RFID Insecurity for Entity Authentication

Abbas Alfaraj, B.Sc. (Eng)

Submitted to Department of Computer Science
University College London
September 2006

MSc in Information Security

RFID Insecurity for Entity Authentication

Abbas Alfaraj, B.Sc. (Eng)

Submitted to Department of Computer Science
University College London
September 2006

Requirements for the Degree of Master of Science
In Information Security

ABSTRACT

Contactless smartcards are widely used for access control and payment such as e-passports and credit cards. It is a form of identity identification (ID) which uses Radio Frequency as a link to communicate with the verifier; therefore it is called Radio Frequency Identification (RFID). RFID is claimed to be secure within the reading range - between RFID tag and the reader- of 10 cm or less. This experiment will show that passive RFID with centre frequency 13.56 MHz is not secure for such critical applications. RFID is not secure for entity authentication as it is vulnerable to Mafia Fraud attack or in other words relay attack. The experiment is demonstrated by two attacks systems. The first attack system was for skimming RFID tag using square loop antenna with one-meter-side. The reading range was up to 1.20 meter. The second attack system was a real-time attack using two circular loop antennas with a diameter of 30 cm. The demonstration of the second attack proves that RFID tags are vulnerable to Mafia attack. The experiment proves that RFID is not secure regardless of the encryption scheme used to protect the communication between the tag and the reader.

Thesis Supervisor: Yvo Desmedt
Title: Professor of Information Security

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisors, professors Yvo Desmedt and Dr. Paul Brennan for their inspiration, guidance and valuable suggestions during the project period.

I would also like to offer my profound gratitude to Mr. Andrew Moss, Mr. Gerald Mcbrearty and the Instrument Shop team for their help throughout the implementation phase of the project in the Electrical Department laboratory.

I shall also thank Saudi Basic Industrial Company (SABIC) CEO Eng Mohammed Al-Mady for providing me the chance to continue my postgraduate studies at UK. He has overwhelmed me with his great generosity.

I am grateful to my parents for their love and moral support through the difficult times. I am also grateful to a person who, even though he died before seeing this thesis, will always be remembered: my uncle Said Ali.

And last but not least, I would like to extend my thanks to every member of my family for the emotional assistance and support that I received during my study period. Special thanks to my lovely wife Amani and my children Rudayna and Ali for the hard times they suffered during my study period.

This project is dedicated to my sister Angam whose never-ending support and encouragement are behind my success; with my special thanks for all that she gives me, despite her illness.

Table of Contents

Table of Figures

Chapter 1

1 INTRODUCTION

1.1 Introduction

The purpose of using a physical token as a proof; such as the passport, driving licence and credit card is to link the person with his/her identity[11]. This concept of identity proof has been used widely for many proposes and to facilitate its wide use, an automatic identification procedures concept (Auto-ID) has been introduced and has recently become very popular in many sectors[13]. The idea behind the Auto-ID is to store identification data in a form of electronic data-carrying device called the smart card [13]. To make the auto-ID more practical and flexible, a contactless technology between the smart card and the reader is being used. The data carrier to transfer data between smart card and the reader is the Radio Frequency (RF), and the system called RFID (Radio Frequency Identification) system [13].

Radio Frequency Identification (RFID) is one form of the electronic automatic identification systems like bar codes, smart cards, and voice recognition, and it is used to identify objects [31]. This technology is often coupled with automatic data capturing systems to identify objects, capture information and transfer them to a computer without data entry [39]. Basically, the aim of these systems is to increase efficiency and reduce data entry during identification process.

RFID (Radio Frequency Identification) systems identify physical objects through a radio interface [14]. The RFID is based on sensing technology [31]. The use of the newly introduced RFID technology has been extended to more than personal identification such as purchasing, distribution logistics, industry, manufacturing companies, and material flow [13]. RFID is similar to bar coding in its concept. Bar code systems use a reader and coded labels that are attached to an item, whereas RFID systems use a reader and special RFID devices that are attached to an item [16]. While bar code systems use optical

signals to transfer information from the label to the reader; RFID systems use RF signals to transfer information from the RFID device to the reader.

1.2 RFID History

The first application of the RFID concept was done by the British military during WWII [10]. They installed transponders in their aircrafts that could respond within an appropriate distance. This response happened when the aircrafts were interrogated by a signal produced by friend aircrafts. The technology allowed them to identify their aircraft from others and the system was called Identify Friend or Foe (IFF) [31]. Since then, the RFID has undergone significant development and improvements for different applications in many sectors [31].

1.3 RFID System Components

The Radio Frequency Identification System is made up of two main components; a transponder/tag and an interrogator/reader [38]. The identification code or data is stored in a microchip attached to an antenna which is called a tag or a transponder like contactless smart cards (Figure 1.3-1). The interrogator, or reader, transmits and receives signals to/from the tag to read the identification code or data by inducing an electromagnetic field that will be coupled by the tag antenna [31].

1.3.1 Transponder/Tag

Historically, an RFID device that did not actively transmit magnetic waves to a reader was known as a tag. An RFID device that actively transmitted waves to a reader was known as a transponder (TRANSmitter + resPONDER) [2]. However, it has become common within the industry to interchange the terminology and refer to these devices as either tags or transponders [2]. The tags are programmed with data that identifies the item to which the tag is attached. Tags can be either read-only, volatile read/write, or write one/read many (WORM) and can be either active or passive [13]. In general, active tags use batteries to power the tag transmitter and receiver, while passive tags are non-battery operated. Tags will be addressed in more details in section 2.3 of this thesis [13].

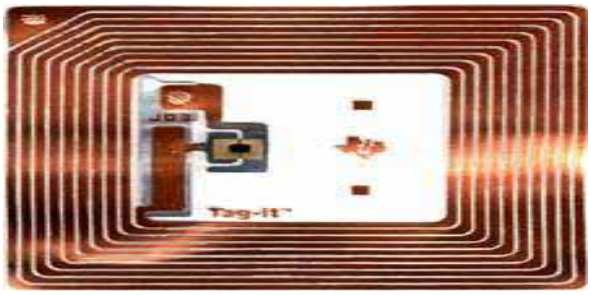

Figure 1.3-1: RFID tag with Antenna (source Tag-it)

1.3.2 Antenna

Each RFID system includes at least one antenna to transmit and receive the RF signals [13]. In some systems, a single antenna transmits and receives the signals; in others, one antenna transmits and another antenna receives the signals [13]. The quantity and type of the antennas used depend on the intended application [13].

1.3.3 Reader

The RFID reader directs the RF transceiver to transmit RF signals, receives the encoded signal from the tag to decode the tag's identification, and transmits the identification with any other data from the tag to the host computer[13]. Firmware in the reader controls reader operations[35]. The user can customize the reader's operations to suit specific requirements by issuing commands through the host computer or a local terminal.

1.4 RFID Categories

The RFID is categorized into two main categories depending on the coupling distance between the transponders and the reader [31, 38]. These are the near-field and far-field systems. The classification depends on the frequency operation of the RFID system [31]. This thesis will focus on RFID that are categorized as a near-filed system that uses inductive coupling of the tag to the reader though RF wireless data link at a frequency 13.56 MHz (

Figure **1.4-1**). The near-field RFID coupling techniques are generally used for short distance communication such as access control [31]. The near-field operates either in low-frequency (LF) or high-frequency (HF) bands which will be narrated in Section 2.7

of this thesis [31]. On the other hand, far-filed systems use higher transmission frequency with capacitive coupling through the electrical field generated between the tag and the reader [31].

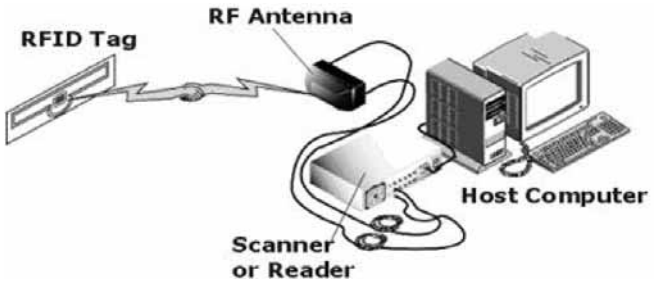

Figure 1.4-1: RFID System Basic Operation [23].

1.5 RFID Applications

The usage of the RFID is rapidly increasing nowadays because of the easy deployment and low-cost of the technology. Some RFID chips cost only 5 cents [16]. In 2003, Philips reported the total worldwide shipment of RFID for that year to be more than a billion [16]. An RFID Journal anticipated that between 20 and 50 million Americans carry RFID chips on a daily basis [16]. The application of RFID has included the supply-chain management like inventory control and retail check-out [31]. The use of RFID has also been extended to payment systems, access control, car immobilization, automatic toll collection, medical records, and cattle herding [13].

1.6 Thesis Goals and Objectives

The goal of this work is to prove that in particular, high frequency (HF) RFIDs (13.56 MHz) are not secure for entity identification. We decided to demonstrate that RFID is subject to the mafia fraud attack or, in other words, relay real time attack.

This thesis includes a deep background for RFIDs system fundamentals, regulations, functionality, and communication theory. The antenna theory for indicative magnetic

field is examined here to aid us understand the basis of designing and analyzing RFID system. Finally, a discussion is presented about the result to draw the conclusion.

Chapter 2

2 BACKGROUND

2.1 Introduction

RF technology is used in many different applications, such as televisions, radios, cellular phones, radars, and automatic identification systems [10]. It was mentioned earlier in section 1.1 that the term RFID (radio frequency identification) describes the use of radio frequency signals to provide automatic identification [39]. Radio waves are classified according to their frequencies, which are expressed in kilohertz, megahertz, or gigahertz [31]. Radio frequencies range from very low frequency (VLF), which has a range of 10 to 30 kHz, to extremely high frequency (EHF), which has a range of 30 to 300 GHz[38]. All relevant RFID technology, concepts, standards, regulations, categories, types, and security will be addressed in this chapter.

2.2 Identification and Its Attacks

Literally identification is the act of identifying, or proving to be someone/something; also, it is the state of being identified [7]. In other words, identification is the process of matching a set of qualities or characteristics that uniquely identifies a person/object [15]. It is a technique used by one party to ensure a second party is very likely the party claiming the identity [5]. Assurance of identification can be increased by a number of practices appropriate to the need. These practices may range from passwords to tokens, signatures, PIN number, smart cards, and public keys with certificates[13].

Due to the high demand for identification, the processes of identifying personal identity need to be automated for more security and convenience. RFID has been introduced as a candidate to automate the identification processes but it has, however, limitations due to vulnerability to several attacks and threads [15, 14]:

1. *Sniffing*. RFID tags are designed to be read by any compatible reading device[30]. Tag reading may happen without the knowledge of the tag owner and may also occur at large distances. This is called skimming the RFID tag, and the attacker can then clone or send the data to another person and broadcast the same signal to the reader [30].

2. *Tracking*. RFID readers in strategic locations can record sightings of unique tag identifiers, which are then associated with personal identities [30]. The problem arises when individuals are tracked involuntarily.

3. *Spoofing*. Attackers can create authentic RFID tags by writing properly formatted tag data on blank or rewritable RFID transponders [14]. Recently, researchers from Johns Hopkins University and RSA Security performed a spoofing attack on RFID [6]. The researchers cloned an RFID transponder, using a sniffed (and decrypted) identifier, which they used to buy gasoline and unlock an RFID-based car immobilization system.

4. *Denial of Service*. Denial of Service (DoS) is when RFID systems are prevented from doing its function properly [18]. Tag reading can be hindered by Faraday cages or signal jamming, both of which prevent radio waves from reaching RFID tagged objects [30].

5. *Replay attacks*. Attackers can intercept and retransmit RFID queries using RFID relay devices between the tag and the reader [21]. These retransmissions can fool readers and the attacker can impersonate the tag.

The idea of the attack in this thesis can be formalized through the Chess Grandmaster problem [5, 8]. Assume that a little girl plays chess with two grandmasters. The way for her to win a game is to move black pieces on one game and white pieces in the other game. Because white goes first, she will wait until the first grandmaster moves, and then she will replay his move to the other game versus the second grandmaster. She will win one game against the grandmaster because she is actually acting as a middleman between the two grandmasters playing [8]. This idea will be used to make the real time attack or relay attack between reader and the tag. Someone can act as a middleman between the tag

(prover) and the reader (verifier) to fool both of them and gain access to perform the required attack. Simply, a victim with an RFID tag is somewhere in the market while the attacker wants to gain access to a building using the victim's RFID access card. Another attacker is chasing the victim on the market with equipment that can send RF signal to the tag from an appropriate distance. The victim RFID tag will reply to that RF signal, and then the attacker on the market will capture the signal to send it to the other attacker who is standing close to the access door via a very fast link. The attacker close to the access door has RFID equipment that is capable of emitting the received RF signal. The reader doesn't know if this signal is coming from the real tag or from the fake RFID device! [21].

This attack was demonstrated by Kfir and Wool in their paper [21]. The attack system was composed of two RFID devices, one called Ghost, which is close to the reader, and the other is the so called Leech, which will be close to the RFID tag [21]. There is a fast digital bidirectional communication channel between the Ghost and the Leech to exploit the attack in a timely fashion. Their model is illustrated in Figure 2.2-1 [21].

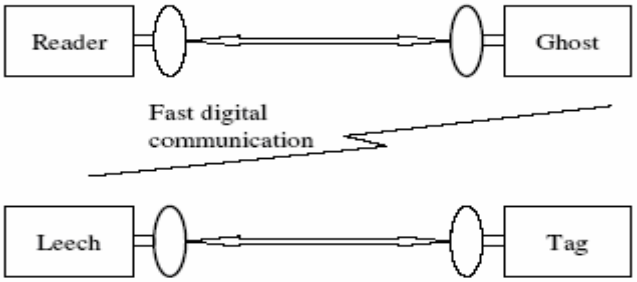

Figure 2.2-1: Kfir and Wool Attack System [21].

2.3 RFID Tags Types

It was mentioned earlier in Section 1.3, that the basic RFID hardware components are tags and readers. There are two basic types of a tag; passive and active [7].

1. **Passive RFID tags** have no battery [13]. They draw power from the RFID reader which emits electromagnetic waves that induce a current in the tag's antenna.

Semi-passive tags use a battery to run the chip's circuitry but communicate by drawing power from the RFID reader [7].

2. **Active RFID tags** have a battery which is used to run the microchip's circuitry and to broadcast a signal to a reader, similar to the way a cell phone transmits signals to a base station [7].

Active and semi-passive tags are useful for tracking high-value goods that need to be scanned over long ranges, such as railway cars on a track, but they are more costly than passive tags, making them too expensive to use for low-cost items [31]. Because passive tags operate without a battery, they have no lifetime but they possess a short reading range and require a high-power reader [18]. The experiment of this thesis will be for passive tags only which is inductively coupled.

2.3.1 Inductively Coupled RFID Tags

Most of the currently used inductive RFID tags are passive [31, 38]. Those tags are powered by the magnetic field generated by the reader [13]. The tag's antenna receives the electromagnetic energy powered by the reader [13]. The tag modulates that energy emitted through its transducer and transmits the data back to the reader [13]. The antenna in an inductive RFID tag is made from a coil of copper or aluminium wire [13].

2.3.2 Capacitively Coupled RFID Tags

Capacitive coupling tags use the electric field power generated by the reader to make the communication [31]. They eliminate the metal coil antenna by using a conductive link. Those types of tags have a very limited range [31].

2.3.3 Read-Only and Read-Write

Tags can be read-only or read/write [13]. A read-only memory tag has an identification code that is recorded at the time of manufacturing. Read-only tags are much cheaper and are typically used in passive tags [13]. Conversely, read/write tags can have their memory rewritten many times. Because they enable their ID codes to be changed, they offer

greater functions but they are not widely used because of their greater cost compared to the read-only tags [13].

2.4 Regulation and Standardization

RFID systems come in four common categories based on their operating radio frequencies [1]. These frequency ranges are known as the ISM bands (Industrial Scientific and Medical bands) [39]. Table 2.4-1summarizes the RFID frequency ranges and their applications [31].

Table 2.4-1: Summary for RFID Frequency for Passive Tags.

	Frequency Range	Typical Reading Range	Tag type	Application
Low-frequency-LF	125-134.2 kHz and 140-148.5 kHz	~1.5 feet; low reading speed Near-field	Passive	Access control, animal tracking, point of sale applications
high-frequency-HF	HF: 13.56 MHz	~3 feet; medium reading speed Near-field	Passive	Access control, smart cards, item-level tracking
Ultra-high-frequency-UHF	868 MHz-928 MHz	up to 15 feet; high reading speed Far-field	Active	Pallet tracking, supply chain management
Microwave frequency	2.45 GHz	~3 feet; high reading speed Far-field	Active	Supply chain management

The International Standardization Organization (ISO) and Electronic Product Code (EPCglobal Inc) have defined a set of rules or requirements that the RFID system components (tags, readers) must meet to operate effectively. Those rules and requirements currently have a standardized RFID technology that covers air interface operational requirements to ensure RFID systems meet the intended design [27]. Those standards are summarized below [15, 39]:

- ISO 11784 & 11785 - These standards regulate the RFID of animals in regards to Code Structure and Technical concept.
- ISO 14223/1 - RFID of Animals, advanced transponders - Air interface

- ISO 10373 RFID for access control.
- ISO 10536 RFID for identification cards
- ISO 14443 A/B used for access controls, E-passport [18].
- ISO 15693 RFID used at point-of-sale for payment
- ISO 18000 RFID for item management air interface
- EPCglobal - this is the standardization framework that is most likely to undergo international standardization according to ISO rules as with all sound standards in the world. Currently, the big distributors and governmental customers are pushing EPC heavily as a standard Requirements of ISO/IEC 14443 Type B Proximity Contactless Identification Cards

Yet there is no global public standard that governs the frequencies used for RFID. Frankly speaking every country can set its own rules. The main published regulations governing frequency allocation for RFID is reference [39]:

- USA: FCC (Federal Communications Commission)
- Canada: DOC (Department of Communication)
- Europe: ERO, CEPT, ETSI, and national administrations
- Japan: MPHPT (Ministry of Public Management, Home Affairs, Post and Telecommunication)
- China: Ministry of Information Industry
- Australia: Australian Communications and Media Authority.
- New Zealand: Ministry of Economic Development

2.5 RFID Interference to Primary Services

The following outline summarizes the RFID tag return frequency interference with other telecommunication services for LF and HF [1].

LF Range: 130 – 148.5 kHz Maritime radio navigation / Mobile (MM), Amateur radio service [31, 39].

HF Range: 4.750 – 8.815 MHz MM, Aeronautical Mobile navigation, Land Mobile navigation, Amateur, Fixed (point-to-point or point-to multi communication) [31, 39].

11.56 – 15.56 MHz Fixed Aeronautical Mobile, Radio Astronomy, and Amateur Radio [39].

2.6 How passive RFID System works?

It was mentioned earlier in the introduction that RFID consists of two components; a tag and a reader. Tags can be passive or active. The experiment of this thesis examines passive tags only, which are tiny resource-limited computers that are inductively powered by the energy of the request signal sent from RFID readers [13]. Once the RFID tag receives energy sufficient to power up its internal electronics, the tag can decode the incoming query and produce an appropriate response by modulating the requested signal using one or more sub-carrier frequencies. These RFID tags can do a limited amount of processing, and have a small storage capacity (<1024 bits) to store the identification code [13].

The interference interaction between the reader and the tag engages low-level functions to meet the requirements of the high-level commands [18]. The reader will transmit power, information, and a clock to the tag [13]. The information is used to identify the answer signals from the tag when multiple-identification or anti-collision protocol is employed; the later is used to authenticate many tags at the same time [13]. The clock is to drive the tag circuitry. The clock could be garneted from the carrier frequency or though load modulation of the carrier, depending on the operating frequency [31].

If the tag is within the reader interrogation zone, then the tag will receive the signal and will process the power, information, and clock. The tag will perform internal processing of the signal to answer the reader by back transmission of the tag identification code stored in the tag memory. This retransmission is done by modulation of the reader signal [31].The details of how the wireless link is established between the tag and the reader will be discussed in Section 4.2 of this thesis.

2.7 RFID Mafia Fraud Attack

The high usage of RFID systems in critical applications has imposed the use of security measures to protect them against threats [14]. However, RFID tags can be read from a far distance without the knowledge of the tag holder irrespective of the type of encryption scheme used to protect the data [16]. Even worse, the RF signal is undetectable by a human being and the RFID tag does not keep a history of the last readings; also RFID tags have no means to detect intrusion [16].

The experiment of this thesis is based on the concept of the Mafia fraud attack [9]. A prover is represented by the tag, and the verifier by the reader on the RFID terminal. The idea is to fool the verifier to make it believe that the attacker is the prover to gain the access as demonstrated in Figure 1.3-1. To perform this attack, a system is designed which consists of two parts. The first part is the stealer, who is chasing the tag holder, or the victim, to read the tag data without his/her knowledge. The stealer will then send the information through a very fast link to the second person (attacker) who comprises the other part of the attack system. The second person will try to trick the reader by sending the captured information and pretending to be the real tag. Simply, the attack is the second person trying to prove his identity to the verifier by answering the queries of the verifier using the stolen original tag information or data. This attack on RFID is exactly as the Mafia fraud attack on identity [9].

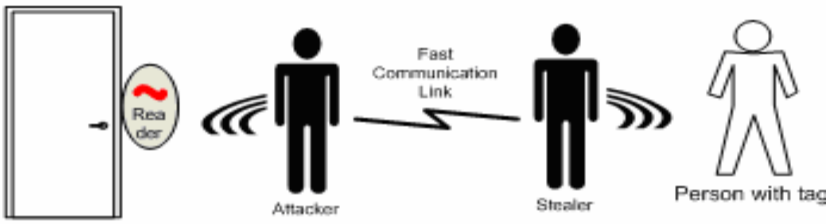

Figure 2.7-1: RFID Mafia Fraud Attack.

Mafia fraud attack assumes the attacker is a low-tech person [8, 9]. This will have a great impact on the system design and the extended reading range that has to be achieved. The assumption of the attacker's knowledge and technical capability reflects how advanced the design of the attack system is.

There are ready-made or built-in devices that can be used to pursue this attack. Those ready devices can approach a reading range up to 30 cm. Their intended use is for RFID assessment and evaluation. For example, Texas Instruments evaluation kit [19], Melexis Development Kit for MLX90121 Transceiver [34]. These are multi-reading RFID tags. They can read LF and HF for different RFID ISO standards. To carry out the attack, the attacker does not need more than purchasing two of these evaluation kits and installing them to work with a laptop or a pocket PC (PDA) through an RS232 interface to proceed with the attack. However, the goal of this work was achieved without using any of these ready- made kits. The system used to make the attack was locally built in the university laboratory for the following reasons:

- *In-house design*: to demonstrate that it is not difficult to build the system locally to carry the out Mafia fraud attack on RFID.
- *Cost*: these kits are expensive, for example the Melexis kit costs around £350.
- *Range*: the reading range of the ready made kits is very short while the locally built system was designed to read from around 1 meter.

2.8 RFID Data Security

The security scheme used for RFID communication between the reader and the tag is based on three-pass mutual authentication. Both reader and tag check the knowledge of the security key without transmitting this symmetrical key through airwaves. The three-pass mutual authentication protocol starts when the tag enters the interrogation zone of the reader. The reader sends the GET_CHALLENGE command to the tag. A random number R_T is generated by the tag and sent to the reader. The reader will generate another random number R_R. Then the reader will do some computations to generate an encrypted data using symmetric-key. The encrypted data is a function of the random numbers (R_T, R_R) and some control data. The reader will send the encrypted data to the tag. [13]

A tag will decrypt the received data using a shared or symmetric-key. The tag will compare the previously generated random number R_T, if they are the same then it means the secret key is the same. The tag will then generate another random R_{T2} concatenate

with R_R and other control parameter encrypted using the shared secret key and send it back to the reader. The reader will decrypt this data using the shared secret key check for R_R, which has been sent previously. If the random numbers are equal then the tag and the reader are satisfied and further communication will take place to perform the required function like gain access (Figure 2.8-1).

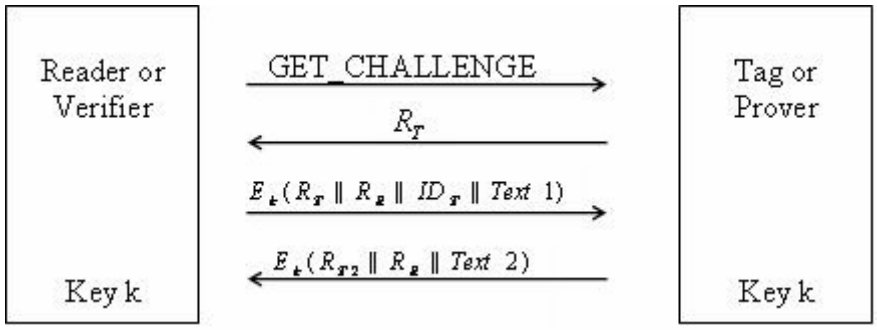

Figure 2.8-1: RFID Secure Communication Protocol.

Prover transcript = $E_k(R_T \| R_R \| ID_T \| Text1)$

Verifier transcript = $E_k(R_{T2} \| R_R \| Text\ 2)$

The RFID mutual authentication protocol involves two parties in an interactive communication; a reader as a verifier and a tag as a prover. This protocol is called Interactive Proof (IP) protocol for entity authentication [8, 24]. The protocol proves the identity as a means of authentication of two parties interacting *m* times and produces the following proof transcript [24]:

$$Commit_1, Challenge_1, \text{Re}\, ponse_1, ..., Commit_m, Challenge_m, \text{Re}\, sponse_m.$$

The output of the protocol is accepted if every checking step conducted by the verifier is passed and is rejected otherwise.

The above RFID identity mutual authentication protocol is similar to Zero-Knowledge Proof protocol. The Zero-Knowledge protocol was originally proposed by Fait and Shamir [9, 11]. The tag secret key becomes a function of the person identity. The tag uses the Zero-Knowledge proof to prove its privet key and identity to the reader without

revealing the secret key in the protocol. Also the reader proves its knowledge of the shared key to the tag without revealing the shard key during the communication [32].

The above protocol is similar to the Zero-Knowledge protocol where the prover transcript sent to the tag -in the second place- is not encrypted [9]. Some of newly RFID systems use improved authentication process. The key k used for the communication between the Verifier (reader) and the Prover (tag) is derived from a shared master key and the tag serial number [13].

2.9 Related Work on RFID Attack

There have been several published papers on RFID technology. Scharfeld's thesis has a broad overview of the RFID theory, standards, regulation, interference, and implementation issues [31]. Kfir and Wool showed that RFID smartcards are vulnerable to relay attack, using Leech and Ghost to make the attack [21]. However, they claimed that they could read the tag using Leech from few tens of centimeters slightly more than the nominal ISO14443 range 5-10 cm [3]. RFID attack tools can be downloaded from RFDump website [17]. A practical relay attack on ISO 14443 RFID has been discussed by Hancke [18]. Hancke's work was similar to Kfir and Wool's work, however, he used RFID link between Leech and Ghost which he called Mole and Proxy. He claimed that this RFID link could reach up to 50 m.

Kirschenbaum and Wool built RFID skimming to validate Kfir and Wool, they built the Leech part of the proposed attack system [22]. They used TI S4100 card reader for their experiment. They claimed that they could approach 25 cm reading rang for ISO 14443 RFID standard.

Massachusetts Institute of Technology and RSA Laboratories have done a lot of research and experiment on RFID technology. Much of this research on RFID has been focused on the privacy issues such as Ari, Rivest, and Szydlo work [20]. They presented a blocking tag approach to prevent any reader from connecting to the tag. RFID overview of privacy problems and solutions was discussed by Garfinkel from MIT research group [16].

Chapter 3

3 DESIGN AND ANALYSIS

3.1 Introduction

To achieve the goal and prove that RFID is vulnerable to Mafia attack, three attack systems were designed. The first attack system was designed previously by Paul Brennan (figure 3.2.1). The second attack system was built based on Kirschenbaum and Wool's system. During the implementation of the second system, the idea occurred to build a third attack system that combined the concepts of both the first and second attack systems.

3.2 First Proposed RFID Attack System

The first design to achieve the goal of attacking an RFID system was designed with the help of Dr. Paul Brennan from UCL Electrical Department (Figure 3.2-1). Basically the design was a coil (antenna), a directional coupler, an RF operational amplifier, an attenuator and a modulator-modulator. The goal of the design was to carry out the attack with simple design and low-cost.

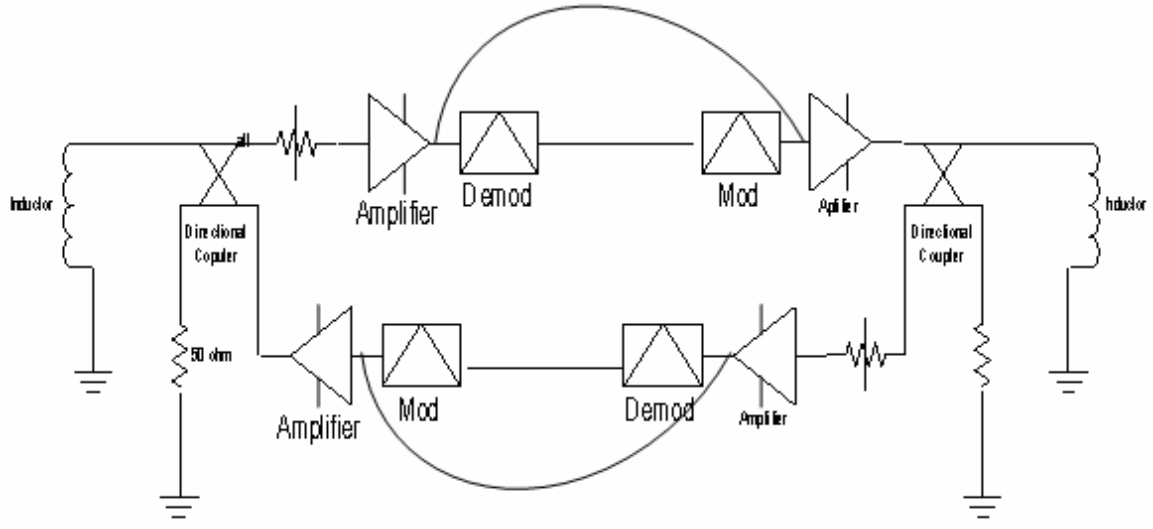

Figure 3.2-1: RFID Attack System Propused by Paul Brennan.

The attack system consists of two identical parts. One part is close to the tag, the other one is close to the reader. The two parts are connected through two links, one is for sending and the other is for receiving signals between the tag and the reader. The inductor or the coil within the reader interrogation zone will capture the power, queries, and clock to send them to the other coil close to the tag. The directional coupler is used to send the incoming signal from the coil to the input of the amplifier. The amplifier then amplifies the signal to send it for a long distance. The demodulator is used to convert the digital signal to an analog for wire transmission. There is a modulator at the other end to reconvert the signal digitally and amplify it to the required signal level. The directional coupler will couple the signal to the coil. The coil will transmit the signal to the victim tag as if it was the original reader. The tag will reply with the required information to the coil. The coil will send the information to the reader, in the way the reader sent the query signal but through the other link (the link below in Figure 3.2-1). The coil close to the reader will emit the incoming signal from the tag to fool the reader to gain access.

The target was to attack the HF range RFID system that operates within the following specifications:

- Operating Center Frequency of 13.56 MHz
- Impedance of 50 Ohm
- Input Power supply of 12V and 50mA
- This RFID system omits 0.5 Watts, equivalent to 27 dBm

It was very hard to find the required RF components with the above specifications and in particular the direction couplers. The purpose of the directional coupler is to route, isolate, separate, and combine signals. Most of the available direction couplers introduce power loss called coupling loss of around 20 dBm [26]. The RFID signal will be lost with this big coupling loss. To find another alternative solution, it was suggested that the couplers can be replaced by circulators. A circulator is nonreciprocal device that has 3 ports. The input of one port n will be an output at port n+1 but not at any port as shown in Figure 3.2-2[26].

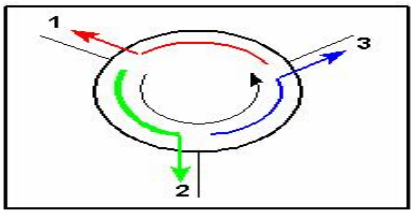

Figure 3.2-2: Circulator (Source [26]).

Circulators are mainly used for microwave signals, which are operating at very high frequency [26]. It was almost impossible to find a circulator with the required specification. Paul's suggestion was to use the old telephony system couplers or switches, which can meet the required specifications. However, those old traditional telephone couplers are not available on the market any more. Paul then suggested using the standard 180˚ hybrid junctions which were easier to find in the market.

The required components to build this RFID attack were ordered from Minicircuits in the US. It took more than four weeks to ship them to the UK. The components were then caught in UK customs for another few weeks for security and legalization issues. Then the idea of experimenting the above RFID attack circuitry was terminated due to the delay in component delivery.

3.3 Second RFID Attack System

Alternatively, another system was designed for this attack. This design was built on the Kirschenbaum and Wool model [22]. They built the RFID card skimmer for only 25 cm range [22]. I validated the same idea but using a different design for the antenna and its matching circuit to extend the reading to ≈ 1 meter; the antenna and its matching circuits will be explored in more details in Section 4.5. The original goal of this attack system was to perform a Mafia attack as shown in Figure 3.3-1. For more details about the figure blocks you may refer to the appendix.

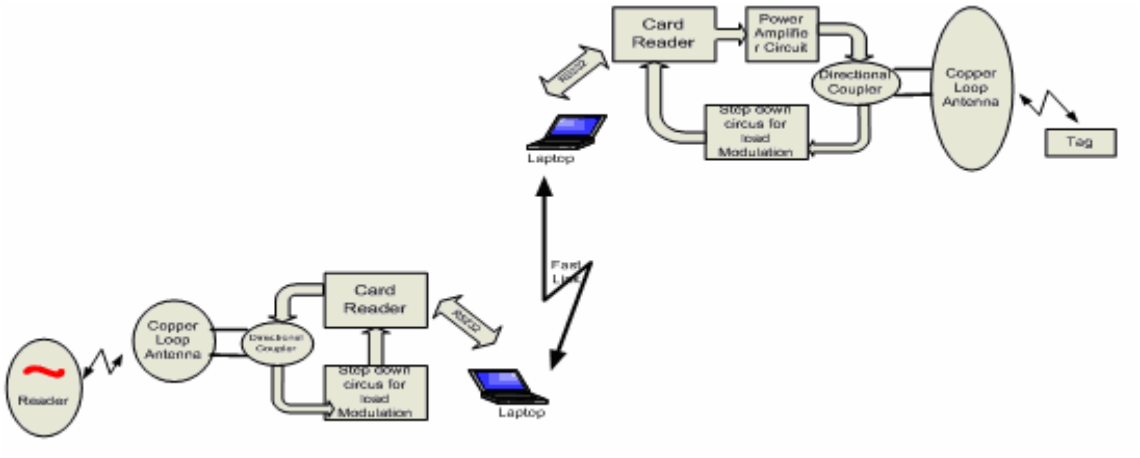

Figure 3.3-1: Second Attack System Design.

It was very expensive and difficult to build the above design, mainly because the requested components are not easily available in the UK. The goal was then reset for this attack system to prove that data from an RFID tag could be read, or skimmed, from a distance of more than 10 cm. Therefore, an RFID skimming system was built, based on Kirschenbaum and Wool's work, using an FEIG Electronics tuning board (see Figure 3.3-2) [12]. The first part of the design (RFID tag skimmer) with target reading range could be successfully achieved in the laboratory. Another cheaper system was designed to achieve the target which is a combination between the initial design and Kirschenbaum and Wool's work as it is explained in the next section.

Figure 3.3-2: FEIG Antenna Tuning Board

(Source FEIG [12]).

3.4 Third Design RFID Attack System

Experience has been gained during the implementation of the second proposed deign with designing and building low-frequency RF antennas and their matching circuits. The initially proposed design was revised with the help of Paul to demonstrate Mafia fraud

attack. This new attack system is a product of merging both the initial and the second designed attack systems. The attack system was built using two loop antennas, two matching circuits, two coaxial directional couplers, and RG58 coaxial cables to connect them (Figure 3.4-1). The design of the loop antenna was based on the HF Antenna Cookbook Technical Application Report [36]. The design of the antenna matching circuits was based on Feig Manual Antenna Tuning Controller paper [12]. The Electrical Engineering Laboratory Network Analyzer device was used to tune the matching circuits to the required capacitance and resistance values for maximum power transmission. The tuning methods and antenna design details will be explained more fully in the antenna design chapter of this report.

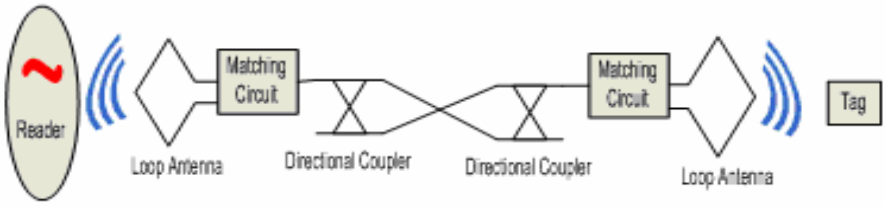

Figure 3.4-1: 3rd RFID Attack System.

The equivalent antenna matching circuit is illustrated in Figure 3.4-2 below. I used variable capacitor 5-50 pF and variable transistor 1-5 KΩ. For the loop antennas, a circular loop with 30 cm diameter was used, which was made of copper of 6.88 mm conductor inner diameter. The antenna was fabricated locally in the EE instrument shop.

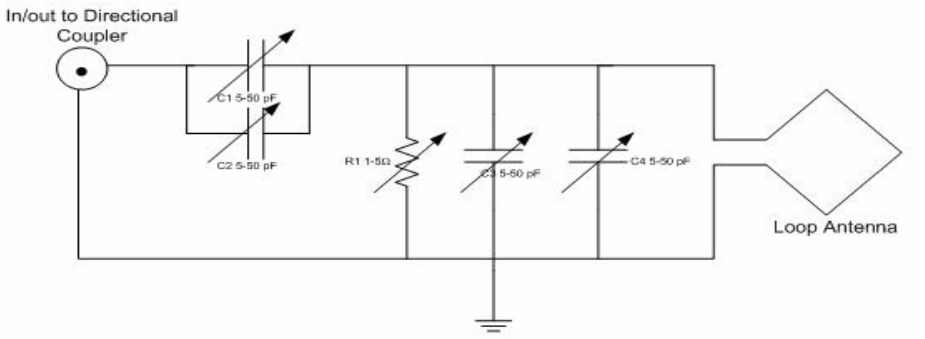

Figure 3.4-2: Matching Antenna Circuit.

Chapter 4

4 ANTENNA DESIGN

4.1 Introduction

The main use of antennas is to transmit radio frequency energy from one location to another [28]. HF RFID antennas are used to transmit RF energy, using free-space as a medium, at centre frequency of 13.56 MHz [28]. As mentioned previously, most of the current RFID systems are in principle an inductive coupling operation. To design an RFID attack system with the required reading range, the antenna theory has to be revised for more understanding of the principle of magnetic phenomena required for this purpose. This chapter will go through principles of the inductive antenna. The design of antennas used to perform the attack for RFID access cards will be discussed at end of the chapter.

4.2 Magnetic fundamentals for Inductive RFID

Maxwell's electromagnetic fundamentals state that any flow of current is associated with a magnetic field [31]. The strength of this magnetic field is represented by H, which can be calculated using equation 4.2.1 [13]. The direction of this magnetic field can be determined by using rule-of-thumb (Figure 4.2-1).

$$\sum \mathrm{I} = \int \mathrm{H}\, ds \qquad (4.2.1)$$

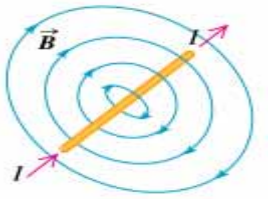

Figure 4.2-1: Magnetic Fieldd Rule of Thump [4].

In RFID, the magnetic antenna used to generate the alternate magnetic fields for inductive coupling are short cylindrical coils or conductor loops as shown in Figure 4.2-1 [13].

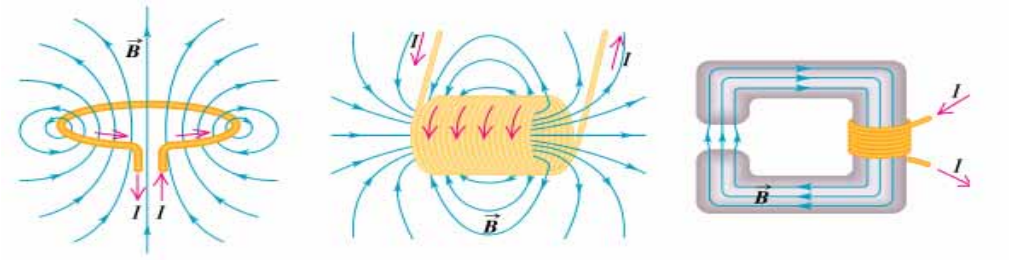

Figure 4.2-2: RFID Circular and Coli Antennas [4].

The equation used to calculate the strength field H in a conductor loop antenna is [13]:

$$H = \frac{I.N.R^2}{2\sqrt{(R^2+x^2)^3}} \qquad (4.2.2)$$

Where N is the number of windings, R is the circle readings, and x is the distance from the centre of the coil [13]. This equation can be simplified based on the shape and the size of the antenna used of the indicative coupling as we shall see later in my loop antenna design [13].

The density of the magnetic flux is measured on a perpendicular section of the surface area, as shown in Figure 4.2-3 [33].

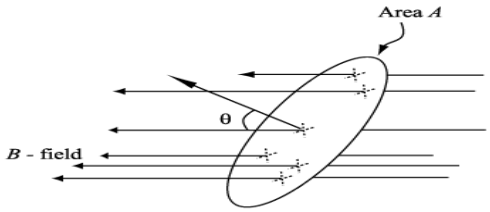

Figure 4.2-3: Magnetic Flux through Intersection Surface [33].

$\Phi = B \cdot A$

$\Phi = BA \cos\theta$

ϕ is the magnetic flux.

B is the magnetic flux density.

A is the area.

θ is the angle between the direction of the magnetic flux and the vector perpendicular to the plane of the area.

Both magnetic field and the magnetic flux will be generated around the conductor antenna regardless of its shape [31]. The inductance of the conductor is the ratio of the enclosed current *I* passing though the loop antenna and the arising flux (Figure 4.2-4) [33]. This inductance can be measured by Equation 4.2.3 [13].

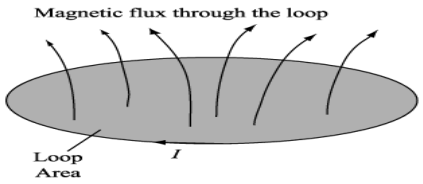

Figure 4.2-4: Magnetic Flux through Loop with Current I [33].

$$L = \frac{N \cdot \phi}{I} \qquad (4.2.3)$$

The inductance Equation 4.2.3 can be mathematically reduced if the conductor loop diameter D is greater than the conductor wire diameter, (d/D < 0.0001) [13]. Then the equation can be rephrased as:

$$L = N^2 \mu_0 R \cdot \ln\left(\frac{2R}{d}\right) \qquad (4.2.4)$$

μ_0 Is the magnetic field constant $4\pi \times 10^{-6} Vs/Am$ [13].

There are two antennas used for any single RFID system [13, 31]. One is used by the transponder or the tag, and the other is used by the reader or the transceiver for reading and writing [13]. If the tag is located in the vicinity of the reader antenna through which the current is flowing, an induced voltage and current will be generated in the tag antenna [31]. The tag antenna will be connected then by the coupling flux generated by both antennas; this is called mutual inductance M. The magnitude of this coupling flux ϕ_{TR} (R stands for reader, T stands for tag) is dependent on the size of the antenna, the position of

the two antennas, and the magnetic properties of the medium such as the permeability μ [13]. Equation 4.2.5 can used to calculate M.

$$M_{TR} = \frac{\psi_{TR}(I_R)}{I_R} \qquad (4.2.5)$$

By doing some basic mathematical substitutions for the Equation 4.2.5 using equations 4.2.1-4.2.4 then the mutual inductance will be [13]:

$$M_{TR} = \frac{\mu_0 \cdot R_R^2 \cdot N_R \cdot R_T^2 \cdot N_T \cdot \pi}{2\sqrt{(R_T^2 \cdot x^2)^3}} \qquad (4.2.6)$$

The mutual inductance for both reader and tag antennas is quantitative description of the flux coupling [13]. A new measurement has been introduced to measure the qualitative flux coupling called coupling coefficient k [13].

$$k = \frac{M}{\sqrt{L_1 \cdot L_2}} \qquad (4.2.7)$$

This coefficient varies between $0 \leq k \geq 1$.

If k = 0, then no coupling at all

If k = 1 then total coupling.

At this point it is important to know the concept of impedance in antenna theory. Impedance is the relationship between the voltage and the current [31].

Voltage represents the electrical field, and current represents the electromagnetic field. The impedance in concept is the description of the relationship between effort and flow as shown in Equation 4.2.9.[31]

$$Z = \frac{E}{H} \qquad (4.2.9)$$

Impedance is a very important parameter for the power transfer between antenna, transmission line, and load circuits and for characterizing the radiation and reaction of the antenna. In this project, I will use the loop antenna, in which the conductor material will have input impedance that can be measured at the end terminals of the conductor antenna [31]. This impedance is represented mathematically as

$$Z = R_{Radiation} + R_{loss} + jX \qquad (4.2.10)$$

$R_{Radiation}$ is the actual antenna radiation

R_{Loss} is the antenna ohmic loss

X is the antenna reactive which is the energy stored in the field around the antenna

The above parameters depend on the shape and material used for the antenna. For an efficient radiator antenna, the reactive will be higher than the radiation resistive. Near-field RFIDs use inductance coupling for which the reactive component must be positive. However, if the reactive component is negative, then it is a capacitance coupling. The transmission line and the antenna matching circuit or load circuit do have impedance as well. Their impedance needs to be matched with the antenna impedance for maximum power transfer without reflection [31]. We will later show how the impedance of the antenna and the matching circuits were matched using the lab network analyzer.

4.3 Resonance and Magnification Factor

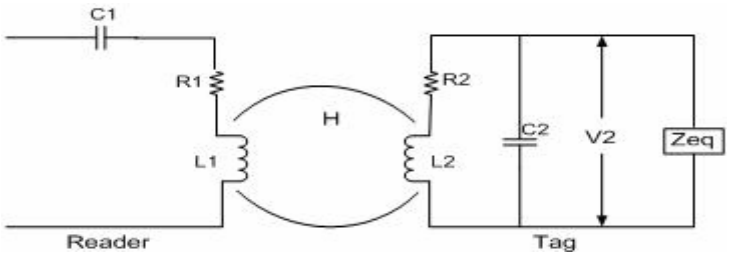

Figure 4.3-1: Equivalent circuits for tag and reader RFID.

The above Figure 4.3-1 shows the LC equivalent circuit of the RFID system tag and reader [13]. LC circuits will maximize the power available at the tag circuits at the operating frequency [31]. The angular frequency or resonant frequency for LC circuits is:

$$\omega = \frac{1}{\sqrt{LC}} \qquad (4.3.1)$$

The goal for the reader is to maximize the output current to increase the field coverage and strength, and therefore capacitor C1 has been added in series with inductor L1. C1 will reduce the impedance to the resonant frequency. However, the goal of the tag is to increase the voltage to drive the tag circuitry. Therefore, a capacitor has been added in parallel C2 to massively increase the impedance at resonant frequency to infinity [31].

The circuit components will influence the voltage induced in the tag, thus the voltage and current step-up in the resonant circuits must be measured at the resonate circuits [13]. The measurement is called magnification factor Q, or quality factor [13].

$$Q = \frac{\omega L}{R} = \frac{reac\tan ce}{\text{resistance}} \qquad (4.3.2)$$

For maximum power coupling Q needs to be maximized as well. However, high Q implies low bandwidth, and therefore a critical trade-off between Q and the bandwidth must be considered [31].

4.4 Reading Range for RFID Devices

There are two conditions that control the reading range between the reader and the tag. First, there must be enough power to energize the tag. Secondly, the reflected signal from the tag must be strong enough upon reaching the reader to be detected without any distortion [13]. Read range is defined as a maximum communication distance between the reader and the tag [13]. In general, the read range of passive RFID products varies depending on the system configuration and it is affected by the following parameters [28]:

- Operating frequency and performance of Antenna coils
- Q of antenna and matching circuit
- Antenna orientation
- Excitation of current
- Sensitivity of receiver
- Coding (or modulation) and decoding (or demodulation) algorithm
- Number of data bits and detection (interpretation) algorithm
- Condition of operating environment (electrical noise), etc.

The read range of 13.56 MHz is relatively longer than that of 125 kHz device. This is because the antenna efficiency increases as the frequency increases [29].

4.5 Experiment Antenna Design

In theory, the reading range, r, is equal to the antenna diameter [29]. the design was based on HF Antenna Cookbook Technical Application Report [36]. The report contains various types of antennas for different reading ranges. The antennas used for this experiment to transmit and receive RF signals are loop antennas, which are theoretically similar to the coils used as antenna. However, it is quite different to calculate and design the loop size at 13.56 MHz. The free-apace wavelength (in meters) at 13.56MHz is:

$$\lambda = \frac{c}{f} = \frac{300\,\mathrm{X}10^{8}\ m/s}{13.56\,MHz} = 22.1\,\mathrm{m} \qquad (4.5.1)$$

With reference to Figure 4.5-1, for loop to be classified as "electrically small" the length w must be less than 10% of the free-space wavelength. That is $w \le 0.1\lambda$ where w is the loop antennas side size. For the loop antenna of 1 m, it is 2.2 meters.

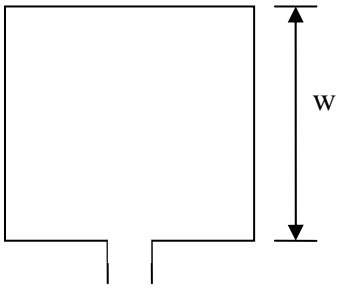

Figure 4.5-1: Square Loop Antenna.

Similarly for a circular loop to be considered electrically small, its diameter must be less than 0.1λ (Figure 4.5-).

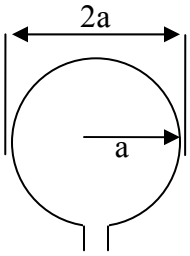

Figure 4.5-2: Circular Loop Antenna 2a < 0.1λ.

The radiation resistance for the square loop antenna of 2.2 meters is given by $RR = 31200\left(\frac{A}{\lambda^2}\right)^2$ which is 139.7 mΩ.

RR is very small and this loop antenna can not technically radiate any power for communicate!

The concept behind RFID communication between tag and the reader is using electrically small loop antenna for magnetic coupling that is loosely coupled transformers [31]. The reader antenna is acting as primary transformer. This is a very important concept in designing RFID antenna which are the basis of the reading range, (r is equal to the antenna diameter).

4.5.1 Copper Tube Loop Antenna

This loop antenna was designed for purpose to skim RFID card and store the data in the computer or PDA. The desired reading rang for this copper tube antenna was 100 cm. Therefore, the loop antenna used was a square shaped (100 x 100 cm). In this phase of the experiment I constructed my loop antenna conductor using 20 mm diameter cooking gas copper tube as described in the report. The loop antenna material used is very cheap and can be found in any building construction shop.

4.5.2 Rectangular PCB Loop Antenna

This antenna was used to prove the concept of the project. The antenna was 17 x 33 cm, and the track size was 1 cm. the reading range was almost 20 cm. I connected this antenna directly to the S4100 reading module without any amplification of the signal or any directional coupler.

4.5.3 Circular Loop Antenna

This antenna was used to do the real-time attack which was previously demonstrated in Figure 4.5.2. The antennas diameters were 33cm and the reading rang was almost 25 cm. A flexible copper tube with 10 mm diameter was used.

4.6 Antenna Matching Circuit

The input impendence of the RFID system with a transmission frequency of 13.56 MHz is 50 Ω [36]. Since the antenna conductor was locally built, a manually adjustable matching circuit was needed for total power transmission without power reflection [36].

There are many matching circuit designs available in Transceiver RFID 13.56 MHz MLX90121 Cookbook [29]. The antenna matching circuit used was a FEIG Manual Antenna Tuning Controller made by FEIG electronics [12]. Below Figure 4.6-1 is the equivalent circuit of this tuning board. This choice was based on the maximum power that can be transmitted (8 Watt). This power will give a greater reading range.

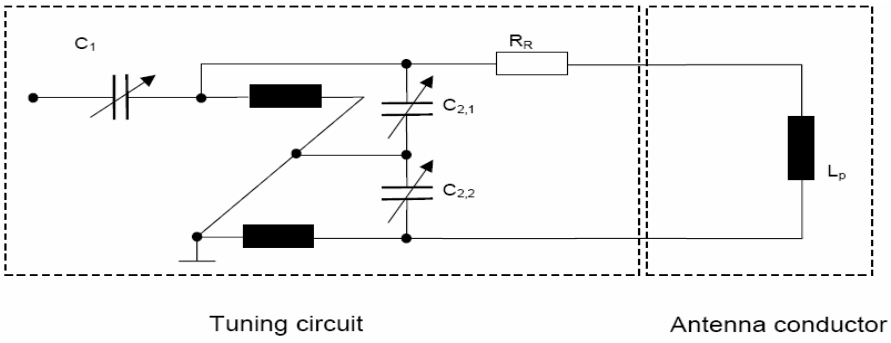

Figure 4.6-1: Antenna matching circuits for the tuning board [12]

4.7 Tuning Antenna Matching Circuit

The installation manual of the matching circuit explains how to tune the matching circuits using the capacitor jumpers and the capacitor trimmers [12]. The EE lab network analyzer has been used to match the circuit with the antenna conductor using the RG58 coaxial cable. There are preset values in the manual for the jumpers for a given antenna size. However, those preset values were not used because the antenna conductor was different from the recommended wire. It was a very crucial part of the experiment to adjust and match the antenna with the tuning circuit at frequency of 13.56 MHz with 50Ω impedance. The network analyzer can measure the magnitude and the phase of the system input to get the right tuning for the trim capacitors in order to match the desired impedance for total power transmission. After a few days of experiments and trial, it was possible to match the circuit with the antenna conductor as shown in the following plots (Figure 4.7-1, Figure 4.7-2) from the network analyzer.

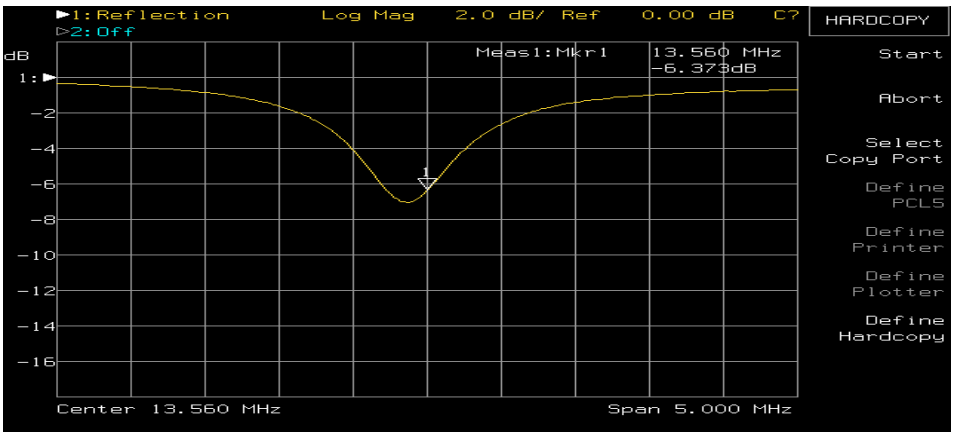

Figure 4.7-1: 100 x 100 cm Network Analyzer Real Reflection Plot.

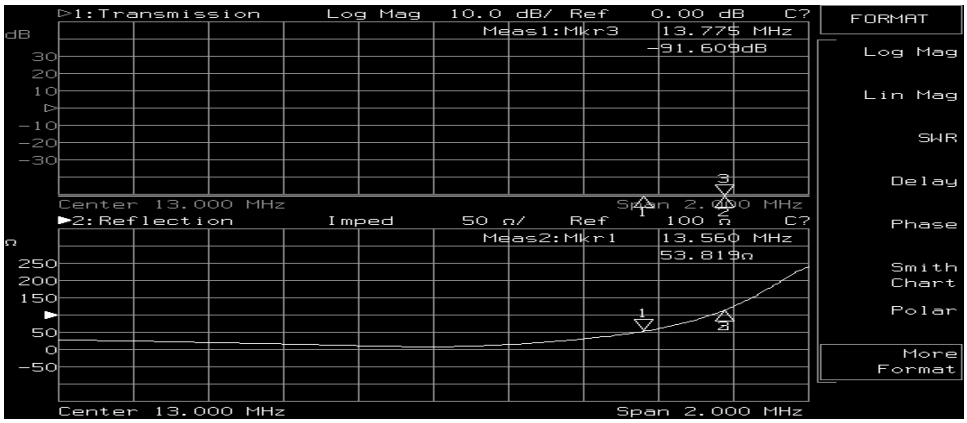

Figure 4.7-2: 100 x 100 cm Network Analyzer Impedance matching Plot.

Chapter 5

5 TESTING AND RESULTS

5.1 Introduction

The practical implementation of the experiment was based on the optimal utilization of the available resources at the university laboratory and the UK electronics shops. Therefore, a lot of improvisation was done due the shortage of the components within the UK. However, the goal was achieved by skimming RFID tags using 100 x 100 cm antenna. Also pursuing relay attack or Mafia attack using the two circular loop antennas of 30 cm diameter. This chapter will show the result of the designed systems to experimentally attack the RFID system.

5.2 Skimming RFID Tags

Using the TI S4100 Multi-Function Reader Module, the designed 33 x 15 cm rectangular PCB antenna with its matching circuit and the RS232 interface, I could skim RFID tags from 20 cm. The S4100 reader is a multi-protocol reader, which can read most of the RFID standards such as ISO 14443 A/B and ISO 15693. Although it is a dual frequency operation (134.4 KHz, 13.56 MHz); it was connected to the HF port as the 13.56 MHz is the desired operating frequency. The reading range was around 25 cm.

To increase the reading range, a larger one-meter square loop antenna was used. The generated power of the S4100 RFID reader was not enough to create a magnetic field [37]. Therefore, the signal was amplified using a voltage drive amplifier which was able to create a very strong magnetic field [25]. The reading range was around 1.20m. The system worked continuously for about 30 minutes then it stopped. After testing the complete design, a very high voltage (≈ 200 volts) was read across the antenna. This induced voltage destroyed some of the amplifier components such as the resister and the inductor. Ideally high rated voltages must be used to sustain the power generated by the

antenna. Unfortunately, those high rated voltage components are not easily found in the UK electronics shops!

The laptop used for this experiment logged all the RFID Oyster card data of the students on the EE lab. I can now easily clone those cards and use them. Microelectronic Integrated System sales programmed RFID tags can be used for this purpose.

5.3 Demonstrating Mafia Fraud attack

The two circular loop antennas were used to demonstrate that RFID is not secure. The antennas were connected through directional couplers. One antenna was close to the RFID reader, and the other was close to the victim tag. The RFID reader signal is transmitted to the tag though these two antennas. The tag responded to the carried signal. The response of the tag was carried back to the reader and access was gained while the tag was in a remote area. The attack was practically implemented as demonstrated in figure 5. The reading distance from the tag to the circular loop antenna was ≈17 cm. If the signal that travels between the reader and the tags (between 2 antennas) is amplified, then the reading range would be expected to exceed 17 cm.

There was a very important observation during the testing phase of the experiment. The reading range kept changing on a daily basis. This fluctuation was due to some environmental factors surrounding the antenna; such as the temperature and humidity. Also the position and the direction of the antenna influenced the transmitted power of the antennas. Those factors had a huge impact on the reading range.

Chapter 6

6 CONCLUSION

6.1 Conclusion

Several suggestions have been proposed to increase the security of the RFID tag, such as the hash-lock approach and the re-encryption approach [20]. However, none could meet the required security criteria to trust RFID tags for critical applications. The only reliable solution is to shield the RFID tags by a Faraday cage which is produced by one company in the form of foil-lined wallets [20].

The experiments of this thesis clearly demonstrated that RFID is not secure for critical applications regardless the encryption scheme used to protect the communication between the tag and the reader. The data that is in the form of a serial number in the tags is still readable by any intruder without the knowledge of the tag owner and without any logging for the tag past readings. The attacker can communicate with RFID tag from a quite far distance (1.2 meter) as proven in this thesis. Areas for future research might focus on extending the reading range between the attacker and the tag to make the mafia fraud attack even easier.

7 REFERENCES

1. (ECC), E.C.C. Compatibility between Inductive LF and HF RFID Transponder and other RADIO Communication System in the Frequency Ranges 135–148.5 kHz, 4.78–8.78 MHz AND 11.56–15.56 MHz, European Conference of Postal and Telecommunications Administrations (CEPT), 2002.
2. AIM. Radio Frequency Identification RFID, Automatic Identification Manufacturers Inc., Pittsburgh, 1998, 1-17.
3. ATMEL. Requirements of ISO/IEC 14443 Type B Proximity Contactless Identification Cards, 2005, 1-28.
4. Becker, J. Magnetic Field & Magnetic Forces *http://www.physics.sjsu.edu/becker/physics51/mag_field.htm*, Physics Department, San Jose University, San Jose State, 2006.
5. Bengio, S., Brassard, G., Desmedt, Y., Goutier, C. and Quisquater, J. Secure implementations of identification systems. Journal of Cryptology, *4* (3). 175-183.
6. Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A. and Szydlo, M. Security Analysis of a Cryptographically-Enabled RFID Device, RSA Laboratories USA, 2005, 1-19.
7. Cavoukian, A. Tag, You're it: Privacy Implications of Radio Frequency Identification (RFID) Technology, Ontario, 2004, 1-42.
8. Desmedt, Y. and Beth, T. Identification Tokens or: Solving the Chess Grandmaster Problem, Springer-Verlag, University of Karlsruhe West Germany, 1998, 1-8.
9. Desmedt, Y., Goutier, C. and Bengio, S. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. Pomerance, C. ed. Advances in Cryptology, Proc. of Crypto~'87 (Lecture Notes in Computer Science 293), Springer-Verlag, Santa Barbara, California, U.S.A., 1988, 21-39.
10. Eagle, J. RFID: The Early Years 1980-1990, MIT, 2001.
11. Fait, A. and Shamir, A. How to prove yourself: Practical Solutions to Identification and signature problems, Springer-Verlag, Santa Barbara, California, USA, 1987, 186-194.
12. FEIG, Feig Manual Antenna Tuning Control. FEIG Electronic GmbH, 2004.
13. Finkenzeller, K. RFID Handbook. John Wiley $ Sons Inc., Hoboken, 2004.
14. Fong, K. RFID Security, Department of Computer Science Southern Illinois University Carbondale, 2005.
15. GAO, U.S. Radio Frequency Identification Technology in the Federal Government, United States Government Accountability Office, 2005, 1-41.
16. Garfinkel, S., Juels, A. and Pappu, R. RFID Privacy: An Overview of Problems and Proposed Solutions IEEE Security & Privacy, IEEE Computer Society, 2005.
17. Grunwald, L. and Wolf, B. RFDump *http://www.rf-dump.org/*, 2004.
18. Hancke, G. A Practical Relay Attack on ISO 14443 Proximity Cards, University of Cambridge, Cambridge, 2004, 1-13.
19. Instruments, T. S4100 Multi-Function Reader Evaluation Kit, Texas Instruments Incorporated, 2004, 2.

20. Juels, A., Rivest, R.L. and Szydlo, M. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, MIT, 2004, 1-16.
21. Kifr, Z. and Wool, A. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems, School of Electrical Engineering, Tel Aviv University, ISRAEL, 2005, 1-14.
22. Kirschenbaum, I. and Wool, A. How to Build a Low-Cost Extended-Range RFID Skimmer, Tel Aviv University, 2006, 1-22.
23. LTD, P.B.N. Basic Introduction to RFID 2006.
24. Mao, W. Modern Cryptography Theory & Practice. Prentice-Hall, Inc., 2004.
25. Melexis. Transceiver RFID 13.56MHz MLX90121 Cookbook. 001 ed., Microelectronic Integrated Systems, 2006, 1-37.
26. NAWCWD Electronic Warfare and Reader Systems Engineering Handbook. Avionics Department of the Naval Air Warfare Center Weapons Division 1993.
27. Office, U.S.G.A. Radio Frequency Identification Technology in the Federal Government, 2005, 41.
28. PLC. 13.56 MHz RFID Systems and Antennas Design Guide, Microelectronic Integrated Systems, 2004.
29. PLC. Transceiver RFID 13,56 MHz MLX90121 Cookbook, Microelectronic Integrated Systems, 2006, 37.
30. Rieback, M.R., Crispo, B. and Tanenbaum, A.S. Is Your Cat Infected with a Computer Virus?, Computer Systems Group University of Amsterdam, Amsterdam, 2005, 1-10.
31. Scharfeld, T.A. An Analysis of the Fundamental Constraints on Low Cost Passive Radio-Frequency Identification System Design Department of Mechanical Engineering, MIT, Massachusetts, 2001, 115.
32. Schneier, B. Applied Cryptography. John Wiley & Sons Inc., 1996.
33. Steven, C.K.-L. Fields/Electromagnetic induction, JCPhysics, 2001, 1-12.
34. Systems, M.I. Development Kit for the MLX90121 Transceiver, Melexis, 2005, 15.
35. TI-RFID. Boot Loader Reference Guide, Texas Instruments, 2003.
36. TI-RFID. HF Antenna Cookbook Technical Application Report, Texas Instruments, 2004.
37. TI-RFID. S4100 Multi-Function Reader Module Data Sheet, Texas Instruments, 2003.
38. UPM. Tutorial Overview of Inductively Coupled RFID Systems, 2004, 1-7.
39. Wikipedia. Radio Frequency Identification, Wikimedia Foundation, Inc, 2006.

8 APPENDIX

The amplifier used in the experiment was based on Melexis Application Note [25]. The equivalent amplifier circuit is as described in below figure 8.1:

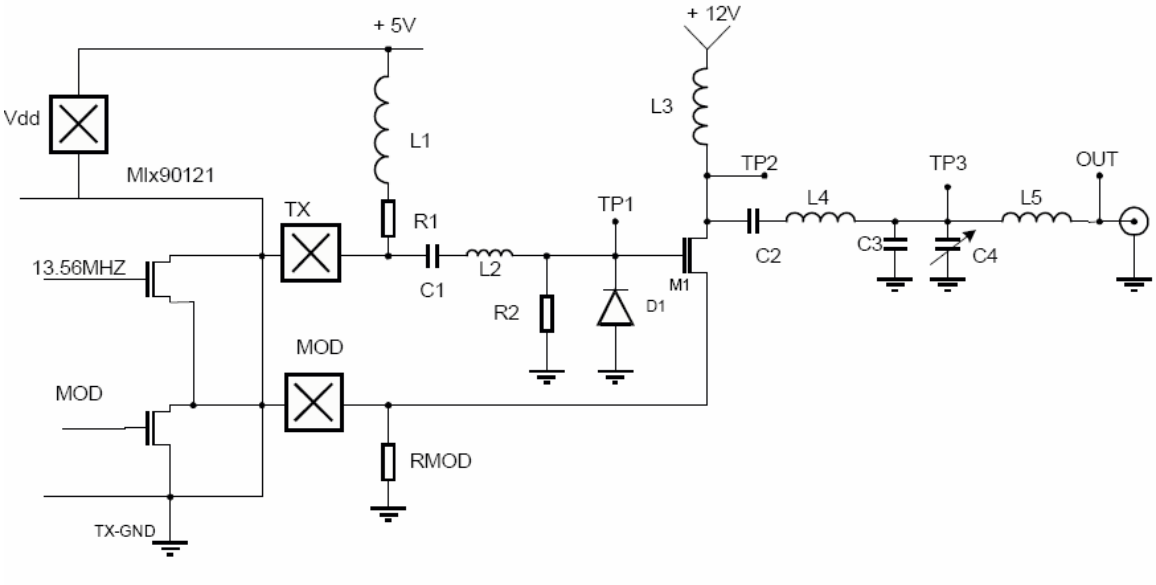

Figure 8.1: Amplifier Equivalent Circuit

The equivalent buffer circuits for incoming signal from the antenna were based on Kirschenbaum and Wool document [22] (see below, figure 8.2).

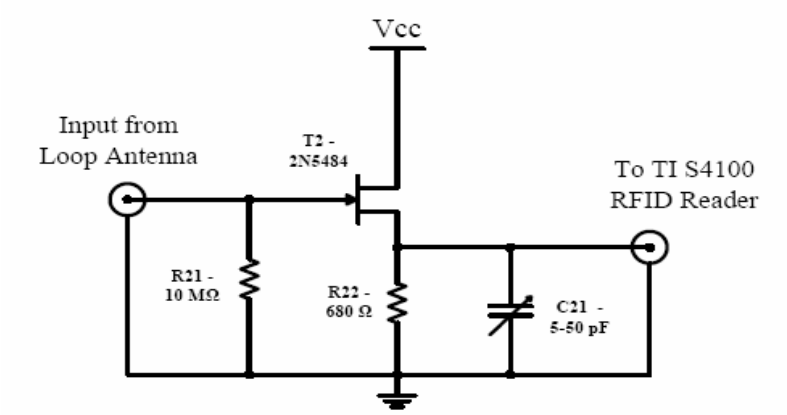

Figure 8.2: Receiving Buffer Circuit (source [22])

The RS232 interface circuitry between S4100 multi-function reader and the laptop was based on the S4100 datasheet document (figure 8.3) [37].

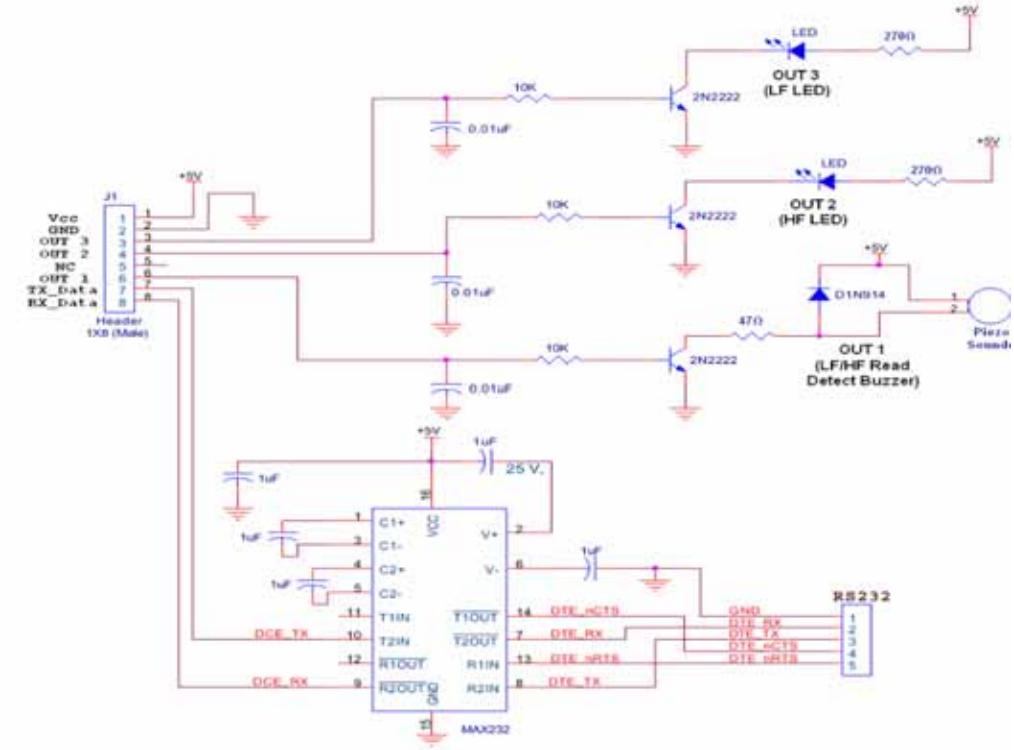

Figure 8.3: interface Circuitry

The firmware uploaded to the S4100 EEPROM was down loaded from the Texas Instrument website [35].

The program used to read the incoming data from the S4100 reader was downloaded from the Texas Instrument website. The code was written using visual basic.