Smart Card Protocol Analysis and Vulenrability Assessment using NFC Reader

Sushant Padmanabhi, Himanshu Mahajan, Mehul Patil, Piyusha Kulkarni, Rishabh Jhamb, Vanshika Rakeshbhai Shah, Amisha Saxena, Navina Sehgal, Simran Gujral, Yash Narang, Yukta Taneja, Harmanjeet Singh, *CIISE, Concordia University*

# **Abstract—** **Smart card are a secure way of transferring data, but security has not been properly handled in numerous applications, such as in public transportation systems. In this project, a methodology to reverse engineer and detect security flaws has been practiced. Specifically, the protocol of a smart card was analyzed. By applying the methodology with a tool, it was possible to access private information to capture tag-reader communications, and even emulate both tags and readers.**

# Introduction

Smart cards are tiny plastic cards with a microprocessor chip inside that can store and process data. These cards are used for electronic payments, access control and authentication. The microprocessor chip on the smart card is used to handle tasks such as encryption, creating of digital signatures and for securing the data. The smart card communicates with the card readers by contact or contactless interfaces by which the transfer of data is possible. Also, they provide a second level of authentication and protection, so they are used for security purposes for the protection of data. These smart cards are used in sectors like healthcare, transportation, banking etc. as they can securely store and transfer data such as medical records, tickets used in transportation, credit card numbers etc.

Diagram

Description automatically generated

1. Smart Card Information

Although smart cards are a secure method of data transport, they are susceptible to many dangers. Smart card security may be threatened by several factors, including logical and physical attacks like malware, and tampering and cloning. Smart card technology may also be vulnerable due to problems with the creation, use, or administration of the cards.

Many countermeasures, like as encryption, authentication protocols, access control systems, and physical security measures, can be used to minimise these dangers and vulnerabilities. Furthermore, it is possible to create and use smart card operating systems and apps to lower the danger of assaults.

Reverse engineering examines the transmission between the smart card and the reader or host device at the protocol level. This can be accomplished using passive or active techniques like eavesdropping, message interception, modification, or injection. The smart card application protocol data unit (APDU), the common means for exchanging data between smart cards and readers, can be revealed using these techniques in terms of its structure, content, and semantics. These techniques, though, are dependent on the implementations, standards, and protocol specifications, and they can be stopped by security mechanisms like authentication, encryption, and integrity checking.

The protocol level of smart card technology is how the smart card and the reader exchange data using the application protocol data unit (APDU) format. There are different types of contacted and contactless intelligent card protocols, such as T=0, T=1, Type A, Type B, etc. These protocols define the physical interface, transmission mode, error detection, and anti-collision methods. Standard protocols ensure interoperability and security, while proprietary protocols may have some advantages or disadvantages.

# Smart cards, Standards and their protocols

## NFC

A wireless communication technique called NFC, or near field communication, allows data to be sent utilising a proximity of up to 10 cm. Transactions are initiated automatically by contacting a reader or NFC device with this relatively straightforward technique [1]. Based on ISO 14443, this is a bidirectional coupling technique. The peer-to-peer mode of NFC's physical and data-link layers is controlled by ISO 18092.

## ISO/IEC 14443 Protocol

There are numerous standards that are being used for RFID, one of them being ISO/IEC 14443[2]. This standard is used for proximity cards with a transmission range of around 15 cm. There is a very common vulnerability that this standard does not provide protection against and i.e. Relay attack. A relay attack is where the intruder relays a message or communication between two people back and forth without the users being aware. There are many attacks already executed and exploited for this standard. Despite that, the countermeasures have not been implemented properly. The ISO/IEC standard operates on proximity cards. This standard is divided into four parts where the first part describes how the integrated card really works physically. The second part covers the communication between the card and the reader. The third part describes the routine that the card follows. The fourth part describes the block transmission protocol. Since the standard is so transparent, it does not provide any security mechanism.  Some countermeasures that are discussed in [2] are check transmission parameters and distance bounding protocols.

## ISO 18092

It standardizes peer-to-peer communication mode for random binary data exchanges. The peer-to-peer mode has a very big role in creating a secondary high-speed connection like Bluetooth or WIFI for the transfer of a large amount of data using NFC [3]. Devices can read or write data of any supported tag types in a standard data format because of this standard. Exchange of data over custom binary protocol is also enabled between devices. Card emulation allows the phone to act as a tag (contactless card) for other readers or POS terminals.

## FeliCa

FeliCa technology, an adaptable and popular element of NFC systems, offers safe and practical contactless communication for a range of purposes [29]. Among the many uses of contactless smart cards and RFID (Radio Frequency Identification) technology in Japan are access control, electronic payments, and public transportation.

The protocol employs amplitude-shift keying (ASK) modulation and runs at a frequency of 13.56 MHz. It allows for data transfer speeds of up to 212 kbps and provides a high level of security thanks to mutual authentication and encryption. The Felica protocol is widely used in Japan in mobile payment systems like Apple Pay and Google Pay, as well as in transportation systems like the SuiCa and Pasmo cards.

## Secure Electronic Transaction Protocol (SET)

In the world of electronic commerce, SET Secure Electronic Transaction is regarded as the key contributor to the payment system. It is an extremely thorough security mechanism that makes use of cryptography to ensure data secrecy. It guarantees both identity identification and payment integrity. The SET protocol's primary and fundamental requirement is that electronic transactions be carried out securely. SET employs two primary types of cryptography—public-key cryptography and secret-key cryptography—as well as techniques for encryption and decoding. A business can generate a public or private key pair and broadcast the public key using public key cryptography. This enables any client to send a secure message to the business. Financial institutions adopt DES (Data Encryption Standard), secret key cryptography, instead of RSA, public key cryptography, to encode PIN numbers [4].

## ISO/IEC 7816 Protocol

The ISO 7816[5] protocol describes the characteristics for a card that has been bent or dismantled in a way. It is crucial for the cards that have embedded chips in them that they are durable in any physical environment and work properly. Although these cards are made in plastic, they also have an expiration date which is usually referred to as till the digits or the chip is visible in the card. If the card is worn torn, the reader might not be able to read the chip from the card and the card might not process as it is supposed to. There are certain procedures that need to be followed for cards that are bent or flexed. All such procedures are standardized in ISO 7816. This is the major factor that this standard is often used. To integrate the circuit of the card, they must select a group of suitable components and integrate them together to make it work for the card. The modern cards are compliant with ISO 7816-2 standard and hence, older versions of this standard cannot be used in recent cards. Europe showed the greatest usage of these cards with ISO 7816 standard. The current dimensions of the card do not allow it to emboss any further. As, the cards used are already a bit embossed to protect the chip and integration of circuits. Instead, what users should be taught is to insert the card properly without bending. The magnetic field in the cards that helps the cards to connect with the ATMs is already an extra feature for the ISO 7816.

## ISO 8583

A standard for systems that exchange electronic transactions using payment cards. The aim of exchange of the payment information is achieved by using TCP/IP sockets. Iso 8583 provides the definition for the message format and the flow for communication which helps in enabling the exchange of transaction requests and the responses between different environments. As per reports, most commonly Mastercard, Visa and Verve networks base their authorization communications in this standard. This standard is not directly used by systems or networks. This standard defines many data fields which are retained in the same systems and later used by each network to adapt the standard with custom usage.

## ISO 7810

ISO 7810 is responsible for the physical properties of identification cards. It helps in defining the dimension, durability, humidity and temperature, stiffness of a card. The standard is a guide for the making and use of different kinds of ID cards. It is not limited to just one type of cards; it consists of different properties for many different kinds of cards. There are four card sizes and that are ID-1 which is mostly banking and ID cards, ID-2 which is for Romanian and other ID cards and visas as well, ID-3 this size is for passport booklets and fourth ID-000 is for sim cards. The standard also defines the metric and imperial measurements for the card [7][8].

## EMV2

The EMV standards for payment systems are managed and developed by the international collaboration known as EMVCo [31]. For processing payments using Near Field Communication (NFC) technology, EMVCo created the EMV 2 protocol. To provide safe and dependable communication between the payment terminal and the NFC-enabled device, such as a smartphone or contactless card, NFC systems employ the EMV 2 protocol. The protocol outlines the flow of data between the terminal and the device, as well as the encryption and decryption of sensitive data such cardholder information. Many payment methods are supported by the EMV 2 protocol, including contactless payments, smartphone payments, and in-app purchases. Also, it accepts a variety of cards, including gift and loyalty cards, debit, credit, and prepaid cards.

The EMV 2 protocol supports dynamic authentication, which means that each transaction creates a unique code that can only be used for that transaction. This is one of the system's important characteristics. This makes it far more difficult for thieves to obtain card information and use it for illegal operations. Ultimately, the EMV 2 protocol is a crucial part of NFC payment systems since it helps to guarantee transactions are safe, dependable, and simple to use.

This protocol is used by public transit cards in cities of USA like Washington DC and Boston.

## NFCIP-1 and NFCIP-2

At information transmission speeds of 106, 212, and 424 kbps, this protocol is described in standards ISO/IEC 18092 and ECMA-340. It specifies modulation, coding, and frame structure [9]. An initiator and a target form the object of communication in NFC. The main methods offered by NFCIP-1 are RFCA (Radio Field Collision Avoidance) and SDD (Single Device Detection) [10]. The SDD is an algorithm that helps the initiator select a particular target from a group of targets in the RF field. Collision issues might arise with the current RFID technology. A scenario when more than two initiators or targets communicate data simultaneously and it is difficult to tell whether data is real is referred to as a collision. The NFC standard uses the RFCA algorithm to tackle the collision problem. RFCA is a method that uses carrier frequency to find additional RF fields and avoid collisions. The first step of RFCA is to validate the existence of other RF fields. The NFC does not produce its own RF field if other RF fields are already present. The SDD, which locates targets within the range, and the RFCA, which forbids the use of two RF fields, allow the NFC to be protected from the attacks like MITM (Man-In-The-Middle).

The NFCIP 2 protocol operates at the ECMA 352 standard and specifies how to select a communication method between the three states described in ECMA 340 to ISO/IECS 14443 and ISO/IEC15693 [9].

## ECMA 385 & ECMA 386

## **A picture containing diagram Description automatically generated**

1. ECMA 385 Standard Structural Model

The Secure Channel Service (SCH) and the Shared Secret Service (SSE) are two services that are supported by ECMA 385 and ECMA 386 [11]. The Open System Interconnection Reference Model (OSI Reference Model) served as a design guide for ECMA 385's organizational structure. The ECMA 385 standard structural model is shown in Fig 2[12]. It separated NFC-SEC User, NFC-SEC, and NFC into three levels. The NFC-SEC standard prevents data modulation and eavesdropping by unidentified third parties. Now, if an NFC user1's phone wishes to contact another NFC user, it must engage the NFC-SEC-SAP (Service Accessing Point) request service. The request from the user will be noted in the NFC-SEC-SDU (Service Data Unit).

The NFC-SEC-PDU (Protocol Data Unit) is created by combining the NFC-SEC-SDU and the NFC-SEC-PCI (Protocol Control Information). With User1's NFC-SEC- SAP, which sits at the intersection of the NFC-SEC layer and the NFC layer, the NFC-SEC- PDU may establish a "NFC connection" with the NFC-SEC User2's NFC-SEC-SAP. They will be motivated to coordinate a common secret value for further communication by this conduct. It is known as the Secure Channel service (SCH) in the ECMA 386 standard. In the ECMA 386 standard, the Shared Secret service (SSE) was defined. To create their secret keys, they will employ the Diffie-Hellman Elliptic Curve technique. They would begin to transmit after creating the SCH and SSE during the connecting phase.

The ECMA 385 standard and the ECMA 386 standard both specify these two services. Nevertheless, the Card Emulated Mode and Reader/Writer Mode do not support these two secure transaction protocols. Only the peer-to-peer mode may be employed with these two services.

# Vulnerabilities in smart cards

Due to its capacity to enable quick and simple procedures, contactless cards are attracting a growing amount of attention from the market. In many instances, these cards may be waved in front of a reader without being taken out of a pocket or wallet. Also, the card is protected from the typical wear and tear impact that affects contact smart cards thanks to contactless communication technology. As a result, contactless cards are being used increasingly often and for a variety of purposes, such as electronic identification documents, payment cards, and electronic tickets, as well as access control for secure settings and facilities.

Contactless cards are vulnerable to security flaws since they employ wireless communication. By establishing contactless connection with the card's chip, it is possible to intercept the signals sent between the card and reader or covertly skim the content of the card. If the card is hacked, the information on it may be utilised to make a copy of the card. Access control techniques are used to limit access to the chip content and functionality, and contactless card connections are frequently encrypted to avoid such assaults. For instance, the system that the card is dealing with can ask the cardholder for a code, such as a Personal Identification Number (PIN), in order to enable access.

## Denial of Service Attacks

A DoS attack on NFC devices or readers can render them unavailable to intended users. One DoS attack scenario involves using a jamming device to disrupt communications between two NFC devices. This interference can destroy transmitted data and cause DoS. Continuous detection of jamming attacks can be used as a solution to this scenario. NFC devices can check the radio frequency field while transmitting and stop data transmission when a jamming attack is detected.

Another type of Denial of Service (DoS) attack that aims to destroy the trust relationship between customers and service providers. The attack involves a malicious actor creating a tag that causes an NFC mobile phone to crash after scanning. The attacker then places the malicious tag on top of the service provider tag. When a customer visits the service provider and scans the tag using their NFC mobile phone, the phone crashes. Since the malicious tag looks like a normal tag, it cannot be linked to the phone crash incident. This attack can destroy the trust relationship between customers and the service provider.

Another scenario of denial-of-service attack is simply touching the device with an empty tag causes it to generate an error message, which can easily occupy the device and make it unavailable. However, the use of an NFC switch can help to prevent this attack scenario. Although the drawback of this solution is that the user must manually turn the NFC functionality on and off each time they need to scan.

## Relay Attacks

A reader can be easily tricked by a relay attack that takes advantage of the possible vulnerability. To carry out such an exploit, two key components are necessary: a mole and a proxy, both of which require a contactless card interface. For a mole to be effective, it must be located near the targeted card, while the proxy needs to be positioned near the reader. By relaying commands and responses, the mole establishes a communication channel between the card and the reader. The targeted card's privileges and rights become accessible to the attacker when they assume the identity of the cardholder using a proxy. This allows them to present themselves as the cardholder to the reader. To evade the safeguards guarding contactless cards, the main aim of a relay attack is to establish a connection with the card reader directly.

This method enables attackers to bypass the security protocols that are already in place. A strategy that may be adopted by attackers is utilizing encrypted communication, allowing the legitimate parties to handle the secure channel separately, thereby averting interference by the attacker. The hacker may choose to overlook the validity of the card and totally disregard challenge-response tactics. Guarding against proxy attacks involves access control mechanisms that rely on effective design to prevent transactions without the essential card code. Fluctuating reliability is a challenge, and even with these mechanisms in place, vulnerabilities can still jeopardize security. Exploiting these weaknesses, attackers can circumvent the system without requisite knowledge like a PIN.

## Non-Invasive And Algorithm Implementation Attack

Non-invasive attacks pose no physical harm to the contactless card and are not specific to a particular card. Once an attacker has developed an attack for a specific processor and software version, they can quickly replicate it on other cards of the same type. The equipment used in these attacks can often be disguised as a normal smartcard reader. Non-invasive attacks are particularly concerning in some applications for two reasons. First, the card owner may not realize that their secret keys have been stolen, so the compromised keys are unlikely to be revoked before they are exploited. Furthermore, non-invasive attacks have the advantage of scalability since the equipment required for executing such attacks can be replicated and upgraded inexpensively.

* *Timing Analysis Attacks:*

Timing attacks leverage the duration taken by a system to execute operations and can potentially expose confidential keys. To illustrate, a perpetrator could exploit precise timing measurements to identify constant Diffie-Hellman exponents, factorize RSA keys, and compromise other cryptographic systems. If a system is vulnerable, the attack can be relatively simple and may only require knowledge of ciphertext.

Different inputs may cause cryptosystems to take slightly different amounts of time to process. This can be due to performance optimizations, conditional statements, processor instructions, and other factors.

Attackers can use timing measurements to find the entire secret key of vulnerable systems. This can be particularly dangerous because the owner of the system may not even realize that their key has been compromised. The performance attributes are commonly contingent on both the input data (i.e., plaintext or ciphertext) and the encryption key.

* *Side Channel Attacks:*

Side channel attacks (SCAs) are different from regular cryptographic attacks because they exploit side channels like power consumption, voltage fluctuations, temperature, or sound to extract secret information from a system. Placing an antenna, magnetic probe, or other sensor close to the device or system allows access to these side channels. There are two primary types of SCAs: simple power analysis (SPA), which uses direct observations of power or electromagnetic measurements to extract secret information, and differential power analysis (DPA).

Diagram

Description automatically generated

1. Communication Between NFC Card, Card Reader and Secure Access Module

To start with, it is crucial to evaluate the possibility of exploiting power analysis attacks on the card key. Power analysis attacks are a type of attack that can be used to extract sensitive information, such as secret keys or plaintext data, by analyzing the power consumption of a device during encryption operations. Attackers can obtain sensitive information by performing repetitive cryptographic calculations with a fixed secret key and different plaintexts. They can collect side-channel signals, such as power consumption measurements, and analyze them to reveal secret keys.

In the case of communication interception between a transfer card and a reader, attackers could potentially gain access to session keys by executing power analysis attacks on the card key. Implementing security measures such as power consumption masking or randomization during cryptographic operations can reduce the risk of these attacks.

## Out of Bound Read/Write Attacks

Data can be written above authorized buffer limits, which can cause software crashes, data corruption, and code execution issues. These out-of-bounds write vulnerabilities, which are brought on by writing outside the permitted area, may be harmful to software systems.

Hackers can carry out illegal code execution and denial-of-service attacks by taking advantage of security flaws. Developers must prioritize resolving vulnerabilities by finding, fixing, and avoiding them in their code to avoid these scenarios. Always keep in mind how important this is for overall software security.

* *Buffer Overflow Attack*

Buffer overflow vulnerabilities are a widely recognized problem that can grant attackers complete control over a program and even the entire system. By allowing them to inject new code, such vulnerabilities are highly concerning in the firmware of Near Field Communication (NFC) readers since they enable attackers to manipulate the function of a privileged program and potentially take control of the entire system. Additionally, buffer overflow vulnerabilities can also impact web applications, potentially causing the execution stack to become corrupted and enabling the execution of unauthorized code. Addressing these vulnerabilities in NFC readers is essential to mitigate security threats.

Diagram

Description automatically generated

1. Buffer Overflow Attack in Smart Cards

The firmware of Near Field Communication (NFC) devices has been found to contain a buffer overflow vulnerability, which is a security issue that has been long recognized. The operation of a privileged program is manipulated by an attacker who carries out a buffer overflow assault to take over the system. While root programs are frequently the target of this kind of assault, other programs may also be impacted. Total control of the host machine can be taken by the attacker if the program has sufficient privileges. When the system is compromised, other techniques or code like "exec(sh)" may be used by the attacker to instantly gain full access. It is important to handle buffer overflows in NFC readers because they present a serious security risk. Buffer overflow flaws in web apps can be very dangerous as they allow hackers to alter the execution stack and run unauthorized code.

These vulnerabilities can exist in both application servers and web servers, particularly in web applications that use libraries like graphics libraries. Custom web application codes can also be vulnerable to buffer overflows. Even though these codes may receive less attention from security teams, they can be more difficult for hackers to find and exploit. Consequently, implementing appropriate security measures to identify and mitigate buffer overflow vulnerabilities in web applications is crucial.

## Man In The Middle Attack

An attacker can carry out a man-in-the-middle attack on Calypso systems by exploiting a weak protocol design. This allows the attacker to recharge a card at a point of service without the terminal's knowledge. The protocol involves the reader sending a signal called Signature Hi to the card to indicate that the transaction on the reader side is complete. The card then commits the transaction on its side and sends the signal Signature Low to the reader if the transaction is successful. The reader commits the data on its side when it receives Signature Low but cancels the transaction if it doesn't receive the signal. The attacker can prevent Signature Low from reaching the reader, causing the reader to cancel previous transactions while the card is charged, and the new ticket number is stored in the card's memory.

Diagram

Description automatically generated

1. Session Hijacking in NFC Cards

Another type of man-in-the-middle attack involves exploiting the plain messages that are sent at the start of a communication. A smart card (ex-OPUS; a transit card) tickets remain valid for two hours from their first use, so an attacker can manipulate the messages related to the last three usages of the card. By changing the time/date information in these messages, the attacker can deceive the reader into believing that an invalid ticket is still valid or that a valid ticket has expired. This is a significant attack that can allow the attacker to use the same ticket for an extended period, regardless of its actual validity.

## Eavesdropping Attack

Although the communication range of NFC devices is limited to a few centimeters, eavesdropping attacks are still possible. The attacker's proximity to the target device depends on factors such as equipment used, location of the attacker, and communication mode. Passive mode is more difficult to eavesdrop on because the target device draws its power from the electromagnetic field generated by the active device. However, an attacker with sufficient knowledge and equipment, can still capture NFC communication.

There are three ways in which an attacker can launch an information leakage attack on an OPUS card.

The first method involves stealing the unique serial number of the card through Eavesdropping, skimming, or simply looking at the back of the card. This unique ID can be used to track and even identify the card holder by correlating it with other information associated with the card holder such as their purchase history, residential or work address, and daily commute schedule. Although there may be better ways to track or identify a person, this method is still a privacy-violating feature that can be carried out at a distance and in an automatic way without the user's knowledge. Attackers can use this information to create a customer profile for targeted advertising or track the card holder for any other reason.

The second Eavesdropping method involves estimating the time when the OPUS card was purchased by taking advantage of the fact that unique serial numbers are generated sequentially. By collecting many OPUS card IDs, it is possible to deduce the month and year of purchase with ease. With more precise methods, an attacker could reduce this time slot to a day or even less.

The third method involves sniffing or skimming information about the last three usages of the card, such as the bus line or metro station used, through communication with a legitimate reader or by using a Proxmark3 in the vicinity of the card. This information can be used to deduce the daily commute schedule of the card holder and their home or work neighborhood.

# Implementation

## Hardware Used

* NXP MIFARE Classic® 1k
* ISO/IEC 14443 - 3(NFC-A)
* Total memory: 1kb
* Blank, white, printable with a Card Printer
* Write endurance (typical cycles): 200,000.
* Data Retention: up to 10 years
* 4-byte UID
* CRYPTO1 cryptography supported.

## MIFARE Classic 1K Card

The MIFARE Classic 1K card can be configured as either read-only or read/write. A read-only MIFARE Classic 1K card contains information that cannot be changed or updated. This type of card is commonly used for applications such as ticketing or identification, where the information stored on the card is fixed and does not need to be updated. It contains 1 kilobyte of memory and is organized into 16 sectors, each containing 4 blocks of data. Each block can store up to 16 bytes of data and can be either read-only or read/write.

MIFARE Classic 1K contains variety of data as below,

* *User information:* This can include details about the cardholder, such as their name, address, and contact information.
* *Access control information:* This can include data about the areas or facilities that the cardholder is authorized to access, such as a door or turnstile.
* *Payment information:* This can include details about the cardholder's account balance or transaction history for a payment system.
* *Ticketing information:* This can include details about the cardholder's ticket or travel information, such as the destination or amount.
* *Security keys:* MIFARE Classic 1K cards use a proprietary encryption algorithm to secure the data stored on the card. The card can contain various security keys that are used to authenticate the card and protect the data from unauthorized access.

## Crypto1 Protocol

Utilized in the MIFARE Classic 1K smart card is the CRYPTO1 encryption algorithm which employs a stream cipher using 48-bit keys. This algorithm serves to secure the communication established between the reader and the card.

The pseudorandom bitstream used to form the ciphertext is created through application of the CRYPTO1 methodology, which relies on XORing with the plaintext data. Obtaining the key for the pseudorandom bitstream necessitates accessing the key stored on the card in conjunction with the singular serial number of that card. Decoding intercepted conversations between the reader and the card would require a potential attacker knowing both the key and serial number. [16]

The susceptibility of the CRYPTO1 algorithm has made it prone to specific attacks. "Nested attack" is a methodology performed where a series of authentication attempts are carried out, and the responses are then examined to retrieve the key. [15] The MIFARE Classic 1K card's security has been questioned due to this vulnerability, making it unsuitable for high-security applications.

FeliCa, HID iCLASS SE, MIFARE Plus, and DESFire are just some of the more secure smart card technologies available, all more dependable than MIFARE Classic 1K. These options utilize advanced encryption methods, mutual authentication, and extra security features to ensure vulnerability to attacks is minimized. Take note that the smart card selected relies on the system's distinct security requirements and usage.

## Vulnerabilities in MIFARE Classic 1K

The MIFARE Classic 1K card contains multiple known security flaws that may be exploited by attackers to gain access to or change the data on the card. Here are a few instances of these flaws and how they might be exploited:

* Weak encryption: The MIFARE Classic 1K card employs Crypto-1, a proprietary encryption technique that has been found to be vulnerable to certain sorts of attacks. An attacker, for example, may intercept communication between the card and the reader and extract the encryption keys used to safeguard the data on the card using a specialized RFID reader.
* Card cloning: Because the MIFARE Classic 1K card has weak encryption, it is possible for an attacker to create a cloned card that contains the same data as the original card. This can be done using a specialized RFID reader/writer that can copy the data from the original card onto a blank card which needs to be a T5577 card.
* Data manipulation: An attacker who has access to a cloned or genuine MIFARE Classic 1K card can also manipulate the data stored on the card. For example, an attacker could change the access control information on the card to gain unauthorized access to a building or facility.
* Brute-force attacks: The MIFARE Classic 1K card has a limited number of keys that can be used to access the data on the card. An attacker could use a brute-force attack to try all possible combinations of keys until the correct one is found.

## Nested Attack using MFOC

Nested attack is a technique used by MFOC for key cracking of MIFARE classic cards. Using MFOC for a nested attack involves trying out a set of default keys that are hard-coded on the card for authentication. Should there be no luck with the default keys, MFOC moves on to the next phase where it can perform a dictionary attack.

MFOC utilizes a nested approach in a dictionary attack by testing multiple keys (usually drawn from a pre-computed key space or a custom dictionary file) until the correct key is found. Rather than attempting all keys simultaneously, MFOC conducts authentication attempts, with each subsequent attempt using the result of the prior attempt as input. This approach reduces the number of authentication efforts necessary to crack the keys, accelerating and streamlining the attack process.

To increase the likelihood of success and hasten the attack, MFOC utilizes incremental keys search and partial matching, in addition to other techniques. Once the correct key is found, MFOC can read or write data to the card, allowing unauthorized access to the information on the card.

Text

Description automatically generated

1. Figure depicts Key Cracking using Nested Attack with MFOC

## Card Data Duplication Using RC522 & Arduino Uno R3

### We have used Arduino Uno R3 and RC522 modules to read and clone data from one card to another. The RC522 module is a common RFID reader module that is designed to work with Arduino microcontrollers. It communicates with the microcontroller via SPI (Serial Peripheral Interface) and is capable of reading data from Mifare Classic RFID cards.

Graphical user interface, text, application, email

Description automatically generated

Text

Description automatically generated

1. First Figure shows Card A details in NFC Tools and second image shows the copying of Card A data  
   Graphical user interface, text, application, email

   Description automatically generated  
   Text

   Description automatically generated
2. First Figure shows Card B details before writing data in NFC Tools and second image shows the writing of Card A data over Card B  
     
   Graphical user interface, text, application, email

   Description automatically generated
3. Figure shows the data wrote on Card B from Card A

# Conclusion

Our research delved into evaluating the security of different smart card protocols in relation to NFC readers. The report scrutinized various NFC card protocols utilized globally and pinpointed susceptibilities each of them may possess.

To verify our analysis, we executed a pair of attacks - nested attack implementing MFOC and data replication attack integrating RC522 and Arduino Uno. The successful nested attack allowed us to extract the keys of MIFARE Classic cards and attain access to the contents of the cards. All in all, our study highlights the importance of ensuring smart card protocols are secure and less susceptible to hacking.

Our revelations about the ease of replicating a smart card in a data replication attack illuminated the vulnerabilities of smart card protocols to illicit access. As a result, the protection of sensitive information demands implementing heightened security measures. Taking into account the susceptibility of smart card protocols, consistent surveillance and upgrades are essential to fend off threats.

##### References

1. Madlmayr, Gerald, Josef Langer, Christian Kantner, and Josef Scharinger. "NFC devices: Security and privacy." In *2008 Third International Conference on Availability, Reliability and Security*, pp. 642-647. IEEE, 2008.
2. Issovits, Wolfgang, and Michael Hutter. "Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks." In *2011 IEEE International Conference on RFID-Technologies and Applications*, pp. 335-342. IEEE, 2011.
3. https://bitexperts.com/Question/Detail/3360/difference-between-iso-14443-and-iso-18092-i-e-rfid-vs-nfc
4. Parihar, Pankaj Singh, Vikas Kurdia Pankaj Suwalka, and Ratnesh Parasher Deepali Mahatma. "An Implementation of Set Protocol with DES Algorithm."
5. Thorpe, Christina, John Tobin, and Liam Murphy. "An ISO/IEC 7816-4 Application Layer Approach to Mitigate Relay Attacks on Near Field Communication." *IEEE Access* 8 (2020): 190108-190117.
6. <https://en.wikipedia.org/wiki/ISO_8583>,<https://www.ir.com/guides/introduction-to-iso-8583>
7. [Early Discovery of Chronic Non-attenders by Using NFC Attendance Management System](https://ieeexplore-ieee-org.lib-ezproxy.concordia.ca/document/6624813), <https://en.wikipedia.org/wiki/ISO/IEC_7810>
8. Ochomo, Zablon O., Elisha Opiyo, William Okello-Odongo, and J. M. Kizza. "Agent Based Model For Localized Secure Payment Systems Integration." Strengthening the Role of ICT in Development (2010).
9. Shariati, S. Mahdi, A. Abouzarjomehri, and M. Hossein Ahmadzadegan. "Investigating NFC technology from the perspective of security, analysis of attacks and existing risk." In 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), pp. 1083-1087. IEEE, 2015.
10. Eun, Hasoo, Hoonjung Lee, and Heekuck Oh. "Conditional privacy preserving security protocol for NFC applications." IEEE Transactions on Consumer Electronics 59, no. 1 (2013): 153-160.
11. Chen, Cheng Hao, Iuon Chang Lin, and Chou Chen Yang. "NFC attacks analysis and survey." In 2014 eighth international conference on innovative mobile and internet services in ubiquitous computing, pp. 458-462. IEEE, 2014.
12. Azhari, F. (2014), "Quick detection of NFC vulnerability: Implementation weakness exploitation", Information Management & Computer Security, Vol. 22 No. 2, pp. 134-140. <https://doi.org/10.1108/IMCS-09-2013-0067>
13. “MF1S50YYX\_V1 MIFARE Classic EV1 1K -Mainstream contactless smart card IC for fast and easy solution development,” 2018. Available: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX\_V1.pdf
14. F. D. Garcia, P. van Rossum, R. Verdult and R. W. Schreur, "Wirelessly Pickpocketing a Mifare Classic Card," 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2009, pp. 3-15, doi: 10.1109/SP.2009.6.
15. Golić, J.D. (2013). Cryptanalytic Attacks on MIFARE Classic Protocol. In: Dawson, E. (eds) Topics in Cryptology – CT-RSA 2013. CT-RSA 2013. Lecture Notes in Computer Science, vol 7779. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-642-36095-4_16>
16. A. Alrawais, “Security Issues in Near Field Communications (NFC),” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, 2020, doi: <https://doi.org/10.14569/ijacsa.2020.0111176>.
17. T. Kim, Tae Hyun Kim, and S. Hong, “Breaking Korea Tansit Card with Side-Channel Analysis Attack-Unauthorized recharging -,” *https://www.blackhat.com/docs/asia-17/materials/asia-17-Kim-Breaking-Korea-Transit-Card-With-Side-Channel-Attack-Unauthorized-Recharging-wp.pdf*, 2017.
18. https://www.semanticscholar.org/paper/Breaking-Korea-Tansit-Card-with-Side-Channel-Kim-Kim/a3537e75e46a82bcfe222edd0a3ec9b0f0758ab0 (accessed Apr. 03, 2023).
19. Y. C. Lee, “Smart-card-loss-attack and Improvement of Hsiang et al.’s Authentication Scheme,” *Journal of Applied Research and Technology*, vol. 11, no. 4, pp. 597–603, Aug. 2013, doi: https://doi.org/10.1016/s1665-6423(13)71567-0.
20. Z. Zorz, “Vulnerabilities in smart card drivers open systems to attackers,” *Help Net Security*, Aug. 13, 2018. https://www.helpnetsecurity.com/2018/08/13/vulnerabilities-smart-card-drivers/#:~:text=Most%20of%20the%20vulnerabilities%20he (accessed Apr. 03, 2023).
21. J. Markoff, “Vulnerability Is Discovered In Security for Smart Cards,” *The New York Times*, May 13, 2002. Accessed: Apr. 03, 2023. [Online]. Available: https://www.nytimes.com/2002/05/13/business/vulnerability-is-discovered-in-security-for-smart-cards.html
22. “NFC Tutorial | Tutorial on NFC Protocol | How NFC works,” *www.rfwireless-world.com*. https://www.rfwireless-world.com/Tutorials/NFC-Near-Field-Communication-tutorial.html
23. L. Sportiello, “‘Internet of Smart Cards’: A pocket attacks scenario,” *International Journal of Critical Infrastructure Protection*, vol. 26, p. 100302, Sep. 2019, doi: https://doi.org/10.1016/j.ijcip.2019.05.005.
24. “Smart cards: security risks | Computer Weekly,” *ComputerWeekly.com*. https://www.computerweekly.com/ehandbook/Smart-cards-security-risks (accessed Apr. 03, 2023).
25. “What is NFC?,” *STMicroelectronics*, 2023. https://www.st.com/content/st\_com/en/support/learning/essentials-and-insights/connectivity/nfc.html#:~:text=What%20is%20NFC%3F- (accessed Apr. 03, 2023).
26. “A method for resynchronizing a random clock on smart cards ... Didier Moyart -Régis Bevan Oberthur Card Systems.” Accessed: Apr. 03, 2023. [Online]. Available: https://www.nmda.or.jp/nmda/ic-card/proceedings/30-1440-DMoyart.pdf
27. H. Handschuh and H. M. Heys, “A Timing Attack on RC5,” *Selected Areas in Cryptography*, pp. 306–318, 1999, doi: https://doi.org/10.1007/3-540-48892-8\_24.
28. “Low Cost Attacks on Tamper Resistant Devices,” *www.break-ic.com*. https://www.break-ic.com/topics/attack-microcontroller.asp (accessed Apr. 03, 2023).
29. Akiyama, Tomohiro, Tetsuhiro Tanno, Tetsuhiro Sasagawa, and Kumiko Yamaguchi. "Technologies for Further Evolution of Osaifu-Keitai Service—NFC-enabled Mobile Terminals and NTT DOCOMO UIM Card—." *NTT DOCOMO Technical Journal* 15, no. 1 (2013): 13-21.
30. “Sony Corporation - Felica - overview of Felica - what is Felica ?,” SONY. [Online]. Available: https://www.sony.net/Products/felica/about/. [Accessed: 04-Apr-2023].
31. Freitas, Leo, Paolo Modesti, and Martin Emms. "A methodology for protocol verification applied to EMV® 1." In *Formal Methods: Foundations and Applications: 21st Brazilian Symposium, SBMF 2018, Salvador, Brazil, November 26–30, 2018, Proceedings 21*, pp. 180-197. Springer International Publishing, 2018.