Fontys
University of Applied Sciences

An Investigation of “Smart Cards” and their Security

Personal Vulnerability Investigation

April 21st, 2023

Aleksandar Penev
a.penev@student.fontys.nl

Fontys
University of Applied Sciences

Contents

Fontys
University of Applied Sciences

Version Control

Version 0.1	25.03.2023	Created the document template. Wrote Introduction and Preface.
Version 0.2	02.04.2023	Answered the first research question
Version 1.0	20.04.2023	Expanded upon the first research question and finished the next two research questions
Version 1.1	21.04.2023	Finished the last research questions and wrote a conclusion

Preface

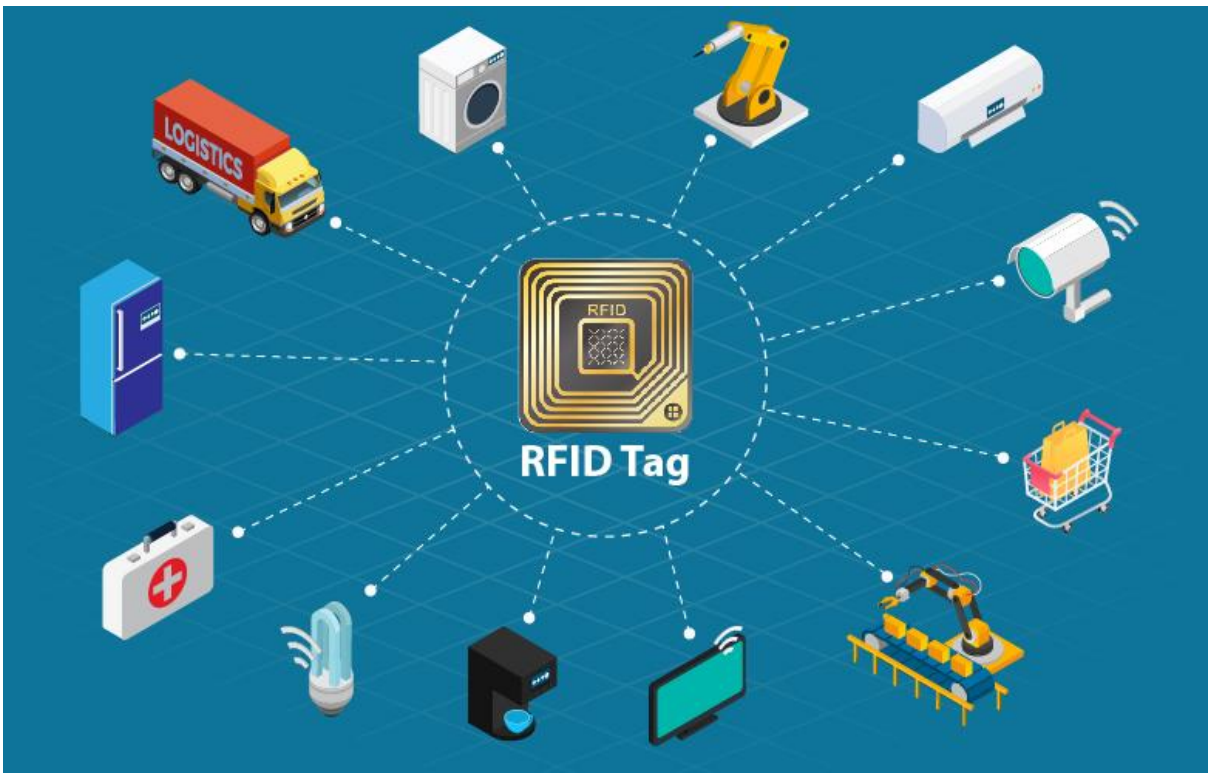
This Personal Vulnerability Investigation document summarizes the result of my work during my school weeks 5-10 of the Cyber Security Specialization I am following at Fontys UAS, which consists of research I have done investigating an object, product, existing systems or technologies, in this case I chose to do it on “smart cards”. The research done during this project is done entirely by me while following the DOT research framework, the appropriate strategies of this framework and their appropriate CMD methods. I spent approximately 25 hours on this document.

Glossary

PVI	Personal Vulnerability Investigation
DOT FRAMEWORK	Development Oriented Triangulation Framework
CMD METHODS	A pack of method/cards that support the DOT framework strategies
RFID	Radio Frequency Identification technology

Introduction

My choice of investigation for this Personal Vulnerability Investigation will be High Frequency RFID Technology. Although the main focus of my research will be the High Frequency range, its security and its vulnerabilities, a substantial part of my research will be focused on the RFID technology in general for the sake of building my understanding of the technology. My final goal for this project is to discover vulnerabilities and even exploit "smart cards" or "contactless cards" that use the High Frequency Range, which are commonly used for various applications such as access control, transportation systems, payment systems etc. During this research I will also shift my focus to other areas of RFID technology. Here's a short explanation of what RFID is:



Radio Frequency Identification Technology or RFID is a form of wireless communication that through the use of radio frequencies, that are in the electromagnetic spectrum, can uniquely identify an object, animal or person. The technology dates back to the 1940s, but it started getting more use after the 1980s, because the hardware of the technology was locked behind high costs. Nowadays the hardware is way cheaper and is used everywhere around the world. Here are some examples:

- *pet and livestock tracking*
- *inventory management*
- *asset tracking and equipment tracking*
- *inventory control*
- *cargo and supply chain logistics*
- *vehicle tracking*

- *customer service and loss control*
- *improved visibility and distribution in the supply chain*
- *access control in security situations*
- *shipping*
- *healthcare*
- *manufacturing*
- *retail sales*
- *tap-and-go credit card payments.*

The Research

The research done in this PVI will be done using the DOT (Development Oriented Triangulation) framework. I will be structuring my research by following all the levels of DOT framework (What, Why and How). The How of my research will follow at least 3 of the "How"s level research strategies (Library, Field, Lab, Showroom and Workshop). Any research strategies used to answer different questions will be accompanied by CMD methods corresponding by the same strategy.

To begin the project, I will create a main research question and surround it with sub-questions that I will need to answer during the making of this document to be able to answer the main research question. Since this is the introduction of the project and haven't answered any of them, there is no way of knowing what questions to ask, that is why the list of the questions will expand or change completely until the end of the project based on the new knowledge acquired. Below you can find the questions that will require research attitude:

- **What are the vulnerabilities and exploitable weaknesses of "Smart Cards", and how can they be exploited or mitigated?**
    - What are the key concepts in order to grasp the basics of RFID technology?
    - What is RFID technology?
    - How does RFID technology work, and what are the different types of RFID systems?
    - What are "smart cards" or "contactless cards"?
    - What are other types of RFID technologies?
    - What are the potential security threats and vulnerabilities of RFID technology?
    - How can attackers exploit these vulnerabilities to gain unauthorized access to systems or data?

What are the key concepts in order to grasp the basics of RFID technology?

To begin this research, I wanted to get into the absolute basics of how Radio Frequency Identification works. So to start answering this question I used the Literature Study method from the Library Strategy to list out all of the embedded technologies and physics principles that create RFID. Here's the list:

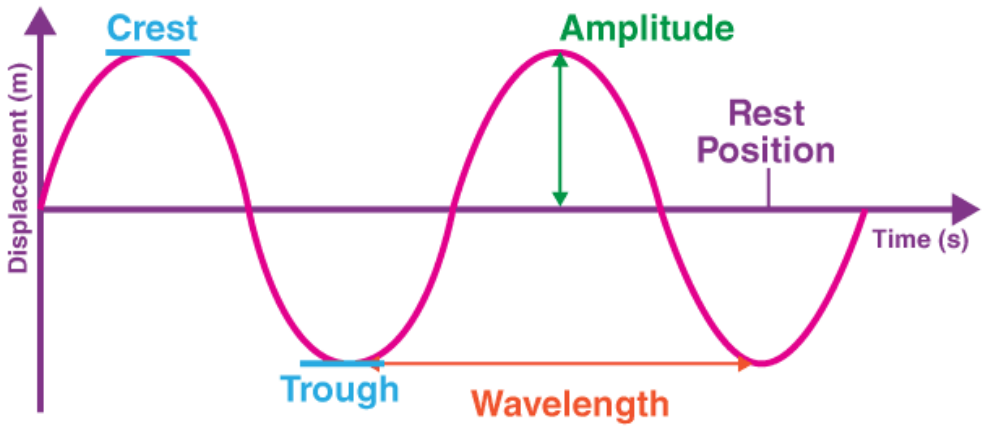
- Radio Waves and the Electro Magnetic Spectrum
- Transmitters and Receivers (Antennas)
- Modulation

Now I will try to go in depth into each one of these key concepts and explain it in the simplest of terms possible. For each one I used the Literature Study method from the Library Strategy to scour the internet and find information about the topics, here's what I found:

Radio Waves and the Electro Magnetic Spectrum

What is a wave?

Waves are a fundamental concept in physics and their behavior is used to proof many theories and understand many natural phenomena (i.e. behavior of light, transmission of sound, etc.). In the most basic of terms, waves are a way that energy travels from one point to another, through space or matter. Here are the key properties of a wave:



What the image misses to include is the Frequency, which is the number of waves that pass a given point per unit of time(seconds), measured in hertz(Hz), which represents one cycle per second. Also a wave is a balance between Amplitude and Wavelength, you can't change one without trading off with the other. This was a very simple explanation, but this is a very broad topic, and it will be impossible to cover everything. I missed Velocity and Phasing.

What types of Waves are there?

As we all know, there are two types of waves known to physicists. They are Mechanical and Electromagnetic waves.

Mechanical waves require a physical medium to "travel". They cannot go through vacuum and need to "resonate with something". Here are some types of mechanical waves:

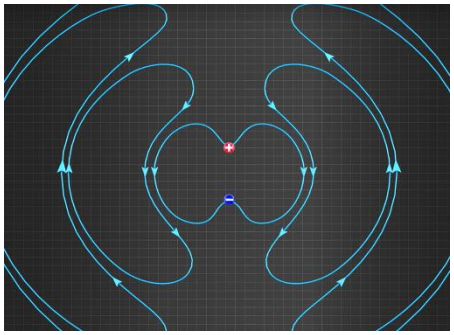
- Sound Waves: They travel through medium such as air. The frequency of sounds that humans hear is typically between 20 Hz and 20,000 Hz.
- Water Waves: Waves that travel through medium like water.
- Ultrasonic Waves: Used for medical imaging, they range between kHz(10^3) and MHz(10^6)
- Infrasonic Waves, Earthquakes (Seismic Waves)

Electromagnetic Waves are a type of are a type of wave that can travel through vacuum and consist of electric and magnetic fields. (Big Oversimplification) Examples of electromagnetic waves include:

- Extremely Low Frequency waves: 0 Hz to 3 Hz - difficult to generate and detect, not used in modern communication technology. DC – direct current
- Radio Waves: 3 Hz to 300 GHz - these are the waves RFID uses, broadcast radio and television signals, cellular communication and GPS.
- Microwaves: 300 MHz – 300 GHz – these waves overlap with radio waves, but they are more frequency ranges rather than defined categories. They include Wi-Fi, Bluetooth, microwave ovens and radars.
- Infrared Light: 300 GHz to 400 THz – used in heating and sensing applications.
- Visible Light: 400 THz (blue) to 700 THz (red) – the type of wave that we all know and love. Light!
- Ultraviolet Light: 700 THz to 30 PHz – Applications: sunburns, sterilization of equipment, synthetic dyes, can cause fluorescence in substances (used reflective paint on money), cancer.
- X-Rays: 30 PHz to 30 EHz – used to study properties of matter at the atomic/molecular scale. Also used for medical imaging
- Gamma Rays: 30 EHz to –EHz – Used in medical imaging, used for studying the properties of matter at a subatomic scale.

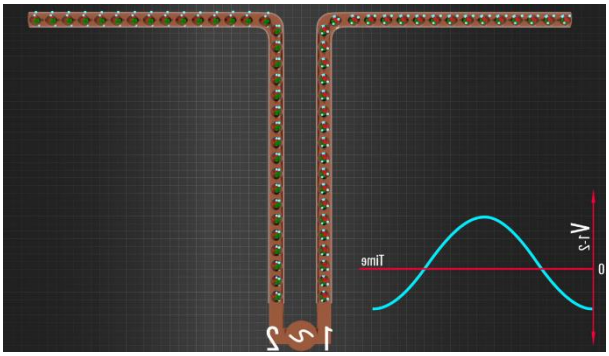
Transmitters and Receivers // Antennas

Antennas are widely used in the field of telecommunications. Antennas receive an electromagnetic wave and convert it to an electric signal OR receive an electric signal and radiate it as ana electromagnetic wave. I will try explaining the process with pictures:

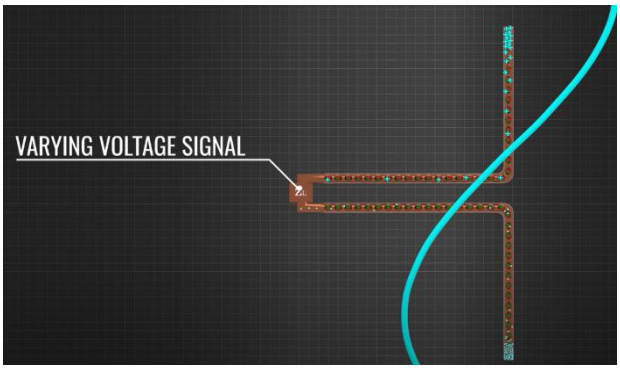


Imagine 2 charged particles in a magnetic field that are constantly changing their positions. Their velocity of “shifting” positions creates an electromagnetic wave. So, if we can change the velocity, we can send information. How do we do that?

Let's take a metal conductive rod and bend it in its centre. Now if we charge its middle, electrons will go into the direction of the voltage, and one side will become positively charged, and when voltage is stopped, the electrons will go back in the opposite direction. This way radio waves are created.



The opposite can also happen, if we apply a magnetic field (see the picture), the charges will shift and if we measure the voltage signal in the middle, we can convert it into output and that same antenna will work as a receiver.



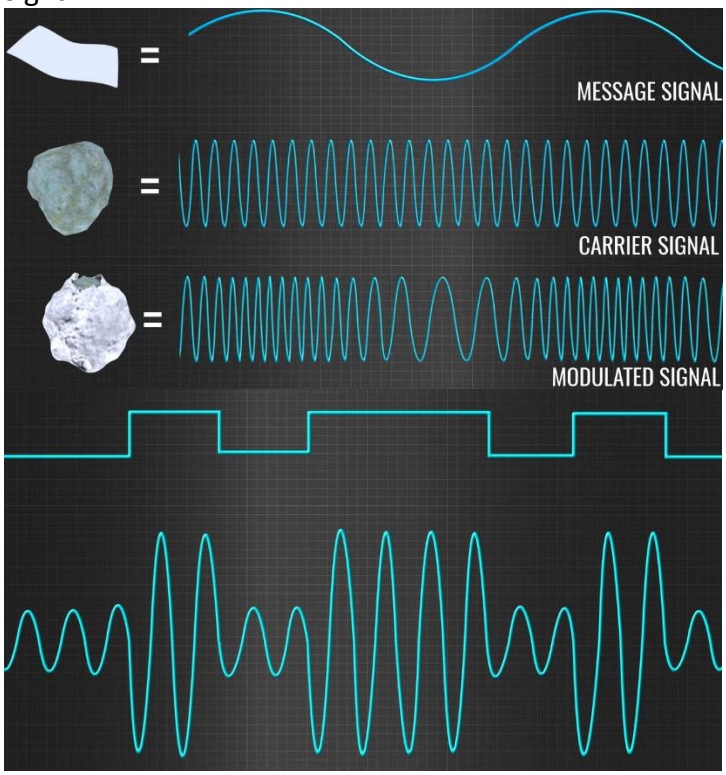
Sadly this was a big oversimplification of the whole process, but the topic is too broad and I can't afford to write too much about it.

Intresting Fact: Nikola Tesla believed that it was possible to broadcast electricity wirelessly through the air, using the process I explained above. Sadly you can't pass that much energy through radio waves to use it for stuff like lightbulbs/appliances, because that energy would have to go through us (people). BUT! We can use it to transmit information.

Transmitters and Receivers, they refer to devices that have antennas attached to them. Imagine that you have two arduino boards antennas, one has a button and the other a light. Now if we program the one with the button to generate an electromagnetic signal, encode it and then use its antenna to broadcast it, this will be called a transmitter. And if we program the other to listen for a signal and power the light when it hears it, that arduino board will be called a receiver.

In summary, the main difference between an antenna and a transmitter or receiver is that the antenna is a passive component, while the transmitter and receiver are active components. The antenna simply serves as a conduit for the electromagnetic signal, while the transmitter generates and encodes the signal, and the receiver detects and decodes it.

Modulation is a hard process to explain, but here's what it is in essence. It refers to the way we send information using radio waves. Instead of straight up broadcasting a signal, we can modulate it to be faster and more reliable. We can combine our message with a carrier signal.



But this is unreliable, and nowadays we use digital modulation.

In this digital modulation, high amplitudes mean 1 and low amplitudes mean 0. This produces high broadband, but if it is combined with a technique called quadrature amplitude modulation, we can send up to 6 bits of information in a single electromagnetic wave!

In essence, modulation is the process of embedding a carrier signal with information in order to transmit it efficiently over a communication channel. It is essential for modern communication allowing efficient and long distance transmission.

What is RFID Technology?

After answering the previous research question, it has been way easier to read and think about the technology. In this question I will focus on what RFID is and what it is used for without going in detail about how it works. So, to start I used the Literature Study method from the Library Strategy.

Radio Frequency Identification Technology or RFID is a form of wireless communication that through the use of radio frequencies, can uniquely identify an object, animal or person. The technology dates back to World War II, when it was used by the British military to identify friendly aircraft. The system that used it was called the Identification Friend or Fore (IFF), and it used to distinguish hostile aircrafts. The IFF system used a combination between radar and RFID. Later between the 1950s and 1960s it was used for field espionage.

However after the 1970s, the technology started getting used in commercial applications, its first commercial use was to tack shipping containers as they were shipped. In the 1980s, the technology started being used as access control, it was used to access building and other secure areas. RFID tags were embedded in keycards or badges, and readers were installed at the entrances to secure areas.

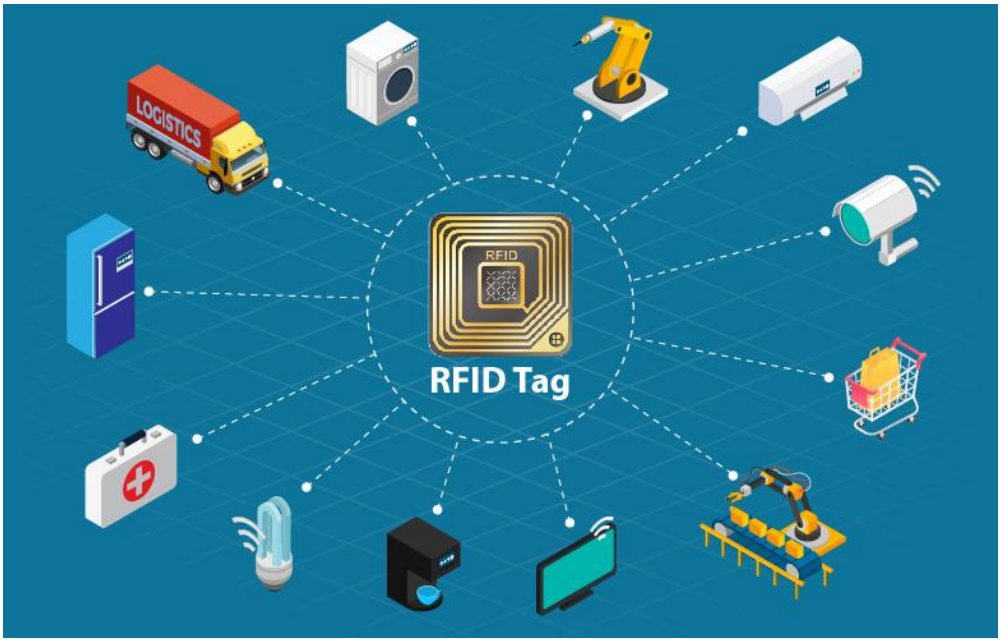
Since then the technology has become even cheaper, and it is used for wide range of applications. Here are some examples the technology is used nowadays:

- *pet and livestock tracking*
- *inventory management*
- *asset tracking and equipment tracking*
- *inventory control*
- *cargo and supply chain logistics*
- *vehicle tracking*
- *customer service and loss control*
- *improved visibility and distribution in the supply chain*
- *access control in security situations*

- *shipping*
- *healthcare*
- *manufacturing*
- *retail sales*
- *tap-and-go credit card payments.*

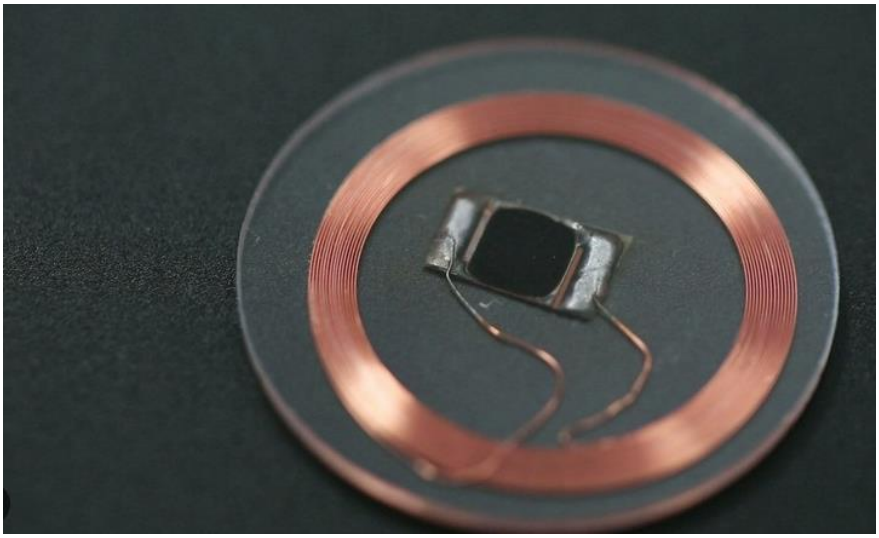
How does RFID technology work, and what are the differences between the types of RFID systems?

In this research question I will aim to explain how RFID works using the knowledge I acquired in my first research question and using the Literature Study method from the Library Strategy.



So there are two main things that RFID technology consists of. One is the Reader/Writer, what that means is that it is essentially a device that has two antennas and is programmed like a 2 in 1, a transmitter and receiver at the same time. The antennas are small and have a range of maximum 5 cm in most cases (depends on the case and the type of Rfid tag, but more on that later). These RFID scanners are designed to work with small electronic devices with a microchip and an antenna.

How do the tags work? There are two types of tags, one is called passive and the other active. The difference is that the passive doesn't have a power source and the active one does. First, the passive on consists of an antenna that captures the scanners signal, powers on the microchip inside, the microchip modulates it and returns it to the scanner.



The active one essentially does the same thing, but it doesn't need to be powered on by the scanner. That allows it to modulate signals from more far away. And even store more information in its microchip, but more on the types of use cases in the next research questions.

What other types of RFID systems are there, and where do "smart" and "contactless" cards stand?

In this question I will focus on learning all the different RFID types and their specification. Again, for this question I used the Literature Study method from the Library Strategy. Here is what I found:

These are all the types of RFID technologies:

- Low Frequency (LF) RFID: LF RFID operates at a frequency range of 125 kHz to 134 kHz. This type of RFID is often used for access control, animal identification, and object tracking. LF RFID has a short read range, typically around 10 centimetres, and is not well suited for applications that require longer read ranges or high data transfer rates.

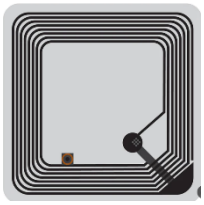
- High Frequency (HF) RFID: HF RFID operates at a frequency range of 13.56 MHz. This type of RFID is commonly used for contactless payment systems, smart cards, and asset tracking. HF RFID has a shorter read range than UHF RFID, typically up to 1 meter, but offers faster data transfer rates and more secure communication.
- Ultra-High Frequency (UHF) RFID: UHF RFID operates at a frequency range of 860 MHz to 960 MHz. This type of RFID is used for inventory management, supply chain management, and asset tracking. UHF RFID has a longer read range than LF and HF RFID, typically up to several meters, and can read multiple tags simultaneously.
- Microwave RFID: Microwave RFID operates at a frequency range of 2.45 GHz. This type of RFID is used for high-speed reading applications, such as toll collection and vehicle tracking. Microwave RFID has a longer read range than UHF RFID, typically up to 30 meters, but requires more power and can be affected by interference from other wireless devices.
- Near Field Communication (NFC): NFC operates at a frequency range of 13.56 MHz and is a type of HF RFID. It is commonly used for mobile payments, access control, and data transfer between devices. NFC has a very short read range, typically up to a few centimetres, but offers secure communication and fast data transfer rates.

All of these type's tags can be active of passive, except for the NFCs, because nfc is usually employed in devices and due to the way they work, they can't be powered on.

Here are some examples for each one of the types mentioned above:

- Low Frequency:
    1. Access Control
    2. Animal Identification
    3. Object Tracking

- High Frequency:
    1. Contactless Payment Systems
    2. Smart Cards
    3. Asset tracking



- Ultra-High Frequency:
    1. Inventory Management
    2. Supply chain management
    3. Asset Tracking

- Microwave:
    1. Toll Collection
    2. Vehicle Tracking
- NFC:
    1. Mobile payments
    2. Data transfer between devices

So, what I learned from this question is that smart cards which I am trying to find vulnerabilities for use the High Frequency range 13.56 MHz. In the following research question, I will focus on finding out the structure of the HF tags and how they work.

How are the High Frequency Cards used and are there any specifications to it?

For this research question I will go in depth of the High Frequency Rfid tags and scanners. For this research question I used the Literature Study method from the Library Strategy. Here is what I found:

High Frequency RFID uses the frequency range of 13.56 MHz. The scanner does not differ from the Low Frequency scanner. It is a board with two antennas, that is programmed to do some kind of logic and connected to other devices that allow it to do some kind of function.

It uses the amplitude shifting key, I explained it in a previous research question, it is when the amplitude of a wave is represented highs meaning ones and lows meaning zeroes. For an RFID system that is considered fast and accurate.

The types of HF RFID are two. We have:

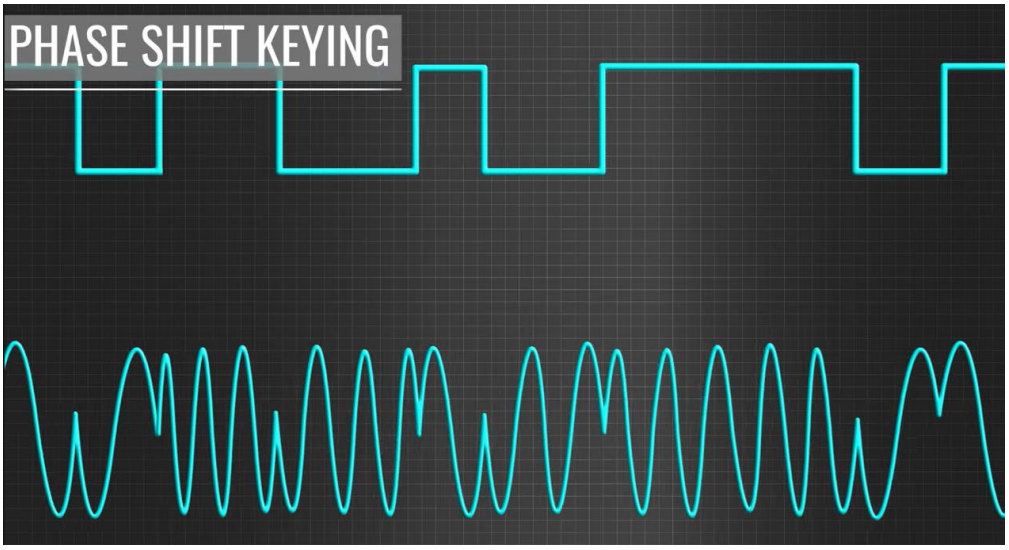
- ISO/IEC 14443: This standard is used for contactless smart cards and proximity cards, including MIFARE cards.
- ISO/IEC 15693: This standard is used for high-frequency RFID tags and readers operating at 13.56 MHz.

Most HF cards used around the world are MIFARE cards. MIFARE is a brand of RFID technology that is based on the ISO/IEC 14443 standard. MIFARE products are widely used for access control, ticketing, and other applications that require secure and fast transactions. Here are the types of products:

- MIFARE Classic: This is the original MIFARE product and is widely used for access control, public transportation, and other applications.
- MIFARE Ultralight: This is a low-cost MIFARE product that is commonly used for disposable tickets and other applications that require low memory.

- MIFARE DESFire: This is a high-security MIFARE product that is commonly used for access control, payment systems, and other applications that require secure transactions.
- MIFARE Plus: This is a newer version of MIFARE that offers improved security and is backward compatible with MIFARE Classic.
- MIFARE SAM (Secure Access Module): This is a separate security module that can be added to MIFARE systems to provide additional security features.

There are also subtypes of these ISO standards. They consist of Type A and Types B. The difference lies in the waves that are transmitted and modulated. Turns out Type A uses the amplitude method I talked about in the earlier research questions explaining the transmitting technology. And Type B use something called Phase shifting transmission. Essentially, they use the same frequency overall, but when they flip 1 to a 0, they rotate the wave by 180 degrees. That requires more expensive hardware and thankfully MIFARE only uses Type A. Here's a picture showing Phase shifting waves:



In this document I will be aiming at finding vulnerabilities in MIFARE Classic cards. In the next research question I will be answering how the MIFARE CLASSIC stores information and how it can be manipulated.

How do the MIFARE Classic tags store information and how can we manipulate it?

To answer this question, I used the Literature Study method from the Library Strategy to scour the internet for information and the Document Analysis method form the Field Strategy to read the documentation provided by MIFARE. Here is what I found:

How do the CLASSIC tags store information? I won't be focusing on the transmission of data, but on the data itself in this research question. The MIFARE CLASSIC has 2 variants, but each one of those variants can be read with the same type of scanner, some may cards may not work with specific scanners, but that is determined by the programming of the scanner, not by its hardware. Here are the specifications of each of the variants:

- MiFARE CLASSIC 1K – it has 1 kilobyte in total, it is spread across 16 sectors, each sector has 4 blocks, and the storage of one block is 16 bytes.
    - In essence 1 sector = 64 bytes and 16 sectors = 64 blocks = 1024 bytes = 1 kb
    - Asd
- MiFARE CLASSIC 4k – essentially the same as the 1k, but it has 40 sectors instead. Which means it can store 4 kilobytes of data. 160 blocks combined.

Here is an example of a CLASSIC 1K that has 3 sectors used, with dummy data in natural language I created:

Sector 1 - Access Control Information and Card UID:

- Block 0: Contains the manufacturer's code and the unique ID (UID) of the card.
- Block 1: Contains access control information for the sector, such as the read/write access permissions. Example: Access LV 1,2,3,4

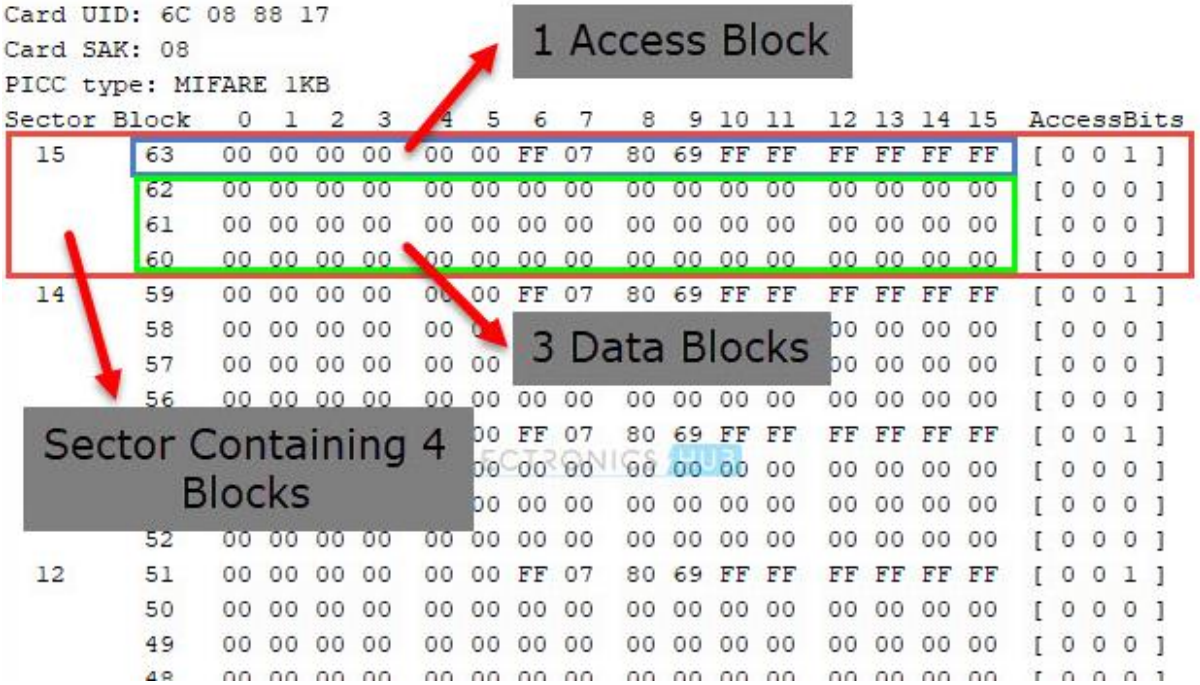
Sector 2 - Personal Information:

- Block 4: Contains the name of the cardholder.
- Block 5: Contains the address of the cardholder.
- Block 6: Contains the phone number of the cardholder.
- Block 7: Unused or reserved for future use.

Sector 3 - Financial Information:

- Block 8: Contains the cardholder's account number.
- Block 9: Contains the current balance in the account.
- Block 10: Unused or reserved for future use.
- Block 11: Unused or reserved for future use.

Now I will show you a real example of a card, containing information:



How can we manipulate the date inside? Changing the contents of a MiFARE CLASSIC tag requires a specialized RFID reader/writer device that is capable of reading and writing MiFARE CLASSIC tags. I actually took such a device from the Fontys ISSD. Here's how it looks:

The process of changing the data of the sector is pretty simple. Here's the basic process:

- Write to the block: Once you have successfully authenticated to the sector, you can then write new data to the block of your choice using the write command. The write command requires the block number and the data you want to write to the block.
- Verify the write: After writing to the block, it's important to verify that the data was written correctly. You can do this by reading the block back from the tag using the read command and comparing the data you wrote with the data you read.
- Repeat for other blocks: If you want to change the contents of multiple blocks, you can repeat steps 2 and 3 for each block you want to modify.

We can even change values inside the card. If for some reason the hex data corresponds to normalized text, and for example it says access control level 1 in the second block in the first sector, we can change it to 5 and save it.

What is the security of the MiFARE CLASSIC 1k?

To answer this question, I again used the Literature Study method from the Library Strategy to scour the internet for information and the Document Analysis method form the Field Strategy to read the documentation provided by MIFARE. Here is what I found:

Of course, it can't be that easy to change the contents of any card. MiFARE has implemented their own proprietary encryption algorithm that secures the communication between the card and the reader. To do that a key is stored on both the card and the reader. The key is 48-bit secret key.

On top of that algorithm have been placed additional measures, like access control list (meaning which data can be read or written to the card and, by whom) and data encryption used to encrypt sensitive data stored on the card, i.e. credit card number.

So, the steps to change the data on the card, I showed in the previous research question become like the following:

- Authenticate the sector: in order to read sectors in general, you have to have the secret key that is stored in the first block of each sector.
- Writing blocks: look at the steps in the previous research question.
- Locking the block, you changed: put a key of your choice in the first block of each sector you changed.

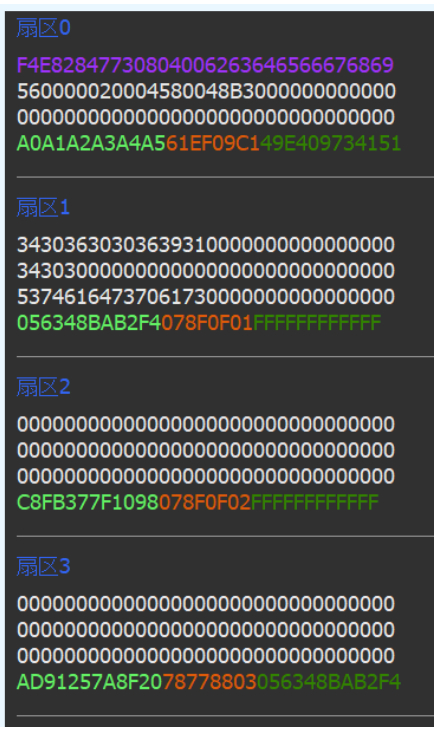
So, these are all defences MiFARE have deployed up until this day. Now in the next research question I will focus on showing exploiting these vulnerabilities.

How can attackers exploit these vulnerabilities to gain unauthorized access to systems or data?

To answer this question, I used the Document Analysis method form the Field Strategy to read the documentation provided by MIFARE and the Security Test method from the Lab Strategy. Here are the different exploitation variations I found:

Default Keys:

The easiest way to crack an mc1k card is by having the key. A solid percent of the cards have default keys. Here are the default keys: #1 FFFFFFFFFFFF / #2 A0A1A2A3A4A5 / #3 D3F7D3F7D3F7. Here's an example of a card I cracked:



This is the card municipality Eindhoven, gives out to residents to open the trash. It used the first default key. What is interesting is that the trash cans in Eindhoven could be opened with any High Frequency RFID or NFC card/tag. I don't know why.

Another story I have, me and a friend tried using the default keys for an arcade mc1k card back in Bulgaria. We tried it only once to check if it works. We dumped the card with 1 credit inside, used it to play a game, and then rewrote the dumped file again on the card. It worked. We told the arcades personnel, but they didn't turn any attention to us because we were kids.

Searching the web for exposed Keys:

Before heading into cracking the cards, you can try searching for the keys online. Here's a list I found:

https://github.com/ikarus23/MifareClassicTool/blob/master/Mifare%20Classic%20Tool/app/src/main/assets/key-files/extended-std.keys.
This list contains the most common keys used in general and then some for specific facilities. Here are some interesting ones I found:

```
531  # Russian Troika card
532  08B386463229
```

These are 60 keys for the contactless reusable cards designed to pay for public transport in Moscow.

Another 20 keys I found were for the Rotterdam UAS campus card.

```
1462  # Rotterdam University of applied sciences campus card
1463  BB7923232725
1464  A95BD5BB4FC5
```

In the file there were over 1450 keys for different facilities. There were keys for French swimming pools, Saint-Petersburg transport system, Armenian Tram transport, Moscow public toilets etc. Sadly, there is no way for me to find out if these keys work or they are already deprived.

Brute-Forcing:

Brute Forcing mc1k card has two sides. The key is 48-bits, that makes 281,474,976,710,656 possible key combinations. If you were to brute force the tag straight up using 100 CPUS, each one testing different keys each microsecond, it would take you 160 years.

A practical approach of Brute Forcing would be using side-channel attack, where you capture the power consumption and electromagnetic waves to analyse and extract the encryption key. I do not completely understand how that one works, but it requires specialized equipment and deep expertise of the card's internal workings.

Physical Approach:

This one is obvious and doesn't require any knowledge of the technology. You can destroy the microchip inside the tag very easily. It is very small and even a single electrostatic touch would fry it. This is hard, because the chip usually is encapsulated, but if you find a way to pierce it with a needle where the chip or the antenna is and insert a small amount of voltage, you can take away someone's access without him even knowing. Another interesting way in theory would be to send a high energy electromagnetic wave. This is kind of hard, because the only waves that can do that are in the upper microwave spectrum, so you would literally have to put it in the microwave for 2 seconds.

Conclusion

Writing about this topic was enjoyable. During the process, I delved into many stories about the use of RFID and its history. I also had the opportunity to enhance my understanding of communication technology by reading extensively on the physics of waves, antennas, and creating radio-waves using oscillating charge and voltage. Although I had studied these topics in high school, this time around, everything actually clicked for me.

In addition, I had the chance to experiment with different cracking methods of MiFARE CLASSIC TAGS. Some of these methods proved successful, while others didn't. I'm excited to share the progress and research I've made during the writing of this PVI at the upcoming presentation. I plan to demonstrate the various tools and strategies that one can use to crack these cards.

Throughout the research process, I utilized the DOT Framework research strategies, employing the Library, Field and Lab strategies to answer different questions. I believe that this approach has enabled me to successfully conduct thorough research on the topic.