader

Figure 10: Time delay in different scenarios

Normally, an offline settlement is performed between the merchant and bank after a few days, and banks hardly check each transaction before giving payment to the merchant. However, when the acquirer bank (that provided the terminal) will go for settlement with the issuer bank of an *MITM card*, the latter may deny to pay because of having no agreement between them. In this case, acquirer bank will be the victim. If banks check all transaction before giving payment to the merchant, it will be detected that selected transactions are performed with unauthorized cards and merchants can be fined or may have to forfeit their money. Thus, merchant becomes the victim here. In either case, we show how the malicious user is able to successfully launch an attack against contact-less payment protocols using our MITM module that is hard to prevent [3].

E. Clarifying Discussions on the Attack

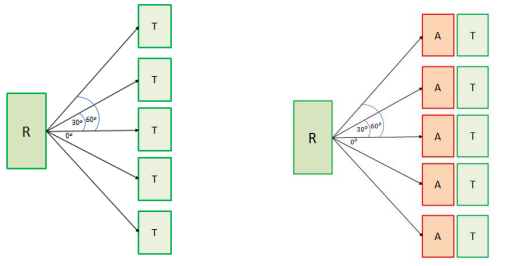
Our MITM attack proposed is practical. The hardware as we explained is feasible for NFC communications in the current form factor we designed above. With simple sniffing and/or skimming techniques, the TC, ARQC of a valid card can be easily obtained for writing on our MITM attack module. Note that one could argue about the feasibility of integrating the

[3]Now, in the case where the *MITM card* is a clone of another card that is legally accepted at a terminal, our attack will still be executable in practice, although in this case, the liability will not be with the terminal or the banks, but rather on the legal owner of either the *original card* or the cloned card. Attackers are less likely to attempt this scenario.

cryptogram components of both the authorized card, and the unauthorized card as a single NFC module, and alternate the information exchanged with the terminal in the same manner as we presented above to create the same attack impact with one hardware device instead of two. While this is doable, and will eliminate the need for a separate MITM module, we think that smart attackers will not prefer this scenario. First off, it forces an attacker to *always* engage in a malicious transaction even if the attacker does not want to do so (since the hardware and protocols are fixed for the device). Also, if terminals employ PUF based detection approaches (presented in Section II), the valid card must be present and not tampered with for a successful PUF based validation. Finally, the presence of a separate MITM module means that discarding it easier for a practical attacker should the need arise to do so, without compromising the *original card*. For these practical reasons, the overall MITM framework we present in this paper is practical. Furthermore, the close physical proximity and collusion between the *MITM card* and the *original card* means that existing protocols proposed in the literature to defend against other attacks in NFC communications (presented earlier in Related Work) are not geared for defending against our MITM attack.

Also, we note that it is entirely possible that our MITM module can be with the terminal as a component designed to sniff cryptogram details of benign cards that could be used later for generating fake/ malicious transactions. In this manner, a terminal need not be tampered with, however, can still engage in malicious sniffing. We do not elaborate on this aspect in more detail, however, this is practical. We also believe that with the wide popularity of NFC based applications in smart tolls, passport based entry systems, inventory tracking (e.g., medicines), new attacks are possible when adversaries leverage our designs in this paper to launch MITM attacks, and investigating these is part of our current study.

Furthermore, in certain cases, there may be much lower limits on transaction amounts that are allowed to be conducted via contact-less payments in order to provide better financial security. While our attack is still feasible in such scenarios, this issue opens up a new spectrum of the cost-effectiveness of an attacker engineering our attack for financial gain. This is also an issue that could be potentially investigated from both an attack and defense perspective.



(a) Normal communication (b) Attacker with card

Figure 11: Reading card in different angles

Table I: Time delay for different angles

Setting	Angle between Card and Reader	Success Rate (%)	Delay (ms)			
			Min	Max	Avg	Stdev
Legitimate	0°	100	66	81	71	7
	30°	100	66	108	79	17
	60°	67	67	109	85	15
Attack	0°	100	777	1883	1199	440
	30°	100	946	2108	1488	581
	60°	56	2251	4527	3383	1299

IV. Experimental Analysis and Insights for Defending Against our MITM Attack

Recall from Section II, where we showed why existing defense strategies cannot apply for our MITM attack. We now report limited experimental results on the physical nature of NFC communications with and without an MITM attack to identify insights for successful defense. First off, we find a significant change in signal strength (amplitude value) in presence of an MITM attacker. However, this change is not due to MITM attacks alone, however, for other reasons like varying proximity between card and reader, molecular absorption etc. Figure 9 shows the change in signal amplitude over time for two separate instances of normal and attack scenarios. Unfortunately, even for two normal scenarios without MITM attacks, the signal amplitudes are vastly different, which precludes amplitude as a reliable marker to detect MITM attacks.

However, with an MITM attack, delays increase. In our experiments, a reader normally takes only 59 to 81 milliseconds (ms) to read a card without an MITM, whereas it takes 777 to 1863 ms (around 20 times more) in presence of an MITM (Figure 10(a)). This is a non-negligible increase in delay that provides mechanisms to detect MITM attacks.

Note that, the delays should also vary depending on message length and medium of communication as per intuition. Therefore, to check if the delay actually varies with the message length, we measure time delay for different message lengths in our experiments. However, since the maximum length of payload gets fixed while being in NFC communications, and since the *nfc.read()* command reads the whole card at a time, the variation in message length does not exhibit any significant effect in delay. This also validates increased delay as the best marker for detecting MITM attacks. It is also important to note that in our experiments, the increase in delays was found to be independent of the medium of communication between the card and the reader (i.e., air, plastic, glass, etc.) as shown in figure 10(b), further validating the impact of leveraging increase in delay to detect MITM attacks.

To further clarify, we present Table I with results obtained from the setup presented in Figure 11. As presented in Figure 11, the reader is at slightly different angles compared to the *original card* with and without the MITM attacker. As we can see, the increase in delays are consistent and non-negligible between the normal scenario and the attack scenario. We also see that beyond an angle of 60° between the reader and the tag, success rate of communication goes down, which also provides a marker for detecting non-aligned MITM attackers.

V. Future Work

We are currently investigating approaches to reduce the form factor of MITM over NFC communications. In this paper, we use three extra devices for attacker. In future, we will try to establish the attack in more convenient way by reducing the number of attacker devices so that the attacker can be thinned further. Also, at present, our attack works in active-passive mood. In future we will analyze if the attack is possible in peer-to-peer communication mode also.

In this paper, we show that existing security mechanisms used for NFC communications fail to prevent our attack. Here, we present limited experimental results on the physical nature of NFC communications with and without an MITM attack to identify insights for successful defense. We plan to conduct many more experiments with MITM attacks over NFC communications to device technologies that are purely algorithmic, or a combination of algorithmic and hardware technologies to combat MITM attacks.

VI. Conclusions

In this paper, we demonstrate for the first time, the practical feasibility of MITM attacks over NFC communications, and also present a practical attack scenario in the realm of contactless payments. We also present important insights that could be used as defense mechanisms against MITM attacks over NFC communications. Our future work lies in demonstrating more convenient forms of MITM attacker modules by reducing the number of physical devices, and also to demonstrate attacks in peer-to-peer communication mode with more devices like smartphones and RFID communications. We will also conduct more rigorous theoretical and experimental studies on a combination of algorithmic and hardware technologies to detect MITM attacks in NFC communications. Naturally, the issue of designing robust defense protocols against MITM attacks is also a topic of our future work.

VII. Acknowledgment

This research study was funded by Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh under its Higher Training and Research Programme, and in part by the US National Science Foundation under Grants CNS 1205695 and IIS 1559588.

References

[1] E. Haselsteiner and K. Breitfuss, "Security in Near Field Communication (NFC)", Workshop on RFID Security, 2006.

[2] A. Suraperwata and I. Pratiwi, "Solutions to Near Field Communication (NFC) Vulnerabilities Against Interception Type Attacks", CISAK, 2013.

[3] S. Kavya, K. Pavitra, S. Rahman, M. Vahini, and N Harini,"Vulnerability Analysis And Security System For NFC-Enabled Mobile Phones", International Journal of Scientific and Technology Research Volume 3, Issue 6, 2014.

[4] J. Daemen, V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard", Springer Science & Business Media, Mar 9, 2013.

[5] A. Mahalanobis, "Deffie-Hellman Key Exchange Protocol, Its Generalization and Nilpotent Groups", PhD thesis, Florida Atlantic University, August 2005.

[6] Di Ma, Anudath, N. Saxena, and T. Xiang, "Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing", IEEE Transactions on Dependable and Secure Computing (Volume: 10, Issue: 2, March-April 2013).

[7] W. Nel, A. Burger, "Proving Cybercriminal's Possession of Stolen Credit Card Details on Compromised POS Devices", 5th International Conference on Management Leadership and Governance, 2017.

[8] G. Madlmayr and J. Langer, "NFC Devices: Security and Privacy", Third International Conference on Availability, Reliability and Security, 2008.

[9] NFC Forum. Available at: http://www.nfc-forum.org, Last accessed on January 19, 2017.

[10] M. Mehrnezhad, F. Hao, and F. Shahandashti, "Tap-Tap and Pay (TTP)", Newcastle University, 2014.

[11] "NFC Shield V2.0", http://www.seeedstudio.com/depot/NFC-Shield-V20-p-1370.html, Last accessed on January 19, 2017.

[12] "Arduino UNO", https://www.arduino.cc/en/Main/ArduinoBoardUno, Last accessed on January 19, 2017.

[13] "Arduino Mega 2560", http://www.arduino.cc/en/Main/ArduinoBoard Mega2560, Last accessed on January 19, 2017.

[14] http://www.statista.com/statistics/251306/nfc-payment-transaction-value-in-the-united-kingdom/

[15] Leonid Bolotnyy and Gabriel Robins, "Physically Unclonable Function -Based Security and Privacy in RFID Systems", PerCom'07, 2007.

[16] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, "Lightweight Secure Search Protocols for Low-cost RFID Systems", ICDCS'09, June 2009.

[17] P. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia, and M. Rimondini, "Efficient and Practical Authentication of PUF-Based RFID Tags in Supply Chains", 2010 IEEE International Conference on RFID-Technology and Applications (RFID-TA), June 2010.

[18] L. Dongsheng, Z. Xuecheng, Li Yongsheng, and Li Xiaohuang, "Anti-collision algorithm for RFID systems", Journal of Huazhong University of Science and Technology, 2006-09.

[19] G. Shu-qin, WU Wu-chen, H. Li-gang, and Z. Wang, "Anti-collision algorithms for Multi-Tag RFID", Radio Frequency Identification Fundamentals and Applications Bringing Research to practice, February 01, 2010.

[20] M/Chip, Acquirer Implementation Requirements, "MasterCard PayPass".

[21] "Hacker's Demo Shows How Easily Credit Cards Can Be Read Through Clothes And Wallets", https://www.forbes.com/sites/andygreenberg/2012/01/30/hackers-demo-shows-how-easily-credit-cards-can-be-read-through-clothes-and-wallets/#248d41bf78a6, Last accessed on April 3, 2017.

[22] "Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers", http://www.emv-connection.com/downloads/2016/06/Contactless-2-0-WP-FINAL-June-2016.pdf, Last accessed on April 3, 2017.

[23] "Contactless Specifications for Payment Systems", Book B, Version 2.6, July 2016.

[24] Mart Bakhoff, "EMV (Chip-and-PIN) Protocol", December 15, 2014.

[25] De Ruiter, Joeri, and Erik Poll. "Formal analysis of the EMV protocol suite." Joint Workshop on Theory of Security and Applications, Springer Berlin Heidelberg, 2011.

[26] J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is Broken", IEEE Symposium on Security and Privacy, May 2010.

[27] "Visa Integrated Circuit Card Specification", Version 1.5, May 2009.

[28] Technical Specification, "PayPass M/Chip", Version 1.3, September 2005.

[29] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones", International Conference on Availability, Reliability and Security, 2009.

[30] V. Coskun, F. Soylemezgiller, B. Ozdenizei, and K. Ok, "Development and Performance Analysis of Multifunctional City Smart Card System", International journal of Computer, Electrical, Automation, Control and Information Engineering, 2014.

[31] W. Park, D. H. Kim, and D. Lee, "Vulnerability of Rechargeable RFID Tag Card Based on NFC", International Journal of Control and Automation, (Vol. 8, No. 4, 2015).