NTNU
Innovation and Creativity

Security and Privacy in RFID Applications

Torstein Haver

Master of Science in Communication Technology
Submission date: June 2006
Supervisor: Svein Johan Knapskog, ITEM
Co-supervisor: Martin Gilje Jaatun, SINTEF

Norwegian University of Science and Technology
Department of Telematics

Problem Description

RFID technology is permeating our society, and is rapidly becoming a part of the daily life of the average man and woman. Advocates of RFID focus on the advantages of this development, but generally dismiss any concerns raised over privacy implications.

The assignment consists of experimentally deciding detection distances for passive RFID tags intended for proximity identification, and determine the level of effort required to increase these detection distances beyond the maximum stipulated by the manufacturer. Suitable systems to use as a basis for the research include the new RFID-enabled biometric passports, contactless access cards and contactless payment cards.

Standards for the 13.56 MHz frequency band (ISO14443 and ISO15693) will serve as a natural starting point and will likely be the most appropriate for this assignment.

Furthermore, it shall be experimentally determined to what extent commercial applications are susceptible to tracking by unauthorized third parties, e.g. by strategically placed RFID readers. In this context, the efficiency of various forms of shielding may also be evaluated.

Based on experimental and theoretical results, new solutions that are better suited to serve relevant privacy needs will be proposed. These solutions will also be evaluated with regard to usability, functionality and cost.

Assignment given: 16. January 2006
Supervisor: Svein Johan Knapskog, ITEM

Abstract

Radio Frequency Identification (RFID) is a very versatile technology. It has the potential to increase the efficiency of many common applications and is thus becoming increasingly popular. The main drawback is that the general principles the technology is built on are very vulnerable to attack. The ID imbedded in every chip combined with the openness of the radio interface exposes the users to tracking. As additional sensitive information may be stored on the tags, the user may also be exposed to other security and privacy threats.

This thesis investigates how easily the reading distance of RFID tags can be increased by modifying a regular reader. A thorough presentation of general privacy and security threats to RFID systems is also given together with an analysis of how the results from the experiments influence these threats. General countermeasures to defend against threats are also evaluated. Finally, the thesis investigates how easily a user can reduce the reading distance of tags he is carrying by physical shielding.

The general results are that moderately increasing the reading distance of RFID tags by modifying a regular reader is possible. It is, however, not trivial. Given that the attacker has extensive knowledge of the technology and its implementation, obtaining extensive increases in reading distance by using very sophisticated techniques may be possible. Users can, on the other hand, relatively easily decrease the reading distances of tags by physically shielding them.

The obtainable reading distance using an electronics hobbyist's tools, skills and knowledge is sufficient to greatly simplify the execution of several attacks aimed at RFID systems. As the technological development is likely to increase the obtainable reading distance even further, inclusion of on-tag security measures for the future is of great importance.

Preface

This report is written as a master's thesis in the tenth semester of the five year master program at the Department of Telematics, Norwegian University of Science and Technology.

The thesis is part of my specialization in Information Security and has been carried out for Sintef ICT and the Norwegian University of Science and Technology. The work started early January 2006 with submission date June 14 2006.

I would like to thank Professor Svein J. Knapskog at the Department of Telematics for many stimulating discussions about RFID security and privacy. My supervisor at SINTEF ICT, Martin Gilje Jaatun, also deserves my gratitude for participating in discussions, giving invaluable input and generally following-up throughout the writing process. Further, Bård Myhre and his colleagues at SINTEF have my gratitude for helpful tips and input at the lab. My fellow students at the study hall also deserve warm thanks for their support, helpful inputs and patience.

Table of Contents

Figure List

Table List

Equation List

Abbreviations

AC - Alternating Current
ASK - Amplitude Shift Keying
CEPT - European Conference of Postal and Telecommunications Administrations
DoS - Denial of Service
EAS - Electronic Article Surveillance
ECC - Electronic Communications Committee
EIRP - Effective Isotropically-Radiated Power
EMP - Electromagnetic Pulse
ERO - European Radiocommunications Office
ERP - Effective Radiated Power
ETSI - European Telecommunications Standards Institute
FCC - Federal Communications Commission
FSK - Frequency Shift Keying
HF - High Frequency
IC - Integrated Circuit
ICAO - International Civil Aviation Organization
IEC - International Electrotechnical Commission
ISM-band - Industrial, Scientific and Medical band
ISO - International Organization for Standardization
ITU - International Telecommunication Union
ITU-R - ITU Radiocommunication Sector
LDS - Logical Data Structure
LF - Low Frequency
OEM - Original Equipment Manufacturer
PCB - Printed Circuit Board
PSK - Phase Shift Keying
RF - Radio Frequency
RFID - Radio Frequency Identification
SNR - Signal-to-noise ratio
SRD-band - Short Range Devices band
UHF - Ultra High Frequency
VCP - Virtual COM Port
VDI - The Association of German Engineers

1. Introduction

This thesis studies security aspects of Radio Frequency Identification, RFID. The technology is permeating the society, and is rapidly becoming part of everyday life for more and more users. Thus, the implications of insecure systems are increasing. This thesis will look at the security of RFID Proximity tags at the physical layer. The thesis will attempt to determine the maximum reading distance of RFID tags, and the technology's inherent susceptibility to tracking and other threats will be assessed. Further, the effect of physical shielding will be investigated.

1.1. Background

Radio Frequency Identification (RFID) is a generic term for systems transmitting the identity of an object from a tag to a reader using radio frequency waves. Combined with transfer of other data, and possibly cryptographic functions, this transfer of identity can form elaborate protocols supporting advanced systems such as Access Control Systems, Payment Systems and Article Surveillance Systems.

RFID is by no means a new technology, but it has long been quite expensive. However, the constant development in production techniques etc. has resulted in a substantial decrease in prices of RFID systems. The prices are now low enough to allow RFID systems to be economically feasible for a broad range of applications. This has resulted in an exponential growth of applications utilizing RFID. This growth is further catalyzed by advocates of RFID proclaiming the efficiency and usefulness of the technology. However, the rapid diffusion of RFID into everyday life of its users has also led to questions being asked about the security of such systems. One such question is how easily individuals can be tracked if they carry RFID tags.

All manufacturers of RFID systems test the maximum reading range of their readers before these are put into production. However, these readers are generally not optimized for maximum reading range. Further, they are subject to regulations regarding the transmitting power etc. over the radio interface. Thus, even though the maximum reading range of standard RFID readers are restricted to a few centimeters, optimized illegitimate readers may be able to read tags at far greater distances.

1.2. Objective

The main objective of this thesis is to determine how easily the reading range of commercial RFID systems can be increased. This will be done by experimentally testing several different approaches with increasing complexity and determine the effectiveness of each approach. Based on the results, assessment of how easily tags used in commercial applications can be tracked will be made. A secondary objective is to determine how easily tags can be physically shielded to prevent unwanted reading. This will be done by experimentally testing various forms of shielding.

1.3. Risks and Uncertainties

In undertaking an experimental study of the physical properties of RFID systems, one of the most prominent risks is the risk of lack of detailed protocol information. The RFID systems studied in this thesis are mostly based on standard protocols, but even within such standards, there is room for variations. This means that it may prove difficult to design new equipment from scratch that will interoperate smoothly with existing equipment. This is further enhanced by the fact that few commercial actors are willing to provide detailed information regarding their systems if they fear that the inquirer is attempting to prove that their systems are insecure.

As this thesis is written as part of a specialization in Information Security, lack of technical expertise on electronic circuits, radio techniques, appropriate measurement techniques etc. may also become a problem. This may result in much of the thesis being based on experiments performed by others, and as worst case scenario result in a purely theoretical literature study. Lack of expertise may also slow the work down leading to difficulties in keeping the deadline. The time constraint is extra important as there may be hold ups due to delivery times etc. if equipment or components have to be bought.

1.4. Scope

This thesis aims at determining how easily the maximum reading distance of commercial RFID systems can be increased, and consequently determine the tags' susceptibility to skimming and tracking. The effect of physical shielding will also be tested. If time permits, further investigations into the threat of eavesdropping will be made.

The focus of this thesis will be on systems for Access Control and Biometric Passports. Both these systems are generally based on the "ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards – Proximity cards" standard[1], and hence this standard will serve as a reference point. Other important standards such as the "ISO/IEC 15693: Identification cards – contactless integrated circuit(s) cards – Vicinity cards"[2] and "ISO/IEC 10536: Identification cards – contactless integrated circuit(s) cards – Close-coupled cards"[3] will not be assessed. The tags studied in this thesis will therefore exclusively be passive tags that operate in the 13.56 MHz frequency range.

Further, the experiments will mainly regard the lower layers of the RFID protocols. Thus, security features implemented at the application layer will be discussed, but generally not be tested in the experiments as they normally give little protection against threats such as tracking.

1.5. Method

This thesis will mainly be based on an experimental approach. The maximum reading distance of certain RFID systems, and how easily this can be increased, will be attempted determined through several experimental approaches. Experiments to determine how easily unwanted reading can be prevented by physical shielding of tags will also be performed. Further, if time permits, experiments will be performed in an attempt to investigate the possibility of eavesdropping on RFID systems. The experiments will also be complemented by theoretical analyses of threats to RFID systems and relevant countermeasures.

1.6. Clarification of Terms

Throughout this thesis, terms are used that may be easy to misunderstand. Clarifications of some important terms are therefore given below.

"Reading Range" vs. "Reading Distance"

Both *"reading distance"* and *"reading range"* are defined as the maximum 1-dimensional distance between reader and tag when they are communicating. However, *reading distance* is defined as a property of a tag, whereas *reading range* is defined as a property of a reader. *Reading distance* may also represent a property of an RFID system.

In general, the *maximum reading distance* and *maximum reading range* are theoretical concepts as it is not possible to prove it impossible to read tags at greater distances.

When discussing shielding, the "*reading distance"* is defined as the maximum distance where the reader successfully decodes a tag's reply to a Select-command in more than 50% of the attempts.

"Coil" vs. "Coil Antenna"
The term *"coil antenna"* is throughout this thesis used to describe an antenna shaped as a coil. Such an antenna normally consists of a coil, matching circuits, connectors etc. The term *"coil"* refers to the actual coil of the antenna. Thus, a *"coil"* is a part of a *"coil antenna"*.

1.7. Thesis Outline

Chapter 2 gives a thorough introduction to the RFID technology including its history and current applications. Chapter 2 also describes RFID standardization and regulations.

RFID security is examined in chapter 3. Several known threats and attacks are also outlined in this chapter together with various on- and off-tag security enhancements to thwart these attacks.

Chapter 4 outlines the thought process of the early stages of this thesis. It lists several approaches for extending the reading range of an existing reader together with advantages and disadvantages of each approach. Hypotheses for the experiments are also given here.

Chapter 5 gives more detailed descriptions of the experiments. The equipment is listed and more accurate accounts of how the experiments were performed are given. The results from each experiment are also listed. Further, some relevant experiments performed by others are described together with an outline of their most important results.

The results from the experiments are discussed in chapter 6. This chapter also contains an analysis of general RFID security together with implications of increased reading distance. Finally in chapter 7 conclusions are drawn and in chapter 8 a brief description of potential future research areas are presented.

2. The Technology

In the following some important aspects of general RFID technology will be outlined. The system components will be discussed briefly, the basics of RFID history will be outlined, and some physical principles will be explained. Further, some applications utilizing RFID are described, and some of the most important RFID standards are listed.

2.1. RFID Components

RFID is a generic term for systems transmitting the identity of an object from a tag to a reader using radio frequency waves. Thus, an RFID system is generally composed of two components;

- The *tag* or *transponder* which is connected to the object being identified, and
- The *reader* or *interrogator* which is used to read information from the tag.

Figure 1 shows a RFID system setup.

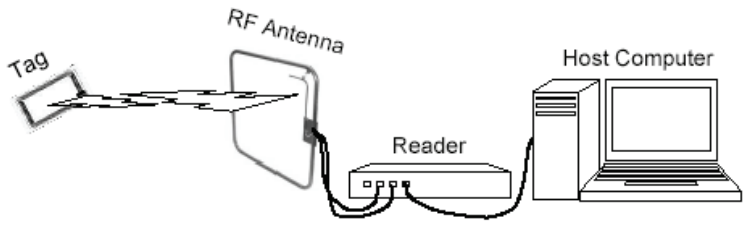

Figure 1: RFID components [4]

In some RFID systems a separate component called a writer is used. This component is used to write information to tags. This functionality can, however, easily be incorporated in the reader, and most systems therefore do not make use of a separate writer component.

In a general RFID system there are more tags than readers.

2.1.1. RFID Tags

An RFID tag is an information carrying chip. It generally carries the identity of the associated object, but can also store other information relating to the object. All tags incorporate an antenna for radio frequency communication. Further, tags may incorporate batteries, state logic, microprocessors etc. The memory may also be divided

into a general memory sector and a secure memory sector. The general memory sector is then available to readers, whereas the secure memory sector is used for storing keys etc. and is generally not available to readers.

Figure 2 shows an example of a regular RFID tag.

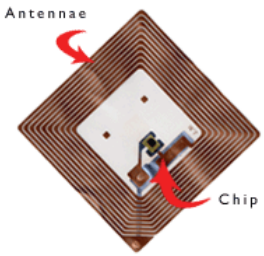

Figure 2: A regular RFID tag [W1]

Tags come in many different forms and shapes, and it is thus useful to classify them. One common way of classifying tags is by their operating frequency[5]. Tags operating at below 135 kHz are normally referred to as Low Frequency (LF) tags, those operating at 13.56 MHz are referred to as High Frequency (HF) tags, those operating at 868 MHz and 915 MHz are referred to as Ultra High Frequency (UHF) tags, and those at 2.43 GHZ are referred to as Microwave tags.

Another very common way of classifying tags is by how they acquire their operational power[6]. Some tags incorporate their own power supply in form of a battery. These tags are called active tags. This is an easy-to-understand approach, but results in physically large tags with limited lifetimes. Further, batteries are not suitable in some environments. The other way of supplying power to tags is by electric or magnetic induction. These tags are known as passive tags and rely on electric or magnetic fields set up by the reader for power. The major drawback of this type of tags is their limited reading distance due to the limited range and strength of the electric and magnetic fields. However, they do not need a battery and can thus be much smaller and will generally have extensively longer lifetimes.

A third class of tags known as semi-passive tags are tags that incorporate a battery for internal processing, but utilize the energy from the reader to transmit the reply[6]. These tags combine the advantages and disadvantages of both passive and active tags. As they incorporate a battery, they can not be made as small as passive tags, but they have longer reading distances as they only need energy from the reader to send the reply, not

for the internal processing. Their lifetimes will also generally be longer than for active tags.

RFID tags come in all forms and shapes, and will generally be designed to fit the application. According to [6], the smallest tag ever made is the Hitachi mu-chip. This chip was designed to be imbedded in sheets of paper and be used to track documents printed in an office environment and was thus only 0.4mm thick. Tags used for access control are often shaped as card type ID-1 as specified in the "ISO/IEC 7810 Identification cards – Physical characteristics" standard[7], that is, in the shape of regular credit cards. Other tags may be far larger, such as tags used in transport systems etc. Figure 3 shows some tags with special shapes.

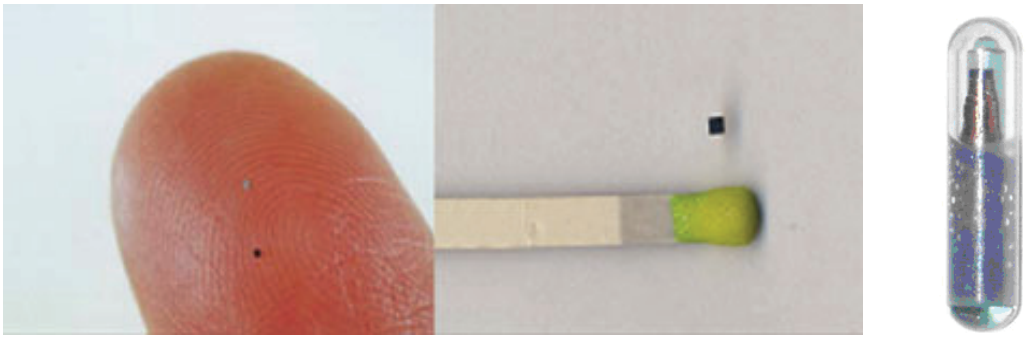

Figure 3: Hitachi mu-chip and EM Microelectronic glass ampoule tag [W2], [W3]

As the shape and size of a tag generally affects the shape of its antenna, it also greatly affects the maximum reading distance. In general, smaller tags have smaller antennas, and therefore shorter reading distances.

2.1.2. RFID Readers

RFID readers are the interrogating part of RFID systems. They come in many different forms and shapes, but in general, all readers incorporate a radio frequency module, an antenna and a control system. Readers may also comprise memory modules or interfaces, such as USB, in order to connect to backbone databases, processing systems etc. Figure 4 shows 3 different RFID readers.

Figure 4: Various RFID readers [W4], [W5]

To communicate with tags, the reader sets up an interrogation zone in form of an electromagnetic field. This field powers the tags and may be interpreted as an "Are there anyone there"-signal. Whenever a tag enters this interrogation zone it is activated by the field and replies with an "I am here"-signal to the reader. The reader can then query the tag for information.

2.2. RFID History

As mentioned, RFID is not a new technology. Already during World War II RFID was pioneered by the British to identify their own planes as they returned from raids over Europe[6]. The early radar techniques could spot airplanes, but not determine whether they were friendly or not. To improve the system the British tagged their airplanes, and could thus identify them using RFID. This system was known as "Identification, Friend or Foe".

Since World War II, RFID has developed quite far. During the 1960s, the first commercial activities relating to RFID were launched[W6]. The 1970s were primarily characterized by developmental work, and notable advances were made at research laboratories and academic institutions. In 1977 one of the first RFID systems introduced to the market was launched by Los Alamos Scientific Laboratories in form of an access control system[6].

The 1980s were characterized by implementation of RFID systems[W6]. The first RFID system for collecting tolls for toll roads was implemented in Norway in 1987, and several other systems for transportation, personnel access and animal identification were also launched during this decade.

During the 1990s, large scale employment of automatic toll collection using RFID was seen[W6]. Other applications such as applications for dispensing fuel, access control for vehicles, ski passes etc. were also gaining widespread use. With the development of the 13.56 MHz RFID systems in the first half of the 1990s it became, for the first time, possible to incorporate a transponder system in the 0.76 mm thick ID-1 format[5]. This made many RFID systems much more practical.

In the recent years, implementation of RFID has more or less exploded. Countless numbers of applications have been launched, and the technology is becoming an integral part of more and more people's everyday lives. The security aspect of RFID is also slowly gaining more attention.

2.3. Physical Principles

Radio frequency communication is a fundamental part of RFID systems. In order to understand how this is accomplished, a basic understanding of the underlying physical principles is necessary.

2.3.1. Magnetic Fields

All moving charges are associated with a magnetic field[5]. Thus, if a current flows through a wire, a magnetic field is generated around the wire. The magnitude of this magnetic field is described by the *magnetic field strength, H*, and is dependant on the magnitude of the current flowing through the wire. The direction of the field etc is shown by Figure 5.

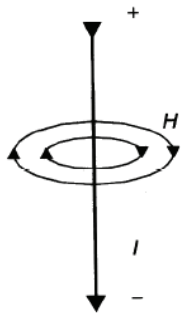

Figure 5: Lines of magnetic flux around current-carrying conductor [5]

If several wires are placed in parallel, the magnetic field strength is increased. In principle, sending a current through a coil is equivalent to sending the same current

through a set of parallel rings. The magnetic field is increased for each winding on the coil. Thus, coils are used by readers as antennas for setting up the magnetic field referred to as the interrogation zone[5]. The principle is exemplified in Figure 6.

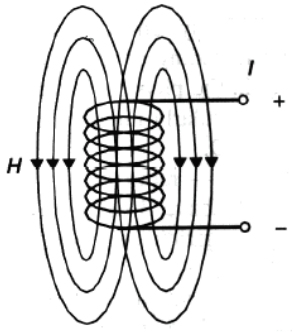

Figure 6: Lines of magnetic flux around a current-carrying coil [5]

The strength of the magnetic field decreases as one move away from the centre of the coil. The magnetic field strength (H) at a distance x along the X-axis can be estimated by Equation 1.

$$H = \frac{I \times N \times R^2}{2\sqrt{(R^2 + x^2)^3}}$$

Equation 1: The magnetic field strength along the x-axis of a round coil [5]

Alternating magnetic fields are always associated with an induced electric field and are thus known as electromagnetic fields[5]. The relative strengths of these fields depend on several factors such as the operating frequency of the system, the physical dimensions of the generating antenna and the distance from the antenna[W7]. For example, some antennas are designed to generate magnetic fields whereas some are designed to generate electric fields. Further, inside what is known as the radian sphere, a sphere around the generating antenna with radius $\lambda/2\pi$ (where λ is the wavelength), the magnetic field dominates the electromagnetic relationship[W7]. Outside this radian sphere, the electric field dominates. This radian sphere thus also marks the boundary between what is known as the *"near field"* and the *"far field"*. The near field is the field within this radian sphere where the magnetic field is dominant, whereas the far field is the field outside the radian sphere where the electric field is dominant. In general, inductively coupled RFID systems only work within the near field. Outside the radian sphere the magnetic field strength decreases so rapidly that harvesting its energy becomes practically impossible. With a frequency of 13.56 MHz, the near field of

inductively coupled systems extends to approximately 3.5 meters. The exact physics behind this phenomenon is, however, beyond the scope of this thesis.

2.3.2. Power Supply to Passive Tags

If a coil is placed within a varying magnetic field, the magnetic field exerts a force on the electrons in the coil antenna[5]. This force results in a current flowing through the coil which can be used to charge a capacitor which again can provide power to a tag. Tags therefore use coils as antennas. Figure 7 shows how the coils are connected by the magnetic field.

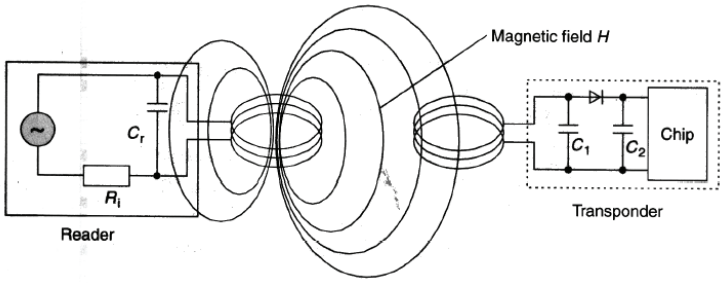

Figure 7: Power supply to an inductively coupled transponder [5]

This principle is referred to as inductive coupling and is much the same as what is used in transformers[5]. The efficiency of the power transfer between the reader and the tag is dependant on several factors including the frequency of the system, the area of the coil and the number of windings. The relative angle between the two coils and the distance between them also affects the power transfer.

2.3.3. Optimal Antenna Diameter

As one moves away from a coil antenna, the magnetic field strength decreases[5]. The magnetic field strength does, however, peak at a certain ratio of distance x from antenna to antenna radius R. Therefore, for each given reading range of an RFID system, there exists an optimal radius for the reader antenna. This optimal radius can be derived from Equation 1 and is, for a round coil antenna, given by Equation 2.

$$R = x \times \sqrt{2}$$

Equation 2: Optimal antenna radius [5]

However, as the radius of the coil is increased, the maximum magnetic field strength generated by the antenna decreases. Thus, unless the other factors influencing the

magnetic field strength are adjusted according to the increased coil radius, the field may be too weak to power tags even at zero distance from the coil. In other words, more current or more windings is necessary if a larger coil antenna is used.

2.3.4. Antenna Tuning and Impedance Matching

As described above, a magnetic field set up by a coil will induce a current in another coil inserted into the field. However, in order to optimize the power transfer between two such coils, they must be tuned to the correct frequency. This process is often referred to as impedance matching and must be performed on the reader and tag antenna to optimize the power transfer[5, 8].

Generally, when dealing with AC-circuits, a load must have the same impedance as the driver in order to maximize the power transfer[9]. The impedance of a circuit element is defined as the relation of the phasor voltage (Vγ) across it to the phasor current (Iγ) flowing through it, as defined by Equation 3.

$$Z = \frac{V_r}{I_r}$$

Equation 3: Definition of impedance [8]

In general, capacitors and coils may be added to the circuits in order to change their impedance[8]. By adding a capacitor in parallel to a coil antenna, the impedance of the antenna can be changed. The result is also a parallel resonant circuit[5]. The capacitance (C) of the ideal capacitor for an antenna is dependant on the inductance (L) of the coil and the operating frequency (f) of the system, and can be calculated using the Thomson equation given by Equation 4.

$$f = \frac{1}{2\pi\sqrt{L_2 C_2}}$$

Equation 4: Thomson equation[5]

2.3.5. Data Transmission

In RFID systems, data transmission is achieved by modulating the magnetic field in different ways[5]. In many systems a different technique is used on the forward channel (from reader to tag) than on the backward channel (from tag to reader). This is due to the scarce resources available to the tag relatively to what is available to the reader.

Forward Channel

On the forward channel data transmission can easily be done using for example Amplitude-, Frequency- or Phase- Shift Keying (ASK, FSK or PSK)[5]. These are all techniques used by a reader to modulate a carrier wave or a field it is generating. As the names suggest, ASK involves varying the amplitude of the field in cord with the data to send, FSK involves varying the frequency of the field, and PSK the phase of the field.

Backward Channel

As the tags do not generate a field of their own, the techniques used on the forward channel are not directly applicable to the backward channel. Thus, other techniques are necessary.

Load modulation and backscatter techniques are two common ways for tags to send data to the reader[6]. Both techniques involve modulating the field already set up by the reader. Generally, systems operating within the near field of readers utilize load modulation whereas systems operating in the far field utilize backscatter techniques. As only near field systems will be investigated in this thesis, backscatter techniques will not be discussed further.

As mentioned earlier, whenever a coil is inserted into a varying magnetic field, a force acts upon the electrons in the coil resulting in a current flowing through it. This current draws its energy from the magnetic field[5]. The reduction of energy in the field can be registered as a voltage drop over the generating antenna. Thus, by switching a load resistor, connected to the tag's coil antenna, on and off in chord with the data to send, the tag draws energy from the field in a pattern dependant on the data. The data can then be extracted by the reader through the same pattern measured as voltage drops at the reader's coil. This technique is generally referred to as load modulation.

Load modulation is a very simple and effective technique in systems with scarce resources. It does, however, present a few restrictions on the system. Firstly, load modulation can only be used within the near field of a reader[5]. If a coil is inserted into the far field of a reader, the reader will not register the same drop in voltage over its antenna, and thus be unable to receive the data. Secondly, load modulation only works as long as the tag can modulate an existing field set up by a reader. That is, the reader must generate the carrier wave throughout the entire transmission from the tag.

2.4. The Singulation Process

Communication through the use of load modulation is quite efficient for RFID tags. However, if more than one tag should try to modulate the reader's field at the same time, the reader would not be able to distinguish the transmissions, and would not be able to correctly decode either of them. Thus, if more than one tag enters the interrogation zone of a reader at the same time, the reader needs a procedure for selecting the tags so that they can be read in turn. This process is known as the singulation process. One common example of a singulation protocol is the Dynamic Binary Search procedure[5].

In order for the Dynamic Binary Search procedure to work, the reader must be able to detect the exact bit position at which a collision occurs. This can easily be done by coding the data with for example Manchester code, i.e. the value of each bit is coded as a positive or negative change in transmission level[5]. In this way, a collision would result in the transitions cancelling each other. As shown by Figure 8, this is easily detectable for the reader.

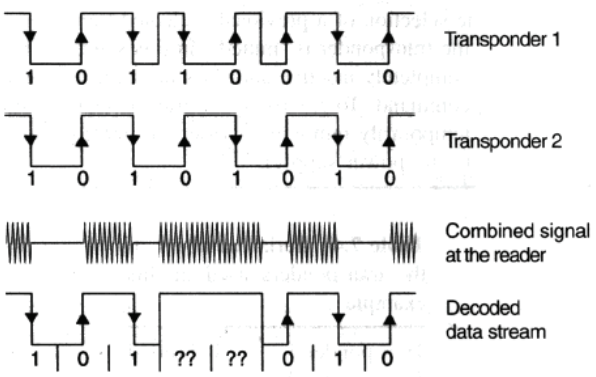

Figure 8: Collision behavior for Manchester code [5]

The main idea behind the Dynamic Binary Search procedure is that the reader broadcasts a Request message containing a prefix. All tags in the reader's interrogation zone with an ID starting with the prefix in question answer the request with the rest of their ID. If only one tag responds, the reader has the whole ID of this tag. If more than one tag responds, at least one collision occurs. The reader detects the collisions and extends the prefix to the position of the first collision. This way only one of the tags responsible for the first collision will answer the next Request message. This procedure is repeated until an answer without collisions is detected. When this happens, the reader has the whole ID of a tag, and includes this in a broadcasted Select command. This way

only the tag in question will answer subsequent messages. This procedure is analogous to searching trough a binary tree where each tag ID represents a leaf node in the tree.

When the read operation is complete, the reader issues an UnSelect command including the ID of the selected tag. This causes the tag to remain silent for a short while and thus prevent it from causing unnecessary collisions when the reader is trying to singulate other tags in the interrogation zone.

2.5. RFID Applications

RFID technology is permeating more and more application areas. In the following, a short overview of some of the most common applications will be given, together with some of the applications that are envisioned in the near future.

2.5.1. Electronic Article Surveillance Systems

One widely used application of RFID is Electronic Article Surveillance (EAS) systems. It was mainly developed by Sensormatic and Checkpoint, two commercial companies founded in the late 1960s[W6].

The main idea behind EAS systems is to limit shoplifting by the use of RFID tags. Each item is equipped with a tag that is removed or destroyed upon payment. All exits are equipped with antennas such that a customer leaving the store has to pass through the interrogation zone of a reader. Whenever the reader detects a tag, an alarm is set off. Thus, if the customers do not pay for their goods, an alarm is set off as they leave the store.

2.5.2. Contactless Smartcards

RFID is also very common in contactless smartcards. Regular, contact-based smartcards rely on electrical contacts linking the reader and an integrated circuit on the card, and are used in a vide variety of applications involving access control, ticketing, payment systems etc. However, if the electrical contacts are polluted, communication may not be possible. Contactless smartcards based on RFID solve this problem by the use of wireless communication. No physical contact is necessary, and thus contactless smartcards can be used in more harsh environments than regular contact-based smartcards. Further, contactless smartcards also relive the user of the physical effort of inserting the card into the reader. The contactless smartcard can actually be read while it is still in the user's handbag[5].

2.5.3. Transport systems

RFID is also widely used within transport industries. For example, a standard way of tracking containers is by the use of a unique identification number[5]. This number is traditionally painted on the side of the container, and whenever a container enters or leaves a depot, the identification number is manually registered in a database. The efficiency of such a procedure is greatly increased if the identification number is stored in an RFID tag. By the use of a handheld reader, the clerk at the entrance to the depot can then easily update the database by reading the tag.

The European Eurobalise S21, a security and control system for European railways, is another example of an RFID application in the transport industry[5]. Traditionally, speed limits, stop signs and control information have been relayed to the driver by the use of signs and light signals. The Eurobalise S21, however, utilizes RFID to convey the same information. Attached to the underside of each locomotive is an RFID reader. Restrictions etc. along the track can then be encoded in RFID tags located on the sleepers. When the locomotive travels past a sleeper with a tag, the tag is read and the information is displayed to the driver. An autopilot function may also be realized in the same way by letting the on-board computers act on the information directly, without waiting for the consent of the driver.

2.5.4. Container Identification

When filling gas bottles, it may be very important that the gas is filled on the correct type of bottle. A mismatch between the gas and bottle may be fatal[5]. If, however, each gas bottle is tagged with an RFID tag, and each filling station is equipped with a reader, mismatches can be identified more easily. Whenever a bottle is to be filled, the tag on the bottle is read and the bottle type (which is either stored on the tag or in a database entry linked to the tag's ID) is checked with respect to the type of gas. If there is a mismatch, the filling station rejects the bottle. This way, a human error in the bottle selection process is rendered harmless.

RFID can also be used to distribute the costs of waste disposal more fairly[5]. If the amount of waste produced by participants in a waste disposal regime is very uneven, an even split of the costs may not be desirable. By tagging each waste disposal bin, and equipping each garbage truck with a reader and some way of measuring the amount of waste, the entity responsible for waste disposal can easily keep track of the amount of

waste generated by each participant. This information can then be used to calculate a more fair distribution of the costs.

2.5.5. Industrial Automation

Industrial automation is another important use of RFID. RFID can, for example, be used to improve the assembly line production method[5]. Each object moving down the assembly line can be tagged with a tag containing relevant data to the production process. This data is then instantly available at each new station along the line. In the automobile production process, this could be used to store the buyer's preferences on the tag, and letting each station along the route optimize the car with respect to these preferences.

2.5.6. Substitute for Bar Codes

RFID has also been envisioned as a substitute for bar codes in the retail industry[10]. Compared to traditional bar codes, RFID tags have the potential to store substantially more information. Instead of identifying an item group as bar codes do, RFID systems could use sufficiently long article numbers to identify individual items. The tags could also store information such as expiration dates etc. Further, RFID readers are not dependant on direct line of sight in order to read tags. This greatly speeds up the checkout process at the counter. As RFID readers can singulate tags and read them one at a time, a customer would not even have to remove the goods from the shopping cart, but could actually just push the cart in front of a reader's antenna.

If each item in a store was tagged with an RFID tag, these tags could also be utilized after the goods have been bought. If, for example, the customer's refrigerator was equipped with an RFID reader, the refrigerator could notify the customer when he is out of a certain item or if the expiry date for some of the goods has passed. Similarly, an RFID enabled washing machine could notify a customer if he tries to wash incompatible clothes at the same time (for example red and white socks).

An example of an organization working towards the world-wide adoption of RFID in supply chain management is EPCglobal, Inc.[W8]. The major obstacle for this world-wide replacement of bar codes with RFID tags seems, however, to be the increased costs. The cost of RFID tags is constantly decreasing, but bar codes are still much cheaper.

2.5.7. E-Passports

A relatively recent development is the use of biometric data in passports. If a digital image of the passport holder is stored in the passport, automatic facial recognition can be used at the border. A new picture taken at the border is automatically compared to the one stored in the passport, and the passport holder is only allowed to pass if the two images match each other. This increases the security of the passport system as automatic facial recognition is much more accurate than manual facial recognition. However, there must be some means of transferring the picture stored in the passport to the border control so that the comparison can be performed. This can be done using RFID, and passports utilizing this technology are often known as e-passports[11].

The U.S. government has decided to include biometric data in their passports, and utilize RFID to communicate with the chip in the passport[12, 13]. The implementation is based on the International Civil Aviation Organization's (ICAO) specification for Biometric Deployment of Machine Readable Travel Documents. This specification includes descriptions of the air interface and relevant security mechanisms, including a security mechanism referred to as Basic Access Control (BAC). This mechanism utilizes a code optically printed on the cover of the passport to compute a key used for access control and encryption[14]. Even though claims have been made that the security of this scheme is too low, inclusion of such security measures is a step in the right direction.

The decision to implement e-passports in the U.S. also affects all members of the U.S. Visa Waiver Program who are required to implement similar passport systems for visa-free entry into the U.S. Further, an analogous passport system utilizing RFID, but also incorporating finger prints as biometric data, will be implemented in the European Union[15].

2.6. RFID Standards

There are many different RFID standards on the market today. Giving a complete list of all would be impossible. However, there are some standards and standardization agencies that are more prominent than others. A brief list of some important RFID standards is given below.

2.6.1. The International Organization for Standardization

The International Organization for Standardization (ISO) is one of the main contributors to the standardization of RFID[W9]. On some topics, ISO works together with the International Electrotechnical Commission (IEC)[W10]. Some of ISO's most important standards related to RFID include:

- Animal Identification
  - ISO 11784: "Radio-frequency identification of animals – Code structure"
  - ISO 11785: "Radio-frequency identification of animals – Technical concept"
  - ISO 14223: "Radio-frequency identification of animals – Advanced transponders"

- Contactless Smart Cards
  - ISO/IEC 10536: "Identification cards – contactless integrated circuit(s) cards – close-coupled cards"
  - ISO/IEC 14443: "Identification cards – contactless integrated circuit(s) cards – proximity cards"
  - ISO/IEC 15693: "Identification cards – contactless integrated circuit(s) cards – vicinity cards".
  - ISO/IEC 10373: "Identification cards – test methods"

- Container Identification
  - ISO 10374: "Freight containers – Automatic identification"

- Item Management
  - ISO/IEC 15961: "Information technology – Radio frequency identification (RFID) for item management – Data protocol"
  - ISO/IEC 15962: "Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions"
  - ISO/IEC 15963: "Information technology – Radio frequency identification for item management – Unique identification for RF tags"
  - ISO/IEC 18000: "Information technology – Radio frequency identification for item management"

- ISO/IEC 18001: “Information technology – Radio frequency identification for item management – Application requirements profiles”

2.6.2. Other Standardization Organizations

The Association of German Engineers (VDI) has also contributed to the standardization of RFID[5]. Among their standards we find:

- Electronic Article Surveillance
  - VDI 4470: “Anti-theft systems for goods”

The International Civil Aviation Organization (ICAO) is a major contributor to the standardization of biometric passports[W11]. Their most important standards include:

- Biometric Passports
  - “Biometrics Deployment of Machine Readable Travel Documents”
  - “Development of a Logical Data Structure – LDS For Optional Capacity Expansion Technologies”
  - “PKI for Machine Readable Travel Documents offering ICC read-only access”

EPCglobal, Inc. is a joint venture between GS1 (formerly EAN International) and GS1 US (formerly Uniform Code Council, Inc.) working for the standardization of RFID in supply chain management[W8]. Among their standards we find:

- Retail Management
  - "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9" ("Gen2 Specification").

2.7. RFID Regulations

As RFID is becoming more common, laws for governing the technology is becoming increasingly important. In the following, some important aspects of RFID regulations will be presented.

2.7.1. RFID Legislation

RFID systems utilize radio waves to communicate. Thus, they are subject to the same laws and regulations as general radio systems. The frequency spectrum is generally

regarded as a scarce natural resource, as equipment operating in overlapping frequency bands may cause interference. Thus, in addition to general regulations, regulations exist to effectively utilize the frequency spectrum[W12]. These regulations are often based on licensing. Each radio application is licensed to operate within an allocated frequency band. As radio waves propagate without respect of political boundaries, the licensing is often based on international cooperation. Several international standardization organizations exist to facilitate such agreements, such as the International Telecommunication Union (ITU), the Electronic Communications Committee (ECC) and the European Telecommunications Standards Institute (ETSI).

The International Telecommunication Union is a specialized agency of the United Nations with responsibility for standardization and allocation of the radio spectrum[W12]. The radiocommunications branch of ITU, the ITU-R, is mainly responsible for overseeing and facilitating inter-governmental negotiations to develop legally binding agreements between sovereign states. These agreements are embodied in the Radio Regulations which form the heart of the ITU-R's work with allocation of the frequency spectrum. Another part of the Radio Regulations, the Table of Frequency Allocations, is a list of all services and frequency bands allocated in different regions kept by ITU-R.

The Electronic Communications Committee is the committee that brings together the radio and telecommunications regulatory authorities of the 46 European Conference of Postal and Telecommunications Administrations' (CEPT) member countries[W13]. The committee is supported by the European Radiocommunications Office (ERO). One main objective of ERO is to develop proposals for a European Table of Frequency Allocations and Utilisations.

The European Telecommunications Standards Institute is another standardization organization working for standardization of information and communication technologies[W14]. Its main objective is to provide a forum in which all key participants can contribute to develop standards for harmonization of such technologies.

In addition to these international organizations, individual countries may have their own legislative authorities in charge of national legislation, such as the Norwegian Post and Telecommunications Authority[W15]. In the U.S., this task is performed by the Federal Communications Commission (FCC)[W16].

Even though licensing is an effective way of preventing harmful interference, excessive intervention from the authorities may be harmful[16]. For example, if every new

application utilizing low-power, short-range radio communication requires allocation of its own frequency band, the number of possible applications will be impractically low, and applications would probably be drowned in paperwork before entering the market. To avoid such problems, some frequency bands are reserved for unlicensed use, that is, they can be used without prior licensing. These bands are generally known as Industrial, Scientific and Medical (ISM) or Short Range Device (SRD) radio bands[W12].

The main advantage of ISM bands is that the bands can be used without individual permission. The equipment must, however, tolerate interference generated by other equipment operated within the same band. To minimize these problems, requirements are set that all equipment must fulfill in order to be allowed to operate within the bands. For example, the European Radiocommunications Committee has decided that the frequency bands 6765 - 6795 kHz and 13.553 - 13.567 MHz should be exempted from individual licensing[16]. That is, radio communication equipment operated within these frequency bands can be used freely throughout the CEPT member states without special permission from the authorities as long as they fulfill the requirements of Table 1.

Table 1: Technical characteristics of equipment [16]

Frequency Band	Field strength	Antenna	Channel Spacing	Duty Cycle (%)
6765-6795 kHz	42 dBμA/m at 10 m	Integral (no external antenna socket) or dedicated	No channel spacing – the whole stated frequency band may be used	No duty cycle restriction
13.553-16.567 MHz	42 dBμA/m at 10 m	Integral (no external antenna socket) or dedicated	No channel spacing – the whole stated frequency band may be used	No duty cycle restriction

RFID tags complying with the ISO/IEC 14443 standard[1] operate at a frequency of 13.56 MHz +- 7 kHz. That is, they operate within the frequency band 13.553-16.567 MHz. Thus, as long as they have an integral or dedicated antenna and a field strength less than 42 dBμA/m at 10 meters, they can be freely used throughout the CEPT member states without special permission. Similar requirements for this frequency band are formulated by the other standardization organizations. Thus, RFID systems can generally be used without special permission throughout the most of the world.

For each frequency spectrum different regulations apply. Table 2 shows an overview of regulations for various RFID frequency ranges.

Table 2: Overview of RFID frequency ranges and regulations [W17]

Frequency range	Comment	Allowed field strength / transmission power
9-135 kHz		42-72 dBμA/m at 10 m
6.765-6.795 MHz	SRD	42 dBμA/m at 10 m
7.4-8.8 MHz	Mainly used for EAS	9 dBμA/m at 10 m
13.553-13.567 MHz	ISM, ISO 14443, ISO 15693, ISO 18000-3 etc.	42 dBμA/m at 10 m
26.957-27.283 MHz	ISM	42 dBμA/m at 10 m
433 MHz	ISM, rarely used for RFID	10-100 mW
865.6-868 MHZ	SRD, Europe only	500 mW ERP[1]
902-928 MHz	SRD, U.S./Canada only	4W EIRP[2], spread spectrum
2.4-2.483 GHz	ISM. Europe only 2.446-2.454 GHz	U.S.: 4W EIRP, Spread spectrum Europe: 4W/500mW (indoor/outdoor)
5.725-5.875 GHz	ISM	U.S.: 4 W EIRP Europe: 25 mW EIRP

[1] Effective Radiated Power
[2] Effective Isotropically-Radiated Power

2.7.2. The RFID Bill of Rights

Privacy is generally considered a user's right. Hence, in addition to laws governing the frequency spectrum etc., Garfinkel[17] raises the question of regulations regarding the privacy of users. There are already some laws governing what can and can not be done with data collected about users etc. However, such laws are generic in nature, and more specific laws tailored at RFID systems may be desirable. The RFID Bill of Rights consists of 5 rights any user of RFID systems and purchaser or RFID tagged products should have according to Garfinkel[17]:

- The right to know if a product contains an RFID tag.
- The right to have embedded RFID tags removed, deactivated, or destroyed when a product is purchased.
- The right to first class RFID alternatives: consumers should not lose other rights (e.g. the right to return a product or to travel on a particular road) if they decide to opt-out of RFID or exercise an RFID tag's "kill" feature.
- The right to know what information is stored inside their RFID tags. If this information is incorrect, there must be a means to correct or amend it.
- The right to know when, where and why an RFID tag is being read.

3. General Security Aspects

The security aspect of the RFID technology is getting more and more important. A short overview of the most important security aspects will be given below.

Definitions of the various threats and attacks referred to are given in chapter 3.2.

3.1. General Security and Privacy Measures

Generally, low-cost RFID tags have very limited resources, and may therefore not be able to support sophisticated security procedures based on encryption[6]. This problem is exacerbated by the constant industry pressure to develop even cheaper tags. Surprisingly, these limitations may actually be an advantage to the security architect[6]. For example, a complex computer communicates with the internet through a complex set of protocols. Making sure all these protocols are secure and interoperate securely, is extremely difficult. RFID tags on the other hand, are limited to communicate with readers in a very constrained manner. This makes it easier to develop security measures tailored at RFID devices. A brief introduction to some important general security and privacy measures is given below.

3.1.1. Labeling

One important aspect of RFID privacy is that RFID tags can be read without the users' knowledge. Thus, if users do not know that they are carrying RFID tags, they are not aware that they may be tracked on basis of these tags. Labeling of products containing RFID tags is thus a very common, and generally effective, means of protecting users' privacy[6]. By labeling an entity that contains an RFID tag, users are made aware of the tag's presence. This makes it possible for users to take further steps to protect their privacy by for example removing or destroying the tag, or by the use of other privacy measures. Labeling is also stated as part of the RFID Bill of Rights[17].

The drawback of labeling is that it provides very limited privacy protection in itself. The label merely notifies the user of a potential threat, it does not help the user neutralize this threat.

3.1.2. Destruction of Tags

One possible corrective measure a user may take when discovering unwanted tags, is to destroy them. Some tags are equipped with built-in kill-commands. That is, a reader can

send the tags a special kill-command including a protective password, rendering the tags permanently inactive. The password is included to prevent unauthorized killing.

Other approaches for deactivating tags are by physically damaging them. This can for example be done by removing the antenna. On the other hand, if tags are imbedded in goods, this may be difficult. Another approach is to subject the tag to an electromagnetic pulse (EMP). The intuitive way to do this is to fry the tags in a microwave oven. However, as this may also damage the goods within which the tag is embedded, it has been proposed to use a small apparatus referred to as an RFID-Zapper[W18] to create the EMP. This RFID-Zapper can be built from a low-cost disposable camera and destroys tags without harming the goods within which the tag is embedded. The RFID-Zapper is also portable, enabling users to destroy the tags upon purchase of the tagged goods.

However, killing of tags is only effective at protecting privacy if users are aware of all tags they are carrying. The approach is therefore not sufficient to guard users' privacy and should be used in conjunction with other privacy enhancements.

Further, as the killing of tags provides excellent privacy protection against threats posed by the tags, it also removes the possibility of post-point-of-sale use of these tags. That is, if tags are killed upon purchase, they can not later be used in applications such as smart-homes. To support such post-point-of-sale use of the tags, IBM has, according to Wired Magazine, suggested the use of Clipped Tags[W19]. The main idea is that each tag is equipped with a removable antenna. When this antenna is removed, the tags still work, but can only be read at a very limited distance. Thus, the tags can be utilized by the user in smart-home scenarios etc., but are hard to track or exploit by adversaries. This approach promises increased privacy protection, but it also limits the utility of the tags.

3.1.3. Faraday Cages

Another very easy, yet not necessarily practical, way of guarding an RFID tag is by using a Faraday cage[6]. A Faraday cage is an enclosure designed to exclude electromagnetic fields. Thus, by keeping an RFID tag within a Faraday cage, the tag can not be read. It is generally assumed that almost any form of metallic coating will act as a sufficient Faraday cage as to prevent all communication with an enclosed tag. A brief investigation of how easily a Faraday cage can be constructed is performed as part of this thesis.

The drawback of using a Faraday cage is its impracticality[6]. A Faraday cage will only protect a tag from being read while the tag stays within the Faraday cage. This may be practical for smartcards used in access control systems where a wallet lined with metal foil prevents the tag from being read until the card is removed from the wallet and explicitly presented to the reader. However, if a piece of clothing is tagged with an RFID tag, keeping it inside a Faraday cage when it is being worn is practically impossible. Thus, Faraday cages are extremely effective at protecting user's privacy, but their impracticality implies that they at best can be a partial solution.

The approach using Faraday cages also suffers from the same drawbacks as the approach using killing of tags. Unless the user knows he is carrying a tag, it is hard to shield it. Thus, Faraday cages are best utilized together with other privacy enhancements such as labeling.

3.1.4. Blocker Tags

A blocker tag is a privacy and security concept proposed by Juels, Rivest and Szydlo[18]. The blocker tag is very similar to a regular RFID tag, except that it has the ability to block the singulation algorithm used by the reader to singulate tags. By sending two different UIDs to the reader, the blocker tag simulates a collision. If this is done every time a reader broadcasts a Select-command, the reader is tricked into believing that all possible tags are in its interrogation zone.

Blocker tags may thus be used to establish a safe zone around the tag, preventing readers from reading tags within the zone. In a supermarket scenario, a blocker tag may be added to the shopping bags customers use to carry their purchased items home[18]. This way, the tags can freely be read inside the supermarket, but once the customer pays for the goods and puts them in the shopping bag, the blocker tag blocks all further communication. Thus, after the customer leaves the supermarket, the tags on the purchased items pose no threat to the customer's privacy. Once the items are removed from the shopping bag, the tags are operable again. Thus, unlike the use of kill-commands or other approaches including the destruction of tags, the use of blocker tags allows further use of the tags after purchase. This may be useful in smart-home scenarios etc.

Further, unlike shielding and destruction of tags, blocker tags prevent all communication inside a safe-zone and hence helps protect a user's privacy even if the user is unaware of a tag.

In order to make blocker tags more flexible, it is possible to implement a form of selective blocking[18]. This implies that the blocker tag only simulates a collision for a selected subgroup of UIDs referred to as a privacy zone. Thus, a reader is allowed to read all tags except those with a UID belonging to the privacy zone.

The main drawback of blocker tags is the lack of flexibility[6]. Selective blocking improves the situation, but more flexibility may be desired. Further, if the population of blocker tags is low, a user may be tracked merely on the basis of the blocker tag itself. This is possible as adversaries may associate a user with the unnatural density of tags simulated by the blocker tag.

3.1.5. The RFID Guardian

A very flexible approach to privacy protection is the RFID Guardian, a concept for centralized security and privacy management of RFID tags introduced by Rieback, Crispo and Tanenbaum[19]. The main idea is that tags may be equipped with insufficient resources to perform the cryptographic computations necessary to protect a user's privacy. And even if the tags used are high-end tags and thus can support the necessary protocols, users may find it inconvenient to manage all the keys etc. for all tags they are carrying. Rieback et al, thus suggest offloading the security functionality to a separate battery-powered device known as the RFID Guardian. This device will have greater computational resources, and can thus protect the user more efficiently. The main functionalities of the RFID Guardian include auditing, key management, access control and authentication.

The RFID Guardian is essentially a portable, battery-powered device capable of two-way communication with RFID tags. It is carried by a user, and performs all security functions necessary for secure communication between the tags and readers. The guardian thus establishes a privacy zone around the user in which only authenticated readers are allowed access. The authentication procedure is performed by the guardian. Access control is enforced through jamming. In essence, the guardian blocks all attempts by readers to access tags. This can either be done by crude jamming or through the use of selective blocking (a kind of blocker-tag simulation). The guardian further acts as a proxy, relaying requests from authenticated readers to the tags. As the guardian is battery-powered and thus has greater computational power, more elaborate (and hence more secure) security protocols can be used. This increases the security of the system as a whole.

The guardian may also perform auditing to keep a list of all tags inside the privacy zone. This effectively enables the user to take corrective actions if unknown tags are present.

Since the guardian forces all read-attempts to go through the proxy, the tags remain invisible to readers until they are authenticated by the guardian. This implies that adversaries are unable to track tags under the guardian's protection. If the guardian in itself is untraceable, so is the user under its protection.

The main advantage of the RFID Guardian compared to other security measures for RFID tags is its flexibility. Users can influence the security level by interacting with the guardian, and if the guardian has some way of knowing its position etc., context-awareness may be utilized to further increase the flexibility of the system.

One main problem with the RFID Guardian is the range[20]. As the guardian is supposed to guard all tags in the user's vicinity, it must have a range of 1-2 meters. Nominal reading ranges for ISO 14443 readers are generally around 10 cm. How the reading range is to be increased to 1-2 meters is not specified in the RFID Guardian paper[19].

Even if the physical limitation of the guardian's range is overcome, there are a few further drawbacks of the RFID Guardian concept. Firstly, the guardian represents a single point of failure[19]. If, for whatever reason, the guardian fails or is compromised, the user is unprotected. Secondly, since the guardian is a separate device, it may easily be lost or forgotten. If, for example, the guardian is left at home, it offers no protection. This problem can partially be alleviated by incorporating the functionality into existing devices such as PDAs or cell phones which may be harder to forget. This, however, only partially alleviates the problem as such devices may as well be forgotten or lost.

Another major drawback of the RFID Guardian is its battery-based power supply. If the battery is exhausted, the guardian offers no protection. This represents a weakness adversaries may abuse by launching repeated requests directly to the tags[19]. These requests will be blocked by the guardian, hence draining the guardian of power. This will eventually lead to exhaustion of the guardian's batteries, and hence leave the tags unprotected.

3.1.6. Randomizable Contents and Insubvertible Encryption

Another approach to privacy protection for tags with low computational resources is proposed by Ateniese, Camenisch and Medeiros[21]. They suggest letting authorized

readers randomize the tag content upon each reading operation. The randomization process is based on insubvertible encryption. The basic idea is that an authorized reader stores a mark on the tag using public key cryptography. At each interaction with an authorized reader, the total tag content is randomized using a public key. The randomization process is thus such that authorized readers may still recognize the original data and then also the original mark on the tag. Unauthorized readers on the other hand which do not have access to the private key do not have this capability. As the data on a tag is randomized at each interaction with an authorized reader, adversaries can not recognize a tag after the tag has encountered an authorized reader.

If an unauthorized reader overwrote a tag and left a similar mark on the data, this could potentially be recognizable after the tag has encountered authorized readers. However, the authorized reader will detect that the mark is not computed by an authorized reader and will then overwrite the tag with safe but meaningless data. This destroys the adversary's possibility of tracking the tag.

In general, randomization with insubvertible encryption allows legitimate readers, but not adversaries, to track a tag.

The main advantage of such an approach is that it does not destroy the tags, and thus allows post point-of-sale use of them. Further, randomization and insubvertible encryption does not require computational capabilities on the tags as the readers perform all the computation. Separate keys for each randomizing reader are not necessary either. Only multiple-write capability is necessary on the tags, and the costs of the system may thus be kept low.

The main drawback of this approach is that it does not prevent tracking in cases where the time between each interaction with authorized readers is long. This can, however, be relatively easily prevented by increasing the interaction frequency with authorized readers.

Another drawback of this approach is that the system is vulnerable to cloning. As the tags have multiple-write capability, the same data can be written to several tags. However, in many RFID applications cloning is not a problem. Hence, if it is assumed that cloning is only a problem pre point-of-sale when the tags may be used for inventory etc., the problem may be solved by including an extra tag either in form of a separate tag or as a dual-core. This tag could then be hard-coded with an immutable ID. At the point-of-sale this tag or this part of the tag's core is deactivated, and only the randomizable part remains.

3.1.7. Summary of General Security and Privacy Measures

Table 3 lists a summary of general security measures and what they protect against together with their main advantages and drawbacks.

Table 3: Summary of advantages and drawbacks of security and privacy measures

Security Measures	Protects Against	Advantages	Drawbacks
Labeling	Unknown tag presence	RFID Bill of Rights	No protection in itself
Destruction of tags	Tracking	Effective	Prevents further use
Faraday cages	Tracking Skimming	Effective	Impractical
Blocker tags	Tracking Skimming	Effective More practical than Faraday cages	May be considered Denial of Service. May be tracked in scarce populations
RFID Guardian	Most attacks	Flexible	Problems with implementation
Randomization	Tracking	Low costs	Tracking between interactions Does not prevent rewriting

3.2. Known Attacks and Common Countermeasures

Many RFID tags have very limited resources. These tags may rely on external protection such as supplied by the general security measures mentioned above. However, if a tag has the resources to support some form of on-tag security measures; it should be implemented to increase the security of the tag.

In the following, an introduction to some of the most important attacks aimed at RFID systems will be given together with an overview of possible countermeasures to protect against the attacks. The most important attacks include:

- Physical attacks
- Skimming attacks
- Spoofing attacks
- Denial of Service (DoS) attacks
- Eavesdropping
- Tracking
- Relay attacks
- RFID viruses

3.2.1. Physical Attacks

Physical attacks involve physically attacking a tag in order to gain information stored on the tag[22]. Such physical attacks may include distorting the power to the tag, disrupt the circuit, using a laser or an electron beam to read from or write to the tag etc.

Countermeasures

These attacks may be thwarted by making the tags tamper proof or by the use of other physical countermeasures such as shielding[22]. As tampering with tags is a general problem with integrated circuits (IC) and independent of whether the IC is used in an RFID tag or not, it will not be discussed further.

3.2.2. Skimming Attacks

Skimming attacks mean attempting to perform unauthorized reading of tags. In general, if a tag lacks proper security measures, it answers to any reader. In systems such as the biometric passport system proposed by ICAO, skimming attacks are feared as they may be part of an RFID bomb[14]. That is, a bomb that scans its blast radius for RFID tags and only explodes when the data stored on the set of tags in its vicinity fulfils a list of demands. It could for example be set to explode when a certain person passes or when at least 10 persons of a particular nationality are in its blast radius.

Countermeasures

Skimming attacks are generally thwarted by the use of a shared secret[5]. By demanding that a reader authenticates itself to the tag before the tag divulges any of its stored data, unauthorized reading may be prevented.

Examples of authentication mechanisms for RFID are Symmetric Authentication and Hash-Lock.

Symmetric Authentication can be performed with a master key for all readers and tags constituting a domain, or with a master key and derived keys for each tag[5]. In both cases the reader first queries the tag for a challenge (R_a). This challenge is a random number generated by the tag. In the case where derived keys are used, the tag also includes its ID in the answer. The reader then derives the key (k) if necessary, and replies to the tag with a Token $T_1 = e_k(R_b||R_a||Text_1)$ where R_b is a random number generated by the reader, Text is an optional text string and $e_k(x)$ denotes the encryption of x under the key k. The tag then decrypts the token using the same key and replies with another Token, $T_2 = e_k(R_{a2}||R_b||Text_2)$. The communication pattern is shown by Figure 9.

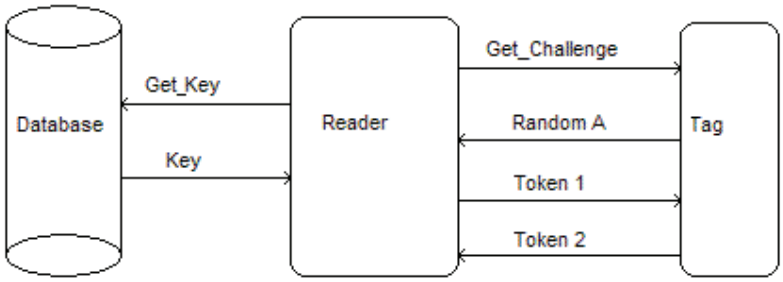

Figure 9: Mutual symmetric authentication [23]

This way the tag knows it is communicating with an authorized reader as only authorized readers have the necessary knowledge to compute the token T_1. Similarly, the reader knows it is communicating with an authorized tag as only authorized tags have the necessary knowledge to decrypt the token T_1 and reply with the correct the token T_2.

Hash-lock is a somewhat different approach to the authentication issue. With the use of this mechanism, tags are normally in a locked mode[24]. When in the locked mode, tags only reply with their metaID, the hashed representation of their ID. As hash-functions are assumed to be one-way functions, an adversary is not able to deduce the ID of a tag from its metaID. An authorized reader, on the other hand, is assumed to have access to a list of (metaID, ID) tuples over all known tags. Thus, with a simple search in the database the authorized reader gains knowledge of the tag's ID. This ID is then sent back to the tag as a key for unlocking the tag. If this ID is correct, the tag enters an open

mode where it will answer any request from readers. Figure 10 shows the message sequence of the Hash-Lock authentication process.

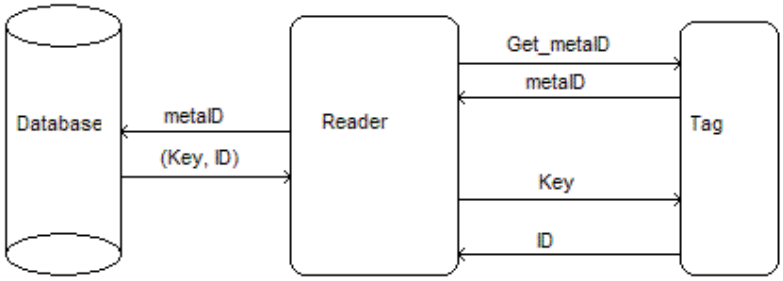

Figure 10: Authentication using Hash-Lock [24]

To prevent tracking based on the metaID sent from a tag, the metaID can be modified to metaID=R_a||hash(ID||R_a) where R_a is a random number[24]. This enhanced mechanism is known as Randomized Hash-Lock. From an adversary's point of view, the metaID will be indistinguishable from a random string. The reader will, on the other hand, still be able to find the ID by first hashing all known IDs with R_a and then search the database for a match. This protection against tracking comes at a price of heavily increased processing. This is, however, usually acceptable as the processing burden is placed on the reader and not on the tag.

Both the regular Hash-Lock mechanism and the Randomized Hash-Lock mechanism involve sending a key to unlock the tags openly over the radio interface. Adversaries can thus eavesdrop on the communication and deduce the key needed to unlock the tags. Hence, a further enhancement known as Randomized Double Hash-Lock has been proposed to solve this problem[22]. The mechanism is similar to Randomized Hash-Lock, but instead of sending the ID directly to the tag, the reader sends a metaKey=hash(R_a||ID) (note that R_a||metaKey≠metaID). As the tag already knows both R_a and ID, the metaKey can easily be checked. Figure 11 shows the communication pattern of the Randomized Double Hash-Lock authentication process.

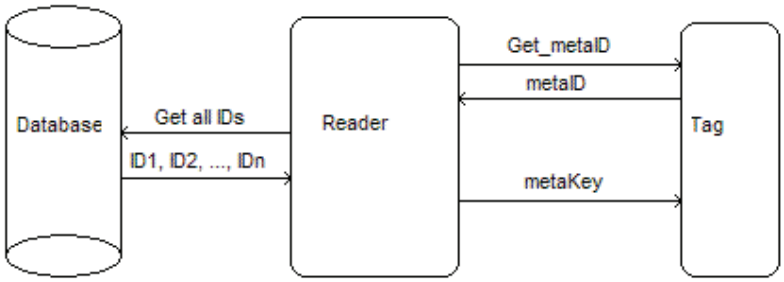

Figure 11: Authentication using Randomized Double Hash-Lock [23]

Compared to mutual authentication, Hash-Lock is an authentication procedure that moves most of the processing burden to the reader. While this is practical as it saves resources for the tag, it only provides one-way authentication. That is, it protects against skimming attacks, but adversaries may perform replay attacks to fool a reader into believing it is communicating with an authorized tag. Thus, Hash-Lock does not offer protection against spoofing etc.

In addition to prevent skimming attacks by utilizing on-tag security measures, they can also be thwarted using physical shielding or devices such as Blocker Tags or the RFID Guardian.

3.2.3. Spoofing Attacks

Adversaries may be able to create "authentic" tags by writing "correct" data to a blank or rewritable RFID tag. This kind of attack is known as a spoofing attack. An example of such an attack was performed by researchers from John Hopkins University and RSA Laboratories who succeeded in unlocking a vehicle immobilizer system by reverse engineering and cracking the system and subsequently spoofing the reader using the data obtained[25].

Countermeasures

Spoofing attacks are generally prevented by restricting access to the "correct" information. Without this information, the attack can not be performed. A secret key, needed as part of an authentication procedure, may be introduced as part of the "correct" information. This key is then stored in a restricted area of memory that can not be read and is never transmitted by the tag as plaintext. This way, adversaries can not get hold of the complete "correct" information, and will never pass as an authentic tag.

However, many systems rely on secrecy of the algorithms and protocols to enhance the security provided by the cryptography, and hence settle for short key lengths[25]. This

was the case with the immobilizer system spoofed by the researchers from John Hopkins University and RSA Laboratories. This violates Kerchoffs' law which states that a system should be secure even if everything except the key is known. Thus, spoofing attacks are best prevented by proper cryptographic protocols with sufficiently long keys.

3.2.4. Denial of Service Attacks

Denial of Service attacks mean attacks aimed at disrupting the normal service of a system. As RFID is a wireless technology, DoS attacks can be accomplished relatively easy by for example jamming the operating frequency. A DoS attack can also be performed by replying to every request during the singulation process like a blocker tag. This way the reader always detects a collision and is unable to singulate tags.

Another form of DoS attacks are aimed at the tags of an RFID system. By deactivating or destroying a tag, a system can be halted as the reader is no longer able to read the tag. Malicious deactivation of tags is usually done by utilizing inherent weaknesses or by built-in deactivation commands. For example, Australian researchers have recently found a weakness in "first-generation RFID tags" to perform a DoS attack whereupon the tags grant the researchers access to their memory[W20]. Destruction of tags can also be done in several ways, for example by physically removing the tag's antenna or by frying the tag in a microwave oven or utilizing an RFID-Zapper[W18].

Countermeasures

DoS attacks are generally very hard to defend against and there are therefore no good mechanisms to thwart DoS attacks all together. However, DoS attacks are often easy to detect, and the attacks can therefore often be stopped before they do too much harm. Crude jamming can for example easily be detected by passive listening to the operating frequency. Blocking of the singulation algorithm can also be detected as it signals an extreme density of tags in the interrogation zone[18]. Altogether, countering DoS attacks implies the use of automated detection mechanisms as well as manual countermeasures such as well established control routines etc. As with many other detection systems, a trade-off between false positives and false negatives must be made.

Another important notice is that equipment that may be used to perform DoS attacks may not always be unwanted. For example, an RFID-Zapper[W18] may be a valuable tool for a user wishing to destroy tags inside lawfully bought clothes or other merchandise to protect himself from tracking and thus protect his right for privacy. The problem arises when such tools are used for malicious purposes.

3.2.5. Eavesdropping

Eavesdropping implies unauthorized passive listening to ongoing RFID communication. As RFID systems are wireless, eavesdropping can be accomplished quite easily.

Countermeasures

One of the easiest ways of preventing eavesdropping is for systems to encrypt their communication before sending the data over the wireless link. This way the adversaries may be able to hear the communication, but not decipher it. Such encryption would also include protection against skimming as one requires knowledge of a secret to decrypt messages from the tag.

3.2.6. Tracking

The fundamental idea of RFID is that each tag is equipped with an ID. Thus, if an adversary can read this ID from a tag, tags can be recognized as they move in time and space. This may enable adversaries to track the tags.

However, tracking is a multilayer problem[26]. Hiding the identity of the tag used by the application layer does not help if an adversary can track the tag on the basis of a static lower layer identifier. For example, during the singulation process tags send an identifier to the reader as their "call-signal". This enables the reader to handle the tags one at a time. This identifier must be available to the tag independent of what is used on the application layer. Thus, this identity is often hard-coded by the manufacturer.

Countermeasures

To prevent tracking, one must prevent the tag from revealing any form of static identifier to unauthorized parties. Thus, the identity used on the application layer must only be divulged after proper authentication procedures have been accomplished. However, this is not enough to prevent tracking as an identifier is necessary as a call-signal for the tag. There is, on the other hand, no need for this call-signal to remain the same from session to session[6]. Hence, instead of sending a static identifier as their call-signal, tags may send a pseudorandom number. Given that the number of tags simultaneously in an interrogation zone is small compared to the entropy of the pseudorandom number used as the call-signal, the probability of collision is negligible. If including a pseudorandom number generator in tags is too expensive, a less expensive approach is to supply the tags with a set of pseudonyms[6]. A drawback of such an approach is, however, that adversaries may harvest all the pseudonyms using repeated

scanning. If this happens, the adversary may still be able to track the tag. On the other hand, if the tags only change their pseudonym after a few minutes, such an attack becomes much more difficult. The delay circuit needed for such delayed change of pseudonym is relatively inexpensive.

As mentioned above, if tags do not have the computational resources to perform any form of randomization operation, this burden can be offloaded to the readers at the cost of the tags being traceable between each interaction with an authorized reader[21]. The utility of such an attack is, however, probably quite low.

Another form of countermeasure to tracking is shielding. If tags are physically shielded, they do not respond to requests sent by readers. Thus, the reader has no way of detecting the tag, and the tag can not be tracked.

As mentioned earlier, if it is impossible to track the RFID Guardian, then tags shielded by the guardian will also be shielded from view. Thus, under these assumptions, the RFID Guardian may be used to prevent tracking.

3.2.7. Relay Attacks

RFID systems are extensively used to authenticate users in access control systems and payment systems. The authentication process is often based on a challenge-response protocol involving a shared secret, and access is only given after the user has proved his knowledge of the secret through his possession of the RFID tag[5]. Similar protocols are used to authenticate users in payment systems. The main assumptions made by such systems are that the tag read by the reader is the genuine tag, and that this tag is presented by the authentic user who is standing close to the door or cashier.

A relay attack is an attack that breaks these assumptions. In a relay attack aimed at an access control system, an adversary uses someone else's credentials to gain access to an access restricted area or system. This is done by fooling the victim's tag and the reader into believing that they are communicating with each other, while they are both actually communicating solely with the adversary. That is, a relay attack is a kind of man-in-the-middle attack. The layout of a basic relay attack is shown in Figure 12.

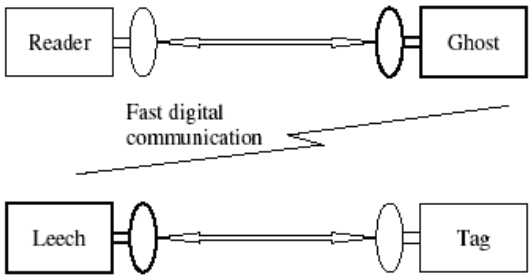

Figure 12: Basic system overview for a Relay Attack [4]

A practical example of a relay attack has been illustrated by Gerhard Hancke[27]. Hancke built a mole (leech) and a proxy (ghost) capable of communicating together using fast, short-range RF-communication. The mole interfaces with the user's RFID-tag and appears as a regular reader. The proxy interfaces with the reader of the system and appears as a regular tag. Each request from the reader to the proxy is forwarded to the mole. The mole then sends this request to the tag, and hence obtains a valid response from the tag. This response is sent back to the proxy, which forwards the response to the reader. As the response from the proxy is a response from an authentic tag, the proxy is authenticated. If the attack was aimed at an access control system, the user carrying the proxy would then gain entry to the access restricted area if the tag being interrogated by the mole is authorized to gain entry. If the attack was aimed at a payment system, the adversary successfully charges the costs to the victim's credit card.

Access to an access restricted area or system can be gained in several other ways. For example, the adversary can steal the user's RFID-tag or steal the shared secret in some other way. However, if the user notices that his tag is gone or that the shared secret has been compromised in some other way, actions can be taken to prevent the information from being used. The same principle holds for payment systems. The main advantage of a relay attack, from an adversary's point of view, is thus that it can easily be performed without the user's knowledge[27]. By placing the mole in an unsuspicious object such as a briefcase, the mole can be brought in range of the user's tag without the user being aware of it. Thus, the adversary gains access and there is generally no way to detect it.

Countermeasures

A relay attack is not easy to guard against. As stated by Hancke, a relay attack is not really a breach of the cryptographic protocols constituting the authentication mechanism[27]. In authentication protocols all communication is protected using encryption. However, the adversary does not need to understand the communication in order to perform the relay attack. The encrypted information is merely forwarded. Thus, the encryption provides no protection against this kind of attack.

There are, however, ways of making relay attacks more difficult to perform. One of the main weaknesses of relay attacks is that they introduce delays in the communication. Thus, if the timing constraints of the communication performed during the authentication process are tightened, relay attacks become more difficult to perform. However, as each layer in the protocol stack introduces further delays into the system, reliable bounding protocols must be implemented on the physical layer[28].

An example of a distance bounding protocol to tighten the timing constraints in RFID systems is given by Hancke and Kuhn[28]. As many other distance bounding protocols, this protocol relies on the principle that nothing travels faster than light. By measuring the time from a challenge is sent to a correct response is received, an upper limit for the distance between reader and tag can be calculated. Tags are then only authenticated if they are acceptably close to the reader. If only authentic tags can compute the correct response to any given challenge, proxies can't pass as authentic tags without forwarding the challenge to the user's tag. However, if the user is far away, the delay introduced by the radio link between proxy and mole is too great resulting in the reader denying the proxy access.

Activation of tags by the user is another way of preventing relay attacks[4]. This implies that tags only answer to readers when they are activated by the user through for example a mechanical or biometric activator. For example, the U.S. Government has decided to introduce an anti-skimming material in the cover of the new e-passports so that the passports can only be read after the user has explicitly opened the passport[13]. This makes it practically impossible for adversaries to interrogate a tag without the user's knowledge.

Another way of defending against relay attacks is by the use of a Two-Factor-Authentication architecture[4]. That is, if, in addition to proving possession of an RFID tag, a user must prove the knowledge of a secret (such as a personal identification number, PIN) in order to be authenticated, relaying the communication between reader and tag is not enough to gain unauthorized entry. The adversary must then also gain knowledge of the user's secret (PIN-code). The drawbacks of such a system is, however, that it eliminates some of the convenience the contactless system was originally meant to offer.

Shielding the RFID tags is also a possible way of protecting against relay attacks. This can be done by using a Faraday cage or by the use of more sophisticated countermeasures such as an context-aware RFID Guardian. As with the use of a Two-

Factor-Authentication architecture, this approach eliminates some of the convenience of the contactless system.

3.2.8. RFID Viruses

Generally, data stored on RFID tags are implicitly trusted. The general belief has been that the resources of RFID tags are too limited to pose any serious threat. It has, however, recently been shown that this trust may be unfounded. According to Rieback, Crispo and Tanenbaum[29], it is not only possible to launch attacks at RFID back-end system or RFID middleware from RFID tags, but this can be done even from low-cost tags with a memory only capable of storing 127 characters. The malicious code can take the form both of a worm and a virus, and can thus spread either through back-end network connections or through the RFID system itself. Rieback et al also give a simple, practical example of how an RFID virus can be written to attack an RFID system through the use of an SQL injection attack. Other possible attacks that can be launched by RFID viruses include buffer overflow attacks and code insertion attacks.

Countermeasures

The attacks that so far have been demonstrated launched by RFID viruses, such as buffer overflow attacks, code or SQL injection attacks etc. are all known types of attacks. There are also well known ways of preventing them, such as bounds checking, disabling back-end scripting languages, parameter binding, limit database permissions etc. The main drawback is that system designers do not seem to expect malware from RFID tags[29]. Further, due to the vast amount of code making up backbone and middleware systems, errors are bound to happen. According to Wired Magazine[W21], Ari Juels, research manager at RSA Laboratories, compares today's situation with RFID to the Internet in its early stages: Security features are not built into the systems in advance, and this is being paid for in terms of viruses and other attacks later. In other words, the spread and harm done by RFID viruses could be reduced by utilizing well known countermeasures to malicious code, but apart from this being quite difficult in itself, convincing system designers that it is important is hard to accomplish.

3.2.9. Summary of Attacks and Countermeasures

In general, there are many ways of attacking RFID systems. There are also many ways of defending against the attacks. Defense mechanisms can either be implemented into the system or their utilization can be left to the user. Thus, one may talk about system-side countermeasures, that is, countermeasures implemented into the system, and user-

side countermeasures, that is, security measures utilized by the user to protect him from threats not countered by the systems themselves.

Table 4 summarizes the attacks and categorizes the different countermeasures depending on who is responsible for their implementation.

Table 4: Summary of attacks and possible countermeasures

Attack	System-side countermeasures	User-side countermeasures
Physical attacks	▪ Tamper proof tags ▪ Shielded tags	
Skimming	▪ Authentication ▪ Symmetric Authentication ▪ Hash Lock	▪ Shielding ▪ Blocker Tags ▪ RFID Guardian
Spoofing	▪ Secret information ▪ Authentication	
Denial of Service	▪ Swift detection ▪ Manual countermeasures	
Eavesdropping	▪ Encryption	
Tracking	▪ Random identifiers ▪ Randomization	▪ Shielding ▪ RFID Guardian
Relay	▪ Distance bounding ▪ Separate activation by user ▪ Two-factor-authentication	▪ Shielding ▪ RFID Guardian
RFID Viruses	▪ Bounds checking ▪ Parameter binding ▪ Limited permissions ▪ etc.	

3.3. Short Range as a Security Measure

The short reading distance of most RFID systems is emphasized by many as an important security feature of the systems[6]. For example, to skim a tag in a system with short reading distance, the adversary must get his unauthorized reader very close to the tag, a task that may be very difficult to perform without the victim's knowledge. Perhaps even more importantly, though, the short reading range of RFID readers makes tracking a much more extensive task. The shorter the reading range, the larger number of strategically placed RFID readers are needed to track tags. With a reading range limited to 10 cm, the threat of tracking may be almost negligible. With a reading range of 1 m, on the other side, tracking may be feasible. Thus, long reading range may be seen as a threat to RFID systems, a fact that may influence manufacturers to deliberately limit the reading distance of their systems.

There is, however, one major flaw in this reasoning. The reading distance of a RFID system, as specified by the manufacturer, is not the absolute maximum reading distance. The reading distance is determined by several factors, some tied to the tag, and some to the reader. The tag is controlled by the original developers of the system, but the unauthorized reader used by the adversary is not. This implies that the original manufacturer of the system controls some of the aspects influencing the reading distance, but not all. For example, the original designer controls the modulation technique used, the operating frequency, the size of the tag's antenna etc. Thus, the size of a tag's antenna may deliberately be reduced to limit its reading distance. Similarly the modulation technique may be chosen to make long range reading more difficult. However, the original designer does not control the size of the reader's antenna, the power emitted by the reader, the sensitivity of the reader when sensing the answer from the tag etc. Thus, even if the system has been deliberately designed to have a short reading distance, an adversary may use a modified reader with extended reading range. This is likely to be further emphasized by the rapid technological development. In other words, it may be possible to extend the reading range in the future, even though it is not possible at present.

This implies that a manufacturer of RFID tags basically has no way of knowing the absolute maximum reading distance attainable with the use of a modified reader. However, greater reading range implies higher costs. Thus, an idea of the reading range attainable at a certain cost may be known. This enables the tags to be designed in such a way that the costs of building the modified reader exceed the costs associated with a successful attack on the tags.

4. Experimental Approaches

As described in chapter 3.3, the threat posed by various attacks at RFID is dependant on the achievable reading distance of the RFID tag. An extended-range RFID reader is thus a valuable tool for adversaries. In this chapter several approaches to extending the reading range of a plug-and-play reader is outlined. Each approach is further analytically assessed as to its simplicity and whether it is likely to yield a significant increase in reading distance of an RFID tag. Further, an approach for testing the effect of physical shielding of tags is outlined.

The different approaches represent the thought process performed in the early phases of the work with this thesis.

4.1. General Principles for Extending the Range

The most efficient way to obtain long reading distances for an RFID tag would be to specifically tailor the system with long range in mind. The tag should for example be equipped with a power source in form of a battery to reduce the energy needed to be harvested from the electromagnetic field, the antennas should be large to increase the efficiency of the power transfer, the power emitted by the reader should be high to power the tag at greater distances, etc.[5]. The reading distance of the system would then be quite extensive.

However, for adversaries trying to skim or track existing tags, designing a new RFID system optimized for long reading distance is not an option. Most of the system parameters would already be set by the original designer of the system. The adversary has, however, complete control over the reader, and could thus design his own reader optimized for long range communication. This approach, on the other hand, is an extensive task. An easier approach is to modify an existing reader. Either way, increasing the reading distance of an existing RFID tag may be possible. According to Kfir and Wool[4], it should be possible to build a reader, either from scratch or by the use of an existing reader, which is capable of communicating with tags over a distance of 40-50 cm.

Many readers on the market today are available as complete plug-and-play readers, and as OEM-modules (Original Equipment Manufacturer). That is, one can buy complete readers that work at once, or one can buy the control module of a reader, and then integrate this with an antenna, interface for communication with a pc etc. An adversary

could therefore either modify a complete reader or buy an OEM module and design the rest of the reader by himself. As the former approach is the one most probably attempted by adversaries, this is the one investigated in this project.

4.2. Extended Range - Powering of Tags

To power passive tags, the magnetic field strength around the tag must be above a certain threshold[5]. By increasing the strength of the magnetic field set up by the reader, tags can be powered at greater distances. Several ways of increasing the magnetic field strength is outlined below.

4.2.1. Optimal Antenna

One of the most important components of an RFID reader is its antenna. As mentioned above, for each possible reading range there exists an optimal antenna diameter. The antennas shipped with standard readers are often quite small, and are thus optimized for short reading ranges[5]. Increasing the diameter of the coil antenna should therefore increase the reading range of such readers.

The magnetic field strength is also affected by the number of windings on the coil antenna[5]. Increasing the number of windings should therefore increase the reading range of the reader.

However, larger antennas also pick up more external noise[4]. Further, the antennas shipped with standard readers are generally finely tuned to the reader[5]. They are tuned to the specific frequency of the system, and the impedance is finely matched to that of the reader. This results in resonance step-up and enables optimal performance when used with the specified reader. If a new antenna is built, this must be similarly tuned to the reader in order to maximize its performance. If not, power may be lost to reflections etc., and the performance of the new antenna may be poorer than the performance of the old antenna, even if it is much larger and contains several more windings. The tuning of the original antenna is generally done by professionals utilizing professional tools. For a radio amateur, this fine tuning may prove difficult, and the expected increase of the reading range using this approach is therefore very uncertain.

Hypotheses:

- *Increasing the area of the coil antenna will have a positive effect on the reading range*
- *Increasing the number of windings on the coil will have a positive effect on the reading range*
- *Both increasing the area of the coil and the number of windings will have a positive effect on the reading range*
- *Building a home-made antenna that has a positive effect on the reading range is time consuming and relatively difficult*

4.2.2. Amplifier

From Equation 1 we have that the magnetic field strength around a coil is affected by the current flowing through the coil. Thus, if the current flowing through the reader's antenna can be increased, the magnetic field strength can be increased. This could be done using an amplifier.

However, increasing the current flowing through the reader's antenna leads to increased internal noise[4]. This may make it harder to detect the reply from the tag.

Further, the communication between reader and tag is based on load modulation. That is, the tag sends data to the reader by stealing energy from the magnetic field in a pattern dependant on the information. This stolen energy is sensed by the reader as drops in the voltage over its coil antenna. Inserting an amplifier between the reader and its antenna would increase the voltage over the reader's antenna. It would, however, also prevent the control module of the reader from measuring the voltage over the antenna as the amplifier is in the way. Thus, tags could be powered at greater distances, but the reader would not be able to receive data from the tags.

On the other hand, it ought to be possible for the receiver to bypass the amplifier, and in this way get some kind of measurements of the voltage over the antenna. This would make it possible to receive data as normal, but with greater range due to the increased magnetic field strength.

However, the magnetic field strength around the tag at the maximum distance between reader and tag will only be slightly above the required minimum to power a tag regardless of whether an amplifier is used or not. Hence, the energy dissipated in the tags load resistor will remain constant at maximum distance between reader and tag even if an amplifier is used to increase this maximum distance. Thus, as the amplitude

of the signal sent by the reader is greatly increased, the relative amplitude of the voltage drops experienced over the reader's coil will be much smaller. This makes it harder for the reader to detect the answer, and hence limits the range of the reader. As with the simple amplifier-approach, this approach will also lead to higher levels of internal noise. Thus, even if it is possible to find a way to bypass the amplifier and obtain measurements of the voltage over the reader's antenna, the amplifier makes it harder to detect the data sent from the tag.

Hypotheses:

- *Using an amplifier to amplify the signal sent to the antenna will prevent the reader from reading tags.*
- *Amplifying the signal sent to the antenna will have a very limited effect on the range, even if a way to measure the voltage drops is found.*

4.3. Extended Range - Detection of Data

As mentioned above, to extend the reading distance of an RFID system, tags must be powered at greater distances. However, if this is done, the bottleneck that remains is the reader's ability to receive the tag's response over the noise. In the following, how to improve this ability of the reader is discussed.

4.3.1. Retransmissions

Tags communicate with readers through load modulation. That is, the reader decodes information from small voltage drops over its antenna. The reader's ability to detect relatively small changes in voltage over its coil antenna is therefore important when trying to extend the reading distance of an RFID system. Increased sensitivity comes with increased cost, and thus standard commercial readers will generally not have greater sensitivity than necessary for normal communication[5].

As the distance between the tag and the reader increases, the relative amplitude of the voltage drops decrease. Therefore, the signal-to-noise ratio (SNR) decreases, and the reader is more likely to misinterpret the received signal[5]. However, if the signal sent from the tag contains redundancy, the information may be decoded correctly even with erroneous detection of the signal[30]. This implies that increased redundancy should result in greater range.

As an adversary generally has no control over the underlying communication protocol, introduction of redundancy can not be done directly. However, it is possible to poll the tag several times, and thus obtain several answers. For example, the ISO/IEC 14443 standard[1] allows the reader to request an unlimited number of retransmissions[4]. Even if all transmissions are erroneous, there will often be some correlation between them "pointing" at the correct answer. The higher number of retransmissions, the greater the possibility of decoding the transmission correctly. For example, one could poll a tag 100 times, and take a majority vote for each bit position. This would give a fairly good estimate of the correct transmission. Kfir and Wool[4] estimate that merely 5 retransmissions give a high probability of decoding the transmission correctly.

This approach is likely to have a significant effect on the range of an RFID system. However, it has some apparent weaknesses. Firstly, as the approach requires the same request to be sent several times before the correct answer can be determined, it requires considerable modifications to the original reader. Secondly, the attack is quite slow. This may be a problem if the tag has a short dwell time in the interrogation zone. Still, the increased range partly alleviates this problem as it increases the interrogation zone which results in longer average dwell times.

Further, a reader has a minimum level SNR needed for obtaining signal-lock[4]. This level is dependant on several factors such as reader architecture and implementation, but is hard to optimize. Even though the approach may lead to an increased range, it will still be limited by the SNR.

Hypothesis:

- *Utilizing retransmissions will have a significant, positive effect on the reading range.*

4.4. The Effect of Physical Shielding

As mentioned above, a Faraday cage may be an effective, if not practical, way of protecting a tag against most types of attacks. Generally, it is assumed that almost any kind of metallic coating is sufficient to completely prevent all communication with enclosed tags.

A very brief test of how easily communication with tags can be prevented can be performed by placing the tags in different proposed Faraday cages and attempt to read

them. The reduction, if any, in reading distance for each type of Faraday cage may then be recorded.

Examples of possible types of Faraday cages include:

- Wrapping of aluminum foil
- Metallic card holder
- Leather wallet
- Leather wallet with content
- Leather wallet lined with aluminum foil

Hypotheses:

- *Wrapping a tag in aluminum foil completely shields the tag from the reader.*
- *Placing a tag inside a metallic card holder completely shields the tag from the reader.*
- *Placing a tag inside a leather wallet reduces the reading distance, but does not completely shield the tag from the reader.*
- *Placing a tag inside a leather wallet with content severely reduces the reading distance.*
- *Placing a tag inside a leather wallet lined with aluminum foil completely shields the tag from the reader.*

5. The Experiments

In the following, detailed descriptions of how the different experiments were performed are given. The equipment is outlined, and some technical information is given. The results, if any, from each experiment are also presented. Finally, some similar and complementing experiments simultaneously performed by others are outlined together with their results.

5.1. The Equipment

Several different types of equipment were used in the experiments. A short description of the equipment is given below.

5.1.1. The Reader

All experiments were based on modifying or enhancing the performances of a standard plug-and-play reader of the type *"ACG HF Dual ISO Short Range USB Plug & Play Module"* (hereby referred to as *"ACG reader"*, RDHS-0404N0-01[31]. This reader operates at 13.56 MHz and supports both the ISO 14443A and the ISO 14443B protocols. In addition to supporting ISO 14443A/B tags, the reader also supports the whole MIFARE® family. It is equipped with a built in antenna with approximate dimensions 55x85 mm. The reader communicates with a computer through a USB 2.0 interface. Any frames that do not pass a CRC-check are rejected by the reader. The specified maximum reading range is 95 mm. The reader is shown in Figure 13.

Device ID: 4005022148

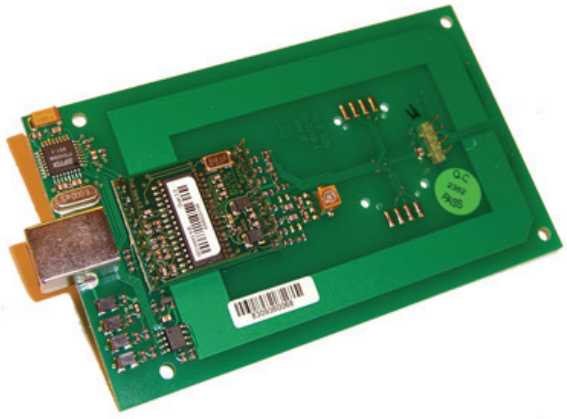

Figure 13: ACG HF Dual ISO Short Range USB Plug & Play Module

5.1.2. The Tags

To get a good picture of how the reader performs in different situations, several tags were used. Table 5 lists the properties of all tags used in the experiments.

Table 5: RFID tags used in the experiments

Tag	Chip type 1	Chip type 2	UID	Magnetic stripe	Stored data
1	MIFARE 1k	None	F4 53 67 41	No	540329321
2	MIFARE 1k	None	34 50 67 41	No	None
3	MIFARE 1k	EM4102 (125 kHz)	F4 57 09 21	Yes	540329321
4	MIFARE 1k	EM4102 (125 kHz)	A4 81 09 21	Yes	540288312
5	MIFARE 1k (old type)	None	F6 F7 2C EF	Yes	None

All the tags are normally used in access control systems and are in the card type ID-1 format. As many access control systems rely on backward compatibility in the form of magnetic stripes, some of the tags used in the experiment are equipped with magnetic stripes. The information stored here, if any, is not considered in the experiments. The tags are shown in Figure 14 with a pen used to show the scale.

Figure 14: The tags used in the experiments

Both single-chipped tags and double-chipped tags were tested. The double-chipped tags have a 125 kHz RFID chip as well as the 13.56 RFID MHz chip. Some tags had information stored in their memory whereas others were blank. Such variations were tested in case memory content or additional chip types influenced the power consumption and hence the attainable reading distance of the tags.

5.1.3. The Computer

The computer used in the experiments was an AMD Athlon^{tm} XP1700+, 1.47GHz with 1GB RAM running Microsoft Windows XP Professional, version 2002, service pack 2.

5.1.4. The Computer Software

In order to operate the ACG reader from a computer, the appropriate programs/drivers were needed. These are freely available on ACG's web site[W22].

The following programs/drivers were needed on the computer to facilitate communication between user and reader:

- ACG HF Dual ISO Reader DLL v3.2.0
- FTDI VCP Driver v1.0.2176
- ACG HF Dual ISO Reader Utility v3.1.0

The Reader Utility software communicates with the reader through a COM port. However, the reader was only equipped with an USB 2.0 interface. To facilitate the communication between these two interfaces, a Virtual Com Port (VCP) driver was needed.

Figure 15 shows a screenshot of the utility software used in the experiments.

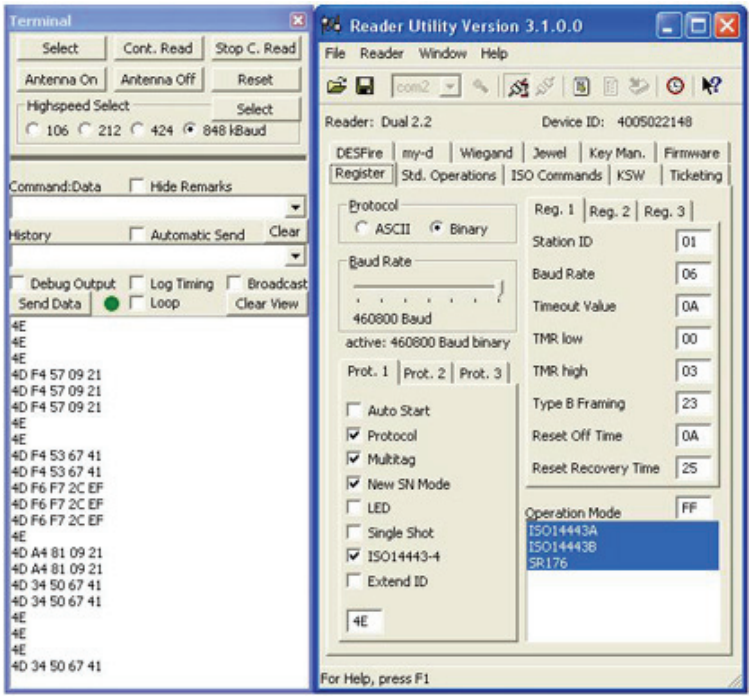

Figure 15: Screenshot of the reader utility software

5.1.5. The Laboratory Equipment

To perform the experiments related to retransmissions, an oscilloscope was necessary. This oscilloscope needed the capability to be triggered by the modulation of the standing carrier wave in addition to being able to store captured data to disk. Two different oscilloscopes were used under the experiments:

- Hewlett Packard 16500B Logic Analysis System
- Tektronix TDS 2014 Four Channel Digital Storage Oscilloscope

Figure 16 shows the Tektronix oscilloscope used in the experiments.

Figure 16: Tektronix TDS 2014 oscilloscope

5.1.6. The Stand

To facilitate exact measurements of the distance between the reader and the tags, a special stand was built. To avoid magnetic interference from metallic substances, wood was chosen as building material. The stand is shown in Figure 17.

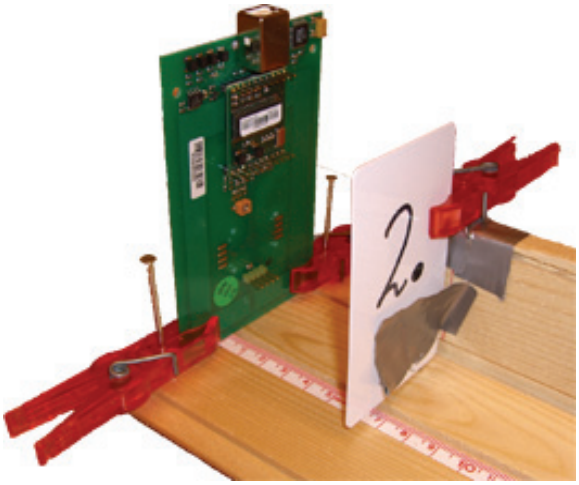

Figure 17: The stand used in the experiments

In general, the stand was made of two planks of wood. One was used as the base for the stand and had a groove cut into it. The other was allowed to slide through this groove. The reader was fastened to one end of the base whereas the sliding plank had a mechanism to hold the tag. This way the distance between reader and tag could be varied. Measuring tape was fastened along the groove in order to measure the distance.

5.2. The Approaches

In the following, more detailed descriptions of how each attempt to extending the reading range was performed are given. The results are also indicated.

5.2.1. Reference Measurements

In order to know how the performance of the reader changes with the various modifications some reference measurements were necessary. To facilitate this, the range attainable for each of the tags was measured using the unaltered plug-and-play reader. For each tag, the reader performed at least 100 read-attempts, and the number of successful and unsuccessful attempts was noted. The procedure was repeated as the tag was moved away from the reader so as to find the point at where the reader no longer was able to decode the answer correctly.

Table 6 shows the percentage successful read-attempts for each tag at various distances between reader and tag.

Table 6: Percentage of successful reading-attempts, reference measurements

Card	Distance (mm)								
	10 - 50	**55**	**57.5**	**60**	**65**	**70**	**75**	**77.5**	**80**
1	100%	100%	100%	100%	100%	100%	99.5%	66.5%	1.5%
2	100%	100%	100%	100%	100%	100%	100%	62.5%	22%
3	100%	90.5%	9.5%	0%	0%	0%	0%	0%	0%
4	100%	100%	0%	0%	0%	0%	0%	0%	0%
5	100%	100%	100%	75%	0%	0%	0%	0%	0%

From the obtained data in Table 6 one can see that the unmodified reader has a success rate over 50% when reading

- Card 1 at a distance of 77.5 mm
- Card 2 at a distance of 77.5 mm
- Card 3 at a distance of 55 mm
- Card 4 at a distance of 55 mm
- Card 5 at a distance of 60 mm

More detailed measurements are available in the appendix.

5.2.2. Optimal Antenna

This experiment corresponds to the approach outlined in chapter 4.2.1.

The idea of this experiment was to extend the reading range of an RFID reader by using an antenna optimized for greater reading range. Several different antennas were to be made using copper wire wound around spikes fastened to a plate. The antennas should differ in both number of windings and area of the coil. To facilitate impedance matching with the reader's antenna, the antennas should be attempted tuned to an impedance of 50Ω using appropriate adapters.

Table 7 shows the antennas intended for testing the optimal antenna size.

Table 7: Antennas intended for testing optimal antenna size

Antenna	Coil diameter (cm)	Building material	Number of windings
1	10	Copper wire	5
2	10	Copper wire	15
3	25	Copper wire	5
4	25	Copper wire	15
5	40	Copper tube	1

In order to test the new antennas, the original connections between the reader's OEM-module and the on-board antenna would have to be cut. The new antennas could then be attempted attached to the OEM-module to test the reading range.

As performing this experiment would mean cutting the original connection between the reader's OEM-module and the on-board antenna, the reader could not have been used for other measurements afterwards. Thus, this experiment would have to be performed last. However, due to lack of expertise, proper equipment and components for tuning the antennas' impedance, constructing the antennas became too time consuming and had to be abandoned. No antennas were therefore made, and no measurements were obtained.

5.2.3. Amplifier

This experiment corresponds to the approach outlined in chapter 4.2.2.

The idea of this experiment was to increase the current through the reader's coil antenna using an amplifier. However, no suitable amplifier was found that allowed the reader's control module to measure the voltage over its antenna at the same time as the current was amplified. This experiment was thus abandoned, and no measurements were obtained.

5.2.4. Retransmissions

This experiment corresponds to the approach outlined in chapter 4.3.1.

The idea of this experiment was to poll the tag for the same information several times, and then utilize the correlation between the decoded signals to find the correct decoding. This can be done in several ways. For example, Kfir and Wool[4] propose to use either software based retransmissions or signal-processing based retransmissions. Software based retransmission is the most intuitive of these as it implies letting the software controlling the reader take a majority vote for each bit in a frame. However, it requires that the reader used relays frames to the controlling software even if they are faulty. The ACG reader used in these experiments is, on the other hand, programmed to reject any answers from the tag that do not pass the cyclic redundancy check (CRC). This prevents the use of software-based retransmissions with this reader.

Signal-processing based retransmissions, on the other hand, is based on interleaving the frames to produce a jumbo frame. This processing can be performed either in hardware or in software directly on the reader's control module. However, it requires extensively more information about the reader as well as general knowledge from the attacker. As extensive information about the ACG reader was not available, this approach could not be used.

A third approach is to manually detect and decode the signals. The necessary processing can then be performed offline using appropriate software. This is not a practical way of performing the attack, but it suffices as a proof-of-concept approach. This third approach was therefore chosen to be tested in these experiments. If the experiment was successful, a more practical attack could be launched by writing software to control a different reader with the necessary ability to relay faulty frames.

The experiment was performed by measuring the signals sent to and from the reader using probes from an oscilloscope attached to the reader's antenna. The modulation of the carrier wave by the tag was then attempted detected.

The carrier wave at 13.56 MHz was easily detected by the oscilloscope. However, the answer from the tags in form of modulation of this carrier wave could not be identified. Both manual and automatic triggering was attempted to capture the desired waveforms, but neither was successful. Thus, the information sent from the tags could not be decoded, and the principle of using retransmission could not be tested.

A peculiar effect experienced, however, was that the reading range of the reader was drastically reduced when the probes from the oscilloscope was attached to its antenna. A brief test with different oscilloscopes with different sets of probes was performed to

rule out the possibility of a faulty oscilloscope or faulty probes. However, the same results were obtained for both oscilloscopes and all probes.

Table 8 shows the percentage successful reading attempts in this situation.

Table 8: Percentage successful read-attempt with probes attached to the reader

Card	Distance (mm)			
	10	**15**	**20**	**25**
1	100	74	0	0
2	92	0	0	0
3	93	0	0	0
4	96.5	0	0	0
5	98	82	48	0

5.2.5. The Effect of Physical Shielding

This experiment corresponds to the approach outlined in chapter 4.4. The idea of the experiment is to test how easily a Faraday cage for protecting RFID tags can be constructed.

The tags were first placed within a certain type of Faraday cage. They were then fastened to the stand in turn, and the range was measured using the same procedure as for the reference measurements. That is, the tags were attempted read at least a 100 times at several different distances from the reader, and the number of successful and unsuccessful attempts for each distance was noted. This procedure was repeated for 5 different kinds of Faraday cages:

- Wrapping of aluminum foil
- Metallic card holder
- Leather wallet
- Leather wallet with content
- Leather wallet lined with aluminum foil

Figure 18 shows the leather wallet with content used as a Faraday Cage. The content added to the wallet consisted of the tag, 6 regular credit cards, 2 bank notes and 2 coins.

Figure 18: Leather wallet with content tested as a Faraday Cage

Table 9 shows the reading distances obtained with the various forms of shielding. The column *"Actual"* is the achieved reading distance in absolute terms (mm) whereas the column *"Percentage"* is the achieved reading distance compared to the reference measurements in chapter 5.2.1. More detailed results are presented in the appendix.

Table 9: Achieved reading distance with the use of various types of Faraday cages

Card	Type of Faraday Cage						
	Aluminum Foil	Card Holder	Wallet		Wallet with Content		Wallet with aluminum foil
	Actual	Actual	Actual	Percentage	Actual	Percentage	Actual
1	0	0	62.5	80%	57.5	74%	0
2	0	0	62.5	80%	60.0	77%	0
3	0	0	42.5	77%	27.5	50%	0
4	0	0	42.5	77%	32.5	59%	0
5	0	0	45.0	75%	40.0	67%	0

From Table 9 one can see that an empty leather wallet decreases the reading distance with between 20% and 25%. A wallet filled with "normal" wallet content reduces the reading distance even further to a total reduction of 23% to 50%. Wrapping a tag in aluminum foil or placing it inside a metallic card holder completely prevents the ACG reader from communicating with it. A leather wallet lined with aluminum similarly prevents the ACG reader from communicating with enclosed tags.

5.3. Similar Experiments Performed by Others

After the work with this thesis began, Kirschenbaum and Wool released a paper titled "How to Build a Low-Cost, Extended-Range RFID Skimmer"[20]. The work behind this paper is very similar to the experiments attempted in this thesis, and the results are thus complementing those outlined above. A brief overview of the experiments performed by Kirschenbaum and Wool is given below together with their most important results.

5.3.1. Optimal Antenna

Kirschenbaum and Wool[20] replaced the original reader antenna with their own home-made 10x15 cm printed circuit board (PCB) antenna. Without any further adjustments to the reader they managed to increase the reading range of their Texas Instruments Multi-Function Reader evaluation kit from about 65 mm to 85 mm. This constitutes a 30% increase in reading range by merely utilizing a larger antenna. They also constructed their own 40 cm-diameter copper-tube loop antenna. The reader was, however, not powerful enough to drive this antenna, and no tags could be read. Figure 19 shows the two antennas.

Figure 19: PCB and Copper-Tube antennas used by Kirschenbaum and Wool [20]

Both antennas were made using a hobbyist's tools, budget and knowledge. The total cost of their home-made RFID skimmer was well below $100, and the main expense was the Texas Instruments reader costing about $60.

However, constructing and tuning the antennas was not trivial. The most straight-forward approaches to fine-tune an antenna to a reader require the use of expensive

apparatus such as an RF Network Analyzer. Thus, these approaches are only applicable for adversaries with a high budget. Other tuning methods require only oscilloscopes and other low-cost equipment an electronic hobbyist may be assumed to have. However, these procedures were very time consuming. Thus, even though Kirschenbaum and Wool managed to construct a more optimal antenna than the one shipped with the reader, they discovered that fine-tuning the antennas to the reader was very time consuming.

5.3.2. Amplifier

Kirschenbaum and Wool's[20] experiment included the use of a Load Modulation Receive Buffer that was placed between the antenna and the antenna input of their Texas Instruments reader module. This buffer attenuated the signal from the antenna before it reached the reader. This way a standard amplifier could amplify the signal sent to the antenna without disturbing the reader. The circuit diagram of the Load Modulation Receive Buffer is shown in Figure 20.

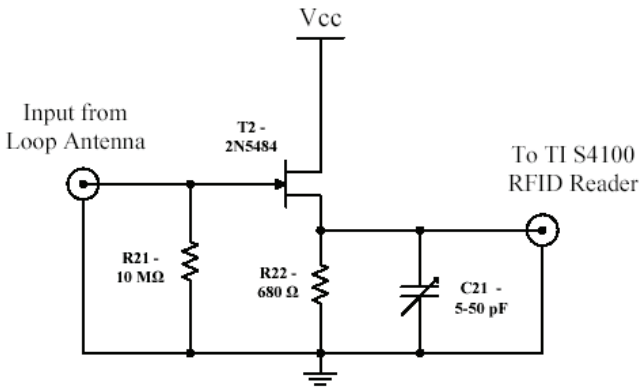

Figure 20: Load Modulation Receive Buffer used by Kirschenbaum and Wool [20]

Further, Kirschenbaum and Wool utilized a 40 cm-diameter copper-tube loop antenna and a variable voltage power supply. Using this constellation and a supply voltage of about 14.5 volts they managed to read tags at a distance of over 250 mm. This constitutes a 280% increase in reading range compared to their original reader.

Based on the results from their experiments, Kirschenbaum and Wool predict that with some further refinements to the equipment, reading ranges of about 350 mm should be easily obtainable. This corresponds to a 440% increase in reading range.

6. Discussion

RFID technology is rapidly permeating our society as the constant technological development continues to drive the prices downwards. This rapid development naturally raises questions about the technology's security aspects. As discussed in chapter 3, there are many ways of attacking RFID systems. There is, however, similarly many ways in which such attacks can be thwarted. Despite this, it does not seem clear to all RFID system designers just how their systems can be attacked and how they can prevent it.

In the following, the security aspect of RFID systems' reading distance is discussed. The results from the experiments are studied together with an assessment of sources of uncertainties and errors in the results. The threats posed by known attacks are analyzed together with an evaluation of the various on-tag and off-tag security and privacy measures available to defeat them. Lastly, some important general security and privacy aspects are discussed.

6.1. The Short Reading Distance of RFID Systems

As discussed in chapter 3.3, the very limited reading distance of RFID systems based on the ISO/IEC 14443 standard[1] is often considered a security mechanism in itself as it makes many attacks much harder to perform. Thus, increased reading distances may be considered a threat to such RFID systems.

The main focus of this thesis is to evaluate the reading distance of RFID systems and determine how easily the reading range of an RFID reader can be increased. Several attempts have been made to increase the reading range, and the results are discussed below. Further, each hypothesis is either confirmed or rejected. However, as not all experiments yielded conclusive results, this is not possible for all hypotheses. In these cases it is indicated whether the hypothesized effect seems likely or not. The term *"Hypothesis NOT rejected"* is used to indicate such situations where the hypothesized effect seems likely, but the results supports no definite conclusions.

6.1.1. Reference Measurements

The reference measurements confirmed the limited range of the ACG reader. According to the reader's OEM-module's data sheet, the maximum range of the OEM-module should be 95mm, depending on antenna and tag. The on-board antenna measures about 55x85 mm, and should, by Equation 2, be optimized for reading ranges of about 40-60

mm. As the on-board antenna can reasonably be assumed to be finely tuned to the reader, reading ranges of up to 80 mm are not surprising.

As seen from the measurements, the tags have quite different reading distances. Tags 1 and 2 have approximately the same reading distances. So have tags 3 and 4. This grouping of the tags is not surprising as the difference between tags 1 and 2 and tags 3 and 4 is only their memory content and the read operation performed does not involve reading of the memory. Further, the reading distance of tag 5 is expected to be shorter than the reading distances of tags 1 and 2 as tag 5 is an older version of tags 1 and 2.

However, the reading distances of tags 1 and 2 are much longer than for tags 3 and 4. Tags 3 and 4 contain a secondary chip. The shorter reading distance may thus be because of the increased power consumption due to this chip.

Based on the results, a maximum reading range of 95 mm depending on the tag, as specified in the reader's datasheet, does not seem unlikely. Such a reading range is, on the other hand, too short to pose any serious threat to an RFID system.

6.1.2. Optimal Antenna

Due to lack of time and expertise, no experiments involving replacing the on-board antenna were performed. However, as mentioned in chapter 5.3.1, a similar experiment was performed by Kirschenbaum and Wool[20]. By constructing their own antenna, they managed to increase the reading range of a standard RFID reader with 30%. The total cost of the reader and antenna was well below $100, and no expensive tools or instruments were used during the construction.

A similar 30% increase in reading range for the ACG reader would result in reading distances of up to 120 mm. This is a significant increase in reading distance, but it is still too short to pose any serious threat to an RFID system. The experiment's significance is, nevertheless, that it serves to demonstrate the possibility of increasing the reading distances of RFID systems. Further, if a 30% increase is possible merely by using a hobbyist's tools, knowledge and budget, one can imagine what might be possible using professional production techniques and unlimited budget. However, Kirschenbaum and Wool also demonstrated that fine-tuning an antenna to a reader was very time consuming.

Based on the experience gained when attempting the experiments and on the results obtained by Kirshenbaum and Wool, the following can be said about the hypotheses:

Hypotheses and results

- *Increasing the area of the coil antenna will have a positive effect on the reading range.*
  Hypothesis confirmed.
  As demonstrated by Kirschenbaum and Wool, increasing the area of the coil antenna results in a moderate positive effect on the reading range.

- *Increasing the number of windings on the coil will have a positive effect on the reading range.*
  No results obtained.

- *Both increasing the area of the coil and the number of windings will have a positive effect on the reading range.*
  No results obtained.

- *Building a home-made antenna that has a positive effect on the reading range is time consuming and relatively difficult.*
  Hypothesis confirmed.
  As demonstrated by Kirschenbaum and Wool, fine-tuning a home-made antenna to a reader is time consuming and relatively difficult as several standardized procedures are ineffective.

6.1.3. Amplifier

No experiments involving amplifying the current through the reader's coil was attempted as no suitable amplifier was found. However, as mentioned in chapter 5.3.2, a similar experiment was performed by Kirschenbaum and Wool[20]. They attenuated the signal from the antenna using a Load Modulation Receive Buffer before this was fed to the receiver, and thus bypassed the difficulties with the amplifier. This resulted in a 280% increase in reading distance of their RFID system. They also predict a further 160% increase to be possible by small refinements to their equipment.

A 280% increase in reading range, such as the increase obtained by Kirschenbaum and Wool, makes relay attacks much more practical. The 40 cm-diameter copper tube loop antenna they used can easily be made portable. It can also easily be fitted inside an inconspicuous looking briefcase to strengthen the attack's element of stealth. This enables an adversary to merely walk by or stand within an arm-lengths distance of a victim in order to perform a relay attack. This could easily be done in for example an

elevator or in the queue at the supermarket. As no-one would react to a person carrying an unsuspicious briefcase, no-one would notice the attack.

On the other hand, a 280% increase in reading distance is probably not enough to enable high-scale tracking of tags.

The attack performed by Kirschenbaum and Wool is noteworthy in that it only utilizes an electronics hobbyist's skills and tools. The total budget was also only $100. Hence, even though the process was time consuming, it implies that significant increases in reading ranges are possible even with a low budget.

Based on the results obtained by Kirshenbaum and Wool, the following can be said about the hypotheses:

Hypotheses and results:

- *Using an amplifier to amplify the signal sent to the antenna will prevent the reader from reading tags.*
  Hypothesis confirmed.
  As demonstrated by Kirschenbaum and Wool, the reader is unable of reading tags without the use of a Load Modulation Receive Buffer.

- *Amplifying the signal sent to the antenna will have a very limited effect on the range, even if a way to measure the voltage drops is found.*
  Hypothesis rejected.
  As demonstrated by Kirschenbaum and Wool, extensive increases in reading range can be achieved with the use of an amplifier together with Load Modulation Receive Buffer.

6.1.4. Retransmissions

Using an oscilloscope to capture waveforms with the objective of detecting and manually decoding the modulation of the carrier wave was an impractical approach. As described in chapter 5.2.4, correctly adjusting the oscilloscope to trigger on the modulation of the carrier wave representing the answer from the tags was not achieved. The carrier wave was easily detected, but it was not possible to locate the information sent from the tags. Thus, few concrete results were obtained.

As shown in Table 8, the reading range was drastically reduced when the probes from the oscilloscope were connected to the reader. Different oscilloscopes with different sets

of probes were tested to rule out the possibility of a faulty oscilloscope or faulty probes. However, the same results were obtained for both oscilloscopes and all probes and it can therefore be concluded that the problem is not due to these apparatus in themselves. The problem may on the other hand be an undetected impedance mismatch between reader, oscilloscope and probes. However, no results were obtained to support any definite conclusion. Thus, this problem cannot be ruled out as part of the reason why manually detecting the signal from the tag using the oscilloscope was not achieved.

As the oscilloscopes affected the reading range, and no detectable signals from the tag could be read, no definite conclusion can be drawn. The experiment does, though, show that using an oscilloscope to capture waveforms is not a practical approach. It does not, on the other hand, imply that the principle of introducing redundancy to increase the reading range is faulty.

A more practical approach to introduce retransmissions is suggested by Kfir and Wool[4]. They suggest implementing retransmissions into either the computer software controlling the reader or in the reader-module itself. The first of these approaches requires that the reader hardware relays the transmission to the controlling software, even if it is faulty and does not pass the CRC-checks. As outlined in chapter 5.1.1, the ACG reader did not fulfill this requirement. It is also likely that many other RFID readers on the market are programmed to discard faulty frames. Thus, even though this approach may be effective at extending the reading range, finding a suitable reader may be difficult.

The second approach suggested by Kfir and Wool does not require the reader to relay faulty frames[4]. It does, however, require substantially more knowledge about the reader implementation and is a much more demanding attack.

In general, retransmissions seem to be an effective way of increasing the reading range of an RFID reader, but it is not trivial. Implementing such a system requires either the use of special readers fulfilling certain criteria, or significant amounts of knowledge on the attacker's side. However, if one combines such an approach with the approach used by Kirschenbaum and Wool[20], increasing the reading range with several hundred percent is not unthinkable. This would make relay attacks even more practical. If the increase approaches 1000%, tracking may also become possible. By for example equipping lamp posts along a road with such skimmers, coarse tracking of pedestrians is feasible. An even scarier scenario may be tracking of e-passports by strategically placed readers inside airport terminals etc.

However, retransmissions introduce delays in the communication. This may not be a problem for legitimate use of the technology, but it may make it harder for the mole in a relay attack to obtain an authentic response from a tag and relay this to the proxy within the window allowed by potential distance bounding protocols etc. On the other hand, the delay does not affect adversaries trying to track tags, as they are only interested in the lower-layer static identifier emitted by each tag. As this is only one frame retransmitted several times, the introduced delay is probably negligible. The increased reading range will, however, at worst only enable very coarse tracking of tags.

Based on the experience gained when attempting the experiments, the following can be said about the hypotheses:

Hypotheses and results:

- *Utilizing retransmissions will have a significant, positive effect on the reading range.*
  Hypothesis NOT rejected.
  Retransmission seems an effective way of increasing the reading range of a reader, but no measurements to support any conclusions were obtained.

6.1.5. The Effect of Physical Shielding

Physical shielding has a significant effect on the reading distance of RFID tags. Simply wrapping the tags in aluminum foil or placing them inside a metallic card holder completely prevents the ACG reader from reading them. The same effect is experienced if the tags are placed within a leather wallet lined with aluminum foil. If the tags are placed in an empty leather wallet, or a leather wallet containing credit cards and coins and other "normal" wallet contents, the reading distance is decreased, but the tags are still readable. Drastically reducing the reading distance of tags can thus be accomplished relatively easily.

However, it is difficult to conclude anything about the maximum reading distance obtainable when tags are shielded. The data only regards the ACG reader's ability to read shielded tags, not a modified reader's ability to read the tags. Adversaries may therefore be able to read shielded tags at far greater distances than what is possible with the ACG reader.

As demonstrated by Kirschenbaum and Wool[20], reading distances for unshielded tags of up to 35 cm should be possible, but achieving this is not trivial. Simple shielding such as a leather wallet reduces the reading range of the ACG reader by up to 25%. A

similar effect for the modified reader should then result in reading distances of up to 28 cm. However, as modified readers generally are more sensitive, the effect of shielding can be assumed to be even better. Thus, relay attacks aimed at contactless smartcards as part of access control or payment systems might actually be prevented, or at least made much more difficult, by simply keeping the contactless smartcard in the wallet when it is not in use. Shielding also seems an effective way of further strengthen the protection against tracking.

Based on the results from the experiments, the following can be said about the hypotheses:

Hypotheses and results:

- *Wrapping a tag in aluminum foil completely shields the tag from the reader.*
  Hypothesis NOT rejected.
  Aluminum foil completely prevents the ACG reader from reading tags, but generalizing the results to include all readers is not possible.

- *Placing a tag inside a metallic card holder completely shields the tag from the reader.*
  Hypothesis NOT rejected.
  A metallic card holder completely prevents the ACG reader from reading tags, but generalizing the results to include all readers is not possible.

- *Placing a tag inside a leather wallet reduces the reading distance but does not completely shield the tag from the reader.*
  Hypothesis confirmed.
  An empty leather wallet decreases the reading distance with 20-25% when attempted read with the ACG reader.

- *Placing a tag inside a leather wallet with content severely reduces the reading distance.*
  Hypothesis confirmed.
  A leather wallet with content decreases the reading distance with 23-50% when attempted read with the ACG reader.

- *Placing a tag inside a leather wallet lined with aluminum foil completely shields the tag from the reader.*
  Hypothesis NOT rejected.
  An aluminum foil lined leather wallet completely prevents the ACG reader from reading tags, but generalizing the results to include all readers is not possible.

6.1.6. Experimental Errors and Uncertainties

An important aspect of every experiment is its sources of errors and any uncertainties introduced in the results. The main source of errors and uncertainties in these experiments is the stand. Firstly, the reader was held in place using clamps. These clamps were, however, not strong enough to rigidly hold the reader in the exact same position as the tags were moved or replaced. As the effective power transfer between reader and tag is dependant on the angle between the two coils, this may have affected the results. The tags were fastened to the stand in a similar way. Thus, also small variations in the angle of the tags may have affected the results.

Further, RFID is a wireless technology and is thus vulnerable to electromagnetic noise. Hence, the environment may have introduced some uncertainties in the results.

A measuring-tape was used to measure the distance between reader and tag. This tape may have been inaccurately placed on the stand. The measuring tape may therefore have introduced errors in the results.

However, a strong effort was made to minimize errors and uncertainties. For example, the measuring tape was fastened to the stand using nails. This helped prevent variations between measurements. The number of clamps holding the reader was also increased to increase the strength of the apparatus. Further, duct-tape was used to reduce the flexibility of the apparatus holding the tag. This significantly decreases the amount of uncertainties in the experiments.

The contactless cards used in the experiments were very thin and the distance from the reader could therefore be quite accurately assessed. However, when investigating the effect of shielding, the tag was placed inside a Faraday cage. The Faraday cages varied in thickness, and measuring the exact distance between reader and tag thus became much more difficult. The results from these experiments must therefore be considered less accurate than the reference measurements.

In general, the spacing between measurement points in the experiments was set to 5mm. However, in chapter 5.2 and in the appendix the reading distances of some tags are given with 0.5mm accuracy. The distances given with 0.5mm accuracy merely represent measuring points between two regular measuring points spaced 10mm apart and should therefore not be assumed to have higher accuracy than the other results.

6.2. Applications, Threats and Countermeasures

In the following some example applications of RFID are discussed with respect to relevant threats and countermeasures. The applications are chosen as breaches in security may have severe negative consequences for the systems' users.

6.2.1. Contactless Access Control and Payment Systems

Contactless access control and payment systems are by nature vulnerable to attack. As the rewards for breaking the systems are generally high, the motivation and resources available to the attacker are quite high. Further, such systems are becoming increasingly popular. Appropriate security and privacy measures are thus essential.

The most basic aspect of contactless access control and payment systems is that they must be immune to skimming and subsequent spoofing. Unless such protection is in place, adversaries may obtain access credentials or credit from a victim by skimming the tags while bumping into the victim on the street or while standing next to the victim in an elevator etc. If the adversary uses a skimmer with extended reading range as demonstrated by Kirschenbaum and Wool[20], obtaining the access rights or credit becomes even easier. Thus, the cost of adding encryption capability to such RFID tags should be justifiable.

A further security enhancement justifiable in such systems is a two-factor-authentication architecture. By introducing a PIN-code or other password as part of the authentication procedure, merely skimming a tag would not be enough. However, many users find such architectures troublesome as they remove some of the convenience of the contactless systems.

If cryptographic capabilities are added to the tags, some further security enhancements could be added at relatively low costs. For example, tags used in contactless access control and payment systems are often carried by users around the clock. Thus, they expose their users to the threat of tracking. The tags tested in the experiments are all

intended for use in access control systems. They did, however, send their static UIDs to any reader querying them, without any form of prior authentication. This is consistent with the ISO/IEC 14443 standard[1] which allows randomized UIDs, but does not demand their use. If the tags already possess cryptographic capabilities, adding a random number generator to generate random UIDs for each session should not be too costly.

Further, contactless access control and payment systems are vulnerable to relay attacks. Any on-tag security measures implemented do not protect against this kind of attack. The threat is, however, very real. With the increased reading distances demonstrated by Kirschenbaum and Wool[20], the threat has become even more serious. Introducing a two-factor-authentication architecture to make spoofing more difficult also partly alleviates the problem of relay attacks, but more accurate countermeasures such as high-resolution distance bounding protocols should be added to secure the systems.

Thus, a secure contactless access control or payment system should at least include proper on-tag security measures and an authentication mechanism including a PIN-code. The tags should also utilize random identifiers to prevent tracking, and if the readers utilize distance bounding protocols the threat of relay attacks can be minimized.

6.2.2. E-Passports

E-passports store information generally regarded as sensitive by the user. Thus, proper privacy protection is important. A fundamental property of a passport system is that it must be resistant to spoofing. Hence, security measures to protect the e-passport system against such attacks are also important. Further, the information stored on e-passports can be used by adversaries for malicious purposes, and the user's security must also be attended to.

Protection against spoofing is managed by digitally signing the content of each e-passport and tying the data to the information printed inside the e-passport. Thus, data from one e-passport can not be copied to another, and new data written to an e-passport can not be appropriately signed. Further, the information stored on the e-passport should be impossible to read unless the e-passport is explicitly presented by the user. This is managed by printing a key needed for access control in the e-passport. Until the e-passport is opened and this key is read, the access control enforced by the e-passport is not passed. As passport systems are generally less sensitive to increases in costs than access control and payment systems, including such on-tag security measures is not problematic.

If the reading range of malicious readers can be increased, e-passports become more vulnerable to threats such as tracking as the tags used are based on the ISO/IEC 14443 standard[1] using static identifiers. This could with little extra costs be mitigated by using random UIDs. The threat is, however, already reduced as at least the U.S. government has decided to add some form of anti-skimming material to the cover[12, 13]. As demonstrated by the experiments, this seems to have a devastating effect on the reading distance.

Unlike contactless access control and payment systems, e-passport systems are not susceptible to relay attacks. At border controls, a digital picture is read from the e-passport and a new picture is taken of the passport holder. The user is only allowed to pass if these two pictures match. This procedure constitutes an effective Two-Factor-Authentication architecture preventing relay attacks.

Thus, the recommendations for e-passports specified by ICAO are generally quite thorough when discussing the security and privacy of e-passports. If an anti-skimming material is included in the cover of the e-passport, malicious readers capable of reading tags at greater distances pose a very limited threat to the e-passport systems.

6.3. General Security Aspects

In addition to threats at specific applications, some aspects of RFID security are very generic in nature. A discussion of some important security aspects is given below.

6.3.1. Location Privacy and Tracking

One of the key privacy threats with respect to RFID is tracking. As long as this threat is imminent, or at least as long as the users perceive this threat as imminent, the technology can not become a ubiquitous technology. The RFID Bill of Rights, and legislation regarding mandatory labeling of tags, is a step in the right direction, but there is still far to go. Firstly, knowing about a tag and having the right to kill it, does not necessarily mean the user wants to kill it. Secondly, the tags may be needed if a customer wants to return a product to the store. Thus, ways of preventing tracking of un-killed tags are necessary.

The RFID Guardian is a powerful and flexible approach to guaranty privacy[19]. However, there are several physical limitations regarding its implementation. Hence,

today the RFID Guardian is more a theoretical concept rather than a practical countermeasure.

The use of blocker tags are then a much more practical approach. However, in a scarce population, users may be tracked merely on the basis that they are carrying a blocker tag. In dense populations this does not present a problem. On the other hand, in very dense populations the density of blocker tags may become a problem in itself as the collective effect may start to look like a DoS scenario.

A very effective way of preventing tracking is by the use of Faraday cages. As shown by the experiments performed as part of this thesis, wrapping a tag in aluminum foil or placing it inside a metallic card holder completely prevents the ACG reader from reading them. This is extremely useful for example for e-passports. By incorporating metal foil or mesh in the cover of the e-passport, reading the e-passport without opening it becomes very hard. The approach is, however, not practical for all applications as not all tags can be placed inside a Faraday cage while in use.

A common characteristic of all the approaches outlined above is that they may all be classified as user-side countermeasures. That is, it is up to the user to decide whether they want to use it or not. The drawback is that users are only protected if they explicitly acquire the countermeasure and start using it. As long as privacy is considered the users' right, this can not be considered fair. System-side privacy enhancements on the other hand require increased on-tag resources. This prevents their use in many applications requiring low-cost tags. Thus, development of new, cheap system-side privacy enhancements is needed.

An example of such an enhancement is randomization by insubvertible encryption[21]. In such a scheme all processing is left to the readers, and the costs of the system can thus be kept relatively low. However, as the data is only randomized at each encounter with an authentic reader, tags may be tracked between each such encounter. Hence, randomization is a promising approach, but it is still in need of refining.

6.3.2. The Development of New Threats

RFID technology is undergoing a very rapid development. As this development proceeds, new threats may arise, and new types of attacks may become feasible. Thus, trying to foresee the development is quite important for RFID system designers.

The most recent development affecting the security of RFID systems is the demonstration of the world's first functional RFID virus[29]. Effective RFID viruses have long been assumed impossible to write due to the limited resources of RFID tags. Therefore, security capable of thwarting any attacks launched by viruses has not been built into existing systems. As demonstrated, however, this assumption is faulty, and many systems in use today are therefore highly vulnerable to attack.

A man-in-the-middle attack being launched at RFID systems in form of a relay attack is a relatively recent development. Such attacks can be thwarted by the use of for example high-resolution distance bounding protocols[28]. The problem is that most RFID systems do not utilize such security measures as the systems' designers did not realize that the attack was feasible. This implies that many existing contactless access control and payment systems and other systems are quite easy to circumvent.

A similar situation was experienced with the Internet in its early days. No-one thought about building security into the Internet in advance, and now a galloping arms race between system designers and hackers is experienced as more and more advanced worms and viruses are released. Similar situations are likely to arise in the future as lack of foresight will result in system designers leaving out security measures. This may be done because the threats do not seem imminent and the cost of including proper security measures cannot be justified. With time, the parameters change, and security must be added in retrospect. This results in a spiraling situation where security engineers and hackers compete at being the first to reach the next step, a situation with generally no happy ending. The total costs of securing systems in such a way is generally much higher than the costs of including the security measures from the start.

The threat of tracking ISO 14443 tags is one threat that may seem unlikely today. However, as demonstrated by Kirschenbaum and Wool, moderately increasing the reading distance of such tags can be done quite easily[20]. As the technology continues to evolve and prices continue to drop, further increases in reading distance may be possible. Further, as costs drop, more readers can be employed in a tracking scheme. Thus, security measures to prevent tracking should be implemented today, even if the threat seems to be at most moderately dangerous.

In general, to avoid costly situations as outlined above, foresight is important. Even though an attack seems unlikely when a system is designed, it is quite possible that it becomes feasible during the system's lifetime. This is especially likely for RFID systems which are subject to a very rapid technological development. Thus, security measures to thwart the attacks should be included from the start both to prevent

vulnerability as new attacks are discovered and to prevent increased cost due to retrospective inclusion of countermeasures.

7. Conclusions

RFID is a very versatile technology that has the potential to increase the efficiency of many common applications. The main drawback is that the general principles the technology is built on are very vulnerable to attack. The ID imbedded in every chip combined with the openness of the radio interface exposes the users to tracking. As additional sensitive information may be stored on the tags, the user may also be exposed to other security and privacy threats. If the reading distance of RFID systems can be increased with a low level of effort, the threats become even more dangerous. For example, one of the main difficulties of relay attacks is that the mole must be within reading distance of the victim's tag for the attack to succeed. With increased reading distance, the element of stealth throughout this process increases, and the attack is more likely to be accomplished unnoticed.

The Possibility of Increasing the Reading Distance of Tags

In general, increasing the reading distance of an RFID system is possible. Even for ISO 14443 tags which are generally assumed to have a very short reading distance, moderately increasing the reading distance is possible. This is illustrated by the 250 mm reading distance obtained by Kirschenbaum and Wool. This reading distance was obtained using only an electronics hobbyist's tools and knowledge. The budget was only around $100. This implies that moderately increasing the reading distance of RFID systems is relatively easy. However, to obtain such reading ranges a large antenna has to be constructed and finely tuned to the reader. This is possible, but time consuming. Further, a finely tuned Load Modulation Receive Buffer or similar device must be introduced into the circuit. The complexity of this is not beyond the scope of an electronics hobbyist, but it is not trivial. As with the antenna, fine tuning this to the reader is also time consuming. Thus, increasing the reading distance of ISO 14443 tags is possible with a low budget, but it is time consuming and far from trivial.

In order to obtain extensive increases in reading distance, more sophisticated techniques such as retransmissions must be utilized. If this can be done using software to control a modified reader, attacks based on this procedure are feasible. However, unless it is possible to find a reader that relays faulty frames, signal-processing based retransmissions must be attempted. This requires substantially more knowledge and can be considered relative hard to do, but it is not impossible. Alternatively a new reader can be built from scratch. It can therefore not be concluded that extensively increasing the reading distance is impossible. This approach is, though, much more difficult. Regardless, further increases in reading distance must be considered feasible given that the attacker has sufficient resources in form of time and money.

The Effect of Increasing the Reading Distance of Tags

Any increase in reading distance greatly decreases the effort necessary to successfully carry out a relay attack. Thus, the increases in reading distances proved possible by Kirschenbaum and Wool implies that relay attacks are much easier to perform than one might presume with the generally assumed 10 cm maximum reading distance.

To effectively track a person over open terrain, extreme increases in reading distance are necessary. However, to track a pedestrian as he walks along a road may be possible with extensively shorter reading distances. Readers may be installed in the lamp posts along the road, and even though the interrogation zones of the readers do not overlap, tracking is performed by registering which lamp posts the pedestrian passes. Similar tracking could be performed indoors to track movements inside an office building etc. The reading distances obtained by Kirschenbaum and Wool are, on the other hand, too short even for this kind of tracking. However, the introduction of retransmissions promises to increase the reading distance even further, perhaps to the point where this kind of tracking becomes feasible.

The Effect of Physical Shielding of Tags

Many RFID systems in use today have a low level of on-tag security measures. Users of such systems wanting to protect themselves from unwanted reading of their tags may try physically shielding the tags. This is an extremely effective way of decreasing the reading distance of an RFID tag. For many applications such as payment systems where the tag is in form of a credit card generally kept in a wallet or in a card holder, physical shielding is also very practical. Merely lining the wallet with aluminum foil or using a metallic card holder is enough to completely prevent a standard reader from reading the tags. It may still be possible for modified readers to read a shielded tag, but shielding by aluminum foil or metal card holders is likely to at least drastically decrease the reading distance.

In general, physical shielding of tags is an extremely effective way of preventing both unauthorized reading of tags and tracking. However, for the user to keep the tags inside a Faraday cage is not always practical. Hence, a similar, but for some applications more practical approach, is to equip the tag with some form of built-in Faraday cage. This approach is in use to protect e-passports against tracking and skimming. This may add additional costs to a system, but the reward is greatly increasing the difficulty of performing tracking, one of the most feared threats to an RFID system.

Alternatives to Physical Shielding

Blocker tags and the RFID Guardian represent other user-side approaches to prevent unwanted reading and tracking of tags. However, these suffer from drawbacks such as the possibility of tracking in sparse populations and problems with implementation. Further, demanding the users to protect themselves may be considered unfair. Thus, protection ought to be implemented into the system in form of on-tag security measures or other system-side security measures such as randomization using insubvertible encryption. This last approach, however, suffers from the possibility of tracking between each interaction with a legitimate reader. Either way, it is a step in the right direction.

General Conclusions

Many systems in use today may be considered secure. For example the e-passport system proposed by ICAO efficiently deals with many attacks, and assuming the proposed algorithms are secure, the e-passport system may be considered a secure system. However, other systems may not deal with threats in such an efficient way. The dangers threatening access control systems, for example, are quite similar to the dangers threatening e-passport systems. However, access control systems are more sensitive to costs. Thus, important security mechanisms may be left out. Given the consequences of breaches in security for such systems, this is quite disturbing.

In general, everybody agrees that security is important. However, no one wants to pay for it. The challenge is thus often to find the appropriate level of security that both meets cost constraints and the users' need for privacy and security.

Further, it is always important to learn from previous mistakes. The Internet is burdened with attacks from viruses and worms as security against such attacks was not built into the systems in advance. Similarly, RFID systems are suffering from attacks the designers originally deemed impossible. Therefore, even though it seems that extensively increasing the reading distance of RFID systems is practically impossible, the security of the systems should be good enough to withstand the threat of much greater increases in reading distances. This would probably be much cheaper than adding security in retrospect, and it would close the window of vulnerability i.e. minimize (or remove) the time interval from a threat is discovered until security is retrospectively added.

8. Future Work

This thesis has attempted to determine how easily the reading distance of an RFID system can be increased. The experiments yielded limited results, but combined with the results obtained by Kirschenbaum and Wool, several conclusions can be drawn. However, retransmission has been proposed as an approach for further increasing the reading range of an RFID reader. An unsuccessful proof-of-concept experiment was also performed as part of this thesis. However, further investigations ought to be performed. A direct implementation in software or hardware could be tested to assess the obtainable increase in reading range.

The results obtained when investigating the effect of physical shielding are quite useful. It might, however, be quite interesting with more generic results. This can be obtained by investigating the signals on the air-interface, and not only the results given by a specific reader. Measurements could also be taken inside a Faraday cage to assess the strength of a signal from the reader after penetration of the cage.

Further, the U.S. government has decided to include an anti-skimming material in the cover of their e-passports. To what extent this prevents unwanted reading should be investigated. Measurements of the obtainable reading distance of an opened e-passport carrying such an anti-skimming device are also needed.

Further, the inclusion of on-tag security measures is too expensive for many applications today. Even if the prices continue to drop, there will always be applications that could benefit from RFID, but are prevented from using it due to the costs of necessary security and privacy features. Thus it is likely that there will be a continuing need for research on effective, low-cost security measures.

9. References

Different kinds of sources are referenced throughout this thesis. *"General References"* contains papers, books and other reliable sources. *"Web References"* contains web pages and other unspecific sources. Some of these are websites of highly reputable organizations whereas others may be less reliable sources such as magazines etc.

9.1. General References

[1] International Organization for Standardization, "*ISO/IEC 14443: Identification cards - Contactless integrated circuit(s) cards - Proximity cards*," 2000.

[2] International Organization for Standardization, "*ISO/IEC 15693: Identification cards - Contactless integrated circuit(s) cards - Vicinity cards*," 2000.

[3] International Organization for Standardization, "*ISO/IEC 10536: Identification cards - Contactless integrated circuit(s) cards - Close-coupled cards*," 2000.

[4] Ziv Kfir and Avishai Wool, "*Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*," School of Electrical Engineering, Tel Aviv University, Tel Aviv, Israel 2005.

[5] Klaus Finkenzeller, *RFID Handbook; Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed. Munich, Germany: Wiley, 2004.

[6] Simson Garfinkel and Beth Rosenberg, *RFID; Applications, Security, and Privacy*. Upper Saddle River, NJ: Addison-Wesley, 2006.

[7] International Organization for Standardization, "*ISO/IEC 7810: Identification cards - Physical characteristics*," 2003.

[8] Antti V. Räisänen and Arto Lehto, *Radio Engineering for Wireless Communication and Sensor Applications*. London, the United Kingdom: Artech House, 2003.

[9] Domine Leenaerts, Johan van der Tang, and Cicero Vaucher, *Circuit Design for RF Transceivers*. Dordrecht, the Netherlands: Kluwer Academic Publishers, 2001.

[10] Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song, "*An Approach to Security and Privacy of RFID System for Supply Chain*," presented at IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04), 2004.

[11] International Civil Aviation Organization, "*Biometrics Deployment of Machine Readable Travel Documents*," Montreal, Canada, Technical Report, 21 May 2004.

[12] U. S. D. o. State: "*Electronic Passport, Proposed rule*", 2005 http://www.mattababy.org/~belmonte/Home/Politics/Letters/050404_Department_of_State.txt, (Accessed: 2 March 2006)

[13] U. S. D. o. State: "*Electronic Passport, Final Rule*", 2005 http://www.lexisnexis.com/practiceareas/immigration/pdfs/695156a.pdf, (Accessed: 2 March 2006)

[14] Ari Juels, David Molnar, and David Wagnar, "*Security and Privacy Issues in E-Passports*," RSA Laboratories and UC Berkeley 2005.

[15] T. C. o. t. E. Union: "*Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.*" 2004 http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_385/l_38520041229en00010006.pdf, (Accessed: 2 March 2006)

[16] E. R. Committee: "*ERC Decision of 12 March 2001 on harmonised frequencies, technical characteristics and exemption from individual licensing of Non-specific Short Range Devices operating in the frequency bands 6765 - 6795 kHz and 13.553 - 13.567 MHz*", 2001 http://www.ero.dk/documentation/docs/doc98/official/pdf/ERCDEC0101.PDF, (Accessed: 7 May 2006)

[17] Simson L. Garfinkel, "*Adopting Fair Information Practices to Low Cost RFID Systems*," presented at Ubiquitous Computing 2002 Privacy Workshop, Göteborg, Sweden, 2002.

[18] Ari Juels, Ronald L. Rivest, and Michael Szydlo, "*The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy*," in *CCS 2003*. Washington, DC, U.S.: ACM, Association for Computing Machinery, 2003.

[19] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "*RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management*," Department of Computer Science, Vrije Universiteit, Amsterdam, The Netherlands 2005.

[20] Ilan Kirschenbaum and Avishai Wool, "*How to Build a Low-Cost, Extended-Range RFID Skimmer*," Tel Aviv University, Tel Aviv, Israel, February 2, 2006.

[21] Guiseppe Ateniese, Jan Camenisch, and Breno de Medeiros, "*Untraceable RFID Tags via Insubvertible Encryption*," presented at Conference on Computer and Communications Security, Alexandria, U.S., 2005.

[22] Peter Longva, *"Security aspects of RFID based e-payment,"* Master's Thesis at Department of Telematics, Norwegian University of Science and Technology (NTNU), Trondheim, 2005

[23] Torstein Haver, *"Security and Privacy Issues with the use of Radio Frequency Identity Tags (RFID),"* Minor Thesis at Department of Telematics, Norwegian University of Science and Technology (NTNU), Trondheim, 2005

[24] Stephen August Weis, *"Security and Privacy in Radio-Frequency Identification Devices,"* Master's Thesis at Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology (MIT), Massachusetts, 2003

[25] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo, "*Security Analysis of a Cryptographically-Enabled RFID Device*," The John Hopkins University Information Security Institute and RSA Laboratories 28 January 2005.

[26] Gildas Avoine and Philippe Oechslin, "*RFID Traceability: A Multilayer Problem*," in *Financial Cryptography and Data Security*. Roseau, the Commonwealth of Dominica, 2005.

[27] Gerhard Hancke, "*A Practical Relay Attack on ISO 14443 Proximity Cards*," (Manuscript), University of Cambridge, 2005.

[28] Gerhard P. Hancke and Markus G. Kuhn, "*An RFID Distance Bounding Protocol*," presented at IEEE/Create-Net SecureComm 2005, Athens, Greece, 2005.

[29] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "*Is Your Cat Infected with a Computer Virus*," in *PerCom 2006*. Pisa, Italy, 2006.

[30] Simon Haykin, *Communication Systems*, 4th ed. New York, U.S.: John Wiley & Sons, Inc., 2001.

[31] ACG Identification Technologies GmbH, "*ACG HF Dual ISO Short Range USB Plug & Play Module Datasheet*," Walluf, Germany April 2005.

9.2. Web References

[W1] Preemptive Media *"Zapped!"*
http://www.zapped-it.net/info.html,
(Accessed: 24 May 2006)

[W2] IEEE Distributed Systems Online *"T-Engine: Japan's Ubiquitous Computing Architecture Is Ready for Prime Time"*, 2006
http://csdl2.computer.org/comp/mags/pc/2005/02/b2004.pdf,
(Accessed: 24 May 2006)

[W3] PhidgetsUSA.com *"Small Glass Ampoule Tag"*,
http://www.phidgetsusa.com/cat/viewproduct.asp?category=3000&subcategory=3200&SKU=RFTGASM,
(Accessed: 24 May 2006)

[W4] InfoChip Systems Inc. *"InfoChip Tire Module"*,
http://www.infochip.com/prod_tire.htm,
(Accessed: 24 May 2006)

[W5] Socket Communications *"CF RFID Reader Card 6E"*,
http://www.socketcom.com/product/RF5400-542.asp,
(Accessed: 24 May 2006)

[W6] The Association for Automatic Identification and Data Capture Technologies, AIM *"Shrouds of Time: The history of RFID"*, 2001
http://www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf
(Accessed: 23 February 2006)

[W7] UPM Rafsec *"Tutorial overview of inductively coupled RFID Systems"*, 2003,
http://www.rafsec.com/rfidsystems.pdf,
(Accessed: 10 May 2006)

[W8] EPCglobal, Inc.
http://www.epcglobalinc.org,
(Accessed: 18 May 2006)

[W9] International Organization for Standardization
http://www.iso.org,
(Accessed: 7 May 2006)

[W10] International Electrotechnical Commission
http://www.iec.ch
(Accessed: 9 June 2006)

[W11] International Civil Aviation Organization "*Machine Readable Travel Documents*",
http://www.icao.int/mrtd,
(Accessed: 7 May 2006)

[W12] International Telecommunications Union
http://www.itu.int,
(Accessed: 8 May 2006)

[W13] European Radiocommunications Office
http://www.ero.dk,
(Accessed: 7 May 2006)

[W14] European Telecommunications Standards Institute
http://www.etsi.org,
(Accessed: 7 May 2006)

[W15] Norwegian Post And Telecommunications Authority
http://www.npt.no,
(Accessed: 7 May 2006)

[W16] Federal Communications Commission
http://www.fcc.gov
(Accessed: 1 June 2006)

[W17] Klaus Finkenzeller, *"Radio-Frequency-IDentification, Frequencies for RFID-systems"*, 2005
http://www.rfid-handbook.de/rfid/frequencies.html,
(Accessed: 18 May 2006)

[W18] Anonymous, "*RFID-Zapper*," presented at 22nd Chaos Communication Congress, Private Investigations, Berlin, Germany, 2006.
https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN)
(Accessed: 1 June 2006)

[W19] Mark Baard, *"Retail-Safe RFID Unveiled",* in Wired Magazine 2 May 2006
http://wired.com/news/technology/0,70793-0.html
(Accessed: 6 June 2006)

[W20] Michael Crawford, "*Australian researchers confirm RFID DOS attacks*" in Computerworld 11 April 2006
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,110424,00.html,
(Accessed: 26 April 2006)

[W21] Annalee Newitz, *"The RFID Hacking Underground,"* in Wired Magazine 14 May 2006
http://www.wired.com/wired/archive/14.05/rfid.html?pg=1&topic=rfid&topic_set=
(Accessed: 1 June 2006)

[W22] ACG Identification Technologies GmbH
www.acg.de,
(Accessed: 07 March 2006)

Appendix

All measurements from all experiments are listed below.

In the cases where a card contains a magnetic stripe, the side of the card carrying the magnetic stripe is referred to as *"side 1"* whereas the other side of the card is referred to as *"side 2"*.

In general, side 1 of the tags was directed towards the reader during the experiments. However, to rule out the possibility of which side directed to the reader influenced the reading range, some measurements were performed with side 2 towards the reader. Such measurements were only performed at distances close to the maximum reading distance measured with side 1 towards the reader.

In each table, the column *"Suc"* shows the number of **suc**cessful read attempts. The column *"Att"* show the total number of read **att**empts made. The column *"Total read attempts"* shows the sum of the two previous columns, "*Side 1 towards reader*" and *"Side 2 towards reader"*.

The column *"With probes attached"* shows the successful and total number of read attempts made with probes from the oscilloscope attached to the antenna. A brief test with a different oscilloscope and several different probes was performed to rule out the possibility of a faulty oscilloscope or faulty probes affecting the measurements. The results were, however, similar for both oscilloscopes and all probes.

Measurements Card 1

Dist (mm)	Side 1 towards reader		Side 2 towards reader		Total read attempts		With probes attached	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	100	100	0	0	100	100	60	60
20	100	100	0	0	100	100	48	65
30	100	100	0	0	100	100	0	60
40	100	100	0	0	100	100	0	60
50	100	100	0	0	100	100	0	60
60	100	100	0	0	100	100	0	60
65	100	100	0	0	100	100	0	60
70	100	100	0	0	100	100	0	0
75	99	100	100	100	199	200	0	0
77,5	57	100	76	100	133	200	0	0
80	3	100	0	100	3	200	0	0

Dist (mm)	Card in Metallic Folder		Card in Aluminum Foil		Card in Leather Wallet		Card in Leather Wallet with Contents		Card in Leather Wallet lined with Aluminum Foil	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	0	100	0	100	100	100	100	100	0	100
20	0	100	0	100	100	100	100	100	0	100
30	0	100	0	100	100	100	100	100	0	100
40	0	100	0	100	100	100	100	100	0	100
50	0	100	0	100	100	100	100	100	0	100
55	0	100	0	100	100	100	100	100	0	100
57,5	0	0	0	0	100	100	65	100	0	0
60	0	100	0	100	91	100	0	100	0	100
62,5	0	0	0	0	30	100	0	0	0	0
65	0	100	0	100	0	0	0	0	0	100

Measurements Card 2

Dist (mm)	Side 1 towards reader		Side 2 towards reader		Total read attempts		With probes attached	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	100	100	0	0	100	100	55	60
20	100	100	0	0	100	100	0	60
30	100	100	0	0	100	100	0	60
40	100	100	0	0	100	100	0	60
50	100	100	0	0	100	100	0	0
60	100	100	0	0	100	100	0	0
65	100	100	0	0	100	100	0	0
70	100	100	0	0	100	100	0	0
75	100	100	100	100	200	200	0	0
77,5	43	100	82	100	125	200	0	0
80	0	100	44	100	44	200	0	0

Dist (mm)	Card in Metallic Folder		Card in Aluminum Foil		Card in Leather Wallet		Card in Leather Wallet with Contents		Card in Leather Wallet lined with Aluminum Foil	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	0	100	0	100	100	100	100	100	0	100
20	0	100	0	100	100	100	100	100	0	100
30	0	100	0	100	100	100	100	100	0	100
40	0	100	0	100	100	100	100	100	0	100
50	0	100	0	100	100	100	100	100	0	100
55	0	100	0	100	100	100	100	100	0	100
57,5	0	0	0	0	100	100	80	100	0	0
60	0	100	0	100	100	100	80	100	0	100
62,5	0	0	0	0	94	100	0	100	0	0
65	0	100	0	100	0	100	0	0	0	100

Measurements Card 3

Dist (mm)	Side 1 towards reader		Side 2 towards reader		Total read attempts		With probes attached	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	100	100	0	0	100	100	56	60
20	100	100	0	0	100	100	0	60
30	100	100	0	0	100	100	0	60
40	100	100	0	0	100	100	0	60
50	100	100	100	100	200	200	0	0
55	82	100	99	100	173	200	0	0
57,5	19	100	0	100	19	200	0	0
60	0	100	0	100	0	200	0	0

Dist (mm)	Card in Metallic Folder		Card in Aluminum Foil		Card in Leather Wallet		Card in Leather Wallet with Contents		Card in Leather Wallet lined with Aluminum Foil	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	0	100	0	100	100	100	100	100	0	100
20	0	100	0	100	100	100	100	100	0	100
25	0	100	0	100	100	100	100	100	0	100
27,5	0	0	0	0	0	0	100	100	0	0
30	0	100	0	100	100	100	1	100	0	100
35	0	100	0	100	100	100	0	100	0	100
40	0	100	0	100	100	100	0	0	0	100
42,5	0	0	0	0	100	100	0	0	0	0
45	0	100	0	100	0	100	0	0	0	100

Measurements Card 4

Dist (mm)	Side 1 towards reader		Side 2 towards reader		Total read attempts		With probes attached	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	100	100	0	0	100	100	58	60
20	100	100	0	0	100	100	0	60
30	100	100	0	0	100	100	0	60
40	100	100	0	0	100	100	0	60
50	100	100	100	100	200	200	0	0
55	100	100	100	100	200	200	0	0
57,5	0	100	0	100	0	200	0	0
60	0	100	0	100	0	200	0	0

Dist (mm)	Card in Metallic Folder		Card in Aluminum Foil		Card in Leather Wallet		Card in Leather Wallet with Contents		Card in Leather Wallet lined with Aluminum Foil	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	0	100	0	100	100	100	100	100	0	100
20	0	100	0	100	100	100	100	100	0	100
25	0	100	0	100	100	100	100	100	0	100
30	0	100	0	100	100	100	100	100	0	100
32,5	0	0	0	0	0	0	89	100	0	0
35	0	100	0	100	100	100	0	100	0	100
40	0	100	0	100	100	100	0	100	0	100
42,5	0	0	0	0	100	100	0	0	0	0
45	0	100	0	100	0	100	0	0	0	100
50	0	100	0	100	0	100	0	0	0	100

Measurements Card 5

Dist (mm)	Side 1 towards reader		Side 2 towards reader		Total read attempts		With probes attached	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	100	100	0	0	100	100	118	120
15	100	100	0	0	100	100	99	120
20	100	100	0	0	100	100	58	120
30	100	100	0	0	100	100	0	120
40	100	100	0	0	100	100	0	120
50	100	100	0	0	100	100	0	0
55	100	100	100	100	200	200	0	0
60	100	100	50	50	150	150	0	0
65	0	50	0	50	0	100	0	0

Dist (mm)	Card in Metallic Folder		Card in Aluminum Foil		Card in Leather Wallet		Card in Leather Wallet with Contents		Card in Leather Wallet lined with Aluminum Foil	
	Suc	Att	Suc	Att	Suc	Att	Suc	Att	Suc	Att
10	0	100	0	100	100	100	100	100	0	100
20	0	100	0	100	100	100	100	100	0	100
30	0	100	0	100	100	100	100	100	0	100
40	0	100	0	100	100	100	100	100	0	100
42,5	0	0	0	0	100	100	0	100	0	0
45	0	100	0	100	100	100	0	100	0	100
50	0	100	0	100	0	100	0	0	0	100
55	0	100	0	100	0	100	0	0	0	100