Chapter 4

A Methodology for Evaluating Security in Commercial RFID Systems

Tiago M. Fernández-Caramés, Paula Fraga-Lamas,
Manuel Suárez-Albela and Luis Castedo

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/64844

Abstract

Although RFID has become a widespread technology, the developers of numerous commercial systems have not taken care of security properly. This chapter presents a methodology for detecting common security flaws. The methodology is put in practice using an open-source RFID platform (Proxmark 3), and it is tested in different fields, such as public transportation or animal identification. The results obtained show that the consistent application of the methodology allows researchers to perform security audits easily and detect, mitigate, or avoid risks and possible attacks.

Keywords: RFID, security, pen testing, LF, HF, ISO/IEC 14443, ISO/IEC 7816, ISO/IEC 11784, ISO/IEC 11785

1. Introduction

In the last years, RFID has been applied throughout industry and services, thanks to its ease of use and its multiple practical applications, including animal identification, access control, passport verification, transportation and payment cards, car access control, supply chain traceability, logistics, or toll payments. However, despite becoming an everyday technology, many public and private entities have not considered the security of RFID systems as a basic requirement. In fact, it is easy to find many commercial systems that contain critical security flaws and vulnerabilities [1, 2] that allow for cloning tags or for straight signal replaying. Such vulnerabilities let attackers access certain services or facilities, get or alter personal information, and even track people.

Fortunately, secure mechanisms can be applied to prevent the attacks aforementioned, including the use of cryptography, the automatic detection of rogue devices [3], the enhancement of the resistance to cloning [4], the secure storage of critical data in remote databases or the use of secure physical modulations and medium access control (MAC) protocols. Nonetheless, it is common to find commercial RFID systems that have such security features disabled or detect already-broken RFID security systems still in use.

Taking the considerations previously mentioned into account, this chapter describes a methodology that allows researchers to evaluate the most common security flaws and details the necessary tools for applying such a methodology.

The rest of this chapter is organized as follows. Section 2 first reviews the most common security threats that can be used against RFID systems and then describes some of the latest RFID hardware/software security tools available. Section 3 exposes the methodology proposed for analyzing RFID security. In Section 4, the methodology is tested in different commercial systems. Finally, Section 5 is devoted to conclusions.

2. Security in RFID

2.1. Basics on attacks against RFID systems

Information security has been classically governed by what is known as the CIA Triad: confidentiality, integrity, and availability. Confidentiality is related to the importance of protecting the most sensitive information from unauthorized access. Integrity consists in protecting data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes, they can be undone if some damage occurs. Finally, availability is the possibility of accessing the data when needed. If any of these three principles is not met, then security can be said that it has been broken.

Like other technologies, RFID is exposed to security threats and, specifically, to attacks on the confidentiality, integrity, and availability of the data stored on the tags or on the information exchanged between a reader and a tag.

The term risk refers to the probability of occurrence of an event that causes damage to an informational asset. Two kinds of risks can be basically distinguished:

- Security risks. They are derived from actions able to damage, block, or take advantage from a service in a malicious way. The action is usually carried out with the objective of obtaining a profit or just for damaging the access to certain service. The most common services provided by RFID systems are access control to facilities and payments.
- Privacy risks. These risks affect the confidential information of the users. RFID tags can store data of the payments they performed or the transportation route followed by the user/owner.

In real life, most risks are a mixture of both security and privacy risks: they threaten RFID security in order to get access to the information stored or to the data related to a transaction.

http://dx.doi.org/10.5772/64844

A classification of RFID attacks can be seen in [5]. The following are the most common attacks associated with security risks:

- Tag isolation. It is technically the simplest attack and probably the most common. It consists in blocking the tag communications to avoid sending data to the reader. It is usually carried out by means of a Faraday cage or by jamming RF signals.
- Tag cloning. The unique identifier (UID) and/or the content of the RFID is extracted and inserted into another tag [6]. Cloning is commonly used for accessing restricted areas or for decreasing the price of certain goods in supermarkets.
- Denial of Service (DoS) attacks. The reader is flooded with such a large amount of information that it cannot deal with the signals sent by real tags [7]. Other techniques are based on emitting radio noise at the operating frequency of the RFID system.
- Command injection. Some readers are vulnerable to remote code execution just by reading the content of a tag [8].
- Signal replaying. It consists in recording the RFID signal in certain time instants with the objective of replaying it later.
- Remote tag destruction. There exist RFID zappers that are able to send energy remotely that once rectified, is so high that certain components of the tag might be burned. Researchers have also found that it is possible to misuse the kill password in some tags (Electronic Product Code(EPC) Class-1 Gen-2) with a passive eavesdropper and then disable the tags [9].
- SQL injection. Like in the case of command injection, it has been found that some reader middleware is susceptible to the injection of random SQL commands [8].
- Virus/Malware injection. Although difficult to perform in the vast majority of RFID tags due to their low storage capacity, it is possible in certain tags to insert malicious code that is able to be transmitted to other tags [8].
- Man-in-the-Middle (MitM) attacks. They consist in placing an active device between a tag and the reader in order to intercept and alter the communications between both elements [10, 11].
- Relay/Amplification attacks. They consist in amplifying the RFID signal using a relay; thus, the range of the RFID tag is extended beyond its intended use [12].
- RFID skimming. They consist in the use of portable point of sales terminals to make unauthorized and fraudulent charges on payment cards.

Attacks associated with privacy risks include the following:

- Unauthorized access to personal data. Many systems store private data on the tag or transmit them when a tag and reader exchange information.
- Personal tracking. This is probably the most feared, since an attacker might determine routes, purchases, and habits of a specific person. The information may be even used for marketing purposes.

2.2. Hardware tools for auditing RFID security

In recent years, a number of projects have been developed with the aim of facilitating researchers' low-level access to RFID communications. Some of them are just software tools that can be used with commercial RFID readers (RFIDiot [13]), while others involve specific hardware (Proxmark 3 [14], Tastic [15], OpenPCD [16], OpenPICC [17], Chameleon Mini [18]), or certain firmware (Proxbrute for Proxmark 3 [19]). Hardware developments are specially interesting: some devices can emulate readers (Tastic, OpenPCD); others can emulate just tags (OpenPICC); and a few can emulate both kinds of devices (Proxmark 3, Chameleon Mini).

There are not many academic platforms developed to test RFID security. An example can be found in [20], where a microcontroller and Field-Programmable Gate-Array(FPGA)-based tag platform is presented with the aim of evaluating high-frequency (HF) and ultra-high-frequency (UHF) RFID tags. The latest development as of writing is the Chameleon Mini, which has been promoted by the Ruhr University (Bochum, Germany): it is a versatile RFID tag emulator compliant with ISO/IEC 14443 and ISO/IEC 15693 (for instance, it currently supports MIFARE Classic 1K/4K/Ultralight emulation).

The platform selected in this chapter to analyze RFID security was Proxmark 3, which is an open-source system able to transmit at LF (125–134 KHz) and HF (13.56 MHz). The system contains an Atmel AT91SAM7S256 (256 KB of flash and 64 KB of RAM), an FPGA (Xilinx Spartan-II), and an 8-bit analog-to-digital converter (ADC). It is powered through an USB and has a SV2 connector for the antenna, which contains four pins: two are for the HF antenna, and the other two are for the LF antenna. All these components can be observed in **Figure 1.** Among Proxmark features, it is relevant its ability to sniff the communications between a reader and different tags, and the possibility of emulating a reader or a specific tag.

When the Proxmark acts as an RFID receiver, the signal that comes from the antenna goes through the ADC and is converted from analog to digital. Then, the digital data are sent through an 8-bit bus to the FPGA, where it is demodulated. Finally, the signal is sent from the FPGA to the microcontroller through the Serial Peripheral Interface(SPI) to deal with the RFID protocol. When the Proxmark acts as a transmitter, the same steps are performed but in reverse

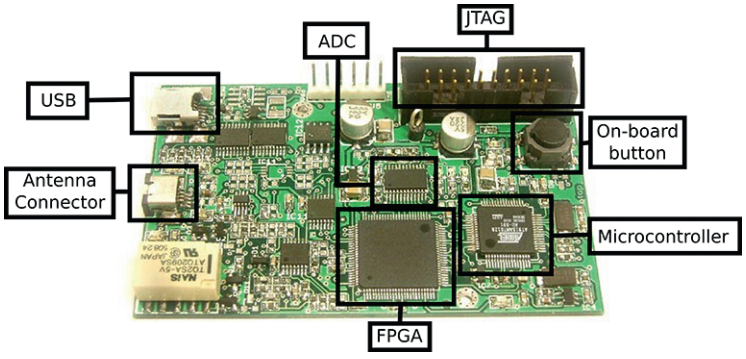

Figure 1. Main components of Proxmark 3.

http://dx.doi.org/10.5772/64844

order. The FPGA modulators/demodulators are developed in Verilog, while the Atmel microcontroller is programmed in C.

3. A methodology for evaluating RFID security

3.1. Methodology proposed

In order to automate the evaluation of security in commercial RFID systems, a methodology has been devised. A reduced flow diagram is depicted in **Figure 2**. It consists of the following main steps:

1. Visual inspection of the tag. Many tags include the name of manufacturer, the model and, sometimes, the RFID standard. With such data, it is usually easy to get more specific information on the way the tags behave and how to perform security tests.

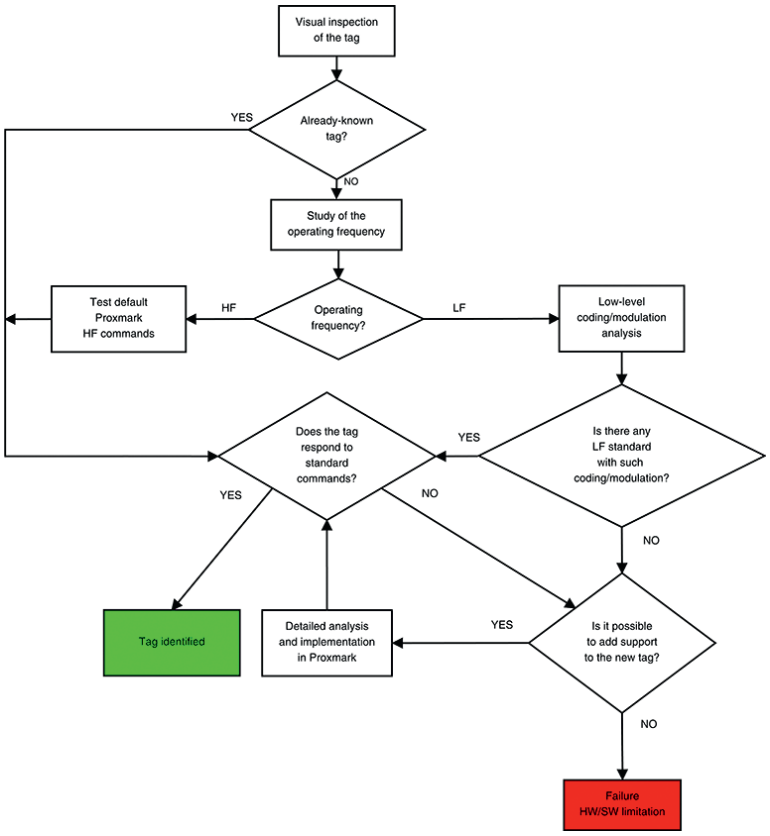

Figure 2. Flow diagram of the methodology.

2. Radio frequency detection. If there are no external signs on the tag, it is first recommended to determine the tag's frequency. In such a case, LF, HF, UHF, and super-high frequency (SHF) tags can be found. There are software and hardware mechanisms to determine which is the operating frequency, like using a spectrum analyzer, or disassembling the tag or the reader to observe the hardware components of the radio interface.

3. Modulation and coding detection.

4. Standard identification. Once obtained the three previous parameters (frequency, modulation, and coding), it is straightforward to determine whether there exists an RFID standard compliant with such configuration. If it is not the case, the research could become tricky, since it might involve a proprietary protocol. However, when working with LF, HF, and UHF tags, standards are usually followed.

5. Sniff and emulate communications to perform security tests.

3.2. Applying the methodology with the Proxmark 3

The methodology presented in this chapter can be easily applied to any unknown HF and LF RFID tags. In the next subsections, the analysis is divided into LF and HF tags, since the way they work varies noticeably. As it will be detailed, it is possible to work at a physical level with LF tags, but that is not easy in the case of HF devices.

3.2.1. Detecting the operating frequency

The first step of the methodology consists in obtaining the operation frequency. For such a purpose, one of the antennas (LF or HF) has to be placed far from any tag and the Proxmark command *hw tune* has to be executed. The command gives us the received voltage in the different supported frequencies. Then, the operation has to be performed next to the unknown tag: if one of the voltages has decreased remarkably for a specific frequency, it means that such a frequency is the operating frequency.

Figures 3 and **4** show an example of the process for an LF tag. First, the voltages are checked with the HF antenna connected (note in **Figure 3** that the LF antenna is said to be unusable), and it can be observed that they almost do not change between tests (i.e., just around 1 V). When the same procedure is carried out with the LF antenna (**Figure 4**), the voltages associated with LF frequencies drop substantially (especially of 134 KHz), and therefore, it is concluded that the tag is indeed LF.

3.2.2. Analyzing LF tags

When determining whether a tag follows an LF standard, the first step consists in figuring out the data modulation and coding. For such a purpose, the following sequence of Proxmark commands has to be executed:

- *LF read* [*h*]: the tag is powered with the selected frequency (125 KHz by default, or 134 KHz using the parameter *h*). The command also records the signal transmitted by the tag.

http://dx.doi.org/10.5772/64844

- *Data sample x*: it downloads *x* of the previously recorded samples to the PC.
- *Data plot*: it allows the user to open a new window to plot the signal. It is useful for evaluating the signal visually.
- Different instructions can be used to modify, amplify, decimate, or normalize signal values to ease signal identification.
- If the signal is clean enough, and its modulation has been recognized, the user can try to demodulate it. For instance, if the signal is modulated in amplitude-shift keying (ASK), the command *data askdemod* can be executed. In the case of frequency-shift keying (FSK) modulated signals, *fskdemod* is the right command.

```
proxmark3> hw tune
#db# Measuring complete, sending report back to host

# LF antenna: 0.00 V @   125.00 kHz
# LF antenna: 0.00 V @   134.00 kHz
# LF optimal: 0.00 V @ 12000.00 kHz
# HF antenna: 9.70 V @    13.56 MHz
# Your LF antenna is unusable.

proxmark3> hw tune
#db# Measuring antenna characteristics, please wait..
#db# Measuring complete, sending report back to host
# LF antenna: 0.00 V @   125.00 kHz
# LF antenna: 0.00 V @   134.00 kHz
# LF optimal: 0.00 V @ 12000.00 kHz
# HF antenna: 8.67 V @    13.56 MHz
# Your LF antenna is unusable.
```

Figure 3. HF voltages for an LF tag when is present (second command) or not in the field.

```
proxmark3> hw tune
#db# Measuring antenna characteristics, please wait..
#db# Measuring complete, sending report back to host

# LF antenna: 12.89 V @   125.00 kHz
# LF antenna: 23.36 V @   134.00 kHz
# LF optimal: 24.98 V @   131.87 kHz
# HF antenna:  0.64 V @    13.56 MHz
# Your HF antenna is unusable.

proxmark3> hw tune
#db# Measuring antenna characteristics, please wait..
#db# Measuring complete, sending report back to host

# LF antenna:  9.40 V @   125.00 kHz
# LF antenna: 13.16 V @   134.00 kHz
# LF optimal: 17.32 V @   139.53 kHz
# HF antenna:  0.68 V @    13.56 MHz
# Your HF antenna is unusable.
```

Figure 4. LF voltages when an LF tag is not in the field (first command) and when it is.

Figure 5 shows an example of the signal obtained after carrying out the first three steps previously mentioned. Such a signal can then be demodulated, as it seems to be modulated either in ASK or FSK.

In this case, when the command *askdemod* was executed, it returned an error indicating that it had not been detected an ASK-modulated signal, and in fact, taking a closer look at **Figure 5** it can be observed that the period of the pulses with less amplitude is different from the others. Therefore, it had to be FSK and *fskdemod* demodulated the signal (**Figure 6**).

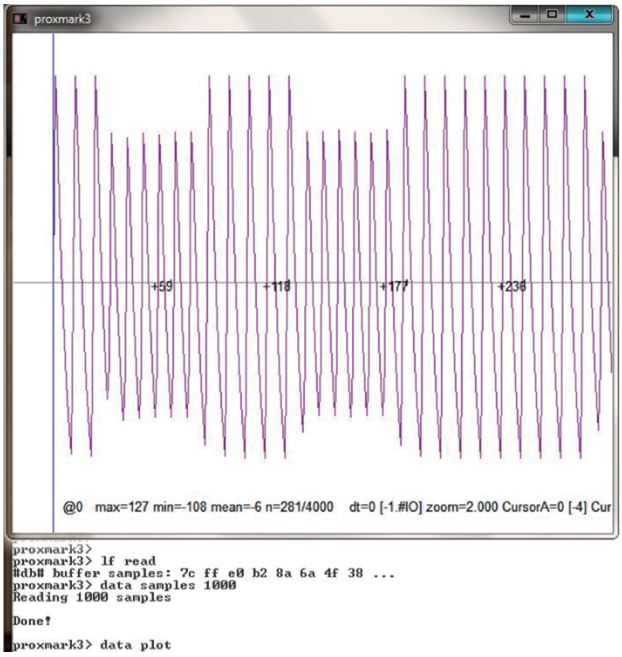

Figure 5. Example of an LF tag signal received.

```
proxmark3> data fskdemod
actual data bits start at sample 6180
length 50/50
bits: '01001010100000101011111111111111111111111111'
hex: 00000950 57ffffff

proxmark3> data fskdemod
actual data bits start at sample 1044
length 50/50
bits: '01001010100000101100110000000000100010010001'
hex: 00000950 5980---1
```

Figure 6. LF tag signal demodulated with *fskdemod*.

http://dx.doi.org/10.5772/64844

The next step consists in searching for a bit pattern, which might lead to determine the length of the identifier. Thus, the signal has to be observed during certain periods of time and look for similarities. In order to understand the transmitted data, it can be useful to find the standard that defines and structures them. For instance, in the previous example, the LF tag was an access control card manufactured by HID [21], whose well-known LF data structures can be extracted and then the UID obtained, as it is shown in **Figure 7**.

At this point, the HID tag can be emulated with the Proxmark using the command *lf hid sim*; and it can even be cloned with a rewritable tag like Atmel T5557.

3.2.3. Analyzing HF tags

HF tags behave in a slightly different way than the LF ones: their signal is so fast that it cannot be processed so easily at plain sight. Moreover, in general, HF tags are smarter than LF tags, and they not only transmit an identifier repeatedly but also perform more complex communications with the reader. There exist many HF transmission modes and protocols. Furthermore, HF tags and readers can vary their modulation during the same transmission. For example, a tag can send FSK-modulated data, while the reader responds in ASK.

The steps required to analyze HF tags are not as clear as in LF, so the study becomes more like a trial-and-error process. For instance, the case of a public transportation card whose data were decoded after trying one by one all the possible combinations defined by the most popular standards until the right one was found is shown in **Figure 8**: first, it was tested ISO/IEC 14443-A, then ISO/IEC 15693 and, finally, ISO/IEC 14443-B.

```
proxmark3> lf hid fskdemod
#db# TAG ID: 95059800---1 (1096)
#db# TAG ID: 95059800---1 (1096)
```

Figure 7. Obtaining the tag UID of an access control LF tag manufactured by HID.

```
proxmark3> hf 14a reader
iso14443a card select failed

proxmark3> hf 15 reader
#db# 0 octects read from IDENTIFY request:
#db# 0 octects read from SELECT request:
#db# 0 octects read from XXX request:

proxmark3> hf 14b read
#db# 3 1 e
```

Figure 8. Determining the RFID standard of an HF tag.

```
proxmark3> data hexsamples
50 08 -- -- -- -- 4e 44
4b 33 -- -- -- -- 44 44
```

Figure 9. UID and control bytes from an ISO/IEC 14443-B compliant card.

The command for reading ISO/IEC 14443-B tags sends an Answer to Request Type B(ATQB) command (0x05, 0x00, 0x08, 0x39, 0x73) and records the tag's answer. The second value of the output can be either 0x00000000 or 0x00000001: if it is "1", it means the reply of the tag was received properly. If it is "0", it means that not all bytes (or none) were received.

In the specific case of the previous tag, the answer of the tag is "3 1 e," so the second value ("1") means that the tag is actually compliant with ISO/IEC 14443-B. The Proxmark is able to return the data after issuing the command *hexsamples*, which shows the UID and additional control bytes (in **Figure 9**).

4. Practical evaluation

In order to validate the methodology proposed, three different commercial RFID systems were analyzed and tested. The next subsections first introduce the tags audited and then give details on the analysis and the steps required testing their security.

4.1. M and T cards

In this section, what we have called "M" and "T" cards are analyzed. Please note that such aliases were given to avoid legal issues, since there are still several hundred thousand units of the cards still in use.

In the case of the M card, it has been used in the last years by the city council of a relevant city in Spain for paying different services such as public transportation, museum access, or sport events. It is said that the council has sold more than 200,000 units of the card.

Regarding the T card, it is an RFID card developed by a Spanish regional government that provides public transportation payment to a population of 2.7 million people. It was designed to be compatible with the M card; therefore, in the next subsection a joint analysis of both cards is performed.

4.1.1. Visual inspection

In plain sight, there are no signs or symbols that indicate the frequency band of the RFID cards. It can be assumed that by the reading range and the amount of information stored, they could be HF tags, but a deeper analysis should be performed to verify it accurately.

http://dx.doi.org/10.5772/64844

4.1.2. Operating frequency and modulation

- Radio frequency. Although both cards seem to be HF, the steps described in Section 3.2.1 have to be carried out to determine whether they are LF or HF. Such steps confirm that they are HF tags.
- Modulation. Once the radio frequency is obtained, it has to be decided which of the possible standards the tags follow, and then, the modulation can be determined. A first fast test consisting in sending commands for ISO/IECs 14443-A, 14443-B, and 15693 standards show that the tags only answer correctly to the ones issued following ISO/IEC 14443-B.

4.1.3. Understanding the underlying protocols

ISO/IEC 14443 [22] is a 13.56 MHz-based standard that defines proximity RFID systems that are usually related to payment cards. ISO/IEC 14443 consists of four parts: (1) physical characteristics, (2) RF power and signal interface, (3) initialization and anti-collision, and (4) transmission protocol. It also defines two kinds of tags (type A and type B), which differ in parts (2) and (3). **Table 1** shows the differences in terms of modulation and coding between both types [in such a table, the reader is called proximity coupling device (PCD), and the tag is the proximity integrated circuit card (PICC)].

4.1.4. Security analysis

4.1.4.1. Obtaining communication traces

The first step for the security analysis consisted in obtaining a good set of data samples of the communications carried out between each card and the reader. Note that data samples were taken during real trips in public transportation. Thus, a laptop with the Proxmark was carried in a backpack, while the RFID antenna cable was placed along the sleeve of a jacket until reaching the tester's hand, where the antenna captured the dialog between the card and the reader.

Once the radio signals were captured by the antenna, they were demodulated and decoded with the Proxmark. The main problem with this setup was electric noise: many samples were

	Type A	**Type B**
PCD to PICC	ASK 100%	ASK 10%
	Modified Miller, 106 kbps	NRZ, 106 kbps
PICC to PCD	Load modulation	Load modulation
	Subcarrier fc/16	Subcarrier fc/16
	OOK	BPSK
	Manchester, 106 kbps	NRZ-L, 106 kbps

Table 1. Modulation and coding used by ISO/IECs 14443-A and 14443-B.

lost because they became corrupted. In fact, none of the first 10 capturing attempts was successful, and it was necessary to perform numerous tests and try three different M/T cards to get a good data set. An example of captured data is shown in **Table 2**.

Timestamp	RSSI	Device	Payload	Additional information
0	142	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f	
1398	112	TAG	00 78 f0	
854			05 00 00 71 ff	
11500			05 00 00 71 ff	
11478			06 00 97 5b	
46342			05 00 08 39 73	
1908			1d 08 10 2a 1d 00 08 01 00 94 60	
554	296	TAG	00 78 f0	
3566			02 80 26 4f 11 0a e7 de	
3146	116	TAG	02 00 14 98 70 10 01 01 76 55 72 90 00 73 65	
36188			03 80 32 00 00 18 ea 98	
1852			00 01 00 00 00 00 00 00	**Fail CRC**
480			00 90 00 1d fe	**Fail CRC**
3676			02 80 2e 01 00 20 43 2f	
2870	203	TAG	02 01 01 e0 f5 ff f5 ff 00 00 00 00 01 f4 07 06 a9 8c ff 00 11 03 e8 00 00 b9 0b ff 00 02 00 01 48 90 00 26 57	
48				(SHORT)
3798			03 80 30 00 00 1d 31 f6	
1580			03	(SHORT)
17462			02 80 28 00 00 04 75 39 34 0d 3a 07 d3	
5778				(SHORT)
34972			03 80 2a 01 00 24 00 15 00 4b 00 01 48 41 19 09 01 00 28 01 37 e5 8c 18 21 10 00 c2 01 01 09 23 00 10 01 00 00 4b d4 72 2b eb 04 ca 20	
14542	203	TAG	03 b3 56 ee 2c 90 00 e6 01	
197304			05 00 08 39 73	
804			33 81 93 bc 3f	**FAIL CRC**

Table 2. Example of a M/T trace.

http://dx.doi.org/10.5772/64844

4.1.4.2. Analysis of the traces collected

It is important to emphasize that the communications of the system analyzed were not encrypted. Furthermore, it is first necessary to understand ISO/IEC 14443-B to determine the meaning of the different messages. The following are the steps performed by a regular ISO/IEC 14443-B system:

1. The tag awaits for a Request Type B(REQB) command.
2. The reader sends the REQB.
3. If the application family identifier (AFI) of the REQB is the one expected, the tag answers with the ATQB and waits for an ATTRIB command.
4. The reader sends the ATTRIB command.
5. If the ATTRIB command is the one expected, the tag sends the ATA (also known as the ATATTRIB, answer-to-ATTRIB).
6. Finally, the tag commutes to the active state, where it is able to exchange data commands with the reader until it receives a DESELECT and commutes to a HALT state.

Regarding the messages transmitted when the tag is in the active state, they can be of three types: i-block, s-block, and r-block. The first one is used for transmitting and asking for data from the application layer. The other ones are for protocol operations or are related to data from lower layers. **Table 3** describes the structure of an i-block, which is the only block that appears in the traces of the communications of the M/T cards.

After analyzing a number of traces, it was concluded that the information contained in the i-block was compliant with ISO/IEC 7816 [23], which has been massively used in credit, debit, and other payment cards. Therefore, it is first necessary to describe briefly the structure of the ISO/IEC 7816 requests and answers.

The typical ISO/IEC 7816 application protocol data unit (APDU) follows the structure shown in **Table 4**.

	PCB	**CID**	**NAD**	**Payload**	**CRC-B**
Length	1 byte	1 byte (optional)	1 byte (optional)	N bytes	2 bytes
Meaning	Protocol control	Card ID number	Node address (for logic addresses)		Cyclic-redundancy check

Table 3. Structure of an i-block.

In **Table 4**, the CLA byte specifies the command class: in case of being equal to 80 or greater (except for FF that is not a valid value), it means that proprietary commands are used. The same happens with the byte INS, which identifies the type of command. The third field on the header is bytes P1 and P2 that in general, refer to memory positions on the card, but they may actually be any parameter(PARAM) of the command.

Field	Description	Length (bytes)
Header	CLA	1
	INS	1
	P1 and P2	2
Lc	Number of bytes transmitted	0, 1 or 3
Data	Payload	Lc
Le	Number of bytes of the response	0–3

Table 4. Structure of an ISO/IEC 7816 APDU command.

Regarding the answers to such commands, they are conformed by two bytes (SW1 and SW2), which are coded according to **Table 5**. The most common answer during a correct sequence of commands is 90-00, but, sometimes, the execution of the sequence can be successful and return a different value.

4.1.4.3. Disassembling the traces

Once the basics of ISO/IECs 14443-B and 7816 are understood, it is possible to process the traces generated by the system.

Contrary to what was illustrated in **Table 2**, the messages "**FAIL CRC**" and "(SHORT)" should not be present, since they are related to data corruption. In the same way, a good trace should have alternating messages from the tag and the reader, instead of containing two consecutive messages from the same device (except from the case when the reader is looking for tags). Taking these facts into account, **Table 6** indicates the relationship between the standard

	SW1–SW2	Meaning
Normal processing	90 00	Ok
Warning processing	61 XX	XX bytes are still pending to be sent
	62 XX	State of nonvolatile memory is unchanged
	63 XX	State of nonvolatile memory has changed
Execution error	64 XX	State of nonvolatile memory is unchanged
	65 XX	State of nonvolatile memory has changed
	66 XX	Security-related issues
Checking error	67 00	Wrong length
	68 XX	Not supported functions in CLA
	69 XX	Command not allowed
	6A XX	Wrong P1–P2 parameters
	6B 00	Wrong P1–P2 parameters
	6C XX	Wrong LE field. There are XX bytes available
	6D 00	Instruction code not supported or invalid
	6E 00	Class not supported
	6F 00	No precise diagnosis

Table 5. Common answers to ISO/IEC 7816 commands.

http://dx.doi.org/10.5772/64844

commands and the trace shown in **Table 2**. As it can be observed, the sequence of messages is not correct: some are missing, and others have not been received in the correct order.

First, at timestamp 12350, the reader sends different REQB commands to wake up tags that are in its surroundings. The first byte of the command is always set to 05, while the second one is the AFI, that is, equal to 0 (i.e., every tag should respond to the request). The byte PARAM varies between both commands, being 00 in the first case and 08 in the second one (they are aimed at waking up tags in different states). Finally, the last two bytes conform the CRC-B field, which checks the integrity of the message.

The second command is the ATQB:

- It always begins with 50.
- The next four bytes are 08 10 2a 1d, which are the pseudo-unique PICC identifier (PUPI, which is fixed for each tag of the system analyzed, but it might be random in other systems).
- Then, the command continues with another four bytes (53 4e 44 4b) that indicate the applications of the tag.

Timestamp	RSSI	Device	Payload	Additional information	Message
0	142	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f		ATQB
1398	112	TAG	00 78 f0		ATATTRIB
854			05 00 00 71 ff		REQB
11500			05 00 00 71 ff		REQB
11478			06 00 97 5b		
46342			05 00 08 39 73		REQB
1908			1d 08 10 2a 1d 00 08 01 00 94 60		ATTRIB
554	296	TAG	00 78 f0		ATATTRIB
3566			02 80 26 4f 11 0a e7 de		i-Block
3146	116	TAG	02 00 14 98 70 10 01 01 76 55 72 90 00 73 65		
36188			03 80 32 00 00 18 ea 98		
1852			00 01 00 00 00 00 00 00	** Fail CRC **	
480			00 90 00 1d fe	** Fail CRC **	
3676			02 80 2e 01 00 20 43 2f		
2870	203	TAG	02 01 01 e0 f5 ff f5 ff 00 00 00 00 01 f4 07 06 a9 8c ff 00 11 03 e8 00 00 b9 0b ff 00 02 00 01 48 90 00 26 57		
48				(SHORT)	
3798			03 80 30 00 00 1d 31 f6		
1580			03	(SHORT)	
17462			02 80 28 00 00 04 75 39 34 0d 3a 07 d3		
5778				(SHORT)	
34972			03 80 2a 01 00 24 00 15 00 4b 00 01 48 41 19 09 01 00 28 01 37 e5 8c 18 21 10 00 c2 01 01 09 23 00 10 01 00 00 4b d4 72 2b eb 04 ca 20		
14542	203	TAG	03 b3 56 ee 2c 90 00 e6 01		
197304			05 00 08 39 73		REQB
804			33 81 93 bc 3f	**FAIL CRC**	

Table 6. M/T trace messages analyzed.

- Next, three bytes (33 81 93) specify different aspects of the communications protocol. Their description and use are beyond the scope of this chapter, but the interested reader can obtain such details in ISO/IEC 14443-3.
- The last two bytes contain the CRC-B.

Another imperfect trace is shown in **Table 7**. However, this trace is useful for illustrating the sequence of commands executed during the exchange.

After the ATQB, at timestamp 1104, the reader sends the ATTRIB command. The command is composed by a first byte (1d) that identifies the command, four bytes that indicate the PUPI from the previous command (08 10 2a 1d), three bytes that determine the communications protocol, a byte (00, the Card Identifier(CID)) that selects a tag and two final bytes that contain the CRC-B.

Timestamp	RSSI	Device	Payload	Additional information	Message
0			05 00 00 71 ff		REQB
804	138	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f		ATQB
936			50 08 10 2a 1d 7f cf		
464	178	TAG	00 78 f0		ATAT-TRIB
12350			05 00 00 71 ff		REQB
11472			06 00 97 5b		
46082			05 00 08 39 73		REQB
804	214	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f		ATQB
1618			00 00	(SHORT)	
3578			02 80 26 4f 11 0a e7 de		
3050			02 00 16 98 70 10 01 01 76 55 00	** FAIL CRC **	
8198			03 80 32 00 00 18 ea 98		
2334	186	TAG	03 0b 09 87 00 00 10 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00 1d ce		
3540			02 80 2e 01 00 20 43 2f		
1708			02 01 01 e0 f5 ff f5 ff	** FAIL CRC **	
1162	275	TAG	02 00 00 b2 90 00 d3 b4	** FAIL CRC **	
3846			03 80 30 00 00 1d 31 f6		
2124				(SHORT)	
840	93	TAG	04 34	(SHORT)	
13524			02 80 28 00 00 04 17 67 7f 16 3a 81 41		
6012	230	TAG	02 e7	(SHORT)	
33958			03 80 2a 01 00 24 00 17 00 4b 00 00 b2 41 19 09 01 00 28 01 30 ed 8c 17 36 10 00 c2 01 01 09 23 00 10 01 00 00 4b 99 76 da 3b 04 46 49		
14544	162	TAG	03 79 a0 ac 57 90 00 1a 0d		
218628			05 00 08 39 73		
804	138	TAG	50 08 10 2a 1d 53 4e 44 4b 33 81 93 bc 3f		
1104			1d 08 10 2a 1d 00 08 01 00 94 60		ATTRIB
554	206	TAG	00 78 f0		ATAT-TRIB

Table 7. Second example of M/T trace.

http://dx.doi.org/10.5772/64844

Then, the tag answers with an ATATTRIB command, which consists in 3 bytes: the first one is the CID (as indicated by the previous command: 00), while the two last bytes are the CRC-B of the message.

After the ATATTRIB, the RFID session is established and the tag is in the active state, ready for transmitting data.

After analyzing a great deal of traces of the M/T system, it was found that a sequence of six pairs of commands was repeated constantly. Since this is just an example of what can be done with the methodology proposed, we will not deepen into the details, but it will be mentioned briefly the structure of the first two pairs of commands.

The first command is always the same: "02 80 26 4f 11 0a e7 de." The standard ISO/IEC 14443-B indicates that it is an i-block, whose first byte means that it is block number 0 and that it does not contain CID or NAD. The last two bytes of the message are the CRC-B, so the transmitted data are composed by five bytes (80 26 4f 11 0a). These bytes follow ISO/IEC 7816: the first one is the CLA byte (80, proprietary command); the second one is the field INS (26); the third and the fourth (4f 11) are P1 and P2 (parameters of the command); and the fifth (0a) is the field LE, which indicates the number of expected bytes to be received from the tag (i.e., 10 bytes are expected).

This first command is followed by the first response of the tag. As it can be observed in **Table 8**, it is almost the same for every tag. Its structure is as follows:

- Byte 1 (02): it indicates that it is an i-block 0.
- Bytes 2–13: ISO/IEC 7816 data. For instance, bytes 2–3 indicate the total number of trips carried out with the card and bytes 12–13 contain the state of the execution of the command (90-00, successful execution).
- Bytes 14–15: CRC-B.

The second request is also always the same: 03 80 32 00 00 18 ea 98.

- Byte 1 (03): i-block 1.
- Bytes 2–6: ISO/IEC 7816 data. Since CLA is 80, the command is proprietary. INS is equal to 32; P1 and P2 are 00 and 00; and LE (expected length of the answer) is 24 bytes.
- Bytes 7–8: CRC-B.

Trace\#Byte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Card1-Trace 1	02	00	14	98	70	10	01	01	76	55	72	90	00	73	65
Card1-Trace 2	02	00	15	98	70	10	01	01	76	55	72	90	00	e2	30
Card1-Trace 3	02	00	17	98	70	10	01	01	76	55	72	90	00	c0	9b
Card2-Trace 1	02	01	40	98	70	10	01	02	07	90	31	90	00	65	ac
Card2-Trace 2	02	01	42	98	70	10	01	02	07	90	31	90	00	47	07
Card3-Trace 1	02	00	0c	98	70	20	01	01	69	87	97	90	00	ba	6a

Table 8. Responses collected for the first command.

The second answer is related to the use of special fares during a trip. **Tables 9** and **10** show examples of traces for different cards. The data are structured as follows:

- Byte 1 (03): i-block 1.
- Bytes 2–27: ISO/IEC 7816 data. For instance, bytes 12–13 and 14–15 indicate the activation and expiration dates of a special fare, and byte 11 the type of fare (e.g., "1" for standard, "3" for reduced fare).
- Bytes 28–29: CRC-B.

The rest of the pairs answer-response contain other interesting information such the balance of the card, the place where the card was recharged (e.g., ATM, bank) or the data about each trip performed (i.e., cost, date, time, line, and vehicle number).

After all the analysis, it was not found a severe security threat in the system, but there are several issues regarding data privacy that developers should consider.

The main problem is that the RFID communications are performed in plain text, without any kind of ciphering, what leads to the possibility of snooping and emulating them. Thanks to that, an attacker can emulate an unauthorized reader and obtain private data such as the credit balance or the specific characteristics of the trips of a user. Note also that many smartphones currently support NFC (near-field communication), which is partially compatible with ISO/IEC 14443-B tags, and it is straightforward to develop an Android application to read the data (there have already been attacks to ISO/IEC 14443-A tags using mobile phones [24]).

The complete disassembling of the protocol opens the possibility to perform MitM attacks, where a third device might alter the data on the RFID transactions in order to get certain benefits (e.g., for instance, to avoid discounting credit on the card).

Trace\#Byte	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Card 1-Trace 1	03	0b	89	87	00	00	10	00	00	00	01	00	00	00	00
Card 1-Trace 2	03	0b	89	87	00	00	10	00	00	00	01	00	00	00	00
Card 2-Trace 1	03	0b	89	87	00	00	10	00	00	00	03	b5	8c	f5	8d
Card 3-Trace 1	03	0b	89	87	00	00	20	00	00	00	01	00	00	00	00

Table 9. First half of different responses to the second commands.

Trace\#Byte	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**
Card 1-Trace 1	00	00	00	00	00	00	00	00	00	00	90	00	1d	ce
Card 1-Trace 2	00	00	00	00	00	00	00	00	00	00	90	00	1d	ce
Card 2-Trace 1	00	10	30	00	00	00	00	00	00	00	90	00	a8	0c
Card 3-Trace 1	00	00	00	00	00	00	00	00	00	00	90	00	08	7d

Table 10. Second half of the responses to the second command.

http://dx.doi.org/10.5772/64844

4.2. Public transportation card of Santiago de Compostela

This RFID card was used until recently in the city of Santiago de Compostela (Spain) to pay for public transportation.

4.2.1. Visual inspection

Like M/T cards, there is no external sign that identifies the underlying RFID technology. We can only see the contacts of traditional smart card interfaces, so there are at least two interfaces: one wired and another wireless.

4.2.2. Operating frequency and modulation

- Operating frequency. Like the previous cards, it is fair to assume that due to its use for public transportation, there is a high likelihood that it is an HF card. And this fact was confirmed by following the verification steps described in Section 3.2.1.
- Modulation. Once determined the frequency band, it is possible to test the commands for the different ISO/IEC standards. After testing, the ones for ISO/IEC 14443-B and ISO/IEC 15693, it was found that the tag responded correctly to ISO/IEC 14443-A commands that indicated that the tag was a MIFARE Classic 1K.

4.2.3. Understanding the underlying protocols

MIFARE is a contactless smartcard technology from NXP Semiconductors [25] that has sold more than 5 billion tags and fifty million RFID readers. It started to be manufactured around 1994–1995, being its first major deployment performed in Seoul's city transportation.

MIFARE is compliant with the first three parts of ISO/IEC 14443-A at 13.56 MHz, although there are certain differences depending on the version of the tag, which has been evolving during the last years.

MIFARE Classic is probably the most popular version of MIFARE cards. These tags use a really simple application-specific integrated circuit (ASIC) that basically stores data. Their memory is divided into sectors and blocks that are protected with a simple access control system. Each sector is divided into four blocks: three of them contain data, while the other one stores the data access permissions and the access keys.

There is not a fixed data format, although there is a special format called *value block* with specific operations for incrementing and decrementing values. Sectors use two keys (A and B). Each key allows for managing different permissions: a key could be valid only for reading data, while the other one could be dedicated to modify them. The first 16 bytes of the internal memory are read-only and contain the serial number and other data related to the model and the manufacturer. Data are coded in Crypto-1, an already-broken cryptographic protocol [26–28].

There are different MIFARE Classic versions:

- MIFARE Classic 1K. Its name derives from its 1024-byte internal storage, which is divided into 16 64-byte sectors.

- MIFARE Classic 4K. It has 4096 bytes for data divided into 40 sectors.
- MIFARE Classic Mini. It stores 320 bytes in 5 sectors (the actual useful data space is 224 bytes).

After MIFARE Classic, NXP created other versions: Ultralight, Ultralight C, DESFire (whose security was broken in 2011 [29]), Plus, DESFire V1 and V2, etc.

4.2.4. Security analysis

As it was explained in the previous subsection, MIFARE Classic cards implement a security system that prevents reading or writing the internal data. However, this system is outdated and has already been broken.

To get the access keys to read and write the different internal blocks, the Proxmark official firmware offers several options. For instance, the command *hf mf mifare* executes the darkside attack [28] to obtain a valid key. Such an attack usually takes from 30s to half an hour (sometimes it has to be executed several times). An example of the output of the system is shown in **Figure 10**, where the A key of the first block is obtained. Then, another attack called "nested authentication" [30] can be performed: it allows remote attackers to obtain the keys of all the other blocks (in **Figure 11**). Once all the keys have been obtained, a dump of the memory can be extracted.

With the dump, it is possible to study the different parameters (e.g., detect memory changes as more trips are carried out) or save it to restore it later and recover the previous credit balance.

```
------------------------------------------------------------------
isOk:01

uid(329c0b0e) nt(76d9cec2) par(6c7494bcc47cbcc4) ks(0a0a0007040d0204)

|diff|(nr)     |ks3|ks3^5|parity          |
+----+---------+---+-----+----------------+
| 00 |00000000| a |  f   |0,0,1,1,0,1,1,#db# COMMAND mifare FINISHED

0|
| 20 |00000020| a |  f   |0,0,1,0,1,1,1,0|
| 40 |00000040| 0 |  5   |0,0,1,0,1,0,0,1|
| 60 |00000060| 7 |  2   |0,0,1,1,1,1,0,1|
| 80 |00000080| 4 |  1   |0,0,1,0,0,0,1,1|
| a0 |000000a0| d |  8   |0,0,1,1,1,1,1,0|
| c0 |000000c0| 2 |  7   |0,0,1,1,1,1,0,1|
| e0 |000000e0| 4 |  1   |0,0,1,0,0,0,1,1|
------------------------------------------------------------------
Key found:721205421911

Found valid key:721205421911
proxmark3>
```

Figure 10. Obtaining access key A from a MIFARE Classic card with Proxmark.

http://dx.doi.org/10.5772/64844

```
Iterations count: 8
|---|----------------|---|----------------|---|
|sec|key A           |res|key B           |res|
|---|----------------|---|----------------|---|
|000|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|001|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|002|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|003|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|004|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|005|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|006|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|007|  721205421911  | 1 |  b0b1b2b3b4b5  | 1 |
|008|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|009|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|010|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|011|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|012|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|013|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|014|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|015|  7712f5411e53  | 1 |  b0b1b2b3b4b5  | 1 |
|---|----------------|---|----------------|---|
```

Figure 11. Access keys cracked for every sector.

4.3. Animal identification tags

Pet identification has been carried out throughout Europe since the late 1990s. RFID tags are generally implanted subcutaneously. The main purpose of this identification was animal health of the most common pets, including cats, dogs, and ferrets (European Regulation 998/2003). The same system is used in Europe for breeding and production of equidae (European Regulation 504/2008), and for public health in ovine and caprine animals (European Regulation 21/2004).

4.3.1. Visual inspection

In this case, a visual assessment to detect any sign of the underlying technology is not necessary, since these kinds of tags are regulated and specified by the different European regulations previously mentioned.

4.3.2. Detailed analysis

In the case of pet identification, European Regulation 998/2003 specifies that tags have to be compliant with ISO/IEC 11784 [31] and ISO/IEC 11785 [32]. They both describe LF tags, existing two different versions: half-duplex (HDX) and full-duplex (FDX and FDX-B). In Spain, most pets wear FDX-B tags, which use biphasic coding.

- Operating frequency. It was verified with the Proxmark that a sample tag (already implanted on a dog) was LF, as it was expected from the information given in the previous section.
- Modulation. In this case, it was not straightforward to recognize the modulation used, because the signals captured had a lot of noise (the tag had been implanted on the dog a

year before these tests were performed). An example of the signals received is shown in **Figure 12**. It was usually required to filter the signal to reduce the noise, obtaining a figure like the one shown in **Figure 13**, which resembles a biphasic coding.

When these experiments were carried out, the official Proxmark firmware did not support FDX-B, so it was necessary to implement it. Such an implementation first filters and demodulates the signal, and then decodes it.

4.3.3. Understanding the underlying protocols

ISO/IEC 11784 and ISO/IEC 11785 are international standards that regulate RFID for animal identification. Each animal transponder contains 64 bits with the information shown in **Table 11** (the data values included were generated randomly).

The system works at 134.2 KHz, and there are two different transmission modes: half-duplex (HDX) and full-duplex (FDX or FDX-B). In HDX mode, the tag is not able to send data and receive power at the same time. Thus, reading consists in powering the tag for a short interval and then waiting for the tag to transmit the data. In this mode, an 8-bit header (always "01111110") and a 16-bit cyclic-redundancy check (CRC) are sent. An additional chunk of 24 bits is also sent and includes information on the application. Data are modulated in FSK and coded with non-return-to-zero (NRZ).

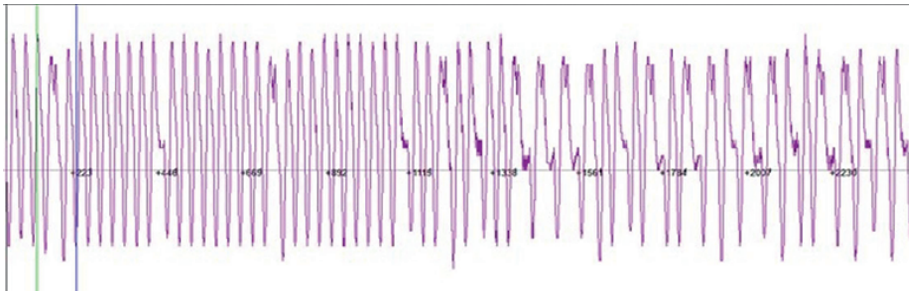

Figure 12. Noisy signal from an animal identification tag.

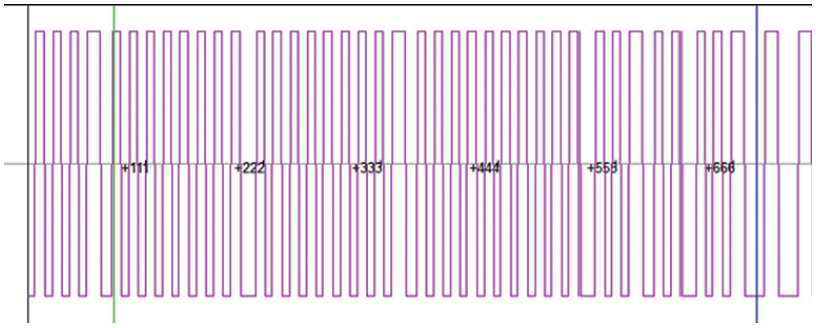

Figure 13. Animal identification tag signal after filtering it.

http://dx.doi.org/10.5772/64844

The tags that operate in FDX-B mode are able to transmit data and be powered at the same time. As it can be seen in **Table 11**, this kind of tags transmits an 11-bit header ("10000000000"), 50 bits of data, 24-bits with the application information and a 16-bit CRC. Moreover, every 8 bits (except for the header) a control bit is added (always "1"). Data are sent in less-significant bit (LSB) order, so, when the reader receives the bits, it can reconstruct them just using simple binary shifts. The bits are modulated in Amplitude-Shift Keying(ASK) and are coded in differential biphase (DBP).

4.3.4. Security evaluation

By making use of the functions implemented, it was straightforward to read data from any FDX-B tag. The software extracts the two main parameters: the country code and the national code (the actual identifier). **Figure 14** shows an example where two consecutive readings were performed: the first one is successful, while the second one shows errors related to a bad reading.

Field\#bit	11	10	9	8	7	6	5	4	3	2	1
	(msb)										(lsb)
Header	1	0	0	0	0	0	0	0	0	0	0
National Code (38 bits)			1	1	0	1	0	0	0	0	0
			1	0	1	0	0	1	1	1	1
			1	0	1	0	0	1	0	0	1
			1	0	1	0	1	0	1	0	1
Country Code (10 bits)			1	1	1	0	0	0	0	0	0
			1	1	1	0	0	0	1	1	1
Data Block Status Flag (1 bit)			1	-	-	-	-	-	-	-	1
Animal Application Indicator (1 bit)			1	1	-	-	-	-	-	-	-
Checksum (16 bits)			1	1	1	0	1	1	1	1	0
			1	0	0	1	0	1	0	1	1
Optional Extra Data (24 bits)			1	0	1	1	1	0	1	1	0
			1	1	1	1	1	0	0	0	1
			1	0	1	0	0	1	0	0	0

Table 11. Internal memory structure of an animal identification tag.

```
Header found, starting data in pos 161
Animal APP
National code: 098104131364
Country code: 981
Obtained CRC: d28d
Calculated CRC: d28d

Header found, starting data in pos 292
Bit control error CC in bit 345
Bit control error in bit 354
Bit control error in bit 372
Bit control error in bit 381
Animal APP
National code: 183524829156
Country code: 249
Obtained CRC: 3ab1
Calculated CRC: 7d8b
```

Figure 14. Example of readings from an animal identification tag.

Security is almost nonexistent in this kind of tags: although writing is not allowed, the tag continuously sends the stored data without any authentication requirement. It may seem that the scenario is not susceptible for including high-security mechanisms, since the objective is to identify the clinical records and the owner of a dog, but in terms of privacy and uniqueness of the identifier, the current system is not effective. Note that, using a device such as Proxmark, it is not only easy to read the data, but also to emulate tags and clone them.

This security problem is even worse when tags are attached to animals aimed at producing human food (e.g., ovine and caprine animals). Cloning or erasing the data breaks traceability, which is the way to determine where an epidemic outbreak was originated.

5. Conclusions

The methodology proposed in this chapter for evaluating security in commercial RFID systems has allowed for detecting relevant flaws in real-world developments, including the following:

- Ability to clone animal identification information.
- Possibility of altering data of certain payment cards.
- Extraction of private information from different transportation cards.
- Possibility of capturing tag-reader communications.
- Possibility of emulating both readers and tags.

Most of the flaws detected were reported to the respective companies, and they have taken the proper measures to mitigate them: in some cases, the system was redesigned to increase security, but most companies had to replace the whole hardware with updated and more secure devices.

The final conclusion is that although RFID systems can implement sophisticated security measures, certain developers have adopted the technology without taking such mechanisms into account. A methodology like the one proposed in this chapter can help to perform audits and determine the security level of an RFID system before taking it from a test environment to a real situation.

Acknowledgements

This work has been funded by the Spanish Ministry of Economy and Competitiveness under grants TEC2013-47141-C4-1-R and TEC2015-69648-REDC.

Author details

Tiago M. Fernández-Caramés*, Paula Fraga-Lamas, Manuel Suárez-Albela and Luis Castedo

*Address all correspondence to: tiago.fernandez@udc.es

University of A Coruña, A Coruña, Spain

References

[1] H. Li, Y. Chen and Z. He. The survey of RFID attacks and defenses. In: 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM); 2012; Shanghai, China. p. 1–4. doi:10.1109/WiCOM.2012.6478720

[2] M. T. Pandian and R. Sukumar. RFID: an appraisal of malevolent attacks on RFID security system and its resurgence. In: IEEE International Conference in MOOC Innovation and Technology in Education (MITE); 2013; Jaipur, India. p. 17–20. doi: 10.1109/MITE.2013.6756297

[3] L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80. doi:10.1109/EURFID.2015.7332388

[4] J. Abawajy. Enhancing RFID Tag resistance against cloning attack. In: Third International Conference on Network and System Security; 2009; Gold Coast, Australia. p. 18–23. doi:10.1109/NSS.2009.101

[5] A. Mitrokotsa, M. R. AU. Rieback and A. S. Tanenbaum. Classifying RFID attacks and defenses. Information Systems Frontiers. 2010;12(5):491–505. doi:10.1007/s10796-009-9210-z

[6] K. Bu, X. Liu, J. Luo, B. Xiao and G. Wei. Unreconciled collisions uncover cloning attacks in anonymous RFID systems. IEEE Transactions on Information Forensics and Security. 2013;8(3):429–439. doi:10.1109/TIFS.2012.2237395

[7] Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28. doi:10.1109/ICASID.2010.5551848

[8] A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States. p. 533–539. doi:10.1109/CTS.2008.4543975

[9] T. L. Lim and T. Li. Exposing an effective denial of information attack from the misuse of EPCglobal standards in an RFID authentication scheme. In: IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications; 2008; Cannes, France. p. 1–6. doi:10.1109/PIMRC.2008.4699588

[10] T. Halevi, H. Li, D. Ma, N. Saxena, J. Voris and T. Xiang. Context-aware defenses to RFID unauthorized reading and relay attacks. IEEE Transactions on Emerging Topics in Computing. 2013;1(2):307–318. doi:10.1109/TETC.2013.2290537

[11] S. Guizani. Implementation of an RFID relay attack countermeasure. In: International Wireless Communications and Mobile Computing Conference (IWCMC); 2015; Dubrovnik, Croatia. p. 1318–1323. doi:10.1109/IWCMC.2015.7289273

[12] A. Francillon, B. Danev and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In: NDSS Symposium 2011: 18th Annual Network & Distributed System Security Symposium; 2011, San Diego, California.

[13] RFIDiot official webpage [Internet]. Available from: www.rfidiot.org [Accessed: June 2016].

[14] Proxmark 3 Community webpage [Internet]. Available from: www.proxmark.org [Accessed: June 2016].

[15] Tastic official webpage [Internet]. Available from: http://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/ [Accessed: June 2016].

[16] OpenPCD Reader [Internet]. Available from: http://www.openpcd.org [Accessed: June 2016].

[17] OpenPICC tag emulator [Internet]. Available from: http://www.openpicc.org [Accessed: June 2016].

[18] Chameleon Project [Internet]. Available from: https://github.com/skuep/ChameleonMini/wiki [Accessed: June 2016].

[19] McAffe's Proxbrute webpage [Internet]. Available from: http://www.mcafee.com/es/downloads/free-tools/proxbrute.aspx [Accessed: June 2016].

http://dx.doi.org/10.5772/64844

[20] M. Feldhofer, M. Aigner, T. Baier, M. Hutter, T. Plos and E. Wenger. Semi-passive RFID development platform for implementing and attacking security tags. In: International Conference for Internet Technology and Secured Transactions (ICITST); 2010; London, Great Britain. p. 1–6.

[21] HID webpage [Internet]. Available from: http://www.hidglobal.com [Accessed: June 2016].

[22] ISO/IEC. ISO/IEC 14443:2000, Identification cards—Contactless integrated circuit(s) cards—Proximity cards.

[23] ISO/IEC. ISO/IEC 7816:1999, Identification cards—Integrated circuit(s) cards with contacts.

[24] Michael Weiß. Performing relay attacks on ISO 14443 contactless smart cards using NFC mobile equipment [thesis]. 2010.

[25] NXP's official webpage [Internet]. Available from: http://www.nxp.com [Accessed: June 2016].

[26] Gerhard de Koning Gans. Analysis of the MIFARE Classic used in the OV—Chipkaart project [thesis]. 2008.

[27] F. D. Garcia, P. van Rossum, R. Verdult, R. W. Schreur. Wirelessly pickpocketing a Mifare Classic card. In: IEEE Symposium on Security and Privacy; 2009; Oakland, United States.

[28] N. Coutois. The dark side of security by obscurity and cloning Mifare Classic rail and building passes, anywhere, anytime. In: International Conference on Security and Cryptography; 2009; Milan, Italy.

[29] D. Oswald, C. Paar. Breaking Mifare DESFire MF3ICD40: Power analysis and templates in the real world. Lecture Notes in Computer Science. 2011; 6917:207–222.

[30] F. D. Garcia et al. Dismantling MIFARE card. In: European Symposium on Research in Computer Security; 2008; Torremolinos, Spain.

[31] ISO/IEC. ISO/IEC 11784:1996, Radio frequency identification of animals—Code structure.

[32] ISO/IEC. ISO/IEC 11785:1996, Radio frequency identification of animals—Technical concept.