TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Giorgi Okroshidze IVSB184054

# FLAWS IN THE IMPLEMENTATION OF RFID IDENTIFICATION AT TALTECH AND IMPROVEMENT SUGGESTIONS

Bachelor's thesis

Supervisor: Aleksei Talisainen
MSc

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Giorgi Okroshidze IVSB184054

# PUUDUSED RFID IDENTIFITSEERIMISE RAKENDAMISEL TALTECHIS JA PARANDUSETTEPANEKUD

Bakalaureusetöö

Juhendaja: Aleksei Talisainen
MSc

Tallinn 2021

# Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Giorgi Okroshidze

02.04.2021

# Abstract

The main goal of this thesis is researching and suggesting improvements to the current RFID access control system implementation at Tallinn University of Technology.

Penetration testing was performed on the various access points using cheap, simple, and easily obtainable devices. The devices selected were the Arduino UNO, an RC522 high-frequency RFID reader/writer module and a UID changeable Gen1 “Magic card and tag”.

The outcome of this testing showed that the system was vulnerable to the cloning attack and could be tricked by fake UID changeable devices which had a valid UIDs written on them. It also displayed that only the card UID is used for granting access, which is transmitted in the open and is easy to obtain.

Following this testing, a couple of improvement options were put forth and discussed with SOYAL, the company whose access devices are used at the campus. The solution which balanced adequate security and expenses was chosen. The perfect option for this turned out to be the SOR encryption offered by SOYAL.

This thesis is written in English and is 31 pages long, including 5 chapters and 9 figures.

# Annotatsioon

# Puudused RFID identifitseerimise rakendamisel TalTechis ja parandusettepanekud

Käesoleva töö eesmärgiks on uurida Tallinna Tehnikaülikoolis praegu kasutatava RFID-ligipääsusüsteemi ning pakkuda sellele välja täiustusi. Töö käigus kasutati erinevate ligipääsupunktide läbistustestimist lihtsate, odavate ja kergesti hangitavate seadmete abil. Valitud seadmeteks olid Arduino UNO, kõrgsageduslik RC522 RFID lugemis-kirjutamismoodul ja muudetava identifikaatoriga Geni "Magic card and tag".

Testimistulemused näitasid, et süsteem on kloonimisründe osas haavatav ja seda saab eksitada võltsitud identifitseerimisseadmega, kuhu on sisestatud kehtivad identifikaatorid. Samuti selgus, et ligipääs antakse üksnes kaardi UID abil, mida edastatakse varjamata kujul ja mille kättesaamine on kerge.

Testimise järel pakuti välja mõned täiustused ja teatati need ka SOYALi firmale, kelle seadmeid ülikool kasutab. Valiti lahendus, mille korral maksumus ja turvalisus olid tasakaalus. Ideaalseks lahenduseks osutus SOYALi pakutav SOR krüpteering.

Käesolev töö on kirjutatud inglise keeles ning sisaldab teksti 31 leheküljel, 5 peatükki ja 9 joonist.

# List of abbreviations and terms

| | |
|---|---|
| RFID | Radio-Frequency Identification |
| ID | Identifier |
| UID | Unique Identifier |
| LF | Low Frequency |
| HF | High Frequency |
| ISO | International Organization for Standardization |
| NFC | Near-field Communication |
| UHF | Ultra-High Frequency |
| DoS | Denial of Service |
| NIST | National Institute of Standards and Technology |
| OSSTMM | The Open Source Security Testing Methodology Manual |
| IDE | Integrated Development Environment |
| USB | Universal Serial Bus |
| Gen1 | Generation 1 |
| Gen2 | Generation 2 |
| CUID | Changeable UID Generation 2 card |
| FUID | Changeable UID Write-Once Generation 2 card |
| NUID | Non-Unique Identifier |
| PICC | Proximity Integrated Circuit Card |
| PUF | Physical Unclonable Function |
| PIN | Personal Identification Number |
| DES | Data Encryption Standard |
| AES | Advanced Encryption Standard |
| KB | Kilobyte |
| AMK | Application Master Key |
| CMK | Card Master Key |
| SOR | SOYAL Open system Rules |

# Table of contents

1 Introduction ........................................ 11
2 Background research ........................................ 12
2.1 About physical access control systems ........................................ 12
2.2 About RFID technologies ........................................ 12
2.2.1 Active and passive RFID systems ........................................ 13
2.2.2 Different frequencies used for passive RFID ........................................ 14
2.3 Common security vulnerabilities in RFID systems ........................................ 15
2.3.1 Spoofing / cloning attack ........................................ 15
2.3.2 Relay attack ........................................ 16
2.3.3 Reverse engineering ........................................ 16
2.3.4 Eavesdropping ........................................ 16
2.3.5 Replay attack ........................................ 16
2.3.6 Power analysis ........................................ 16
2.3.7 Denial of service ........................................ 17
2.3.8 Man-in-the-middle attack ........................................ 17
2.3.9 Security vulnerability summary ........................................ 17
3 Penetration testing on the campus RFID system ........................................ 18
3.1 Planning ........................................ 19
3.2 Reconnaissance ........................................ 20
3.2.1 Theory about the type of system in use ........................................ 20
3.2.2 Examining the readers ........................................ 20
3.2.3 Examining the tags and cards ........................................ 20
3.3 Tool selection & setup ........................................ 22
3.3.1 The choice for the reader/writer device ........................................ 22
3.3.2 The choice for the UID rewritable RFID card ........................................ 23
3.3.3 Hardware setup ........................................ 23
3.3.4 Software setup ........................................ 24
3.3.5 Alternate options ........................................ 24
3.4 Gaining access ........................................ 25

3.4.1 Reading card and tag UIDs ........................................................ 26
3.4.2 Writing card and tag UIDs to fake devices .................................... 27
3.4.3 Testing the fake card and tag ........................................................ 28
3.5 Report ........................................................................................ 29
3.5.1 The problem with the Mifare Classic 1K devices ............................ 29
3.5.2 The problem with the readers in place ........................................... 30
3.5.3 The danger revealed by this testing ............................................... 30
4 Picking a solution for the access control system at the campus .................... 32
4.1 Various options ............................................................................. 32
4.1.1 Correctly configuring the current system ....................................... 32
4.1.2 Adding a simple clone elimination feature ..................................... 34
4.1.3 Implementing a newer system offering proper authentication & encryption (DESFire) ........................................................................... 35
4.2 Discussion with the company SOYAL ................................................ 37
4.2.1 SOR Mifare encryption ................................................................. 38
4.2.2 SOYAL DESFire ........................................................................... 38
4.2.3 Purchasing a programming kit ....................................................... 39
4.3 The proposed solution ..................................................................... 39
5 Summary ........................................................................................... 41
References ........................................................................................... 42
Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis ..................................................................................................... 47

# List of figures

Figure 1. MIFARE Classic Tool access tag read output: (a) part 1, (b) part 2, (c) part 3 ........................................................................................................................ 21

Figure 2. First serial monitor output after loading the “ReadNUID” sketch.................. 26

Figure 3. Serial monitor access tag read output............................................................. 26

Figure 4. Serial monitor student card read error output ................................................ 26

Figure 5. ReadNUID code responsible for student card read error ................................ 27

Figure 6. Serial monitor student card read output ......................................................... 27

Figure 7. ChangeUID code responsible for storing the UID value ................................ 27

Figure 8. First serial monitor output after loading the “ChangeUID” sketch................. 28

Figure 9. ChangeUID access tag UID rewritten successfully output ............................. 28

# List of tables

**No table of figures entries found.**

# 1 Introduction

As the number of employees have grown in businesses and organizations, different methods have been implemented over the years for controlling personnel access to various company assets. Nowadays, one of the most widely used access control systems by most companies is one based on wireless RFID (Radio Frequency Identification) technology. The main reason for this technology being so widely adapted is the fact that it is convenient and cheap to implement. However, because of these characteristics, many organizations have forgotten about the various security vulnerabilities that might accompany such a system if it is not implemented correctly.

This thesis states that there is a problem with the current implementation of the RFID access control system at the university campus. The system in place is not very secure and can be bypassed by a common cloning attack using various inexpensive devices which require little expertise to operate.

Penetration testing will be performed on the current implementation using tools that fit the criteria of being cheap and easy to operate. The testing will try to carry out the cloning attack mentioned and trick the system into granting access to a fake card. Once the testing is done, the findings will be included in the provided report. Afterwards, research will be done on ways to improve the system.

The aim of this thesis is to compare the different options that promise to make the current RFID access control system less likely to be bypassed by the attack mentioned and to pick a solution that will adequately balance security and implementation cost.

The contribution of this work is that the proposed solution can be used by the university to significantly improve the security of the current RFID access control system. Furthermore, this solution can be used by any organization that is facing a similar issue.

# 2 Background research

## 2.1 About physical access control systems

First of all, an access control system is a system used to identify a person and either grant or restrict access to resources accordingly [1]. Although these systems are also used in many software applications, this thesis is dealing with physical access control which is used to restrict entry to a physical space within a business or an organization [2]. Furthermore, this system can be used to manage entrance lock/unlock schedules and to add or remove access restrictions for specific events.

Basic physical access control systems are typically set up in the following way [3]:

They are usually connected to a backend server which stores authorized user IDs (Identifiers) and permissions. These permissions can be granted, modified, or removed entirely. Access is given according to the ID a user provides, and the permissions which are tied to that ID.

A reader is used to get the unique credential needed to authenticate the user. There are various types of readers that have different user identification methods. Some use biometrics, like fingerprints, iris scanning, facial recognition, etc., others use pass phrases, magnetic stripe cards and so on, but the one implemented at the university and, in turn, the topic of this thesis is based on RFID technology which uses radio waves to transmit the user’s ID.

The information from the reader is transferred to a controller which compares it to the credentials stored in the server and sends a signal to accordingly unlock the door or keep it locked.

## 2.2 About RFID technologies

Radio Frequency Identification is a wireless technology that uses access cards or tags which transfer their UID (Unique Identifier) to a reader via the electromagnetic field they generate [4]. Both these cards and tags are equipped with an embedded coil, which acts as the antenna, and a chip, which holds the user's data. Communication between the reader and the media takes place in the following way:

- A signal is constantly being transmitted from the reader that asks for the card's UID.
- When a card is in close proximity to the reader, it receives this signal request with its antenna and promptly transmits its UID which is stored on the aforementioned chip.
- As soon as the transmitted UID reaches the reader, it is sent to the backend-server for authentication.

This is the basic principle behind this technology. However, RFID has been around for a long time, and there have been many different implementations of this technology ranging from cheap ones with simple features all the way up to very expensive devices used for long range tracking and advanced security. The specific functionality of an RFID system depends on two factors: the power source of the access media and the frequency used for communication.

### 2.2.1 Active and passive RFID systems

Based on their power source, there are two types of RFID technologies: active and passive [5].

Active tags have an internal power source, usually an embedded battery. They have considerably long read ranges. They can be used as beacons, for tracking applications, or as transponders, for secure access control systems and so on. However, they are very expensive and only last 3-5 years, at which point they need to be replaced. Active tags are also very bulky and cannot be embedded.

Passive tags, on the other hand, have no internal power source and use the electromagnetic energy transmitted from the reader. This means they can only operate when they are in the vicinity of an RFID reader and have much shorter read ranges compared to active tags. However, these kinds of tags are thinner and smaller in size, are much cheaper to manufacture, and, if they are not damaged, can last a lifetime. Passive tags are used in many applications such as access control, file tracking, smart labelling and so on.

Since passive RFID systems can be deployed in portable, low-cost devices, they are used by many organizations and are the most widespread form of RFID technology. The access control system used at the university also uses passive RFID Technology. As a result, this thesis will mostly focus on these kinds of systems from this point on.

### 2.2.2 Different frequencies used for passive RFID

Both the reader and the card have to be using the same frequency to be able to communicate with each other. The common frequency spectrums used by the access media for passive RFID systems are the following [6]:

- LF (Low Frequency) – In the low frequency spectrum, only 125 kHz and 134.2 kHz are used for RFID applications. Tags using this frequency have a short read range, have the slowest data transfer rate compared to other RFID frequencies, and store the smallest amount of data. Furthermore, they are usually read-only and, because of their limited capabilities, are the least secure. The tags operating at this frequency are called proximity tags.

- HF (High Frequency) – In this spectrum, only the 13.56 MHz is used. Cards using this frequency are able to store more information compared to LF ones and are able to transfer information at much higher speeds. Furthermore, they have a thinner coil compared to low frequency tags and are much easier and cheaper to manufacture. These kinds of cards also have writable sectors that can store data other than the card UID.  On top of that, there are several standards in place for such cards, like ISO (International Organization for Standardization) 14443 for MIFARE technology which includes reader authentication and encryption for better security [7]. NFC (Near-field Communication) also falls under the HF RFID technology, which is used by contactless payment cards, bank cards, mobile phones and so on. Because of their advanced capabilities, high-frequency cards are usually referred to as smart cards. However, it is important to note that not all of the cards using this spectrum are equipped with many of the advanced features.

- UHF (Ultra-High Frequency) – Passive devices using this frequency usually operate between 860 to 960 MHz. They have a very fast data transfer speed and a very long read range – usually around 6 meters. These passive UHF tags are usually used in simple tracking application and are very inexpensive. However, UHF readers themselves are much pricier compared to the ones in lower frequency ranges. This technology is newer compared to the previous two and is rarely used in access control applications.

Out of these frequencies, the HF sector offers the most balanced options when it comes to functionality and price. As a result, and because of the ISO standards and MIFARE technologies behind it, this sector is one of the most commonly used frequencies for access control. As was revealed in the testing phase (see Section 3.2), the access control system currently implemented at the university campus also operates at this frequency.

## 2.3 Common security vulnerabilities in RFID systems

Since no information system is fully secure, RFID based systems also have their fair share of vulnerabilities and are susceptible to various attacks [7]. This section describes some of the more common attacks that can be used to get a hold of unauthorized data or to halt the functionality of a system. Many of these attacks are sophisticated and require specialized tools and skills to perform. However, some are very simple and can be pulled off using easily obtainable, cheap devices with little technical expertise.

### 2.3.1 Spoofing / cloning attack

A spoofing attack occurs when an unauthorized tag poses as a valid tag and gets past security. A cloning attack is a form of spoofing where an individual with malicious intent reads the contents of an authorized tag and creates a copy of the data on a blank tag. Once this process is complete, this newly created device will act as the device whose data was copied. They will be indistinguishable to the reader and the clone can be used to go through secure entrance points. Furthermore, the same data can be copied onto multiple tags, which means unauthorized access can be distributed to many people.

This is the most common attack associated with RFID technology. Moreover, it is a very simple attack to perform on some RFID systems that do not use secure encryption or authentication protocols. This kind of cloning attack can be performed using very cheap devices and little technical knowledge. Because of this, this is one of the most dangerous attacks in the context of RFID systems.

### 2.3.2 Relay attack

The relay attack is another popular RFID attack. Using this method, an attacker uses a device to pick up a signal from an RFID card/tag and relays that signal to a legitimate reader that this tag is linked with. This tricks the reader which believes that the tag is legitimate. The main concern for the attacker is for the original reader and tag to be within the relay distance limit, which is usually not very long. This attack also needs a specialized device and expertise to be performed correctly.

### 2.3.3 Reverse engineering

A reverse engineering attack consists of taking a device apart in order to get to the contents inside and see how it operates. A person with adequate skills can gain access to a card/tag chip and read its memory contents to retrieve the data written on it.

### 2.3.4 Eavesdropping

An eavesdropping attack is very straightforward, it occurs when an attacker uses a device to eavesdrop on the communication between a tag and a reader. During this process, the attacker can intercept the data being transmitted. It is important to note that readers are more susceptible to these kinds of attacks because their transmission power is stronger, while passive cards emit much weaker signals.

### 2.3.5 Replay attack

A replay attack is basically the same as an eavesdropping attack [8]. However, the main difference is that once a valid signal is intercepted, it is recorded. Afterwards, the recorded response can be replayed back to the reader to gain access.

### 2.3.6 Power analysis

A power analysis attack is also similar to an eavesdropping attack, but instead of the whole communication between a tag and a reader, only the power output is monitored. This method does not need overly advanced devices to read the power output. However, translating the power consumption into useable data correctly is very difficult and requires a skilled attacker.

### 2.3.7 Denial of service

The purpose of a DoS (Denial of Service) attack is to render the RFID system unusable. This can be accomplished by various methods. Firstly, a jamming device can be used which will constantly broadcast radio signals matching the frequency of the system. If such a device is placed in close proximity to a reader, the generated noise will interfere with the communication between the reader and a tag. As a result, the system will not be able to function. This is a relatively simple attack, but it needs a device with a strong enough antenna to be practical. Another DoS method is to disable the tags by erasing their contents. However, for this to work the tags need to be fully rewritable, meaning the part that holds the UID (sector 0 block 0) should also be changeable, which is not usually the case.

### 2.3.8 Man-in-the-middle attack

A man in the middle attack is performed with a device that can interrupt the communication between reader and tag and manipulate the information being transferred [8]. This means that the information can be viewed before it reaches its destination and altered information can be forwarded along. This attack also needs a special device and is difficult to execute.

### 2.3.9 Security vulnerability summary

It is clear that there are many different ways for an attacker to exploit the RFID system. However, most of these attacks are very difficult to execute and need skilled attackers with specialized devices to be performed correctly. The most dangerous part, on the other hand, is the fact that the cloning attack, the most common one out of the mentioned, can be executed easily using cheap devices and very little technical expertise if the implemented RFID system is outdated or poorly configured. There are even guides online that demonstrate how this attack can be performed. This information is basically common knowledge at this point, but even so, most of the cheap RFID systems used by businesses and organization are not protected against this sort of attack. For these reasons, the penetration testing section of this thesis (see Section 3) will be focusing on this very attack.

# 3 Penetration testing on the campus RFID system

Penetration testing, also called pen testing or ethical hacking, is the act of performing authorized cyberattacks on a computer system in order to test the security of a specific implementation and report the existing vulnerabilities [7].

Overall, there are different standards, guidelines, and frameworks for this kind of information security testing and ethical hacking, like the NIST (National Institute of Standards and Technology) Special Publication 800 Series [9], OSSTMM (The Open Source Security Testing Methodology Manual) [10], and others. They provide a basic outline on how this sort of testing should be approached.

The type of ethical hacking performed in this section specifically is called physical penetration testing, because it calls for a person to physically walk into a building and test the security controls in place.

For physical pen testing, one can also look towards the various companies that offer it as a service. The approaches of such companies differ slightly depending on the system that is being tested but are usually based on the aforementioned NIST Special Publication 800 Series and OSSTMM at the least [11].

This thesis will also be taking the NIST standard for penetration testing as the basis of this section. The NIST standard for penetration testing is divided into the following four phases [12]:

- Planning - Outlining the specifics of the test like expectations, goals, legal implications, and so on.

- Discovery - Gathering information and scanning systems using different tools and methods.

- Attack - Gaining access to a targeted resource by exploiting vulnerabilities like misconfiguration, system flaws, etc.

- Reporting - Providing a comprehensive analysis of the findings, like the exploited vulnerabilities, risks, and so on.

In the case of this thesis, the specific steps followed during physical penetration testing are outlined in the following subsections:

- Planning - Similar to the NIST "Planning" phase.
- Reconnaissance - Similar to the NIST "Discovery" phase.
- Tool selection & setup - This part will cover the process of choosing and configuring the devices that will be used for breaching the system. It was added because this thesis has specific requirements about the devices that can be used for testing.
- Gaining Access - Similar to the NIST "Attack" phase.
- Report - Similar to the NIST "Reporting" phase.

This segment contains the description of planning the testing, gaining information about the system in place at the campus, choosing appropriate tools for exploiting the system, and actually getting past access control and obtaining unauthorized access, along with the accompanying report of the findings.

## 3.1 Planning

The goal of this testing is to carry out the cloning attack described above with inexpensive, readily available, and easy to use devices in order to create duplicate cards and bypass the RFID security. These kinds of devices are chosen to demonstrate how easily the system can be tricked by an average person.

All the necessary legalities were followed, and testing permission was granted by the TalTech security division. In accordance, the campus building chosen for this testing was the Akadeemia 5 dormitory.

Additionally, since student cards are used for access at university study buildings, instead of dorm access tags/cards, Akadeemia 5 dormitory access was granted on the author's student card which was used for testing the duplication of this type of device as well.

## 3.2 Reconnaissance

The purpose of this section is to collect enough information about the current RFID implementation to be able to properly select tools for exploiting the vulnerabilities in the system [13].

### 3.2.1 Theory about the type of system in use

Firstly, it is important to understand what type of RFID system is in place. Based on the background research, some educated guesses can be made: The system in place is most likely using a passive RFID technology operating at either low or high frequency. This is the most logical, since these are the most widespread forms of radio frequency identification which are used for access control. Additionally, since HF systems are more commonplace and LF ones are considered outdated by today's standards, the most rational choice is that a high frequency system is implemented.

### 3.2.2 Examining the readers

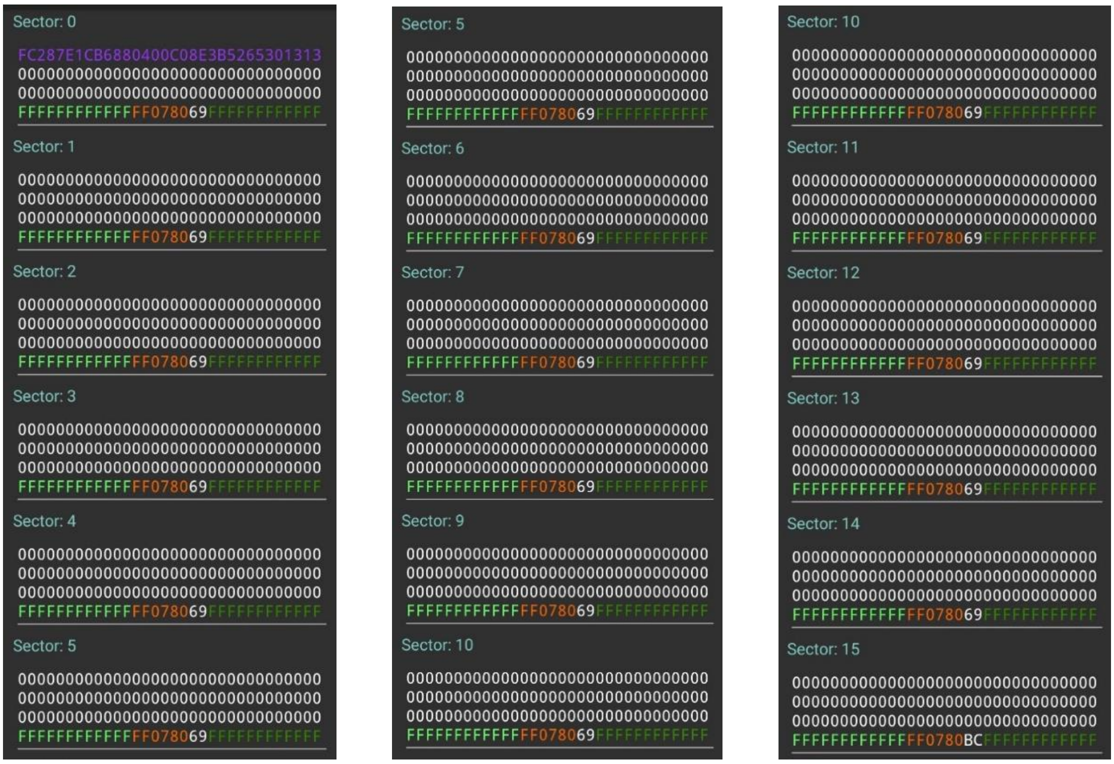
Taking a closer look at the readers in the Akadeemia tee 5 dormitory, branding can be made out on some of them with the text resembling "Soyal" and "Mifare". (This "Soyal" branding can also be read on the dormitory access tag.) This helps secure the outlined theory, since MIFARE systems are known to be using 13.56 MHz frequencies for communication [7]. Moreover, looking through the product selection of this SOYAL company, which offers various access controllers, proximity readers, and so on, the theory is further solidified since they do indeed provide HF readers which look identical to the models that are in the building [14]. After all this, it can be concluded that a high frequency system must be in place.

### 3.2.3 Examining the tags and cards

Upon examining the media devices used for accessing various buildings on the campus, it is made clear that RFID tags or cards are used for entry into dormitories, and student cards, doubling as bank cards, are used for entry into study buildings like IT College. As outlined in the research background (see Section 2), bank cards use NFC for communication, and since NFC falls under HF RFID technology, it can be deduced that the readers must at least allow high frequency operations.

The fact that the HF RFID technology is used by the readers was further verified by using a smartphone equipped with NFC. Almost all smartphones made in the past 8 years are capable. There are many free applications that can read HF RFID tags. There is even an official MIFARE application on android for this very purpose [15], [16]. The "MIFARE Classic Tool" application was used for reading the access tag. The dormitory tag was easily read by the smartphone, which confirmed the outlined theory that HF RFID technology was indeed being used.

The full output of the "MIFARE Classic Tool" application after reading the access tag is presented in figure 1.



```
Sector: 0
FC287E1CB6880400C08E3B5265301313
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 1
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 2
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 3
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 4
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 5
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
```

(a)

```
Sector: 5
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 6
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 7
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 8
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 9
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 10
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
```

(b)

```
Sector: 10
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 11
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 12
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 13
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 14
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF078069FFFFFFFFFFFF
Sector: 15
00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
FFFFFFFFFFFFFF0780BCFFFFFFFFFFFF
```

(c)

Figure 1. MIFARE Classic Tool access tag read output: (a) part 1, (b) part 2, (c) part 3

This proved that the UID of the access tag can be read by any other HF reader. Further information this revealed is that the only data written on the tag is in the first line, which is the manufacturer block of the device and contains the UID itself, along with the manufacturer information. All the other sectors have only 0s written in them. Moreover, since the application successfully read the tag, it indicates that the access tag is of the Mifare Classic 1K type [17]. This specific Mifare technology is older compared to the others, has many flaws, and openly transmits card UIDs (see Section 3.5.1). All in all, only copying the UID of the devices should be enough to bypass the entry system security at the campus.

## 3.3 Tool selection & setup

As mentioned in the previous sections, the main point of this thesis was to bypass the RFID access control security using inexpensive, easily obtainable tools which require little to no technical expertise. The equipment needs to be in the lines of:

- A device operating in the high frequency range - this will act as a reader and a writer. It will be able to read data from genuine access cards and transfer them to clone cards.

- A UID rewritable RFID card - this will be used to trick a valid reader and get past an entry point. The UID of an original card will be written onto this dummy card.

This section is dealing with choosing the appropriate devices and using information available to everyone online to set them up. The setup process will touch on both the hardware and software sides separately. Additionally, this section also discusses alternate device options.

### 3.3.1 The choice for the reader/writer device

For reading and writing to an RFID card, two separate devices were chosen: an Arduino UNO and an RC522 RFID reader/writer module. These two devices have often been used together for RFID vulnerability testing [7], [18]. They are both very inexpensive, are easy to obtain from websites such as Amazon, eBay, and AliExpress, and have accessible documentations.

The Arduino UNO is an open-source microcontroller board built around the ATmega328P microchip [19]. It can easily be connected to a computer and configured using the Arduino IDE (Integrated Development Environment) [20]. There are many libraries available for Arduinos, along with various sketches, or programs, which can be uploaded to the board simply via USB (Universal Serial Bus) from a computer.

The RC522 reader/writer is the most inexpensive RFID module that can be found online [21]. It is a high frequency device based on the MFRC522 RFID integrated circuit reader from NXP which is perfect for this testing. Furthermore, it can easily be hooked up with the Arduino UNO mentioned above and has dedicated Arduino libraries available on GitHub.

The original Arduino UNO can be picked up for around 20-30 USD. However, there are many clones available online which cost closer to 5 dollars. The RC522 module can be picked up for less than 2 dollars.

### 3.3.2 The choice for the UID rewritable RFID card

Most genuine high frequency RFID cards, like the ones from the MIFARE Classic family, cannot be used for cloning purposes. Although they have rewritable sectors, the UIDs on these cards, which reside on sector 0 block 0 and contain the unique ID and manufacturer number of the card, are not changeable.

For changing the UID, one has to turn to RFID “Magic cards” which are manufactured by various Chinese companies [22]. These cards use a chipset that is compatible with normal Mifare RFID systems. Additionally, “Magic card” chipsets do not have the restriction of the original cards, meaning that the sector 0 block 0 can be rewritten, effectively changing the card’s UID. There are different types of “Magic cards” but most of them are also usually obtainable through popular websites like eBay, Amazon and AliExpress, and are very cheap, costing as low as a dollar for a couple of pieces.

The “Magic cards” used for this testing were generic UID Gen1 (Generation 1) tags bought from eBay for 1.75 USD [23]. These tags use a known backdoor command (Unlock code: 0x43 0x40) for rewriting the UID. Because they use the backdoor command, the UID cannot be rewritten by smartphone readers, but can be rewritten by the RC522 module. To keep with the existing formfactor, a “Magic tag” was chosen for replacing the dormitory tag.

### 3.3.3 Hardware setup

First of all, the two devices, the Arduino UNO and the RC522 module, have to be connected to each other. This can be accomplished by using jumper wires. Although using a bread board and soldering would make the connection much more secure and flexible, it was revealed in the testing that if the devices are kept still, they are not even needed.

The Arduino UNO has pin connectors which can be used to simply plug in the jumper cables [24]. The RC522 module also has similar connectors, although the wires will not be as firmly attached as in the case of the Arduino UNO. However, as mentioned, this is not a problem if the device is stationary.

When it comes to correctly connecting the wires, there are many schematics available online that describe the right way of connecting the wires and pins.

Using the USB cable that comes with the Arduino, the setup can be connected to a personal computer or a laptop and will be ready to accept instructions.

### 3.3.4 Software setup

On the software side, for interacting with the UNO the Arduino IDE, which is available on the official Arduino website, has to be used [20]. This software can be used to view, edit, and upload code to the device. Also, the IDE can show the output of the RC522 reader.

Additionally, the RC522 library must be added to the software. There are a couple of options one can choose from. However, the specific one used in this testing is provided by the code author André Balboa on GitHub [25].

This library can be included in the IDE by downloading the zipped code and adding it through the tool bar: “Sketch – Include Library – Add .ZIP library…”. Now all the available sketches will be viewable by going to: “File – Examples – MFRC522”. This code, which looks and functions similarly to code written in the C programming language, can now be edited, and uploaded to the device easily.

### 3.3.5 Alternate options

There are various other devices that can be used for bypassing RFID access control systems. However, they are usually harder to come across, are harder to use, and cost a fair bit more than the ones mentioned above.

One alternative is the Proxmark3, which is a device specially built for hacking RFID systems [26]. It can be operated at multiple frequencies and can even simulate cards. However, this device is significantly more expensive compared to the variants above, costing around 300 USD, and is more difficult to use because of the advanced features it offers. For these reasons, it was passed over for this testing.

Another option is just a generic high frequency RFID reader. These kinds of devices are easy to find and are not very expensive. However, they still need to be connected to a computer to operate and may require additional libraries which might not be as widespread.

When it comes to the “Magic cards” mentioned, apart from the UID Gen1 card, there are also Gen2 (Generation 2) cards [23]. The main difference is that these Gen2 “Magic cards” do not use the known backdoor command to rewrite the UID. Instead, they use the normal block write command in combination with the block key. (This is later explained in the Mifare Classic 1K section.) Furthermore, there are two types of Gen2 “Magic cards”: CUID (Changeable UID Generation 2 card), which can be rewritten many times, and FUID (Changeable UID Write-Once Generation 2 card), which can only be rewritten once and afterwards function as normal cards. The UIDs on these cards can also be rewritten using smartphone readers. These Gen2 cards would also be a great fit for this testing, especially since a smartphone can be used to rewrite them. However, Gen2 "Magic cards" are harder to come across compared to the Gen1 cards, and because of the global restrictions present at the time of working on this thesis, the Gen2 cards were passed over for use in penetration testing.

After all this, it should be clear why the Arduino UNO, the RC522 module, and the Gen1 “Magic cards” were chosen for this testing.

## 3.4 Gaining access

Once the Arduino and the module are set up correctly, and one of the “Magic cards” mentioned above are available, testing can begin.

Looking through the sketch selection in the MFRC522 library, the ones that seem immediately useful are: “ReadNUID” and “ChangeUID”. These two sketches will be used in this section to copy both the dorm tag and the student card UIDs.

### 3.4.1 Reading card and tag UIDs

Logically, the “ReadNUID” sketch is used for reading a card’s UID. Once selected, the code can be uploaded to the Arduino by pressing the upload button in the IDE. This will automatically compile the code as well. After the sketch is uploaded, the output can be viewed in the serial monitor, which is accessed by selecting it from the “Tools” tab.

The first serial monitor output from the current sketch is shown in Figure 2.

```
This code scan the MIFARE Classsic NUID.
02:59:48.859 -> Using the following key: FF FF FF FF FF FF
```

Figure 2. First serial monitor output after loading the “ReadNUID” sketch

For the purposes of this testing, the NUID (Non-Unique Identifier) mentioned in the output is the same as the card UID referred to in the text. Also, the key mentioned has no relevance, since the Mifare Classic 1K card transmits its UID without authenticating.

First, the UID of the dormitory tag was read. The serial monitor output of the access tag read is shown in figure 3.

```
02:52:41.185 -> PICC type: MIFARE 1KB
02:52:41.185 -> A new card has been detected.
02:52:41.232 -> The NUID tag is:
02:52:41.279 -> In hex:  FC 28 7E 1C
02:52:41.279 -> In dec:  252 40 126 28
```

Figure 3. Serial monitor access tag read output

The sketch returned the PICC (Proximity Integrated Circuit Card) type, and the UID in both hexadecimal and decimal numbering systems. This meant that the card was successfully read. This is the UID that was written to the fake tag, which was then used to gain access to the dormitory building.

Continuing to the student card, after the card was placed close to the reader, an error was thrown. The serial monitor output of the error is shown in figure 4.

```
02:56:35.694 -> PICC type: Unknown type
02:56:35.694 -> Your tag is not of type MIFARE Classic.
```

Figure 4. Serial monitor student card read error output

This was very easily fixed, since the code responsible for checking the PICC type of the card was labelled. The code responsible for the student card read error is shown in figure 5.

```
// Check is the PICC of Classic MIFARE type
  if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&
    piccType != MFRC522::PICC_TYPE_MIFARE_1K &&
    piccType != MFRC522::PICC_TYPE_MIFARE_4K) {
    Serial.println(F("Your tag is not of type MIFARE 
Classic."));
    return;
  }
```

Figure 5. ReadNUID code responsible for student card read error

After this was commented out, the reader was able to read the student card easily. The serial monitor output of the student card read is shown in figure 6.

```
02:55:02.116 -> PICC type: Unknown type
02:55:02.116 -> A new card has been detected.
02:55:02.164 -> The NUID tag is:
02:55:02.164 -> In hex:  05 86 B6 81 EA A1 00
02:55:02.211 -> In dec:  05 134 182 129 234 161 00
```

Figure 6. Serial monitor student card read output

Although the type was stated as unknown, the UID was still successfully read.

After obtaining both the dormitory tag and student card UIDs, this information could then be written onto the “Magic cards and tags”.

### 3.4.2 Writing card and tag UIDs to fake devices

For writing the card UIDs, the “ChangeUID” sketch was used, and the output was checked in the serial monitor as was done previously.

Before uploading this sketch, the new UID, which was chosen to be written onto the fake tag, must be inserted in the program. The code responsible for storing the UID value is shown in figure 7.

```
/* Set your new UID here! */
#define NEW_UID {0xDE, 0xAD, 0xBE, 0xEF}
```

Figure 7. ChangeUID code responsible for storing the UID value

After replacing the NEW_UID value with the dormitory UID that was read previously, the sketch can be uploaded to the Arduino. The first serial monitor output from the current sketch is shown in figure 8.

```
02:57:52.098 -> Warning: this example overwrites the UID of your
UID changeable card, use with care!
```

Figure 8. First serial monitor output after loading the “ChangeUID” sketch

Now, the UID rewritable “Magic tag” can be placed next to the reader. The UID was indeed rewritten successfully. The serial monitor output of the access tag UID rewrite is shown in figure 9.

```
03:05:35.320 -> Card UID: DE AD BE EF
03:05:35.367 -> Wrote new UID to card.
03:05:35.414 -> New UID and contents:
03:05:35.414 -> Card UID: FC 28 7E 1C
```

Figure 9. ChangeUID access tag UID rewritten successfully output

As shown in the output, the old UID - DE AD BE EF - was changed with the one copied from the Akadeemia 5 dormitory access tag - FC 28 7E 1C.

After this process, the two tags were virtually identical, and the same output was shown when each was read by the reader.

The same results were achieved with the student card, so there is no need to write down the details of that process.

Now, both the dummy devices are ready to be used for physical testing in the following section.

### 3.4.3 Testing the fake card and tag

When the valid UIDs are successfully written onto the dummy devices, the final step is to test them in the real environment and see if they are able to bypass the entry system.

Both the card and the tag were tested in the Akadeemia 5 dormitory building, and access was granted in both cases with no irregularities. This meant that the access control system implemented at the campus was easily bypassed by the fake cards created using the cloning attack.

Videos of this procedure is available online at the following links:

- Entering with an access tag – (Link)
- Entering with an access tag clone – (Link)
- Entering with a student card – (Link)
- Entering with a student card clone – (Link)

## 3.5 Report

In summary, the tools selected, which met the testing criteria outlined, were able to read the valid UIDs of the authentic media and transfer them to the UID rewritable devices. Following this, the dummy devices were successful in bypassing the current RFID access control system in place at the campus. The goal of this testing was met: the cloning attack was effectively carried out with no advanced knowledge using easily obtainable, rudimentary devices.

The two main reasons for this are that the Mifare Classic 1K devices used are poorly implemented and that the readers at the university only check the card UIDs during communication.

### 3.5.1 The problem with the Mifare Classic 1K devices

It is a known fact that the Mifare Classic devices are the weakest in terms of security compared to all of the other RFID technologies Mifare offers. The cryptographic algorithm these devices use, CRYPTO1, has been analysed and broken on numerous occasions using different methods like brute-forcing [27], reader/tag nonce variation, multiple-sector authentication [28], keystream recovery [29], replaying, re-engineering [30], and so on. However, these are advanced techniques and require strong technical expertise to be performed. On the other hand, as demonstrated, the system at the university was bypassed with a much simpler method. The ease of exploitation is the main issue.

To understand the problem with the university’s implementation of Mifare Classic cards, the memory structure they use must be described [17], [31].

The 1K devices have 16 sectors labelled from 0 to 15. Each sector has 4 blocks, labelled from 0 to 3, that each hold 16 bytes of data. There are 3 main types of these blocks:

- The manufacturer block - this holds the UID and the card manufacturer information. There is only one block of this type on each card, and it is always sector 0 block 0. As stated previously, this block is read only. It is to be noted that the UID in the manufacturer block is transmitted openly upon card activation.

- The data blocks - these blocks are both readable and writable and can contain user data. Furthermore, these blocks are protected, meaning they cannot be read or written without proper authentication.

- The sector trailer blocks - these are the last blocks of each sector. They contain authentication keys, Key A and Key B, and access conditions for that particular sector. The access conditions determine what operations can be performed with each key. Key A is mandatory, while key B is optional. Both keys are 6 bytes in length and are set to all FF values by default.

A major problem with the Mifare Classic setup on the campus, is that the card UIDs are used for granting access. The authentication keys mentioned above are only needed for operations on data blocks. Since the UIDs are transmitted openly upon activation without any kind of reader authentication, this data can be read by anyone with a malicious reader and can be used to bypass the system.

### 3.5.2 The problem with the readers in place

The main problem with the readers used is that they rely solely on the received UID for access control. Furthermore, they do not use any kind of authentication, clone detection or elimination mechanisms. As a result, most widely available dummy cards can easily act as valid cards and trick the system if they use a valid UID.

### 3.5.3 The danger revealed by this testing

Because of the problems outlined above, the system is vulnerable to the cloning attack which can very easily be carried out without any advanced devices or knowledge. If someone with malicious intentions gets a hold of a valid card, he could create fake devices, like the ones demonstrated in this section, and could gain access to private buildings on the campus with very little money and effort. On top of that, the access can be written to multiple devices and distributed to many people. This means that the access copied from a single card can result in multiple unauthorized people breaching the physical security on the campus.

# 4 Picking a solution for the access control system at the campus

There are many different options for improving or updating the RFID access control system at the university campus. These solutions range from minor software changes that can easily be implemented, however are not full proof, to complete system replacement, including hardware and software alteration, guaranteeing advanced security. The level of security they offer also varies in relation to their cost and difficulty of reimplementation.

This section will go over some of the improvement options, will describe a discussion about the mentioned options with the company SOYAL, and will recommend the solution that best balances both the offered security and the upgrade cost.

## 4.1 Various options

### 4.1.1 Correctly configuring the current system

Firstly, the logical solution is to correctly use the security features the current system does offer. Even though compared to newer RFID technologies the Mifare Classic family is considered the least secure, it still has some security features that, when configured correctly, will at least make the system withstand the kinds of simple cloning attempts described in the penetration testing section (see Section 3).

Similar suggestions for improving the Mifare Classic implementation have been described by W. Teepe in his paper “Making the Best of Mifare Classic” [32].

As stated above (see Section 3.5), the main reason the demonstrated cloning attack was successful was the fact that the card UID is used for granting access. This UID is transmitted openly and can easily be read by any other reader. To solve this problem, a different user ID can be used for granting access which would be kept on one of the card’s data blocks. An ID kept on one of these blocks would be harder to obtain by malicious readers because these blocks are protected by authentication keys, unlike the manufacturer block where the UID is stored.

As described above (see Section 3.5.1), for a reader to perform any kind of memory operations on Mifare Classic data blocks, it first has to be authenticated by a mandatory key. These keys are kept in the sector trailer blocks, they can be different for each sector, and are 6 bytes long each. Each data block also has its own access conditions, that are also kept in the trailer, which determine what kind of operations can be done on the block with the correct key. These conditions can render data blocks in a particular sector read-only if needed, or can allow further operations like writing, incrementing, decrementing and so on.

Logically, using the following configuration for the MIFARE Classic card would solve the problem:

The card would be formatted in the following manner: an additional ID will be stored in one of the card's data blocks. This sector will have its unique authentication keys set in the sector trailer block, along with the access conditions, which will only allow the read operation on these data blocks using the correct authentication key. Key A is unreadable by default. Key B can also be set to be unreadable using the access conditions. This way, a reader would have to know the authentication key to read the ID kept on the data block. (For example, this access bit configuration allows only the read operation on the data blocks using key B - 1 0 1.)

Consequently, for each card the following data would be kept in the database: the UID, the data block ID, Key A, and Key B.

The reader would operate in the following manner: It will receive a UID upon card activation as it did previously. Following this, it will use this UID to look up the specific keys for this card. The reader will authenticate with the key it looks up and will send a read command to the sector and block on which the ID is written. After receiving the ID, the reader can compare it with the one in the database and allow access accordingly.

With this system in place, copying the UID will be useless, and to read the ID on the data block an attacker would need to either brute-force the authentication key or get it using one of the advanced attacks. Either way, it will make cloning a card more difficult.

The positive of this solution is that it provides higher security and keeps the price of implementation low. It can be implemented just by changing the data kept on the cards and the software configuration in place for the readers. None of the current hardware devices have to be replaced.

The negative lies in the fact that no matter how it is configured, the Mifare Classic will still not be as secure as its alternatives. This technology has already been broken and can still be bypassed by an experienced attacker utilizing advanced devices. This system is still not protected from attacks like eavesdropping, DoS, reverse engineering, power analysis, and so on.

### 4.1.2 Adding a simple clone elimination feature

There have been numerous proposed anti-cloning methods that used advanced techniques. For example: anti-eavesdropping, bi-directional authentication [33], in which both the card and the reader have to authenticate themselves, PUFs (Physically Unclonable Functions) [34], which are embedded functions that leverage wire delays, challenge-response procedures using PIN-based (Personal Identification Number) access, varying randomization and hash-based access control schemes [35], [36], [37], and so on. However, most of these are hard to implement and require specific hardware to work.

This section will describe a simpler technique which is very straightforward, is much easier to implement, and is automatically used by many of the modern readers on the market. However, this method is not as full-proof as the ones mentioned above. A similar detection and elimination method was described by P. Moravec and M. Krumnikl in the paper “Developing Countermeasures against Cloning of Identity Tokens in Legacy Systems” [38].

The basic idea is that a reader tries to eliminate a clone tag before reading its contents. It does so using rewrite commands, which only affect UID changeable devices, to disable fake cards by rewriting their UIDs to zeros.

As mentioned in the tool selection part, there are a couple of generations of UID changeable “Magic cards”, each with different ways for rewriting the UID:

- Normal Gen1 cards use a well-known backdoor command with the unlock code 0x43 0x40 to rewrite their UIDs.

- Newer Gen2 cards, on the other hand, use the normal block write command with the appropriate authentication key. The authentication key is set to all FFs by default, and since these cards are mostly used by amateurs, is not changed in many cases.

The solution is very simple: The reader sends these rewrite commands before reading a card’s UID. These commands will be ignored by authentic cards since they do not support UID rewriting. On the other hand, fake cards will respond to these commands and will be left unreadable since the UID will be changed to all zeros. Readers can be configured to run both of the commands or just one of them. This does slow down the reading process by a bit. However, it is not an amount that is noticeable to end users [38].

This will render all Gen1 cards and CUID Gen2 cards using the default key bricked. However, it will not work on the FUID Gen2 cards or CUID Gen2 cards using a unique sector key. Since these variations are rarer, it should work on most of the fake cards used by amateurs.

The positive of this approach is the low cost of implementation if it can be added to the readers currently in place. Furthermore, it can be combined with one of the other solutions to increase the overall security.

The negatives are that this will not protect against every type of clone card and can still be bypassed by experienced attackers if they have the necessary tools.

### 4.1.3 Implementing a newer system offering proper authentication & encryption (DESFire)

There are a couple variations of Mifare cards with different levels of security. The Mifare Classic family cards were already touched on. However, as mentioned, this technology is already considered old and has been broken many times. Nowadays, there are newer, more secure options like the Mifare Plus family, and the Mifare DESFire family. This section will be focusing on the Mifare DESFire family cards since they are one of the most secure options available and are also offered by the company "Soyal" mentioned before.

The Mifare DESFire family was first introduced in 2002 and has had a couple of upgrades over the years, with the newest variation, the EV3, being released in 2020 [39]. These types of cards are much more secure compared to the Mifare Classic ones and are backed by various sources as being one of the most secure modern RFID technologies with very strong encryption and authentication methods [40], [41]. They are used for advanced public transportation, highly secure access management, eGovernment applications, and so on. It should be stated that these devices are still passive and still operate in the RFID high-frequency range.

Although these devices have very secure encryption and authentication methods, there are still some possible vulnerabilities and attacks that barely bypass this technology. D. Hurley-Smith and J. Hernandez-Castro analyse the performance of the randomness this technology uses and show that there are some biases when it comes to DESFire EV1 products in their paper “Bias in the Mifare DESFire EV1 TRNG” [42]. Other studies show that side channel attacks, like power analysis, can be used for key extraction and recovery [43], [44]. Furthermore, R. Flynn investigated a DESFire system used for public transportation and demonstrated which attacks affect the different communication modes the DESFire technology uses in his paper “An investigation of possible attacks on the MIFARE DESFire EV1 smartcard used in public transportation” [45]. However, these kinds of attacks depend on the quality of the system implementation, take a very large effort, need advanced devices, and are extremely difficult to pull off even for experienced attackers. For these reasons, the chance of these kinds of attacks occurring is miniscule.

Now, the advantages of this technology will be described. The DESFire cards have some very advanced features that are beyond the scope of this thesis. However, here are some of the basic advantages they offer [46]:

- Advanced Encryption - The first and biggest advantage these cards offer is the fact that they support advanced encryption methods. Unlike the flawed CRYPTO1 algorithm used by the Mifare Classic family, the DESFire family offers a couple of more secure options: 56-bit DES (Data Encryption Standard), 112-bit 3DES, 168-bit 3DES, and 128-bit AES (Advanced Encryption Standard). These cryptographic algorithms are used for mutual three-pass authentication prior to data transmission. This results in a secure communication between the DESFire card and the reader if the encrypted data transfer mode is used. (There are other modes that transmit in plaintext for backwards-compatibility.)

- Advanced Authentication - Without going into the deeper cryptographic parts of these algorithms, the authentication process is basically completed when the reader and the card exchange encrypted data securely in order to verify that they share the same secret or key. This confirms that both entities are permitted to perform operations on each other. Furthermore, a session key is created after this process which is used to keep the communication path secure. A new session key is created after each authentication.

- Memory Size & file system - The memory options for these cards are the following: 2 KB (Kilobyte), 4 KB, 8 KB, 16 KB or 32 KB. The card basically has a file system that allows the installation of multiple applications [47]. An application, in this context, is basically like a secure folder used for storing files. Each application can store up to 32 files and is secured by a key, AMK (Application Master Key) or CMK (Card Master Key), that allows different operations. This kind of secure and flexible system opens up a huge number of opportunities that can be used for different settings.

With the advantages of this solution out of the way, the drawbacks of implementing such a system for access control have to be discussed as well. The first and biggest negative is that it would be very time consuming and very expensive for the university to change the whole access control system. For this to be correctly implemented, all the access cards on the campus have to be replaced. On top of the replacement costs, the reader software has to be changed to work with the system, and new access devices have to also be purchased.

It is undoubtable that the Mifare DESFire family offers a great amount of security and flexibility; however, it has to be considered if the cost of implementation is worth the benefits it offers, and if this kind of advanced security is even needed in this scenario.

## 4.2 Discussion with the company SOYAL

To make sure the options outlined in the previous section can be indeed implemented as described, a discussion was necessary with the company who is the manufacturer of the access devices in place at the campus. As mentioned already, this company is SOYAL (see Section 3.2.2).

After briefly describing the system upgrade options mentioned above in an email, the company was very cooperative and clearly explained the services they provide. Since the emails are confidential, they are not included in this thesis. Mainly, they offered the following options:

- SOR (SOYAL Open system Rules) Mifare encryption
- SOYAL DESFire
- Purchasing a programming kit and implementing encryption without using SOYAL software

### 4.2.1 SOR Mifare encryption

Starting with the SOR Mifare encryption [48], it is developed by SOYAL and uses their software called Mifare Key. This can be added to the system already in place and offers stronger security without needing a change in the current hardware. SOR also offers additional functionality, like holding usernames, setting validity periods, and so on. Of course, these functions can be left unused if they are not needed.

The security of this software basically follows the same logic outlined previously while describing the correct configuration for the current MIFARE Classic system (see Section 4.1.1). It works in the following manner:

A new User ID is assigned to a card and is kept on one of the data blocks - block 9 by default. This data block is protected by the authentication keys, meaning the User ID cannot be read without knowing these keys. This User ID is used to grant access personnel accordingly.

It must be noted that a SOYAL encoder device (725P) must be purchased additionally, with authorization cards, in order to format the access cards. Otherwise, the formatting and encryption can be handled by a local distributor.

### 4.2.2 SOYAL DESFire

Continuing to the SOYAL DESFire, as the name describes, this option uses the much stronger DESFire encryption (see Section 4.1.3). The main part is that all the programming is done by SOYAL as the manufacturer.

In terms of security, this is a much better option. However, it requires all the current MIFARE Classic cards to be replaced with the MIFARE DESFire cards. Additionally, if the current readers are 5 years old or older, they have to be replaced as well. In terms of security, this is the best option. However, it is clear that along with the security benefits, the cost of this implementation also has to be considered.

### 4.2.3 Purchasing a programming kit

Another possibility SOYAL mentioned, is purchasing a programming kit, and implementing the encryption without using SOYAL's software. Additionally, this could possibly allow the implementation of the simple clone elimination feature described previously (see Section 4.1.2). It had to be noted that this is a possibility. However, since the other options are much easier to implement, discussion in this direction was not continued.

## 4.3 The proposed solution

In reality, the best solution should be the one that provides enough security without breaking the bank and requiring a complete system replacement.

Logically speaking, the probability of an experienced hacker appearing with top-tier devices with a plan of attack to break into one of the university buildings is very low. As a result, implementing advanced solutions like the ones providing high-class authentication, encryption, and randomized systems can be considered overkill for this kind of application. This will be costly and will require the replacement of the access devices on the campus, as well as a whole software replacement.

On the other hand, someone trying an attack like the one demonstrated in the penetration testing phase (see section 3) is far more probable. Correctly optimizing the system that is currently in place will be much more cost friendly and will result in an implementation that is more secure and that will be able to withstand the kind of cloning attack that was demonstrated. As a result, correctly configuring the current system without changing the existing hardware devices used on the campus should be enough.

The discussion with SOYAL solidified the described options (see Section 4.2) and much more clearly demonstrated what it will take to implement such upgrades in the current system.

In the end, it is for the university to decide what cost is too much and what cost is reasonable for the outlined problem. However, if cost saving is a priority, because of the outlined reasons, the best option should be to go with the SOR Mifare encryption from SOYAL. This holds the best balance between providing security features and being easy to implement. Of course, if the university will choose not to focus on cost and time saving, SOYAL DESFire is also a fantastic option providing top-tier security and should not be cast aside.

# 5 Summary

The main goal of this thesis was to perform penetration testing on the current RFID access control system at the campus, document the findings, research adequate ways of improvement, and provide a solution to the described vulnerability that would offer descent security while being relatively easy and inexpensive to implement.

This thesis described the steps and the outcome of the penetration testing that was performed on the campus in order to expose the implemented system’s vulnerability to the RFID cloning attack. It also included the tool descriptions for this testing, and an explanation for the existing issues.

Furthermore, this thesis put forth multiple improvement options for the aforementioned problem. Additionally, these options were discussed with the company SOYAL, whose devices and software are used on the campus, to further solidify and ground the proposals.

Finally, a solution was chosen that was the most balanced in terms of security and cost – to leave the current system and hardware in place and implement the SOR encryption provided by SOYAL. Additionally, the SOYAL DESFire was also proposed as a great high-security option if the implementation time and cost that comes with it is not an issue for the university.

While working on this thesis, research was conducted using various academic papers written on the subject of RFID technology, official manuals and documentations describing the functionality of specific systems and devices, existing research performed by experienced professionals, and other online sources which yielded relevant information.

This work will be a great help to the university if improving the current RFID access control system security is ever considered and can be used as a guide for such an occasion. This work will also aid any other company or organization that is facing a similar problem with their access control.

# References

[1] "Know about Access Control Systems and Their Types with Features". [Online]. Available: https://www.elprocus.com/understanding-about-types-of-access-control-systems/#:~:text=Access%20control%20system%20is%20one,a%20reader%20on%20the%20door.&text=By%20this%20card%20access%20control,one%20side%20of%20the%20door.
[Accessed: 15- Apr- 2021].

[2] Integrated Access Security, "What Is the Difference Between Physical Access Control and Logical Access Control?", January 30th, 2020. [Online]. Available: https://www.integratedaccesssecurity.com/blog/access-control/what-is-the-difference-between-physical-access-control-and-logical-access-control/#:~:text=Physical%20access%20control%20is%20the,and%20going%20in%20restricted%20areas.
[Accessed: 15- Apr- 2021].

[3] James Eldred, "Components of an Access Control System and How It Works", October 22nd, 2020. [Online]. Available: https://getsafeandsound.com/2020/10/components-of-access-control/
[Accessed: 15- Apr- 2021].

[4] U. Farooq, M. ul Hasan, M. Amar, A. Hanif, M. U. Asad, "RFID Based Security and Access Control System", IACSIT International Journal of Engineering and Technology, Vol. 6, No. 4, August 2014

[5] Suzanne Smiley, "Active RFID vs. Passive RFID: What’s the Difference?", December 10th, 2019. [Online]. Available: https://www.atlasrfidstore.com/rfid-insider/active-rfid-vs-passive-rfid
[Accessed: 15- Apr- 2021].

[6] "How to Select a Correct Tag – Frequency". [Online]. Available: https://rfid4u.com/rfid-frequency/
[Accessed: 15- Apr- 2021].

[7] Stylianos Kiliaris, "Exploiting NFC and RFID Vulnerabilities in a Penetration Testing Environment Using Arduino", Department of Computing, University of Surrey, Guildford GU2 7XH, August 2020

[8] Q. Xiao, T. Gibbons, H. Lebrun, "RFID Technology, Security Vulnerabilities, and Countermeasures", Defence Research and Development Canada – Ottawa, Canadian Operational Support Command, Canada, January 2009

[9] K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh, "Technical Guide to Information Security Testing and Assessment", Special Publication 800-115, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, September 2008

[10] The Open Source Security Testing Methodology Manual, Institute for Security and Open Methodologies, version 3.02, December 2010

[11] Jeremiah Talamantes, "How To Prepare For Your Physical Penetration Test". [Online]. Available: https://www.redteamsecure.com/blog/how-to-prepare-for-your-physical-penetration-test
[Accessed: 9- March- 2021].

[12] RSI Security, "WHAT IS THE NIST PENETRATION TESTING FRAMEWORK?", August 24, 2020. [Online]. Available: https://blog.rsisecurity.com/what-is-the-nist-penetration-testing-framework/
[Accessed: 9- March- 2021].

[13] "Penetration Testing". [Online]. Available: https://www.imperva.com/learn/application-security/penetration-testing/
[Accessed: 15- Apr- 2021].

[14] Soyal "AR721U – SOYAL WIEGAND READER". [Online]. Available: https://magnet.com.my/product/ar721u-soyal-wiegand-reader/
[Accessed: 15- Apr- 2021].

[15] Gerhard Klostermeier, "MIFARE Classic Tool (MCT)", (2011-2021). GitHub repository. Available: https://github.com/ikarus23/MifareClassicTool

[16] Tim Theeuwes, "Using a mobile phone to clone a MIFARE card", June 20, 2016. [Online]. Available: https://timdows.com/projects/using-a-mobile-phone-to-clone-a-mifare-card/
[Accessed: 15- Apr- 2021].

[17] SonMicro Elektronik, "MIFARE CLASSIC 1K/4K USER MANUAL", Release 1.1.0, November 7th, 2017. [Online]. Available: https://shop.sonmicro.com/Downloads/MIFARECLASSIC-UM.pdf
[Accessed: 15- Apr- 2021].

[18] H. Pereira, R. Carreira, P. Pinto and S. I. Lopes, "Hacking the RFID-based Authentication System of a University Campus on a Budget", 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020

[19] Arduino, "ARDUINO UNO REV3". [Online]. Available: https://store.arduino.cc/arduino-uno-rev3
[Accessed: 15- Apr- 2021].

[20] Arduino, "Arduino IDE 1.8.13". [Online]. Available: https://www.arduino.cc/en/software
[Accessed: 15- Apr- 2021].

[21] NXP Semiconductors N.V. "MFRC522 Standard performance MIFARE and NTAG frontend", Product data sheet, Rev. 3.9 — 27 April 2016. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf
[Accessed: 15- Apr- 2021].

[22] Lab401 Steve, "KNOW YOUR MAGIC CARDS", April 29th, 2019. [Online]. Available: https://lab401.com/blogs/academy/know-your-magic-cards
[Accessed: 15- Apr- 2021].

[23] "Difference of access card uid card, cuid card and fuid card", January 15th, 2020. [Online]. Available: https://developpaper.com/difference-of-access-card-uid-card-cuid-card-and-fuid-card/
[Accessed: 15- Apr- 2021].

[24] "How to use the RFID-RC522 module (RFID reader) with the Arduino Uno", February 7th, 2017. [Online]. Available: https://mschoeffler.com/2017/02/07/how-to-use-the-rfid-rc522-module-rfid-reader-with-the-arduino-uno/
[Accessed: 15- Apr- 2021].

[25] André Balboa, "Arduino library for MFRC522 and other RFID RC522 based modules", (2016-2021). GitHub repository. Available: https://github.com/ikarus23/MifareClassicTool

[26] Proxmark, "Proxmark 3". [Online]. Available: https://proxmark.com/proxmark-3-hardware/proxmark-3
[Accessed: 15- Apr- 2021].

[27] F. D. Garcia, P. van Rossum, R. Verdult, R. W. Schreur, "Wirelessly Pickpocketing a Mifare Classic Card", Radboud University Nijmegen, The Netherlands, 2009

[28] F. D. Garcia, G. de K. Gans, R. Muijrers, P. van Rossum, R. Verdult, R. W. Schreur, B. Jacobs, "Dismantling MIFARE Classic", Institute for Computing and Information Sciences, Radboud University Nijmegen, The Netherlands, 2008

[29] G. de K. Gans, J. Hoepman, F. D. Garcia, "A Practical Attack on the MIFARE Classic", Institute for Computing and Information Sciences, Radboud University Nijmegen, GL Nijmegen, The Netherlands, 2008

[30] M. Morbitzer, "The MIFARE Hack", Radboud University Nijmegen

[31] G. de K. Gans, "Analysis of the MIFARE Classic used in the OV-Chipkaart project", Radboud University Nijmegen, June 2008

[32] W. Teepe, "Making the Best of Mifare Classic", Radboud University Nijmegen, October 6, 2008

[33] K. Bu, M. Weng, Y. Zheng, B. Xiao, X. Liu, "You Can Clone But You Cannot Hide: A Survey of Clone Prevention and Detection for RFID", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 19, NO. 3, THIRD QUARTER, 2017

[34] A. Mitrokotsa, M. R. Rieback, A. S. Tanenbaum, "Classifying RFID attacks and defenses", Springer Science, 29 July 2009

[35] J. Abawajy, "Enhancing RFID Tag Resistance against Cloning Attack", Deakin University, School of Information Technology, 2009

[36] Y. K. Lee, L. Batina, I. Verbauwhede, "EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol", Department of Electrical Engineering, University of California, Los Angeles, Department of Electrical Engineering, ESAT-COSIC, Katholieke Universiteit Leuven, Belgium, 2008

[37] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Laboratory for Computer Science, Massachusetts Institute of Technology Cambridge, 2004

[38] P. Moravec, M. Krumnikl, "Developing Countermeasures against Cloning of Identity Tokens in Legacy Systems", 16th IFIP International Conference on Computer Information Systems and Industrial Management (CISIM), Bialystok, Poland, Jun 2017

[39] "MIFARE". Wikipedia. [Online]. Available:
https://en.wikipedia.org/wiki/MIFARE#MIFARE_DESFire_family
[Accessed: 15- Apr- 2021].

[40] P. Dzurenda, J. Hajny, V. Zeman, K. Vrba, "Modern physical access control systems and privacy protection", 2015 38th International Conference on Telecommunications and Signal Processing (TSP), 2015

[41] J. Hajny, P. Dzurenda and L. Malina, "Secure physical access control with strong cryptographic protection", 2015 12th International Joint Conference on e-Business and Telecommunications (ICETE), 2015

[42] D. Hurley-Smith, J. Hernandez-Castro, "Bias in the Mifare DESFire EV1 TRNG", School of Computing, University of Kent, Canterbury, Kent, 2016

[43] D. Oswald, C. Paar, "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World", Horst Görtz Institute for IT Security, Ruhr-University Bochum, Germany, 2011

[44] T. Kasper, D. Oswald, C. Paar, "Security of Wireless Embedded Devices in the Real World", Chair for Embedded Security HGI, Ruhr-University Bochum, Bochum, Germany, January 2011

[45] R. Flynn, "An investigation of possible attacks on the MIFARE DESFire EV1 smartcard used in public transportation", School of Computer Science and Statistics, The University of Dublin, July 24, 2019

[46] NXP Semiconductors N.V. "MIFARE DESFire EV1 contactless multi-application IC", Product short data sheet, Rev. 3.2 — 9 December 2015. [Online]. Available: https://www.nxp.com/docs/en/data-sheet/MF3ICDX21_41_81_SDS.pdf
[Accessed: 15- Apr- 2021].

[47] "MIFARE DESFire® EV1". [Online]. Available: https://developer.fidesmo.com/documentation/desfire-implementation#:~:text=MIFARE%20DESFire%C2%AE%20EV1%20allows,application%20keys%20assigned%20(APKs).
[Accessed: 15- Apr- 2021].

[48] "SOR" SOYAL Product Line Training Course. [Online]. Available: http://www.soyal.eu/letolt/manualen/SOYAL%20AR-725PDX%20EN.pdf
[Accessed: 22- Apr- 2021].

# Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Giorgi Okroshidze

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Flaws in the Implementation of RFID Identification at TalTech and Improvement Suggestions", supervised by Aleksei Talisainen.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

17.05.2021

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.