Evaluation of the feasible attacks against RFID tags for access control systems

Hristo Dimitrov and Kim van Erkelens
University of Amsterdam

February 10, 2014

Abstract. RFID is a commonly used protocol for access control systems that provide physical security for buildings. The RFID tags used in such a system are often vulnerable for various attacks. In this paper we present an evaluation of those attacks that can be used for the assessment of access control systems. Different implementations of the ISO/IEC 14443 standard for high frequency tags as well as the low frequency tags are examined. Recommendations are given about performing an assessment on different types of systems.

Acknowledgements

We would like to thank our supervisors, Pieter Westein, Jochem van Kerkwijk, and Henri Hambartsumyan, for their support and feedback during this research. We are also grateful for the translation of the Chinese manual by Kevin Cheung. Niels Sijm and Mick Pouw were so kind to borrow us their RFID equipment. We want to thank Gijs Hollestelle for providing information about the Proxmark. And we are grateful to all of the peer reviewers, Pieter Westein, Inge Teunissen and Herbert van Erkelens, who gave their feedback on draft versions of this report.

Contents

1 Introduction

Radio Frequency Identification (RFID) is a commonly used protocol for access control systems, and is also used various application areas such as tracking animals or tracking products in the supply chain. Access control systems are used for physical security of office buildings, companies, factories, home accommodations and public buildings. An access control system consist of a card reader, called the Proximity Coupling Device (PCD), and Proximity Integrated Circuit Cards (PICCs). PCDs are further referred to as readers, and PICCs are further referred to as (proximity) cards or RFID tags.

The most commonly used proximity cards are the MIFARE Classic and the MIFARE DESFire. Many studies have shown the weaknesses in the MIFARE Classic [1–5]. Also, for the more secure MIFARE DESFire several attacks were conducted successfully [6]. Other research classified the known attacks against RFID [7].

Those studies showed the weaknesses in the underlying technology, but little research has been done into the practical application of these attacks for actual physical access control systems. Pawel Rotter [8] proposed a framework for assessing RFID system security and privacy risk. The framework doesn't consider all the technical aspects that are involved with assessing an RFID system, but merely describes the threats.

This study is an evaluation of attacks for assessing the security of a RFID access control system. The focus is on both the high and low frequency tags that are used in such a system. The high frequency tags that are examined are the MIFARE Classic, DESFire, and UltraLight, which are based on the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 14443 standard. The low frequency tags that are investigated are HID (ProxCard) and EM410x. The feasibility of performing various attacks is researched. Examples of attacks are: key retrieval, emulating and cloning.

This report is organized as follows. Chapter 2 states the research questions for this study. The related work towards attacks on RFID access control systems are firstly introduced in chapter 3. Chapter 4 describes the theoretical background for the study. In chapter 5 the methodology is proposed, which leads into our approach. In chapter 6 the findings are presented and are discussed in chapter 7. The conclusion is presented in chapter 8. Also, a proposal for further research is given in this chapter.

2 Research questions

The focus of this research is on testing of the feasibility of known attacks against RFID access control systems and translate it into guidelines for assessing such a system. Therefore the following research question is defined:

Where should one focus on when performing a security testing of an implementation of an RFID access control system?

In order to answer this research question, the following sub-questions are defined as guidelines:

1. What are known attacks against various types of RFID access control systems?
2. How feasible are those attacks and what kind of threat do they introduce?
3. What is the applicability of these attacks for different types of systems?

3 Related work

A study that investigated known RFID attacks is performed by Mitrokotsa et al. [7]. They developed a classification of RFID attacks by structuring the most common attacks into layers. For each attack features and countermeasures are described.

Research focused on the MIFARE Classic is performed by Tan [5]. He investigated three types of practical attacks: key recovery from intercepted authentication, card emulation, and key recovery using the card only. The attacks were launched successfully on two real-world case studies with the use of widely available tools.

The Digital Security research group of the Radboud University Nijmegen performed several studies about the MIFARE Classic. Among these studies Hancke et al. [9] described a practical approach for eavesdropping, unauthorized scanning and relay attacks. The type of RFID token used is ISO 14443-A. This work mainly focuses on the RF communication interface. Both passive as well as active eavesdropping are examined. Active eavesdropping involves the use of a malicious reader and is performed over a longer distance.

Garcia et al. [4] described two attacks for retrieving the secret key from a genuine reader. One of the attacks can be performed successfully with just one or two authentication attempts. When communication is eavesdropped, these attacks can be used to decrypt the traffic. After successful decryption it is possible to clone the card. Garcia et al. [3] also proposed four attacks against the MIFARE Classic that can be executed directly against the tag. Nested authentication is one of the card-only attacks proposed. Courtois [1] described a similar attack. The result of these attacks are the retrieval of encryption keys.

Practical attacks against the MIFARE DESFire (MF3ICD40) are demonstrated by Oswald and Paar [6]. They developed methods to break the mathematical secure cipher Triple-DES (3DES) that is used by the MIFARE DESFire. The paper demonstrates the recovery of the secret 112-bit secret key by performing two side channel attacks, namely power analysis and templates, with the use of low cost equipment.

Issovits and Hutter [10] investigated various methods for exploiting weaknesses of the ISO/IEC 14443 protocol regarding relay attacks. Three different mechanisms of the protocol were exploited. These mechanisms allow for extending the time and can be used for the relay attack, which increases its success rate. Weiss [11] researched different architectures for performing a relay attack. These set-ups are using two Near Field Communication (NFC) mobile phones, two USB NFC devices or a combination of an NFC mobile phone and an USB device.

4 Background

Relevant background information for this study includes RFID techniques and implementations, attacks against RFID tags, and equipment used for attacks.

4.1 RFID techniques

RFID systems can be divided according to the frequency band in which they operate: low frequency, high frequency and ultra-high frequency. Table 1 contains the ranges, in terms of kHz and MHz, for each frequency.

Frequency	**Range**
Low Frequency (LF)	124-134 kHz
High Frequency (HF)	13.56 MHz
Ultra High Frequency (UHF)	866-915 MHz

Table 1: RFID frequencies operating at kHz and MHz

The standard that is relevant for access control systems is ISO/IEC 14443. This standard for high frequency systems is split into four parts: 1. Physical characteristics, 2. Radio frequency power and signal interface, 3. Initialization and anti-collision, and 4. Transmission protocol. Cards may be of Type A or Type B. The differences between these types are mainly in the modulation methods, coding schemes and initialization procedures [12].

Although low frequency tags are used in access control systems, no specific standards are aimed at it.

4.2 RFID implementations

Many implementations of RFID and ISO/IEC 14443 exist. NXP developed the widely used MIFARE chips, which are based on ISO/IEC 14443 Type A. HID Global is a leading manufacturer for high and low frequency cards including iClass, MIFARE, Hitag, LEGIC and ProxCards. We describe the card types that are used in this study, including the most relevant security features.

4.2.1 Low frequency tags

HID cards are low frequency cards which are simpler than high frequency ones. There is no encryption on those cards, only an ID number. This number is sent to the reader and verified by the system if access is allowed [13].

EM410x tags (4100/4102/4105) are developed by EM Microelectronic. These tags are not in production anymore. However, the successor EM4200 is still backwards compatible with EM410x systems. EM410x tags are using the proprietary EM4100 protocol [14].

4.2.2 High frequency tags

The MIFARE Classic card supports part 1, 2 and 3 of the ISO/IEC 14443A. There are two implementations of the MIFARE Classic card namely, the 1K and the 4K. The 1K card contains 1024 bytes of storage divided into 16 sectors as shown in figure 1, and the 4K card contains 4096 bytes divided into 40 sectors. The layout of the 4K cards are similar to that of the 1K cards, only 8 of the 40 sectors are larger ones. They are organized into 16 blocks instead of 4.

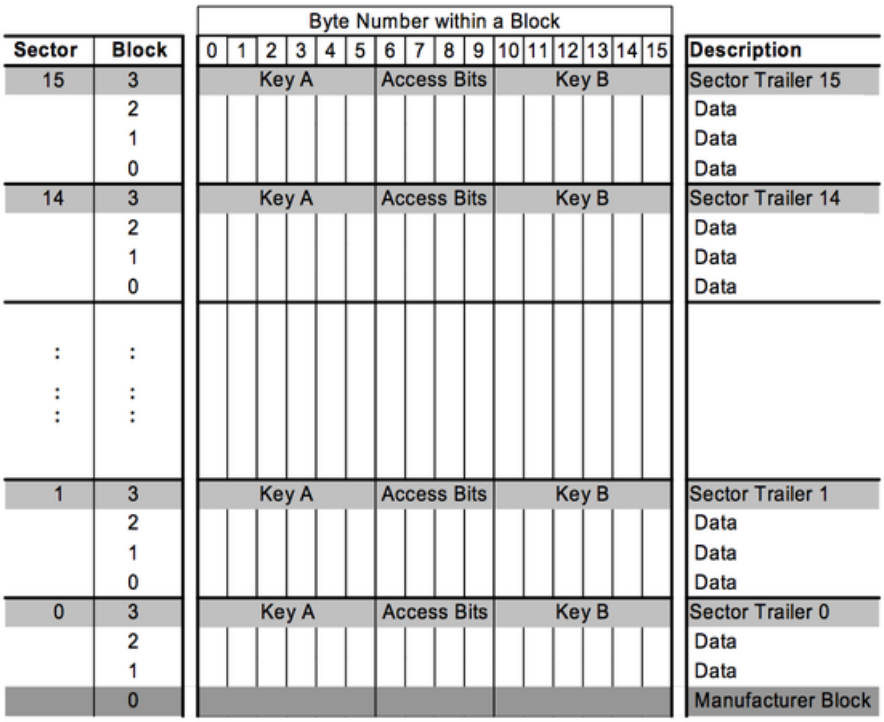

Figure 1: Sector layout of the MIFARE Classic 1K tag[15]

For the encryption of each sector, two sector keys are used. In figure 1 these are named Key A and Key B. Along with the access bits of the sector, these keys are stored in the last block, namely the sector trailer. The access bits define the permitted operations on the sector depending on which key is used.

Besides encryption, the data sheet from NXP describes two other security features of the MIFARE Classic cards. The first one is mutual three pass authentication. In this process random numbers are generated by both the card and reader to verify the responses that are sent. The second security feature is the manufacturer block, which is programmed by the manufacturer with a 4-byte Non-Unique IDentifier (NUID), and is write protected [16]. It is not required to use these security features. Thus it depends on the manufacturer if the features are actually used.

The MIFARE DESFire is a more secure tag than the MIFARE Classic. The cards support all four parts of ISO/IEC 14443A, and uses 3DES or AES as cryptographic protocol. Different variants of the cards are available. The oldest MIFARE DESFire (MF3ICD40) uses 3DES and contains 4 KB of storage. It has two successors, namely the MIFARE DESFire EV1 and EV2. Those cards support AES and have additional security features. One feature that is relevant for this research is the proximity check of the EV2 card [17]. This offers protection against the relay attack that is described in section 4.3.4.

The MIFARE UltraLight is often used for disposable tickets for events or public transport. The card does not use encryption. Its security relies on one-time-programmable (OTP) bits and write-locks. The next generation of the UltraLight, EV1, offers additional protection against cloning by the use of signature checking. Another variant of the UltraLight, the UltraLight C, also offers clone protection, but it uses 3DES for this purpose [18].

4.3 Attacks

This research is about access control systems, so the focus will be on attacks which are more relevant to gaining access to a restricted area by either cloning or emulating an access tag or by relaying the communication to a reader. There are multiple known attacks which aim at those goals. They are described in the following sections.

4.3.1 Key Retrieval and Nested Attack

There are a couple of ways to retrieve the keys for a MIFARE Classic tag. The main idea is that if one manages to get one of the sector keys of the tag, then a so called Nested attack can be used to get all of the rest of the sector keys[19]. The Nested attack makes use of a weakness in the Crypto1 algorithm[4] which is used in the MIFARE Classic tags. The flaw in the algorithm is related to the weak random generator which is being used, however a detailed explanation about the attack is not in the scope of this study. In 75% of the cases, the MIFARE encryption uses one or more of the default MIFARE sector keys [20]. If one of those keys is found, a cryptographic nested attack can be performed in order to recover the other sector keys.

Default Keys The fastest way to retrieve one or more of the sector keys for a MIFARE Classic tag is to perform a Default Key attack[20]. When being produced, the sectors of a MIFARE Classic tag are protected by a set of default keys. This is done so that the tag can be easily initiated. During this initialization the default keys should be changed. However, in most of the cases when such tags are being written to, one only changes the keys to the sectors of the tag, which are being used and those which are still blank are left with the default keys. The default key attack will try all of the default keys on all of the sectors of the tag and check if any of those sectors is left with its default key.

DarkSide Attack If there are no default keys left on a MIFARE Classic tag, one can perform a DarkSide attack in order to find the A key for sector 0 of the tag[3].

Snooping and MFKey There is also a third way to recover a key of a MIFARE Classic tag, in case none of the above methods works. By snooping the communication between the valid tag and the authenticating reader. A valid and complete authentication[4] must be recorded in order for this attack to work. If such a conversation is recorded, there are five values which need to be extracted and passed to the so called MFKey tool. Those values are the Unique Identifier (UID) of the tag, the challenge nonce NT from the tag, the challenge nonce NR from the reader, the answer to the challenge of the tag AR and the answer tho the challenge of the reader AT. The MFKey tool will then use them to recover the A key for sector 0 of the tag.

4.3.2 Tag Emulating

There are a couple of methods which prevent the data from a RFID tag to be read. One of them is by using encryption. In order to read the encrypted data, one must have the keys. Another method is by using Access Control bits[2], which can restrict the reader from reading specific data sectors. If all the data of an RFID tag can be read, then the tag can be emulated by a device. When presented to a reader, the antenna of the device will react as if it is the actual tag, thereby fooling the reader that a valid tag is presented to it.

4.3.3 Tag Cloning

Tag cloning is similar to tag emulating, but instead of emulating the valid tag using a device after the data has been dumped, a clone of the valid tag is being created. This is done by writing the dumped data to another special fully writable tag. Normally not all tags support writing to all of their sectors so a special writable tag is needed, which will allow for a complete overwriting of all of its sectors. For example normal MIFARE Classic tags do not allow for rewriting of the 0 sector, where the UID of the tag is being stored. However, a special writable UID MIFARE Classic tag can be bought, which allows for changing the UID of the tag.

4.3.4 Relay attack

A relay attack is a type of Man in the Middle attack in which authentication is achieved by routing authentication traffic between a valid reader and proximity card through a communication channel. A malicious NFC device reads a proximity card, sends its data to a card emulator at reader's side, which can get successful access by emulating the original card. In contrast with the other attacks described, it is not needed to retrieve any keys for performing the relay attack.

An important aspect of the attack is timing. The round trip time of the packets depends on the physical distance of the NFC devices. A relay attack will fail when the time between a request and response exceeds the maximum time that is set during the initialization phase. If part 4 of ISO14443-A is supported by the card, then the attacker can request more time from the reader by modifying the timing value in the response packet [21].

4.4 Equipment for RFID attacks

Various attacks are possible with an USB NFC reader, which costs about 40 dollar. For more advanced attacks a device called Proxmark 3 can be used. This small device costs about 400 dollar and is designed for eavesdropping and emulating tags. It can be used with low and high frequency antennas. In comparison with an NFC reader, the Proxmark can be used in stand alone mode, because it contains its own operation system. Another advantage is that commands are executed on the operating system itself which results in a faster response time [22].

For the Proxmark there is an active open source community, and the soft- and firmware is continuously in development. For communicating with NFC readers and other NFC devices an open source library, called libnfc, is available. Provided with the library are several example scripts for performing various attacks. There is a difference in the attacks that the devices can perform. For snooping on the traffic between a reader and tag, the antenna from the Proxmark is needed. NFC readers in combination with libnfc are recommend for performing relay attacks as written in related work.

In order to clone an RFID tag, writable tags are needed. There are different types of writable tags. Some of them have a writable UID which makes them more suitable for cloning.

The aforementioned devices are useful for logical attacks, but when more advanced attacks, such as side channel and physical attacks need to be performed, special equipment is needed. The cost of that kind of equipment is a lot higher, and can range from $5K till $100K.

5 Methodology

In this chapter, the hardware and software used is described first. Next, the approach for the experiments is explained.

5.1 Hardware and software

The hardware used in this research consists of access control systems and RFID devices. These devices are used with software that is developed for attacking RFID systems.

5.1.1 Access Control Systems

The access control systems that are examined are two real-world systems and two experimental systems (Table 2). Demo Kit 1 was setup with a wall reader and a door lock by using the management software that was provided by the manufacturer. Three users were created, and were granted access to the doors. Demo Kit 2 was setup with the numeric keypad on the system.

System	Description	Supported tag types
System A	External Company 1	MIFARE Classic 1K
System B	External Company 2	HID
System C	Demo Kit 1	MIFARE Classic 1K and DESFire
System D	Demo Kit 2	EM410x

Table 2: An overview of all the access control systems that were used throughout this research.

Besides the tags that belonged to the above-mentioned systems, another set of tags was used for testing the attacks. All these tags were numbered to be able to refer to these when describing the findings (Appendix A).

5.1.2 RFID devices

Two types of RFID devices are used in the experiments: the Proxmark III and two ACR122 NFC readers. The Proxmark was used with a high frequency and a low frequency antenna. The devices were connected to a Kali Linux virtual machine. Revision 840 of the Proxmark software was installed in accordance to the steps explained on the Proxmark Wiki [23]. Also the firmware was upgraded with this version as explained on the same Wiki [22]. Libnfc 1.7.0 was compiled with the pcsc drivers for the ACR122 as described on the Libnfc forum [24]. The latest versions of both mfoc and mfcuk, 0.10.7 and 0.3.8 respectively, were used.

For the relay attack each of the two NFC readers were connected to a laptop, and the laptops were connected to a switch. For initializing the TCP connection Socat was used. The scripts used for the relay attack are part of libnfc.

5.2 Approach

First the approach for testing the access control systems is explained. After that, the way of classifying the attacks is described.

5.2.1 Attack steps

For each system all the possible logical attacks were examined. For the systems that made use of MIFARE Classic tags the following steps were performed:

1. Retrieve one or more keys by:
   (a) Checking for default keys;
   (b) The DarkSide attack;
   (c) Snooping.
2. Retrieve all of the keys with the nested attack;
3. Emulate the tag with the Proxmark;
4. Clone the tag;
5. Perform a relay attack.

The only attacks that are applicable for the low frequency tags are emulation and cloning of the tag. For the HID tags both of them were tested, and for the EM410x tags only the emulation is tested, because writable EM410x tags are needed for cloning. Most of the attacks were performed according to the information provided by Proxmark [25].

5.2.2 Classification of attacks

Every attack has characteristics that determine the feasibility of the attack. Those characteristics were stated as follows:

- **Time** - What is the time needed for the attacker to conduct the attack?
- **Knowledge and Skills** - What is the required experience that the attacker must have in order to conduct the attack?
- **Resources** - What are the costs that the attacker will need to pay and the equipment that he/she will need in order to conduct the attack?
- **Success Rate** - What is the chance that the attack will be successful?
- **Requirements** - What does the attacker needs in order to conduct the attack?

For the time, knowledge and skills, and the success rate three different levels were defined. The levels for each attack were determined based on the results from the experiments and the theoretical background.

6 Findings

The main purpose of the performed attacks in this research was to gain access to a restricted area by tricking an RFID reader that the real RFID tag with access rights is presented to it. In order to achieve that, three scenarios were examined.

The first scenario is to clone an RFID tag, which has the needed access rights and use the clone to open the respective gate. For this attack to succeed, the attacker needs to have access to a valid RFID tag in order to copy the content of that tag and if the tag uses cryptography for protecting the content, also to find the needed keys. Finally the whole content is written to a writable tag from the same type, which is presented to the authenticating reader for gaining the needed access.

The second scenario is to emulate a valid RFID tag. It is similar to the first scenario in terms that the content of the tag still needs to be retrieved, but the difference is that they are not written to a clone tag, but instead another tag reader is used to emulate the valid RFID tag. This lowers the cost of the attack, since no writable tags are required.

The third scenario is to relay the traffic between the authenticating reader and the valid tag. The advantage of this scenario is that it just forwards the traffic between the reader and the tag, so no dumping of the content of the tag is needed. Because of that it should work with any tag, no matter how strong its cryptographic algorithm is.

The summarized results from the performed attacks on each of the test tags are presented in Appendix B.

6.1 Key Retrieval

In order for an RFID tag to be cloned or emulated, its content needs to be retrieved. For tags like MIFARE UltraLight, EM410X and HID tags which do not implement security this method is rather straight forward. However, for tags like MIFARE Classic or MIFARE DesFire this is not the case. The content of those tags is cryptographically protected, so in order for it to be retrieved, the correct sector keys need to be known. The MIFARE DesFire tags make use of 3DES which is currently considered a secure algorithm[6] and there are no know serious implementation flows for retrieving the keys of a MIFARE DesFire tag[6]. Therefor this research only looks at key retrieval for MIFARE Classic tags.

6.1.1 Default Keys

During the default keys attack we look if the RFID tags contain one or more default manufacturer keys. This differs from implementations.

In table (Table 3) an overview is presented showing the ID of the tag and whether the default keys attack was successful or not. On all RFID tags, the Default Keys attack was successful retrieving one or more default keys.

We also noted that some of the tags had default keys set for all of its sectors. For example the tag of system A only used default keys. In that case it is not necessary to perform any other attacks for finding the keys. However, to compare the results we performed all the attacks on this tag too.

Tag	Status
6	SUCCESSFUL
7	SUCCESSFUL
8	SUCCESSFUL
10	SUCCESSFUL
11	SUCCESSFUL
12	SUCCESSFUL
13	SUCCESSFUL
14	SUCCESSFUL
17	SUCCESSFUL
18	SUCCESSFUL
19	SUCCESSFUL
20	SUCCESSFUL
21	SUCCESSFUL
22	SUCCESSFUL
29	SUCCESSFUL

Table 3: Results from the Default Keys attack for all MIFARE Classic tags.

6.1.2 DarkSide Attack

Only the Proxmark tool was used for testing the DarkSide attack. It successfully recovered the A key for sector 0 of 10 out of the 15 tags on which it was tested (Table 4). For the other five the system started hanging so we were forced to abort it before we were able to get any result. No error messages were displayed, instead it seemed more like a bug, an infinite loop or a thread deadlock in the Proxmark software code.

Tag	Status
6	NOT SUCCESSFUL (Hanging)
7	NOT SUCCESSFUL (Hanging)
8	SUCCESSFUL
10	NOT SUCCESSFUL (Hanging)
11	NOT SUCCESSFUL (Hanging)
12	SUCCESSFUL
13	SUCCESSFUL
14	NOT SUCCESSFUL (Hanging)
17	SUCCESSFUL
18	SUCCESSFUL
19	SUCCESSFUL
20	SUCCESSFUL
21	SUCCESSFUL
22	SUCCESSFUL
29	SUCCESSFUL

Table 4: Results from the DarkSide attack for all MIFARE Classic tags.

6.1.3 Snooping and MFKey

The Snooping and MFKey attack requires a valid authentication between a MIFARE Classic tag and a reader. Only systems A and C were using MIFARE Classic tags, so this attack was only tested on tag 14 for system C and on tag 22 for system A. For performing the snooping with the Proxmark tool, the High Frequency antenna needs to be placed between the tag and the reader, this is not very feasible for the attacker, but if a more powerful antenna is used, the snooping can be performed from a distance. Even though during this research the antenna was placed in the middle of the transmission, there were still some problems with capturing all of the traffic. Sometimes the Proxmark would only capture traffic from one source, either only from the tag or only from the reader. We were able to boost the power of the antenna a little by pushing a switch on the antenna itself. This gave better capture results, but still some messages were not captured and there were a few flipped bits in the captured messages. After multiple attempts on both systems, a complete authentication handshake was captured between a reader from system C and tag 14. The challenges and answers were extracted and passed to the MFKey tool along with the UID of the tag and the A key for sector 0 of the tag was returned. However, we were not able to record a complete authentication handshake for tag 22 (Table 5).

Tag	System	Status
14	C	SUCCESSFUL
22	A	NOT SUCCESSFUL (Could not capture the entire authentication handshake)

Table 5: Results from the Snooping and MFKey attack for MIFARE Classic tags.

6.1.4 Nested Attack

The nested attack was tested on all of the available MIFARE Classic cards. It was performed with varying success with both the Proxmark and the NFC reader (Table 6). When performing the nested attack on MIFARE Classic 4K tags, the Proxmark software freezes after finding all the keys. It failed to print the summary of the results and to generate the dumbkeys.bin file which is used for dumping of the content of the tags. This was because of a bug in the current revision of the Proxmark software[26]. However, all of the found keys were present in the console output up to that point. In order to make use of those keys, they needed to be extracted from the output, arranged in the correct order and placed in a binary file. For that purpose a Perl script was created (Appendix C), which takes as an input the console output from the nested attack and returns a string with all of the keys in the correct order. That string can afterwards be copied to a binary file which will then be used by the dump command to access all the sectors of the corresponding tag.

The results from the Nested attack tests were not very consistent. So we decided to look deeper in to what went wrong. The Nested attack when performed withe the NFC reader was only successful for tags 6, 7 and 11. Actually those were the only three tags that had only default keys for all of their sectors. If we now take a look at the implementation of the Nested attack for the NFC

Tag	Proxmark3	NFC ACR122 Reader	Status
6	Successful	Successful	SUCCESSFUL
7	Successful	Successful	SUCCESSFUL
8	Successful	Error: I/O error	SUCCESSFUL
10	Error: Sending bytes to proxmark failed	Error: I/O error	NOT SUCCESSFUL
11	Error: Sending bytes to proxmark failed	Successful	SUCCESSFUL
12	Successful	Error: I/O error	SUCCESSFUL
13	Successful	Error: I/O error	SUCCESSFUL
14	Error: Sending bytes to proxmark failed	Error: I/O error	NOT SUCCESSFUL
17	Successful	Not Tested	SUCCESSFUL
18	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
19	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
20	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
21	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
22	Successful	Not Tested	SUCCESSFUL
29	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL

Table 6: Results from the Nested attack for all MIFARE Classic tags.

reader, we can see that it is actually a combination of three different things. The NFC reader will first perform the Default Key attack, then it will use one of the found keys to run the Nested attack in order to retrieve the rest of the keys and finally it will dump the data from the tag using the found keys. However if all of the keys are default, there will be no need of running the Nested attack so the nfclib software will skip it and directly start the dumping. Se even though the command for the attack was successful and the content was dumped, the Nested attack was never performed successfully with the NFC reader.

Then we looked into the error that the Proxmark kept displaying when running the Nested attack on tags 10, 11 and 14. There was nothing obvious that distinguishes those three tags from the rest. The error message "Sending bytes to proxmark failed" suggests that there was something wrong with the set up, rather than a security feature of the tag which prevented the the Nested attack from working. We were able to find out that by manipulating the distance between the tag and the Proxmark antenna, sometimes the error would disappear and the Nested attack would start working. The position of the tag had to be precisely on the border of the reachable proximity of the antenna. Unfortunately we were not able to stabilize the connection throughout the entire execution of the attack.

Based on those findings, we can summarize that the: NFC reader was not able to perform a Nested attack on any of our MIFARE Classic tags. And the Proxmark is capable of executing the attack on all of the tags, but sometimes it runs into problems with the communication between the reader and the tag, which can probably be overcome by using a different antenna or adjusting the software. Further we remark that the Proxmark currently has a bug in its software, which prevents it from creating the dump file with all of the found keys only for 4K MIFARE Classic tags.

6.2 Tag Dumping

The dumping of a tag is not an attack, but rather reading the entire data stored on the tag including its UID.

A dump command was performed to all of the MIFARE Classic tags once their keys were retrieved. The command was successful on all of the tags except for anonymous and personal OV chipcards (Appendix B). The Proxmark returned an Access Control error when the dump command was performed on those tags. Apparently this was because the OV chipcard system has added an extra layer of security by using the Access Control bits which are located between keys A and B in the forth block of each sector of the card. Due to the limited time of this research, there was no further work done on attacking this extra layer of security.

All of the MIFARE UltraLight and Low Frequency tags used in this research were read without any problems.

6.3 Tag Emulating

6.3.1 Emulating of MIFARE Classic tags

The emulation of a MIFARE Classic tag was tested on systems A and C (Appendix B). Only one tag was tested per system, since the response of the reader to the emulating device was what is interesting. After dumping tag 22 for system A, it turned out that none of its data sectors were used, they were all empty. The system only performed the authentication handshake and checked the UID of the tag. Therefor the tag for this system could have been easily emulated without needing to know the keys for all the sectors, but just its UID and the keys for sector 0. However, after emulation with the Proxmark of tag 22, the authentication reader did not respond in any way to the presented emulating antenna. Since the dumped data from the tag were correct and the reader did not show any activity, something must have gone wrong with the emulation. When the same emulation was presented to the NFC reader however, it was able to read the UID of the tag. Most likely the problem with the reader from system A was related to the power of the emulating antenna. If the response from the emulating antenna has a different power than what a normal tag would have, then the reader may be able to detect that and ignore the response. However due to lack of time, we were not able to confirm that theory. It could also have been a Proxmark software bug. The tag from system C was making use of the encrypted data sectors. All of those sectors were dumped and emulated successfully. The reader from system C performed a successful authentication handshake withe the emulating Proxmark and gave access to the restricted area.

6.3.2 Emulating of Low Frequency tags

Emulation of low frequency tags was performed on systems B and D. The emulation with the Proxmark of the low frequency HID tag from system B was successful and the reader gave access to the restricted area. When emulating EM410x tag 31 on system D however, the reader did not indicate any activity. This was the same as in the case of emulating tag 22 for the system A reader. Although the antenna was different, maybe the cause of the problem was the same.

6.4 Tag Cloning

The cloning of MIFARE Classic tags was done using a writable UID tag and was successful for both tag 13 of system C and tag 22 of system A. The readers of both systems could not distinguish between the real tag and the clone and gave access to the restricted area. The cloning of the low frequency HID tag 23 from system B was performed on a writable HID tag and was also successful. The reader from system B read the number of the tag and gave access to the restricted area. For the cloning of MIFARE UltraLight tag 24 there was no fully writable MIFARE UltraLight tag. Hence tag 9 was used to be the clone. However because of the specifications of MIFARE UltraLight only the unlocked data sectors could be overwritten, thereby making only a partial copy of the valid tag. No further investigation was done on cloning MIFARE UltraLight tags, because of time restrictions.

6.5 Relay Attack

The relay attack is tested with the cards of system C, but could not be performed successfully on the first try. We think this is due to a software problem. However, we can still define the feasibility of this attack based on the experience obtained with the experiment and work done previously by others. From previous work it becomes clear that a successful attack depends on the implementation. Part 4 of ISO 14443 describes the configuration of time outs for PCDs as described in section 4.3.4. Because this last part is only supported by DESFire tags and not Classical ones, the success rate for DESFire systems is higher.

7 Discussion

7.1 Key Retrieval

7.1.1 Default Keys

The Default keys attack took a couple of seconds to execute for all of the cards. It is executed using the Proxmark by issuing a single command. It can also be performed using a cheaper reader like the NFC ACR122 for example. It has a high success rate. A study shows that 75% of the MIFARE Classic cards that are being used, have at least one default key left[20]. Successfully executing a Default Key attack can provide access to the sectors of the tags for which keys are found and it gives input for performing the Nested Attack. In order to execute a Default Key attack, one must have access to the valid tag. This can be done from a couple of meters distance if a powerful enough antenna is used[27].

7.1.2 DarkSide Attack

In the current version of the Proxmark software the DarkSide attack was optimized and takes about 25 seconds to complete. It is invoked with a simple command with no special parameters and the output is clear to understand. It can be performed using the Proxmark tool with a rather high success rate.

Sometimes it will freeze during the execution, but since there is no error message, it is most likely a software bug and hopefully it will be fixed in the later revisions of the Proxmark software. If successful, this attack will provide the A key for sector 0 of the tag, which can then be used as an input for the Nested Attack. Just as in the case of the Default Key attack one must have access to the valid tag in order to perform it.

7.1.3 Snooping and MFKey

Theoretically the Snooping and MFKey attack is pretty fast. However, it can take some time while the attacker is waiting for a valid authentication to occur on the reader that he is snooping on. Also he may have to retry the snooping procedure multiple times until he/she is able to record a complete authentication handshake. In order to perform this attack, the attacker needs to be familiar with the authentication protocol for MIFARE Classic tags. He/she must recognise which part of the conversation between the reader and the tag is the authentication handshake and must be able to extract the needed values from it. As long as the entire conversation was recorded, this was pretty easy to do. This attack can be performed with the Proxmark or any other High Frequency RFID device, which supports traffic snooping. During this research this kind of attack was only performed for two tags, so we can not draw an accurate conclusion for the success rate of the attack. However, from what we were able to see, it seems that if the attacker manages to record a complete authentication handshake, then the attack is feasible. As the DarkSide attack is successful, the attack will provide the A key for sector 0 of the tag, which can then be used as an input for the Nested Attack. In order for the attacker to pull off the attack by using the Proxmark with its standard antenna, he/she will need to place the antenna between the authenticating reader and the valid tag, while the authentication is taking place. This is not feasible in most situations, however snooping can be performed from a distance by using a more powerful antenna[27]. Using a better antenna will also improve the snooping itself, making it easier to capture all the parts of the conversation.

7.1.4 Nested Attack

The time needed to perform the Nested attack is different based on the type of MIFARE Classic tag on which it is performed. 4K tags take longer than 1K tags. However, this is logical, because for the 4K tags four times more keys need to be retrieved. Other than that, the attacks on both types are fast and will be completed within 1-2 minutes. The attack itself is easy to perform, but for the 4K tags, with the bug in the current revision of the Proxmark software, the attacker needs some programming skills in order to create a script or a program which will extract and arrange the found keys from the console output. This can also be done manually but it will take some time to copy and order 128 keys every time the attack needs to be performed. The attack can be performed with the Proxmark and although theoretically it should be also possible with the NFC reader, we were not able to get it to work. If we consider the bug which freezes the software, to be a successful execution of the attack, simply because all the keys are already found, then the attack has a rather high success rate. When successfully executed, the attack will provide all of the sector keys

for for the given tag, thereby making it possible to dump the content of the tag if the access rights bits also allow for it. In order to be performed, the Nested attack requires one known sector key of the valid tag and also access to it for the duration of the attack.

7.2 Tag Emulating

Once the content of a tag is retrieved, the emulation process does not take any time to complete. It is easily performed by executing one of a couple of simple commands. The Proxmark tool can be used to emulate most of the high and low frequency tags. The success rate with revision 840 of the Proxmark software and the default antennas seems to be intermediate. The gain from this attack is fooling the reader that a valid tag is presented to it and gaining access to a restricted area. The attacker must make sure that he/she is not seen while presenting the emulating device to the reader.

7.3 Tag Cloning

The tag cloning is very similar to the tag emulation attack, but it has some advantages over it. Like the tag emulating once the content of a tag is retrieved, it takes minimal time to write a clone of the valid tag and it is easy to perform. The success rate seems to be higher than the one for the tag emulation. This is, because the problem with the not responding reader is not present with tag cloning. The tag cloning can be performed with the Proxmark tool. However, special writable tags are also needed. The gain is the same as with tag cloning: fooling the reader that a valid tag is presented to it and gaining access to a restricted area. Unlike in case of the tag emulation, the attacker does not need to be extra cautious concerning visibility.

7.4 Relay Attack

Although the relay attack takes more time to get it working, it is a feasible attack when no keys or not all of the keys can be retrieved. The environment is harder to setup than for the other attacks. Two environments need to be setup and they need to be connected through a network. Timing of the attack is important to make the attack successful. Differences in implementation of the system are the defining factor for the success rate of the attack.

	Time	Knowledge & Skills	Resources	Success Rate	Requirements
Default keys	little	easy	Proxmark3 / NFC reader	high	Access to valid tag
DarkSide	little	easy	Proxmark3	rather high	Access to valid tag
Snooping	average	intermediate	Proxmark3	-	Access to a valid authentication handshake
Nested attack	little	intermediate/easy	Proxmark3 /NFC reader	rather high low	Access to valid tag
Emulate tag	little	easy	Proxmark3	intermediate	Dump of a valid tag
Clone tag	little	easy	Proxmark3 / NFC reader A writable tag	high	Dump of a valid tag
Relay attack*	a lot	intermediate	2x NFC reader	-	Simultaneous access to valid tag and reader
	* Attack can be performed without knowing the keys for tags that use encryption				

Table 7: Tested attacks feasibility overview

8 Conclusion

The research question of this report asks for guidelines on which to focus on when assessing a RFID access control system. Based on the tests performed while conducting this research, it becomes clear that there are multiple attacks which can easily be conducted against various implementations of such access control systems. Based on the types of RFID tags that are being used a different security level is established with specific vulnerabilities. Therefore it is logical that the first step, when assessing such a system must be to identify the type of tags which are being used.

If the system makes use of low frequency tags, this should automatically be considered as a security flaw, because of the lack of encryption functionality of those tags and the ease with which they can be cloned or emulated. There are however some low frequency tags which implement access control bits for reading the UID. If such tags are used, the rest of the implementation should be carefully inspected in order for such a system to be classified as secure.

In case high frequency tags are being used in the implementation, there are different aspects to focus on depending on the type of the tags. For MIFARE Classic, there are two very important things that need to be checked. Firstly, one has to make sure that there are no default keys left on any of the sectors of the tag. The new keys should be random and different for every sector. Also the random generator used to produce the keys should be inspected, its output should be as random as possible without any hidden patterns which can be used for predicting the keys. If all this is correctly implemented, the key retrieval attacks will have lower success rate. Secondly, the implementation of the system should properly make use of the encryption capabilities of the MIFARE Classic tags. This means that authentication information should be stored on the encrypted data sectors, and it should be used in the decision of the reader to give or decline access to the restricted area. Implementations which make use only of the UID of the tag should be considered less secure.

When MIFARE DESFire is used, this is already a sign for a more secure system. From the researched attacks in this report, only the relay attack is feasible against DESFire tags. There are still some other attacks which can be performed against this type of tags. For example a side channel attack is one of them. However, those attacks require good knowledge and more expensive equipment[6], so they were not examined during in this research. When assessing a DESFire implementation, the same two things as for the Classic implementation should be looked into. The keys must be as random as possible and the encryption capabilities should be used correctly.

We consider MIFARE UltraLight not suitable for standard access control systems, because of the lack of encryption and the special functionality of the tags, which is designed for other types of RIFD systems. However, the One-Time-Pad bits of a UltraLight tag would make it suitable for special edge case implementations of access control systems. For example one such implementation can be a limited time access tag which is used as a visitors badge on systems with offline readers. If such a system is being assessed, there is one important thing that needs to be verified. Before the reader changes the OTP bits and gives access to the restricted area, he/she should verify that the OTP bits are still writable, and are not locked by the lock bits. If they are locked, the reader will not be able to change them from 0 to 1, thereby the tag will be left valid forever[28].

If another type of high frequency tags is used, further research should be conducted in order to find the specific weaknesses for that type and give advice on how to assess a system which makes use of it.

Regardless of the used tags, there are a few other aspects of the implementation and the company policy which need to be assessed in order for a system to be considered secure. First of all, no sensitive information like BSN numbers, salary amounts, etc. should be written on the tags. This will lower the negative effect in case the data of a tag is being successfully dumped by the attacker. Secondly, the employees should be security aware. They need to know what the risks are and how to lower them. Security awareness will also prompt them to use the system correctly, without any misusing of functionalists. Thirdly, if a system is to be considered really secure, it should provide special enclosures such as aluminium Faraday cages for the RFID tags when they are not used. Those enclosures should prevent any communication to the tag when such is not supposed to happen, thereby making most of the attacks less feasible. And finally the surveillance implementation should be assessed in order to verify that all of the readers are being watched closely. This needs to be done in order to detect when an attacker is presenting an antenna to the reader instead of a valid tag, thereby making the emulating and relay attack less feasible.

Based on the findings of this research, we believe that by following those guidelines, one should be able to perform sufficient assessment of a RFID access control system implementation for a fairly secure environment. In case a high secure environment needs to be assessed, those guidelines will most likely not be enough and some further research will need to be conducted.

Further research could evaluate the attacks that are not investigated in this study. Among these attacks are the more expensive side channel analysis and physical attacks. Furthermore, there are more advanced methods for identifying the exact type of a tag than described in this report.

Acronyms

3DES Triple-DES. 6, 25

HF High Frequency. 7, 25

IEC International Electrotechnical Commission. 4, 25

ISO International Organization for Standardization. 4, 25

LF Low Frequency. 7, 25

NFC Near Field Communication. 6, 25

NUID Non-Unique IDentifier. 8, 25

OTP one-time-programmable. 9, 25

PCD Proximity Coupling Device. 4, 25

PICCs Proximity Integrated Circuit Cards. 4, 25

RFID Radio Frequency Identification. 4, 25

UHF Ultra High Frequency. 7, 25

UID Unique Identifier. 10, 25

A Appendix: List of used tags

Tag	Type	Description	Frequency
1	HID - Writable	Proxmark Demo Card	Low
2	HID - Writable	Proxmark Demo Card	Low
3	HID Proxcard II	Proxmark Demo Card	Low
4	SKIDATA	Ski Resort Card	Low
5	HID - Writable	Proxmark Demo Card	Low
6	MIFARE Classic 1K - UID Writable	Proxmark Demo Card	High
7	MIFARE Classic 1K - UID Writable	Proxmark Demo Card	High
8	MIFARE Classic 1K	Proxmark Demo Card	High
9	MIFARE UltraLight	Proxmark Demo Card	High
10	MIFARE Classic 4K	Proxmark Demo Card	High
11	MIFARE Classic 4K	Proxmark Demo Card	High
12	MIFARE Classic 1K	Demo Kit 1 Card (System C)	High
13	MIFARE Classic 1K	Demo Kit 1 Card (System C)	High
14	MIFARE Classic 1K	Demo Kit 1 Card (System C)	High
15	MIFARE DESFire	Demo Kit 1 Card (System C)	High
16	MIFARE DESFire	Demo Kit 1 Card (System C)	High
17	MIFARE Classic 1K	External Company 3 Badge	High
18	MIFARE Classic 4K	Anonymous OV chipcard	High
19	MIFARE Classic 4K	Anonymous OV chipcard	High
20	MIFARE Classic 4K	Anonymous OV chipcard	High
21	MIFARE Classic 4K	Anonymous OV chipcard	High
22	MIFARE Classic 1K	External Company 1 Badge (System A)	High
23	HID	External Company 2 Badge (System B)	Low
24	MIFARE UltraLight	Disposable GVB 1 hour ticket	High
25	MIFARE UltraLight	Disposable GVB 1 hour ticket	High
26	MIFARE UltraLight	Disposable GVB 1 hour ticket	High
27	MIFARE UltraLight	Disposable GVB 1 hour ticket	High
28	MIFARE DESFire	London Transport OYSTER Card	High
29	MIFARE Classic 4K	Personal OV chipcard	High
30	MIFARE DESFire	University Badge	High
31	EM410X	Demo Kit 2 Tag (System D)	Low

Figure 2: An overview of all the tags that were used throughout this research.

B Appendix: Achievements from the performed attacks

Tag	Type	Keys Retrieved	Dumped	Cloned	Emulated
1	HID - Writable	N/A	√	-	-
2	HID - Writable	N/A	√	-	-
3	HID Proxcard II	N/A	√	-	-
4	SKIDATA	N/A	√	-	-
5	HID - Writable	N/A	√	-	-
6	MIFARE Classic 1K	√	√	-	-
7	MIFARE Classic 1K	√	√	-	-
8	MIFARE Classic 1K	√	√	-	-
9	MIFARE UltraLight	N/A	√	-	-
10	MIFARE Classic 4K	X	-	-	-
11	MIFARE Classic 4K	√	√	-	-
12	MIFARE Classic 1K	√	√	-	-
13	MIFARE Classic 1K	√	√	√	√
14	MIFARE Classic 1K	X	-	-	-
15	MIFARE DESFire	-	-	-	-
16	MIFARE DESFire	-	-	-	-
17	MIFARE Classic 1K	√	√	-	-
18	MIFARE Classic 4K	√	X	-	-
19	MIFARE Classic 4K	√	X	-	-
20	MIFARE Classic 4K	√	X	-	-
21	MIFARE Classic 4K	√	X	-	-
22	MIFARE Classic 1K	√	√	√	X
23	HID	N/A	√	√	√
24	MIFARE UltraLight	N/A	√	X	-
25	MIFARE UltraLight	N/A	√	-	-
26	MIFARE UltraLight	N/A	√	-	-
27	MIFARE UltraLight	N/A	√	-	-
28	MIFARE DESFire	-	-	-	-
29	MIFARE Classic 4K	√	X	-	-
30	MIFARE DESFire	-	-	-	-
31	EM410X	N/A	√	-	X

Table 8: Achievements from the performed attacks against the different tags.

C Appendix: Script for 4K cards

Listing 1: keystring.pl

```
#!/usr/bin/perl
use strict;


my @logfile = ();

my $flag = 0;
my $block;
my %aKeys;
my %bKeys;
my $counter = 0;
my $finalString = "";

for my $i (0 .. 253) {
        $aKeys{$i} = "XXXXXXXXXXXX";
        $bKeys{$i} = "XXXXXXXXXXXX";
}

@logfile = qx(cat keyz.txt);

for my $i (@logfile) {
#print "$i";
        if ($flag == 1 && $i =~ m/^(Found valid key:)([0-9a-f]*).*$/) {
                $aKeys{$block} = $2;
                $flag=0;
#print "Key A Block $block ---- $2\n";
        }
        if ($i =~ m/^(uid)(.*)[ ](.*)[ ](trgbl=)([0-9]*)[ ](trgkey=0).*$/) {
                $flag=1;
                $block = $5;
        } else {
                $flag=0;
        }
}

while ($counter < 256) {
        $finalString = "$finalString$aKeys{$counter}";
#print "A counter $counter ------- $aKeys{$counter}\n";
        $counter += 4;
}

$flag=0;
$counter = 0;

for my $i (@logfile) {
        if ($flag == 1 && $i =~ m/^(Found valid key:)([0-9a-f]*).*$/) {
```

```
                $bKeys{$block} = $2;
                $flag=0;
#print "Key B Block $block ---- $2\n";
        }
        if ($i =~ m/^(uid)(.*)[ ](.*)[ ](trgbl=)([0-9]*)[ ](trgkey=1).*$/) {
                $flag=1;
                $block = $5;
        } else {
                $flag=0;
        }
}

while ($counter < 256) {
        $finalString = "$finalString$bKeys{$counter}";
#print "B counter $counter ------- $bKeys{$counter}\n";
        $counter += 4;
}

print "$finalString\n";
```

References

[1] Nicolas T Courtois. "The dark side of security by obscurity". In: *International Conference on Security and Cryptography* (2009).

[2] Gerhard De Koning Gans, JH Hoepman, and FD Garcia. "A practical attack on the MIFARE Classic". In: *Smart Card Research and ...* (2008).

[3] F.D. Garcia et al. "Wirelessly Pickpocketing a Mifare Classic Card". In: *2009 30th IEEE Symposium on Security and Privacy* (2009). ISSN: 1081-6011. DOI: 10.1109/SP.2009.6.

[4] Flavio D Garcia et al. "Dismantling MIFARE Classic". In: *ESORICS 2008*. 2008, pp. 97 –114. ISBN: 9783540883128. DOI: 10.1007/978-3-540-88313-5_7.

[5] Wee Hon Tan. "Practical attacks on the Mifare Classic". In: *Imperial College London* (2009).

[6] David Oswald and Christof Paar. "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World". In: *CHES 2011, Nara* (2011-09-30).

[7] Aikaterini Mitrokotsa, Melanie R Rieback, and Andrew S Tanenbaum. "Classification of RFID attacks and Defenses". In: *Gen* (2010).

[8] Pawel Rotter. "A framework for assessing RFID system security and privacy risks". In: *IEEE Pervasive Computing* 7.2 (2008), pp. 70–77.

[9] Gerhard P Hancke. "Practical attacks on proximity identification systems". In: *Security and Privacy, 2006 IEEE Symposium on*. IEEE. 2006, 6–pp.

[10] Wolfgang Issovits and Michael Hutter. "Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks". In: *2011 IEEE International Conference on RFID-Technologies and Applications* (Sept. 2011), pp. 335–342. DOI: 10.1109/RFID-TA.2011.6068658.

[11] M Weiss. "Performing relay attacks on ISO 14443 contactless smart cards using NFC mobile equipment". 2010.

[12] *Identification cards – Contactless integrated circuit(s) cards – Proximity cards*. Norm. 2000.

[13] CardLogix Corporation. *Smart Card Types*. URL: http://www.smartcardbasics.com/smart-card-types.html (visited on 01/10/2014).

[14] EM Microelectronic. *EM4200*. URL: http://www.emmicroelectronic.com/Products.asp?IdProduct=282 (visited on 01/22/2014).

[15] KYLE E PENRI-WILLIAMS. "Implementing an RFID Mifare Classics Attack". In: (2009).

[16] NXP. *MIFARE Classic Data Sheet*.

[17] NXP. *MIFARE DESFire Functional specification*. 2008.

[18] NXP. *MIFARE UltraLight Data Sheet*.

[19] Nicolas T Courtois. "Card-Only Attacks on MiFare Classic and Break into Buildings Worldwide". In: (2009).

[20] Lukas Grunwald. "New Attacks against RFID-Systems". In: *GmbH Germany* (2006).

[21] Wouter van Dullink and Pieter Westein. "Remote relay attack on RFID access control systems using NFC enabled devices". In: (2013).

[22] *Compiling the Proxmark from source and flashing.* URL: `https://code.google.com/p/proxmark3/wiki/Compiling` (visited on 01/12/2014).

[23] *Configuring the development environment in Linux.* URL: `http://code.google.com/p/proxmark3/wiki/Linux` (visited on 01/12/2014).

[24] *libnfc developers community.* URL: `http://www.libnfc.org/community/topic/911/problem-installing-libnfc170rc4-now-mfoc/` (visited on 01/13/2014).

[25] *Proxmark3.* URL: `http://code.google.com/p/proxmark3/wiki/HomePage` (visited on 01/12/2014).

[26] *nested command freezes (only on MF 4K).* URL: `http://www.proxmark.org/forum/viewtopic.php?pid=9061` (visited on 01/22/2014).

[27] Klaus Finkenzeller. "Known attacks on RFID systems , possible countermeasures and upcoming standardisation activities." In: (2009).

[28] Matteo Beccaro and Matteo Collura. "OTP circumventing in MIFARE ULTRALIGHT: Who says free rides?" In: (2012).