

WHAT TYPE OF RFID CARDS CAN BE EASILY CLONED BY HARDWARE AVAILABLE ON THE MARKET?

MSc in Cyber Security Evening

Andrzej Mackiewicz

Student ID: 18157815

School of Computing
National College of Ireland

Supervisor: Ben Fletcher

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name: Andrzej Mackiewicz

Student ID: 18157815

Programme: MSc in Cyber Security Evening Year: 2020

Module: Internship

Supervisor: Ben Fletcher

Submission Due Date: 17th August

Project Title: WHAT TYPE OF RFID CARDS CAN BE EASILY CLONED BY HARDWARE AVAILABLE ON THE MARKET?

Word Count: Page Count.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:



Date:

17/08/2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Table of Contents

1. Introduction	4
1.1 Motivation	4
1.1. Research questions	5
1.2. Research mythology	5
1.3. Limitation of research	6
1.4. Structure of the thesis	6
2. System and technology awareness	6
2.1. What are the system elements	6
2.2. How RFID works?	7
2.3. RFID components	7
2.4. How RFID systems operate and their classifications	7
2.4.1. An inductively coupled RFID system	8
2.4.2. Backscatter RFID System	8
2.4.3. Near vs Far Field Communications	8
2.4.4. Classification of the RFID systems based on their frequencies	9
2.5. Cybersecurity awareness	10
3. Cyber Security Research Description	10
3.1. Guiding Principles	10
3.2. Programmatic Approach to Address the Problem Space	11
3.3. Cybersecurity Problem Space	11
4. General Approach	12
4.1. Programmatic Approach	12
4.2. Methodology	12
4.2.1. Use of Specific Arduino and Mifare RC522 Card Reader Antenna	12
4.2.2. Use of Proxmark3 (cheaper version bought from AliExpress)	12
4.2.3. Development based on Bishopfox Tool Description	12
5. Case studies	12
5.1. Case Study 1 Introduction	12
5.1.1. Case Study 1 Challenges	13
5.1.2. Case Study 1 Design of the RFID card/tag	13
5.1.3. Case Study 1 Hardware and software set-up	13
5.1.4. Case Study 1 Method used	15
5.1.5. Case Study 1 Results of the cloning RFID (MIFARE 1K Type)	15
5.2. Case Study 2 Introduction	15
5.2.1. Case Study 2 Challenges	16
5.2.2. Case Study 2 Design of the RFID card	16
5.2.3. Case Study 2 Hardware and software set-up	18
5.2.4. Case Study 2 Method used	19
5.2.5. Case Study 2 Results of the cloning RFID	20
5.3. Case Study 3 Introduction	20
5.3.1. Challenges	21
5.3.2. Case Study 3 Design of the RFID card	21
5.3.3. Case Study 3 Hardware and software set-up	21
5.3.4. Case Study 3 Method used	21
5.3.5. Case Study 3 Results of the cloning RFID	22
6. Conclusion and recommendations	22
6.1. Conclusion	22
6.2. Recommendations	22
Reference:	23

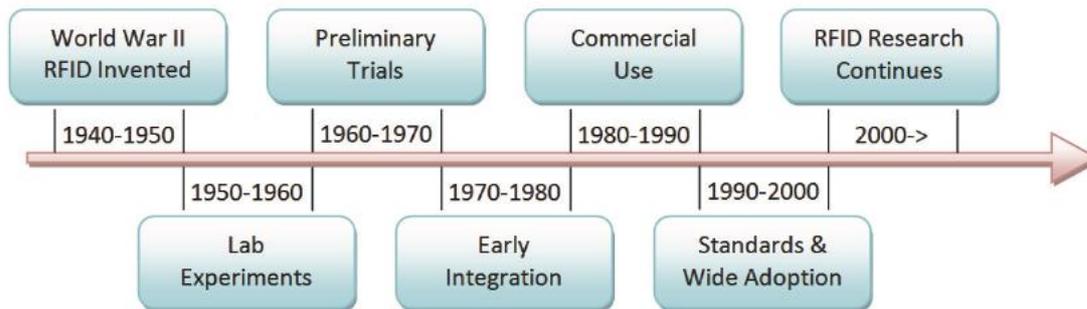
Abstract

The technology used at the end of '40s has advanced, but the security of the RFID has not improved much since. There are still many vulnerabilities that enable accessing information from different types of tags or cards and this thesis addresses those available on the market. RFID systems – tags, sensors, readers, middleware and applications are trying to solve specific business needs. This technology is used in almost everything - from books, clothing and parts of aircraft to medicine and many other environments. The general lack of understanding and awareness leads to confusion about what it is, its capabilities and limitations. This document makes its contribution to the access control, which are badges that are used to access office buildings. Many people expose their identity badges, but forgetting about hackers that might want to steal their identity. This thesis presents different card types and shows their classifications - the problem of exposing badges concerns academic, private, and public life. There are tools on the market that enable to clone them. This research shows how easy it is to clone the latest version of the badges used by companies and colleges in 2020.



1. Introduction

1.1 Motivation



The Continuous Wave radio generation was first created in 1906 by F. W. Alexanderson. The second part of the technology was the Radar, which was developed in 1922 and then used in World War II. The result of the combination of both components was the RFID concept academically proposed by Harry Stockman in 1948. During this time, the device was used to spot enemy planes. The research was continued by many communities, which led to developing Identification Friend or Foe (IFF) technology in the 1950s. In the late 1960s, Sensormatic and Checkpoint have developed the first commercial RFID in Electronic Article Surveillance (EAS) which had an 'on or off' function to prevent theft in shops. The 1970s focus was on tracking vehicles, animals and stock factories. RFID technology was used in toll roads in Norway in 1978 and later has expanded to other countries. The next massive step in RFID usage was noticed in the 1990s, where it was utilised to people's daily activities, like key cards that enable secured access to the same location. From 2000 until today, technology has been commercialised and used by various sectors. [1] Peter Darcy, Prapassara Pupunwiwat (2010), [2] Rich Handley, (2005), [3] n/a. (2017).

RFID technology can be found in almost everything from books, clothing, parts of aircraft to medicine, and many other environments. The overall absence of knowledge leads to general confusion about what RFID is, its capabilities, and its limitations. It is due to a lack of a comprehensive, principles-based and systematic RFID classification scheme. This thesis talks about the RFID types available on the market and systems which enable cards to be used by different organisations. Many people expose their identity badges, forgetting about hackers that might want to steal their identity. Customised hardware and software are required to clone a security card. The thesis shows work of dealing with security and privacy in RFID systems. Mainly, I compare and classify it according to which part of the RFID system each solution could be applied, taking into account different requirements and parameters, including their conformity to RFID standards. Hence, my comparative study targets to provide a full and clear vision of these concerns to help to determine the most appropriate solutions towards any security problem.

RFID technology has been used for security of work badges. The access control systems are fascinating, as they are based on a physical system that opens the door to grant access. Those systems are integrated with advanced IT systems, and at the same time, there are exposures like in any other IT system. The best place to learn about vulnerabilities is a security conference, where we can learn about hacking tricks and tools or exploits. The assumption is that some of the cards are still secure enough. [4] Krebs on security. (2014)

I have built a device that enables stealing information from the card, modifying it and cloning a regular plastic card used by employees as a security badge to enter their office buildings.

My research will prove that most of the users with physical access to one of the readers can extract the encrypted key and then use the key to copy data into any standard writable cards. The leading company on the market is HID. Due to pandemic, those cards are available for testing. The oldest card is from 2006 and the newest is from 2020.

My plan is to show how to go to a coffee shop with a modified garage reader in the backpack and steal information from security cards to obtain access to the company buildings. Next, ask targeted employees some random questions, for example ask for directions and during this process I will obtain all the required information from the card. In the next phase, I will use software available online that allows encoding data into a new card. If the cloned card does not have high privileges, I still should be able to enter the building and steal other user card information. By doing this research, I want to raise awareness about vulnerability in physical security. Security cards used in SCADA installations, hospitals, airports, and many of those places are using HID cards because they are the market leaders. However, their technology was compromised. [4] Krebs on security. (2014). [5] R. Want. (2006).

1.1. Research questions

The beginning of this thesis refers to the lack of knowledge and understanding of RFID security access badge in organisations. The goal is to develop a methodology for cybersecurity awareness in businesses.

Before developing a methodology to show the vulnerability of the security cards, a better understanding is a role in cybersecurity is required:

1) WHERE ARE RFIDS USED? (CATEGORISATION)

The above question is answered by looking at a variety of security measures. Looking at different aspects of RFID usage and the structure of the systems, it leads to the next research question:

2) HOW DOES RFID WORK AND WHAT ARE THE COMPONENTS?

These answers are explained in chapter 2 and can be used to create a body of understanding what components are necessary for the system to work.

Understanding of the elements required to access a building and current methods used lead to the following research question:

3) HOW DO THE RFID SYSTEMS OPERATE? SYSTEM'S CLASSIFICATIONS.

All of the above questions leads to the main question of this thesis:

4) WHAT TYPE OF RFID CARDS CAN BE EASILY CLONED BY HARDWARE AVAILABLE ON THE MARKET?

1.2. Research mythology

Several methods of research have been used to answer the research questions. This part of the document explains which strategy was used and why it was chosen. Online research, semi-structured experts' blogs, literature and a case study have been used to perform the analysis. The manner in which they were executed and the reasoning behind using them are explained next:

- Online research was used to connect literature found with most recent information published by a subject-matter expert (SME) like Bishopfix. Due to their involvement in cybersecurity, these SMEs will most likely have very up-to-date information.
- Semi-structured blogs with field-experts inputs related to the RFID hacks. Those blogs were chosen because they were quickly accessible and had a different relationship to the security of the RFIDs.

1.3. Limitation of research

The COVID-19 pandemic has interrupted my research studies during the build and deployment phase. The epidemic has impacted global supply chains and affected many businesses with worldwide operations, among which I have used some to order hardware for my research. At first, the device which has arrived at the beginning of May 2020, was not compatible with other parts I used for the project. Secondly ordered hardware I have burned, as I am not an experienced electrician. Because of limited availability and broken equipment, my research has stopped until the beginning of July, when compatible parts have arrived.

1.4. Structure of the thesis

Chapter 1 describes the history of RFID technology which starts in 1906, when the first radio transmitter, then describes the primary usage of RFID during World War II and finishes in 2000 when this system becomes commercialised. This chapter talks about various technologies that use RFID and how this research will discover a lack of security for identification badges. Questions related to this research lead to the problem of the study. Chapter 1 includes methods used to develop this study and roadblocks I have had to face.

Chapter 2 includes a description of the elements of the system and RFID components, their classification and how the system works. There are also tables with a detailed description of the electronic microchip, different types of communications and general awareness about RFID cybersecurity.

Chapter 3 describes cybersecurity research which includes guiding principles, programmatic approach to address the problem space.

Chapter 4 talks about the general approach, including a programmatic approach, the methodology of the research, and specific hardware used for this study.

Chapter 5 describes case studies with challenges including mythology, hardware used and results. Each case used different hardware and different types of RFID cards.

Chapter 6 contains legal and ethical consideration that has been used in the research, implication of the decision making and ways of working.

Chapter 7 describes the conclusion and recommendation based on results from chapter 5.

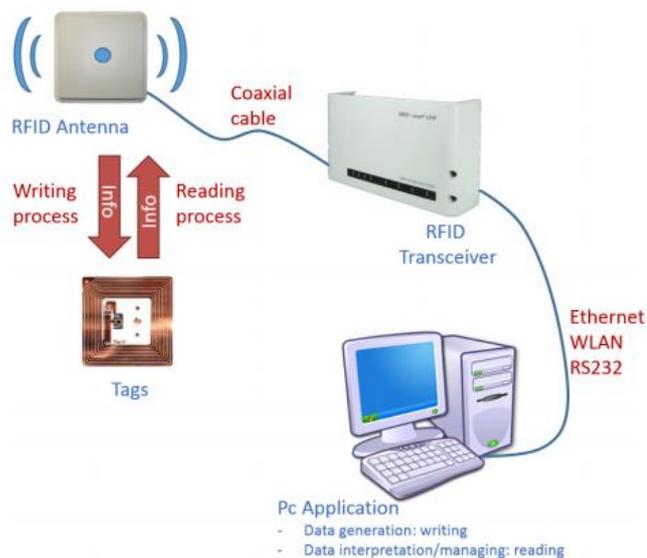
2. System and technology awareness

2.1. What are the system elements?

Radio is a technology of signalling and communicating using radio waves. Radio waves are electromagnetic waves of frequency. Frequency is the number of occurrence of a repeating event per unit of time. It is also referred to as a temporal frequency, which emphasises the contrast to spatial frequency and angular frequency. The period is the duration of time of one

cycle in a repeating event, so the period is the reciprocal of the frequency [7] ID is a symbol that uniquely identifies an object or record. Radio waves are transmitting energy through space rather than using a cable - those waves of electricity and magnetism care with the speed of light. In the second half of the 19th-century wireless communication was developed, where in early 20th-century radio and pictures were sent to everyone's homes into boxes, the television was born. Today everyone uses wireless technology to send and receive all kinds of information by using different techniques like radio, television, mobile phones or the internet. Radio and TV can send waves only one direction from the transmitter to receive. Wireless internet or mobiles are more complicated, because they can do two ways communication, it used receiver to pick up single and transmitter to send back signal. Another use of radio-waves used by plains or ships it emits radio waves and listens for echoes bouncing back off. The other device is anti-shoplifting or door entrance badge which sends radio waves to radar to catch stolen items or open doors/locks. [6,7,8] Wiki. (2020), [9] Chris Woodford. (08/2019).

2.2. How RFID works?



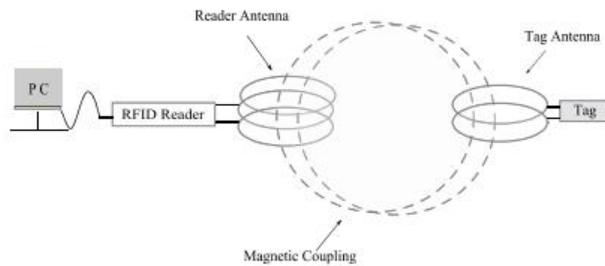
2.3. RFID components

The RFID system is composed of a RFID tag, an antenna and a transceiver (reader) connected to an application. The antenna in the reader establishes a connection with the antenna in the tag. There are different types of RFIDs which are depending on the distance between transceiver and transponders. [10] (n/a). newaverfid.com/.

2.4. How RFID systems operate and their classifications

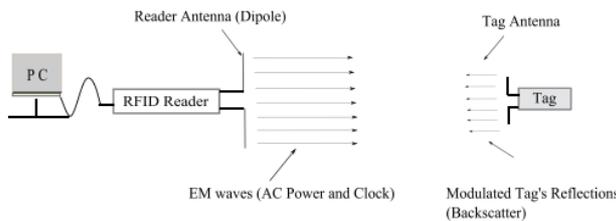
RFID systems communicate by using magnetic or electromagnetic paring. The difference between these systems is in their operating field, which can be near or far. The main property that differs both methods is the range of communication. A fundamental feature of far-field communication is that they have a more extended read range compared to near-field systems. Below presents a comparison of tags that works in both fields. Magnetically or inductively coupled systems works in LF or HF bands. The systems act in a similar way as a transformer system. [11] Enrique Valero. (2015).

2.4.1. An inductively coupled RFID system.



The above picture presents a reader generating a time-varying magnetic field, that has an AC voltage at the tag. Then AC is changed to DC to energise the microchip tag, the antenna coil in the reader tag is in an electric circuit (LC), which has the effect of the maximum energy transfer from the reader to the tag when is in the right frequency. Rate frequency translates to a lower number of turns in the antenna coil. Amplitude Modulation (AM) is achieved once the tag and the antenna get energised. The reader modulates its magnetic field amplitude according to the digital information transmitted to the tag carding its ID by turning on and off its load resistor by its ID, called load modulation. The reader tunes its magnetic field according to the information size or signal frequency transmitted to the tag. [11] Enrique Valero. (2015)

2.4.2. Backscatter RFID System



Electromagnetically Coupled Systems called backscatter systems work in the UHF and microwave frequency. The reader's antenna sends out a continuous electromagnetic wave (EM) containing AC power to the tags to energise their microchips. When communication is achieved (the tag and the reader) by changeable the amplitude of the EM waves reflected the digital data to be transmitted. Far-field backscatter systems may cause problems that do not exist in HF or LF systems. The main problem is the reflection of the reader field. It is due to a similar dimension to the wavelength used and it can cause damping or even cancellation. [12] Raad Raad. (2010)

2.4.3. Near vs Far Field Communications

Factor	Near-field	Far-field
Definition	The region between a reader antenna and one full wavelength of the magnetic field emitted by the reader's antenna	The region beyond one full wavelength of the EM waves transmitted by a reader's antenna
Field range	The magnetic induction range is calculated as $c/2\pi f$, where c is the speed of light and f is the operating frequency. Thus, as operating frequency increases, the magnetic field intensity decreases. The magnetic field decays as $\frac{1}{r^3}$, where r is the distance between the tag and reader measured along a line perpendicular to the reader coil's plane	The range of far-field systems is constrained by the amount of energy received by a tag and the sensitivity of the reader's radio to the signal reflected by the tag. The reflected signal experiences two attenuations. The first attenuation occurs when EM waves travel from the reader to the tag and the second occurs on the waves reflected by the tag. As a result, the energy of the returning signal decays as $\frac{1}{r^4}$, where r is the distance between the reader and a tag
Tag to reader communication	Amplitude modulation of magnetic field.	Amplitude modulation of reflected signals or backscattering.
Frequencies	Low Frequency (LF) , High Frequency (HF)	Greater than 100 MHz or (Ultra HF (UHF), Microwave)
Antenna	Coil	Dipole
Read range	Low ←	→ High
Complexity	Low ←	→ High
Data rate	Low ←	→ High

RFID systems operate in the Industrial, Scientific and Medical (ISM) frequency band that ranges from 100 kHz to 5.8 GHz. The above table summarises the characteristics of RFID systems based on their frequency. [13] R. Want. (2006), [14] Suzanne Smiley. (2016), [15] NATE, TONI_K, A_CAVIS. (2018)

2.4.4. Classification of the RFID systems based on their frequencies

With knowledge of RFID systems, it is time to go deeper into the different types of systems available. RFID systems use different frequency bands within which they operate: low frequency, high frequency and ultra-high frequency. [13] R. Want. (2006), [14] Suzanne Smiley. (2016), [15] NATE, TONI_K, A_CAVIS. (2018)



Criterion	LF	HF	UHF	Microwave
Frequency range	<135 kHz	13.56 MHz	860 - 930 MHz (1)	2.45 GHz
Physical coupling	Inductively-coupled systems.		Backscatter systems.	
Tag to reader communication	A tag uses load modulation to retrieve its ID and uses AM during transmissions.			
Tag characteristics	Passive		Active, passive, semi-passive	Active, passive
Communication boundary	Near Field		Far Field (2)	Far Field
Approximate read range (passive tags)	2m [14]	0.1m - 0.2m [15]	4m - 7m (3)(4)	1m (4)
Standards specifications	ISO 18000-2	ISO 18000-3 Auto ID HF Class 1	ISO 18000-6 Auto , Class 1 ID Class 0, Class 1	ISO 18000-4
Antenna components	Coil (> 100 turns) and capacitor.	Coil (< 10 turns) and capacitor.	Dipole antenna.	Dipole antenna.
Antenna technology	Air-core or ferrite-core coil	Perforated, printed, etched	Perforated, etched, printed	Printed antenna, etched
Effect on human body and water	None	Attenuation	Attenuation	Attenuation
Effect of metal	Disturbance	Disturbance	Attenuation	Attenuation
Data transfer rate	< 10 kbit/s	< 100 kbit/s	< 100 kbit/s	< 200 kbit/s
Cost considerations	A larger antenna is required as compared to other RFID systems, resulting in high tag cost.	Less expensive than LF tags. Best suited for applications that require moderate range.	UHF tags are cheaper than LF or HF tags due to recent advances in IC design.	Microwave systems are expensive as compared to LF, HF and UHF RFID systems.
Typical RFID Applications	Animal tagging, access control, vehicle identification, and container tracking in waste management.	Access control, smart cards, item tagging, ticketing, document tracking, baggage control, laundries, and libraries.	Baggage handling, toll collection and supply chain management.	Electronic toll collection, real time goods tracking and production line tracking.
No. of tags read per second	Lowest ← → Highest		← → Highest	
Tag power consumption	Lowest ← → Highest		← → Highest	
Passive tag size	Largest ← → Smallest		← → Smallest	
Orientation sensitivity	Least ← → Most		← → Most	
Bandwidth	Lowest ← → Highest		← → Highest	
(1) Japan has announced the allocation of the 950 MHz UHF frequency band (2) Recently, many UHF proponents are considering Near Field UHF band (3) Semi passive tags operate on UHF and have a range of 60-80m (4) Active tags operate on UHF or Microwave bands and have a range of more than 100m				

3.2. Programmatic Approach to Address the Problem Space

The following approach is recommended to address the cybersecurity research challenges:

- Adopt appropriate ways of exposing badges: concerning private and public tags
- Understand constraints and dependencies which concern legal and ethical considerations, required skill sets, and technology transfer.
- Implement ways of access control that not only RFID badge allows entering to building/room.

3.3. Cybersecurity Problem Space

RFID technology remains a challenging topic for many researchers. There are several studies that talk about issues related to the RFID, to understand different measures that ensure the security of the data. Challenges are related to technical problems with privacy issues. In the following points, we identify capability gaps or operational limitations of cybersecurity.

Briefly, description of each of these gaps and deficiencies as follows: [22] Jasser Al-Kassab and Wolf-Christian Rumsch. (2008).

- Technical problems - limited space for storing data inside the tag and low data processing. Another problem occurs when the coverage area of one RFID reader overlaps with another reader, which leads to signal interference and multiple reads of the same tag.
- Standardisation problems - According to researchers, there were several efforts dedicated to solve the problem of missing RFID standards, but the issue is remaining in this field. There were created different standards that coexist in parallel with a variety of interests, there is ISO 11784 utilised for tracking of RFID cattle, ISO 14443 for application of smart cards in payments, and ISO 15693 that is applied to vicinity cards. The electronic product codes (EPC) has been thinking to fill this need. The ISO 11785 for interface protocol. The fact that each of the current standards is associated with specific parts of the system makes it hard to deploy and secure data within an RFID system. Standards for tags cannot fail in with the communication standards for the typical case. Thus, it is of the highest importance to consider the compliance to standards when implementing any RFID-based solution. [23] rfidnews.com. (2009), [24] www.iso.org. (2018), [25] www.iso.org. (2019), [26] Mohamed El Beqqal*, Mostafa Azizi. (2017).
- RFID Hacking and Attacks – Technology has many advantages, like performance and facility of execution. However, those will not be useful when privacy and security are not guaranteed. The way data is stored and exchanged with the reader must be confidential. However, to make sure that the system is secured, several pentest attacks should be performed/prevented:

Typical attack	Attack description
Denial of service	The denial of service will cause an RFID system failure by spamming the reader, which will take down the system.
Cloning	Reproducing RFID tags by reverse engineering to get information from a card/tag and then duplicate it.
Tracking	Tracking people with thee, it will and track their movements as long as they are within reader range.

[27] <https://cyberops.in/>.

4. General Approach

4.1. Programmatic Approach

Trial and error is a long experience for this research to build systems that have been created by Bishopfox. It is the most effective method to establish an agile approach that enables to create an operational environment—the solution used for this experiment has been developed several years ago and it is worth checking if currently used badges are still vulnerable to be cloned. This study represents the latest thinking about cybersecurity used for RFID badges that are still in use today.

Consistent during a programmatic response to challenge during this advanced research. Use references from specific authors that believe the advice is the most relevant for cybersecurity problem described in this document. This research will manifest as a regular feedback cycle to an ongoing problem related to RFID cybersecurity researches made around the world. The materials used are only for educational and research purposes. Never attempt to break the law. Due to the COVID-19 pandemic, some additional challenges have appeared and described in the next sections of this research. Three methods used describe badge information, way to still and then clone the card.

4.2. Methodology

Hacking RFID is not as hard as people may think. Most conventional systems, some practical knowledge. UID-based access control.

4.2.1. Use of Specific Arduino and Mifare RC522 Card Reader Antenna

The Mifare Classic tag is used in many places in the world. A card uses stream cypher CRYPTO1 that has been reverse-engineered shortly after the first attack. The first method uses Arduino board, and a RC522 Card Reader/Write antenna, plus free software (code for Arduino) to copy a card is available on github.com. It shows how information is stored and methods used to dump, read and write info to the clean card. [28] Márcio Almeida. (2014).

4.2.2. Use of Proxmark3 (cheaper version bought from AliExpress)

A device called Proxmark III developed by Jonathan Westhues enables reading, copying and cloning RFID tags is a tool used by researchers. A cheaper version was used for this study as an alternative tool with functionality like the original tool. It can read, write and emulate many RFID cards. There are many forums with high skilled members that enable researchers to follow up on the hardware and software challenges.

4.2.3. Tool Development

The silent long-range RFID reader which can steal the badge information from an employee as they walk near this prototype device. It can read low-frequency RFID badge systems used for access to the buildings. The most popular are HID Prox and Indala Prox products. To read HID iCLASS which uses high frequency, a PCB is needed to enable control for this system. The goal is to create penetration tests that demonstrate the risk of the technologies used for access control. This tool can be created without electrical background, just some programming skills. [29] bishopfox.com. (n/a).

5. Case studies

5.1. Case Study 1 Introduction

The first case study was regarding a Mifare Classic card, which uses a RFID reader/writer 'RC522' bought on AliExpress. It comes with a card and a tag. The MFRC522's internal

transmitter is able to drive the reader/writer antenna designed to communicate with ISO/IEC 14443 A/MIFARE cards and transponders without additional active circuitry. The receiver module provides a robust and efficient implementation for demodulating and decoding signals from ISO/IEC 14443 A/MIFARE compatible cards and transponders. The digital module manages the complete ISO/IEC 14443 A framing and error detection (parity and CRC) functionality. [30] www.nxp.com. (2016).

5.1.1. Case Study 1 Challenges

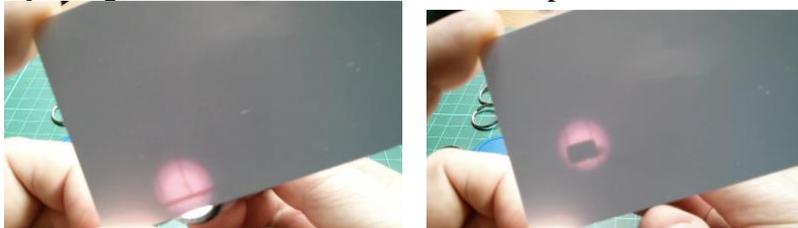
The first challenge was a broken board that I have obtained; after several days of trying different solutions, I have come across an article that describes general hardware issues related to this board. The author advised getting a new board to perform the test.

5.1.2. Case Study 1 Design of the RFID card/tag

On the side of the tag, there is a chip with two pins with metal wings and coil of wire. The coil is nicely round, approx. 20 rounds.



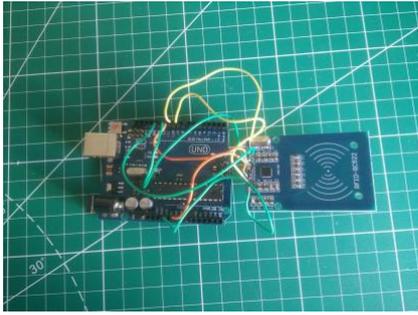
The card is reliable and extremely thin, inside there is a coil of wire around outside the card. By using touch, the coil is visible. The chip connected to the coil is embedded in the card.



5.1.3. Case Study 1 Hardware and software set-up

RFID-RC522 antenna connected to Arduino Uno that is connected to MacBook Pro by USB cable. The library used for this module has been provided by GitHub [31] Miguelbalboa and Rotzbua. (2018). This document describes the pin layout. Reader/writer using 3.3V that's Vcc = "voltage collector collector", Vss = "voltage source source" or Vdd = "voltage drain drain" were used for various additional hardware, RST that is On-RESET, GND that is ground, then we have full SPI implementation SDA, SCK, MOSI, MISO, but SPI generally uses and SS rather than SDA. [32] sparkfun.com/. (n/a). In GitHub notes it says the SDA pin might be named SS on older MFRC522 versions.

Below you can find hardware and cards used for this case study:



The MIFARE TAG's memory has 16 sectors, from 0 to 15. Each **sector** has 4 **blocks**: block 0 to block 3 and every block can store 16 bytes of **data**: from 0 to 15. 16 sectors x 4 blocks x 16 bytes of data = 1024 bytes = 1K memory. This calculation explains why it is called MIFARE 1K TAG, highlighted picture below shows the visual explanation.

```

COM4
-----
Card UID: B3 39 3D 41
Card SAM: 08
PICC type: MIFARE 1KB
Sector/Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 AccessBits
15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
Autoscroll Show timestamp Newline 9600 baud Clear output
  
```

```

COM4
-----
33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
7 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
6 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
5 23 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
4 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
3 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
2 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
1 7 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 1]
6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [0 0 0]
Autoscroll Show timestamp Newline 9600 baud Clear output
  
```

Sector Trailer is a 3rd block of each sector that contains **Access Bits**, which allow to read and write. The last 3 blocks are available for data storage; it means that 48 bytes per 64 are for own use. The Unique Identifier (UID) stored in block 0 and sector 0 it also contains an integrated circuit (IC) manufactured **data** which is highlighted above in purple. Each sector is protected by **secret keys A** and **secret keys B**, data on these tags encrypted by NXP security protocol.

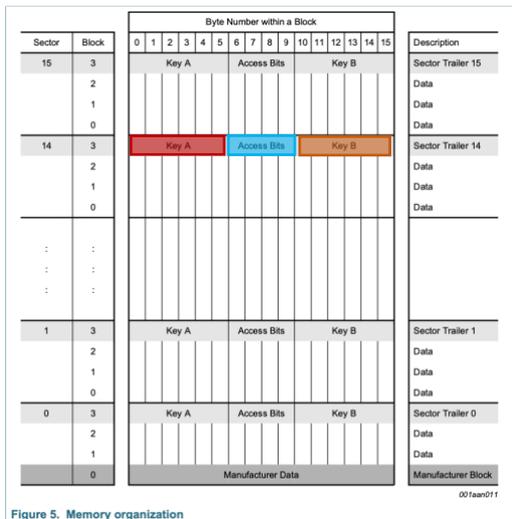


Figure 5. Memory organization

[33]www.nxp.com.

5.1.4. Case Study 1 Method used

I have installed Miguelbalboa library on the machine to read and clone cards. At first, to get information, I used code called DumpInfo. This code contains a very short, but compelling explanation and a sketch about pins. Everything is contained in 'PICC_DumpToSerial' functions. Complete description of this function is available on GitHub.com. This function allows to view dump info presented in point 5.13. In all MIFARE tags it could read UID which was available to view. The above picture shows all available cards that I have tested.

5.1.5. Case Study 1 Results of the cloning RFID (MIFARE 1K Type)

RFID Arduino based project which used RC522 Reader/Writer module. It was very low cost with a pretty easy interface, it allowed me to copy all four cards successfully. It proves that by spending less than 20 euro, there is a possibility to clone a MIFARE 1K type card.

Examples of UID from available cards:

```
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: B3 39 3D 61
Card SAK: 08
PICC type: MIFARE 1KB
```

```
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: C3 86 84 76
Card SAK: 08
PICC type: MIFARE 1KB
```

Example how to cloned UID into a magic card.

```
COM4
Card UID: B3 39 3D 61
Wrote new UID to card.
New UID and contents:
Card UID: B3 39 3D 61
Card SAK: 08
PICC type: MIFARE 1KB

Sector Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 AccessBits
15 63 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
14 59 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
13 55 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
0 3 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
0 B3 39 3D 61 D6 08 04 00 62 63 64 65 66 67 68 69 [ 0 0 0 ]
```

```
COM4
Card UID: C3 86 84 76
Wrote new UID to card.
New UID and contents:
Card UID: C3 86 84 76
Card SAK: 08
PICC type: MIFARE 1KB

Sector Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 AccessBits
15 63 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
14 59 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
13 55 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
0 3 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF [ 0 0 1 ]
2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]
0 C3 86 84 76 B7 08 04 00 62 63 64 65 66 67 68 69 [ 0 0 0 ]
```

5.2. Case Study 2 Introduction

The Proxmark3 Easy is a budget version of the Proxmark3 V2. This tool uses open source software and firmware that is available for download, but it runs only on Windows. The Proxmark3 is dedicated for RFID analysis and provides snooping, reading, emulation,

demodulation, writing, analysis, replaying, modulation, decoding, encoding, decryption and encryption of LF 125kHz – HF 13.56MHz tags. It has capabilities of reading and writing; it can analyse signals received over the air and is able to pretend to be a tag. The Proxmark3 can work in different modes: sniffing mode, emulator mode and reader mode. It can be used in various modulation schemes and protocols, when tags are in range and have a supporting frequency. Proxmark3 RDV4 can be purchased online, a ready-to-go kit can be bought for about 400 euro and a cheaper version from AliExpress for about 50 euro. The budget version is less reliable; however, for this research, it works fine. Left picture shows items available in the Proxmark3 Easy box, right picture shows all available RFID cards used for the research.



5.2.1. Case Study 2 Challenges

Windows OS is needed to use this tool, and as an owner of a MacBook I had to borrow a second-hand laptop with Windows OS that allows the use of an open source software for Proxmark3 Easy. Another challenge was the delivery of the tool, because shipping took longer than expected.

5.2.2. Case Study 2 Design of the RFID card

The 5.1.3. Case Study 1 Hardware set-up and software explains HF cards shown below.



The majority of the LF cards are from HID company and one from COTAG.

⊘ This sign indicates it failed to read the UID from the card.

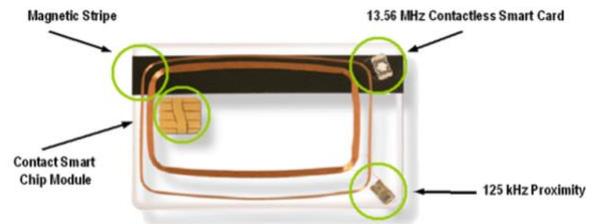
HID

The type of HID cards carries significant markings that identify unique tree characteristics about the construction and personalisation: Static Artwork - the user to identify technology: Seos, iCLASS or HID Prox card other. Dynamic Marking - Allows the user to allocate memory size or program sales number. Slot Punch - marks (dots), in either vertical or horizontal planes, identify ID-1

The data on any access card is a binary numbers of fixed length and used to determine the cardholder

Here are the most common types of cards:

- Magnetic Stripe
- Wiegand (swipe)
- 125 kHz Prox (HID & Indala)
- MIFARE contactless smart cards
- iCLASS contactless smart cards
- Many more



The four-card our card elements:

1. Static artwork identifier (©HID iCLASS, ©HID 0009P)
 - a. 000 - 125 kHz Proximity chip with antenna
 - b. 9 - Revision of chip inside the card
 - c. P - Location of manufacturing
2. Dynamic marking (4* 00123 112233445566-1)
 - a. 4* - Card formatting
 - b. 00123 – Card ID Number (UID)
 - c. 112233445566-1- Sales Order Number
3. Slot punch identifier (vertical example)
4. Contact chip UID and model (contact chip cards only)



Data Wiegand Format:

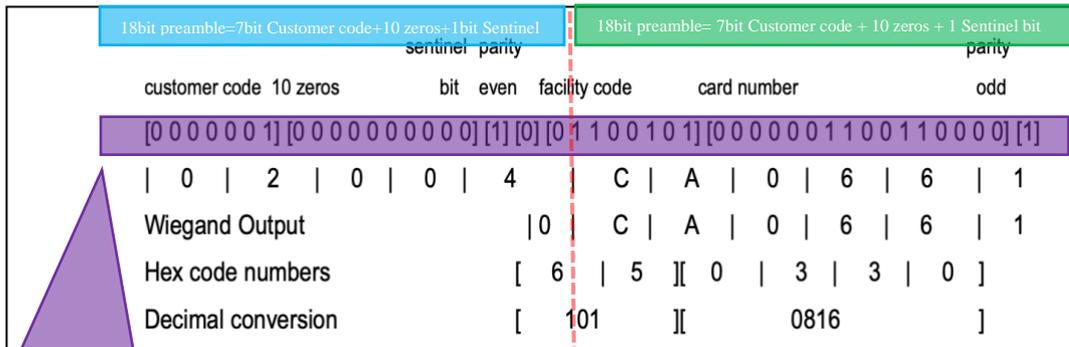
Access control readers and cards use the Wiegand format; unfortunately, the word used carelessly. Here are the basics characteristics must have a specific reader-to-card interface, a specific binary reader to the controller interface. This signal carries data, a standard 26-bit binary card data format, an electromagnetic effect and a card technology. The HID use this format as the cards use standard 26-bit format, which is very specific for binary card data that must follow specific facts:

- The number format must describe the meaning and how to use it. The number of bits indicates the formats. The length of 34-bit, 37-bit, e.tc, the size and location of each data element may change: and
 - 34-bit and 8-bit Facility code may start with bit 2.
 - 34-bit a 12-bit Facility code may start with bit 21.

Example Output [34]HID. (2017), [35]HID. (2016), [36]HID. (2014), [37]HID. (2012).

The following is an example of an ID card with the number of “816” decimal, which will be output by the MaxiProx reader, the number “02004CA0661” hex. Note: The customer c e is never transmitted or displayed: [37]HID. (2012).

10 HEX characters with leading zero drooped



44 bits on HID card = 18bit preamble + 26bit Wiegand

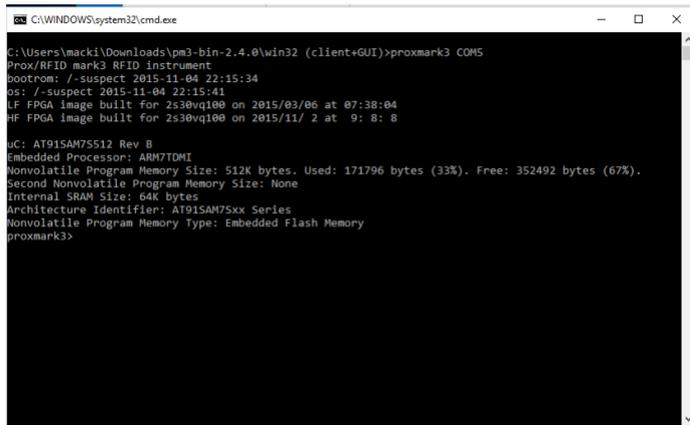
Challenging to find much information regarding COTAG cards comparing to HID. There is information regarding the types and frequency of each tag/card, however, it was not able to datasheet information. There are passive and active tags that work like other RFIDs. One of the advantages of Cotag technology is that both types of cards can be mixed in the same system to provide convenience and cost-efficiency. The card number printed on the back of the card. [38]Vanderbilt. (2017). The COTAG card needs a wake-up command of a sort which other to capture the traces; however, the message was more prolonged than 40k sample. As pre Iceman investigation it is very hard to get UID of COTAG cards it requires a real-time device to get the full repeating binary string of the card. There individualities tools are other than Proxmark3 required to decode from COTAG. [39] Contributor (2012), [40] Iceman. (2017).



5.2.3. Case Study 2 Hardware and software set-up

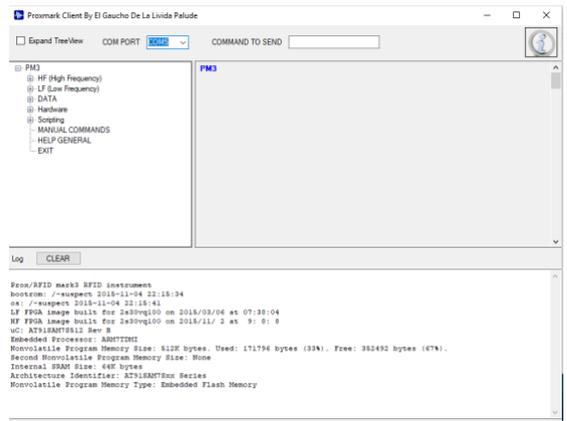
It has an integrated high-frequency HF antenna 13.56 MHz and low-frequency LF antennas 125 kHz because of its small size is used as a portable device for stealing tags UID. The tool kit contains a dual HF/LF antenna, four test cards (T5577, Mifare 1k S50, UID, and CUID compatible), USB cable showed in 5.2 Case Study 2 Introduction. The software can be downloaded from [41] www.proxmark.org. (2013). At first, a laptop should be configured and port needs to be enabled the best one is COM5 as all addons for software have this one set up as default. If this port is busy by other devices, need to go through files in the win32 (client+GUI) and set up FLASH files and GO.bat file to COM (number of your port). There are two ways to use it. 1. client by using the command line to type commands manually. 2. GUI with preselected screens that allow using commands with a graphical interface.

1. Client interface



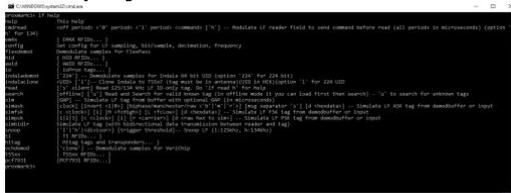
```
C:\WINDOWS\system32\cmd.exe
C:\Users\macki\Downloads\pm3-bin-2.4.0\win32 (client+GUI)>proxmark3 COM5
Prox/RFID mark3 RFID instrument
bootrom: /-suspect 2015-11-04 22:15:34
os: /-suspect 2015-11-04 22:15:41
LF FPGA image built for 2530vq100 on 2015/03/06 at 07:38:04
HF FPGA image built for 2530vq100 on 2015/11/ 2 at 9: 8: 8
uC: AT91SAM7S512 Rev B
Embedded Processor: ARM7DMI
Nonvolatile Program Memory Size: 512K bytes. Used: 171796 bytes (33%). Free: 352492 bytes (67%).
Second Nonvolatile Program Memory Size: None
Internal SRAM Size: 64K bytes
Architecture Identifier: AT91SAM7Sxx Series
Nonvolatile Program Memory Type: Embedded Flash Memory
proxmark3>
```

2. GUI

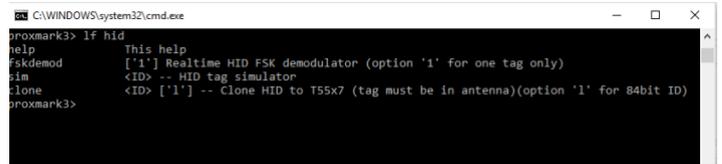


5.2.4. Case Study 2 Method used

The Proxmark3 tool connected to a laptop can use the client or laptop's GUI interface. After setting up ports and software, I had to test all cards available for this research. The client command line was more comfortable to work on and to navigate through output. The majority of the cards were readable. By using the command search' low frequency or 'hf search' high frequency checked each card to determinate type of the card. The point 5.2.2 Case Study 2 Design of the RFID card shows all cards available for this research. By typing 'lf help,' you can find all accessible commands and cards that work with proxmark3.



```
C:\WINDOWS\system32\cmd.exe
proxmark3> lf help
This help
[ ] Realtime HID FSK demodulator (option '1' for one tag only)
[ ] HID tag simulator
<ID> ['1'] -- Clone HID to T55x7 (tag must be in antenna)(option '1' for 84bit ID)
proxmark3>
```



```
C:\WINDOWS\system32\cmd.exe
proxmark3> lf hid
This help
[ ] Realtime HID FSK demodulator (option '1' for one tag only)
[ ] HID tag simulator
<ID> ['1'] -- Clone HID to T55x7 (tag must be in antenna)(option '1' for 84bit ID)
proxmark3>
```

The known command for HID card is 'lf hid' to check other available commands for that hardware: Interest in this to make a copy of it, had to use 'lf hid clone UID':



The example shows that the NCI student number is **102804**. At first, I had to put a card on proxmark3 and used 'lf search' command to get HEX number of the card which is **2184032328**, next replaced a card with blank card type T5577 and used 'lf hid clone **2184032328**' command to clone it. To check the result of the card was successfully cloned, had to used 'lf search' again (bellow screenshot).

```
C:\WINDOWS\system32\cmd.exe
proxmark3> if search
#db# DownloadPGA(len: 42096)
Reading 38000 bytes from device memory

Data fetched
Samples @ 8 bits/smpl, decimation 1:1
NOTE: some demods output possible binary
      If it finds something that looks like a tag
      False Positives ARE possible

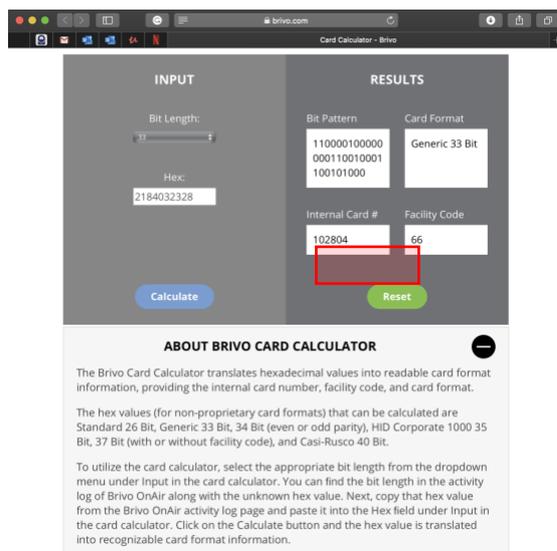
Checking for known tags:
HID Prox TAG ID: 2184032328 (37268) - Format Len: 32bit - FC: 0 - Card: 0
Valid HID Prox ID Found!

proxmark3> if hid-clone 2184032328
Cloning tag with ID 2184032328
#db# DONE!
proxmark3> if search
Reading 38000 bytes from device memory

Data fetched
Samples @ 8 bits/smpl, decimation 1:1
NOTE: some demods output possible binary
      If it finds something that looks like a tag
      False Positives ARE possible

Checking for known tags:
HID Prox TAG ID: 2184032328 (37268) - Format Len: 32bit - FC: 0 - Card: 0
Valid HID Prox ID Found!
proxmark3>
```

The last step is to make sure that the HEX ID and UID are the same. To do that, I had to go to <https://www.brivo.com/card-calculator/> and check if the number matches. In the field “HEX”, I typed “2184032328”, and from the dropdown chose 33 bit (it was the closest one to the version of the card). The result showed that Internal Card # is the same as on the back of the student card.



5.2.5. Case Study 2 Results of the cloning RFID

The Proxmark3 is currently the best tool when it comes to cloning RFID cards, as it is readily available for cloning and skimming. It is a portable platform that can both read and emulate access control tags and cards. This unit is from an open source, including hardware and software, and it can be used for educational purposes. The COTAG card can't be accessed with the Proxmark3, I would need a different type of hardware.

5.3. Case Study 3 Introduction

The RFID hacking tool developed by Bishopfox for penetration testing. [29] bishopfox.com It allows still badge information from the distances to get access to the secured building. This tool reads cards allow frequency cards 125KHZ like HID Prox and Indala Prox. The aim is to of this testing is to show how easy it is still information and clone card. There is information on online n how to create and use this tool as a pentester. Have could not find any forums or information.

5.3.1.Challenges

The challenges are similar like in Study 2 regarding a machine that the run software. Another main problem was that screen which shows the output from the cards. The first screen that been ordered was not compatible with the hardware. When realised it in May, it was already difficult to get parts from outside of Ireland. The second screen was ordered from Italy and during testing, it got burned during the experiment, on top of it Arduino board broke too. Due to pandemic COVID-19 ordering new screen was not considered as there would be not enough time for testing.

5.3.2.Case Study 3 Design of the RFID card

The cards used for this testing would be low frequency described in above 5.2.2 Case Study 2 Design of the RFID card point.

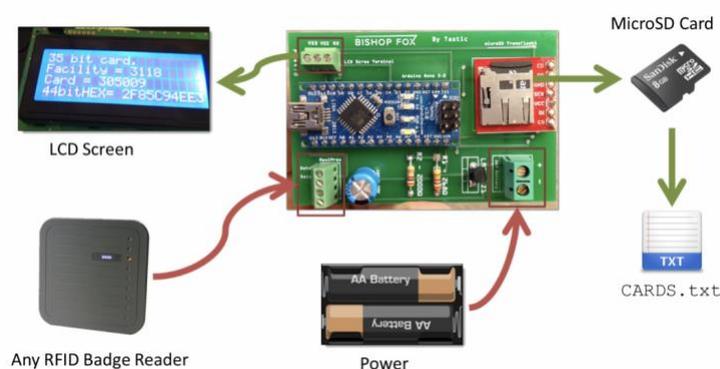
5.3.3. Case Study 3 Hardware and software set-up

I used MaxiProx 5375 bought on eBay and Arduino microcontroller to received data from the antenna. Bixopfox developed PCB in Fritzing to redundant space that would use a breadboard. To this board, connected MicroSD Card reader, Arduino Nano, set of batteries and LCD screen. All hardware is powered up by pressing the button.



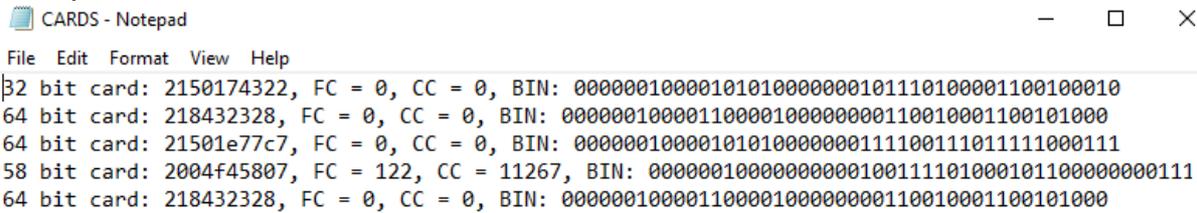
5.3.4.Case Study 3 Method used

The card reader, it is a DIY tool that should read 125KHz like HID Prox and Indala Prox. After soldering all parts, everything worked as expected except LCD. The reader takes card information, next passing them though PCB that send them to screen and microSD card. Received information on the screen: how many cards card has it. Facility code, card id and HEX number should be stored on the microSD card too. Card ID can be decoded in the same way as I did it in 5.2.4 Case Study 2 Method used, and in the end, required to use Proxmark3 to clone card based on the UID received.



5.3.5. Case Study 3 Results of the cloning RFID

My lack of soldering experience led to a burnt hardware. Another reason why it did not work correctly was that there was no battery power, however after recharge it all worked fine. Next step is to scan all available cards and check information on SD card: what bit the card is, facility code, card id and HEX number.



```
File Edit Format View Help
32 bit card: 2150174322, FC = 0, CC = 0, BIN: 00000010000101010000000101110100001100100010
64 bit card: 218432328, FC = 0, CC = 0, BIN: 00000010000110000100000000110010001100101000
64 bit card: 21501e77c7, FC = 0, CC = 0, BIN: 00000010000101010000000111100111011111000111
58 bit card: 2004f45807, FC = 122, CC = 11267, BIN: 0000001000000000010011110100010110000000111
64 bit card: 218432328, FC = 0, CC = 0, BIN: 00000010000110000100000000110010001100101000
```

The above picture shows successfully retrieved HEX and decimal information. The next steps to clone a card is to follow the 5.2.4 Case Study 2 Method.

6. Conclusion and recommendations

6.1. Conclusion

This thesis is to show that hardware available on the market allows cloning current RFID cards used for access control. Arduino and Proxmark3 Easy used in my case study cost less than 50 euro. Open source software allows to clone the card. The last remote tool that allows stealing UID card during a walk around people in the public area to steal their card info. All steps presented in this methodology describe the results of the research on how to clone an employee badge id. In 2020 this research proves that no steps taken to improve the security of HID Prox and MIFARE cards because was able to clone some of them. The cards that protect physical access to workplaces are still vulnerable to attackers that can steal cards ids to enter the building and access sensitive information. The only problem to get the information was COTAG card that required specific hardware to get data, and which was not able to find any device that can clone those cards. It proves that in case studies where HID cards were available, it is easy to clone and COTAG card can't be cloned with currently available hardware. The findings from this thesis apply to most businesses that uses these cards. Most of the companies that use these cards are not aware of vulnerabilities for this brand and type of the card. There is more work to do in case study 3, for example to re-solder parts used to make for stealing card id on the street. Then another future work will be getting aware that allows read and clone COTAG cards as was unfortunate to access information on this card, hope to finish those projects later on this year.

6.2. Recommendations

The RFID's feel weak itself as there a new theft trend called RFID skimming. Because of that trend, there was a need to introduce new wallets or sleeves to secure RFID cards. Protectors may address the data stilling and stop data collection. However, to fully ensure access control to the building, there is a need for an additional PIN or/and biometric signature to identify the owner of the card. RFID is a technology that has many benefits, and should be used as authentication for access control, but, it should be used with additional proof of the identity.

Reference:

- [1] Peter Darcy, Prapassara Pupunwiwat and Bela Stantic (2010) The Challenges and Issues Facing the Deployment of RFID Technology. Available at: <https://core.ac.uk/download/pdf/143854065.pdf>. Last accessed: 2020
- [2] Rich Handley. (2005). The History of RFID Technology. Available: <https://www.rfidjournal.com/articles/view?1338/>. Last accessed 2020
- [3] n/a. (2017). Friend or foe: securing aircraft IFF systems. Available: www.airforce-technology.com. Last accessed 2020
- [4] Krebs on security. (2014). How Secure is Your Security Badge? Available: <https://krebsonsecurity.com/2014/08/how-secure-is-your-security-badge/>. Last accessed 2020.
- [5] R. Want. (2006). An introduction to RFID technology. Available: <https://ieeexplore.ieee.org/document/1593568>. Last accessed 2020.
- [6] Wiki. (2020). Radio. Available: <https://en.wikipedia.org/wiki/Radio>. Last accessed 2020.
- [7] Wiki. (2020). Frequency. Available: <https://en.wikipedia.org/wiki/Frequency>. Last accessed 2020.
- [8] Wiki. (2020). ID. Available: <https://en.wikipedia.org/wiki/ID>. Last accessed 2020.
- [9] Chris Woodford. (08/2019). Radiofrequency (RF and RFID) tags. Available: <https://www.explainthatstuff.com>. Last accessed 2020.
- [10] (n/a). newaverfid.com/. RFID READER ANTENNA BASICS – OPTIMISING TAG SELECTION & DEPLOYMENT. Available: <https://newaverfid.com/blog>. Last accessed 2020.
- [11] Enrique Valero. (2015). Evolution of RFID Applications in Construction: A Literature Review. Available: https://www.researchgate.net/publication/278709835_Evolution_of_RFID_Applications_in_Construction_A_Literature_Review. Last accessed 2020.
- [12] Raad Raad. (2010). Dheeraj K. Klair School of Electrical, Computers, Telecommunications Engineering, University of Wollongong, Northfields Avenue, NSW, Australia; Kwan-Wu Chin; A Survey and Tutorial of RFID Anti-Collision Protocols. Available: <https://ieeexplore.ieee.org/document/5455790>. Last accessed 2020.
- [13] R. Want. (2006). An introduction to RFID technology. Available: <https://ieeexplore.ieee.org/document/1593568>. Last accessed 2020.
- [14] Suzanne Smiley. (2016). Active RFvsvs. Passive RFID: What is the Difference?. Available: <https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid>. Last accessed 2020.
- [15] NATE, TONI_K, A_CAVIS. (2018). RFID Basisc. Available: <https://learn.sparkfun.com/tutorials/rfid-basics/all#introduction>. Last accessed 2020
- [16] Dhanasekaran Raghavan. (2015). Schematic diagram of active RFID System. . Available: https://www.researchgate.net/figure/Schematic-diagram-of-active-RFID-System_fig1_283126585. Last accessed 2020.
- [17] Slawomir Jasek (2018). A 2018 practical guide to hacking NFC/RFID. Available: https://smartlockpicking.com/slides/Confidence_A_2018_Practical_Guide_To_Hacking_RFID_NFC.pdf . Last accessed 2020
- [18] Simon Hill . (03/2019). RFID-blocking products are practically worthless. Here is why. Available: <https://www.digitaltrends.com/cool-tech/are-rfid-blocking-products-worth-your-money-we-asked-an-expert/>. Last accessed 2020.
- [19] WILL OREMUS. (08/2015). The Skimming Scam. Available: <https://slate.com/human-interest/2015/08/credit-cards-passports-and-rfid-fraud-are-special-blocking-wallets-necessary.html>. Last accessed 2020.

- [20] Sid Kirchheimer. (n/a). Hands-Free Pickpocketing. Available: https://www.aarp.org/money/scams-fraud/info-01-2011/scam_alert_handsfree_pickpocketing.html. Last accessed 2020.
- [21] Krebs on security. (2014). How Secure is Your Security Badge. Available: <https://krebsonsecurity.com/2014/08/how-secure-is-your-security-badge/>. Last accessed 2020.
- [22] Jasser Al-Kassab and Wolf-Christian Rumsch. (2008). Challenges for RFID Cross-Industry Standardization in the Light of Diverging Industry Requirements. Available: <https://ieeexplore.ieee.org>. Last accessed 2020.
- [23] rfidnews.com. (2009). SO 11784/85 "STANDARD" WITH BLEMISH. Available: <https://www.rfidnews.com/ISOstandard/ISOstandard.html>. Last accessed 2020.
- [24] www.iso.org. (2018). iso14443. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:14443:-1:ed-4:v1:en>. Last accessed 2020.
- [25] www.iso.org. (2019). Iso 15693. Available: <https://www.iso.org/obp/ui/#iso:std:iso-iec:15693:-3:ed-3:v1:en>. Last accessed 2020.
- [26] Mohamed El Beqqal*, Mostafa Azizi. (2017). Review on security issues in RFID systems. Available: https://www.astesj.com/publications/ASTESJ_020624.pdf. Last accessed 2020.
- [27] <https://cyberops.in/>. (2019). New generation of the hacking RFID. Available: <https://cyberops.in/blog/new-generation-hacking-rfid-attacks/>. Last accessed 2020.
- [28] Márcio Almeida. (2014). Hacking Mifare Classic Cards. Available: <https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf>. Last accessed 2020.
- [29] bishopfox.com. (n/a). RFID-Hacking. Available: <https://resources.bishopfox.com/resources/tools/rfid-hacking/attack-tools/>. Last accessed 2020.
- [30] www.nxp.com. (2016). MFRC522 Standard performance MIFARE and NTAG frontend. Available: <https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>. Last accessed 2020.
- [31] Miguelbalboa and Rotzbua. (2018). Rfid. Available: <https://github.com/miguelbalboa/rfid>. Last accessed 2020.
- [32] sparkfun.com/. (n/a). Serial Peripheral Interface (SPI). Available: <https://learn.sparkfun.com/tutorials/serial-peripheral-interface-spi/all>. Last accessed 2020.
- [33] www.nxp.com. (n/a). MF1S50YYX_V1 MIFARE Classic EV1 1K - Mainstream contactless smart card IC for fast and easy solution development. Available: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf. Last accessed 2020.
- [34] HID. (2017). HID GLOBAL CREDENTIAL IDENTIFICATION MARKINGS. Available: https://www.hidglobal.com/sites/default/files/resource_files/an0109_a.2_credential_id_markings_application_note.pdf. Last accessed 2020.
- [35] HID. (2016). Understanding Card Data Formats. Available: https://www.hidglobal.com/sites/default/files/hid-understanding_card_data_formats-wp-en.pdf. Last accessed 2020.
- [36] HID. (2014). Card Identification Markings Application Note. Available: https://www.hidglobal.com/sites/default/files/resource_files/an0109_a.1_card_identification_markings_an.pdf. Last accessed 2020.
- [37] HID. (2012). MaxiProx® DFM Reader - 5375. Available: https://www.hidglobal.com/sites/default/files/resource_files/21737750-5375-901_e.1.1.pdf. Last accessed 2020.
- [38] Vanderbilt. (2017). Passive Cotag card without magnetic stripe. Available:

- 1.amazonaws.com/mM84sWEKujnf8kRGvmV9LCGK?response-content-disposition=inline%3B%20filename%3D%22v54501s74a1_ib958_023_01_en.pdf%22%3B%20filename%2A%3DUTF-8%27%. Last accessed 2020.
- [39] Contributor (2012). Questions and Requests» Cotag cards?. Available: <http://www.proxmark.org/forum/viewtopic.php?id=1258>. Last accessed 2020.
- [40] Iceman. (2017). Cotag Analysis. Available: <http://www.proxmark.org/forum/viewtopic.php?id=4455>. Last accessed 2020.
- [41] www.proxmark.org. (2013). pm3-bin-2.4.0 . Available: <http://www.proxmark.org/forum/viewtopic.php?id=1562>. Last accessed 2020.
- [42] Chris Woodford. (08/2019). Radio frequency (RF and RFID) tags. Available: <https://www.explainthatstuff.com>. Last accessed 2020.
- [43] James Thrasher. (2013). How is RFID Used in Real World Applications?. Available: <https://blog.atlasrfidstore.com/what-is-rfid-used-for-in-applications>. Last accessed 2020
- [44] ROBERT MCMILLAN. (2012). The Pwn Plug is a little white box that can hack your network. Available: <https://arstechnica.com/information-technology/2012/03/the-pwn-plug-is-a-little-white-box-that-can-hack-your-network/>. Last accessed 2020
- [45] Frank Thornton, Brad Haines, John Kleinschmidt. (2005). RFID Security. Available: <https://www.sciencedirect.com/book/9781597490474/rfid-security>. Last accessed 2020
- [46] Mohamed El Beqqal ; Mostafa Azizi. (2017). Classification of major security attacks against RFID systems. Available: <https://ieeexplore.ieee.org/document/7934622>. Last accessed 2020
- [47] F5 DevCentral. (2014). Elliptic Curve Cryptography Overview. Available: <https://www.youtube.com/watch?v=dCvB-mhkT0w>. Last accessed 2020
- [48] Xu Huang¹, Son Le², and Dharmendra Sharma. (2017). A Taxonomy for RFID Systems. Available: <https://pdfs.semanticscholar.org/6d73/594d0a01539c0a7348909108974388aea0e5.pdf>. Last accessed 2020
- [49] Matt Ward. (2006). RFID: Frequency, standards, adoption and innovation. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.3390&rep=rep1&type=pdf>. Last accessed 2020
- [50] Manfred Aigner (TU Graz), Thomas Plos (TU Graz), Antti Ruhanen (Confidex), Stefano Coluccini (CAEN). (2008). Secure Semi-Passive RFID Tags Prototype and Analysis. Available: <https://docplayer.net/4950927-Secure-semi-passive-rfid-tags-prototype-and-analysis.html>. Last accessed 2020
- [51] Prototype Express. . (n/a). RFID Technology White Paper. Available: <http://www.prototypeexpress.com/rfidwhitepaper.htm>. Last accessed 2020
- [52] Suzanne Smiley. (2016). 7 Types of Security Attacks on RFID Systems. Available: <https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems>. Last accessed 2020
- [53] RFIDNEWS. (n/a). SO 11784/85 "STANDARD" WITH BLEMISH. Available: <https://www.rfidnews.com/ISOstandard/ISOstandard.html>. Last accessed 2020
- [54] ISO. (n/a). ISO 24631-1:2017. Available: <https://www.iso.org/standard/63394.html>. Last accessed 2020
- [55] www.rfidjournal.com. (2017). What Is the Difference Between ISO 15693 and ISO 14443A Tags. Available: <https://www.rfidjournal.com/blogs/experts/entry?11979>. Last accessed 2020
- [56] Norbert Druml*, Manuel Menghin*, Adnan Kuleta†, Christian Steger†, Reinhold Weiss† Holger Bock*, Josef Haid*. (2014). A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6927267>. Last accessed 2020

- [57] Peter H. (2008). Chapter 16: “A Random Number Generator for Application in RFID tags”. Available:
https://www.researchgate.net/publication/226272610_A_Random_Number_Generator_for_Application_in_RFID_Tags. Last accessed 02020
- [58] Murali Kodialam. (2007). Anonymous Tracking using RFID tags. Available:
<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4215727>. Last accessed 2020
- [59] Ritu Tripathi, Sanjay Agrawal. (2014). Comparative Study of Symmetric and Asymmetric Cryptography Techniques. Available:
<https://pdfs.semanticscholar.org/e0e4/810c5276f9c05cc82425fcf911f206c52bef.pdf>. Last accessed 2020
- [60] Flavio D. Garcia Peter van Rossum Roel Verdult Ronny Wichers Schreur. (2009). Wirelessly Pickpocketing a Mifare Classic Card. Available:
<http://www.cs.ru.nl/~flaviog/publications/Pickpocketing.Mifare.pdf>. Last accessed 2020
- [61] Ju Wang, Srinivasan Keshav. (2018). RFID Hacking for Fun and Profit-ACM MobiCom. Available:
https://www.researchgate.net/publication/326560663_Challenge_RFID_Hacking_for_Fun_and_Profit-ACM_MobiCom. Last accessed 2020
- [62] Qinghan Xiao. (2009). RFID Technology, Security Vulnerabilities, and Countermeasures. Available:
https://www.researchgate.net/publication/221787702_RFID_Technology_Security_Vulnerabilities_and_Countermeasures. Last accessed 2020
- [63] Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. (2012). Tutorial: Proxmark, the Swiss Army Knife for RFID Security Research. Available:
https://www.cs.bham.ac.uk/~garciaf/publications/Tutorial_Proxmark_the_Swiss_Army_Knife_for_RFID_Security_Research-RFIDSec12.pdf. Last accessed 2020
- [64] adc.bmj.com. (2018). How to do a postgraduate research project and write a minor thesis. Available: <https://adc.bmj.com/content/103/9/820>. Last accessed 2020.
- [65] www.impinj.com. (). Various Systems Using RAIN RFID Technology. Available:
<https://www.impinj.com/about-rfid/types-of-rfid-systems>. Last accessed 2020.
- [66] RFID.... (). ieeexplore.ieee.org. Available:
https://ieeexplore.ieee.org/search/searchresult.jsp?queryText=An%20introduction%20to%20RFID%20technology&highlight=true&returnFacets=ALL&returnType=SEARCH&ranges=2006_2006_Year. Last accessed 2020.
- [67] Todd Brooks. (2017). CLEARING UP THE CONFUSION FOR YOUR CREDENTIAL OPTIONS. Available: <https://cdn.ymaws.com/naccu.org/resource/collection/7C00E2DA-261A-4BFB-B240-A23790C712BC/03-ClearingUpConfusionForCredentialOptions.pdf>. Last accessed 2020.