Enhancing the Security of Ultra-Light Weight Protocols for RFID Applications

By

Mujahid Rashid

Submitted to faculty of Department of Information Security National University of Sciences and Technology, Rawalpindi in partial fulfillment for the requirement of a M.S Degree in Information Security.

August, 2016

Supervisor Certificate

It is to certify that Final Copy of Thesis has been evaluated by me, found as per specified format and error free.

Dated _____

_____
(Col Imran Rashid, Phd)

Acknowledgements

I am thankful to my Creator Allah Subhana-Watala to have guided me throughout this work at every step and for every new thought which you setup in my mind to improve it. Indeed I could have done nothing without your priceless help and guidance. Whosoever helped me throughout the course of my thesis, whether my parents or any other individual was your will, so indeed none be worthy of praise but you.

I am profusely thankful to my beloved parents who raised me when I was not capable of walking and continued to support me throughout in every department of my life.

I would also like to express special thanks to my supervisor Dr Imran Rashid for his help throughout my thesis.

Finally, I would like to express my gratitude to all the individuals who have rendered valuable assistance to my study.

Dedicated to my exceptional parents and adored siblings whose tremendous support and cooperation led me to this wonderful accomplishment.

Abstract

Every new invention has somehow changed the world either in a good or bad way. Similarly RFID technology has a great impact on the world. RFID is a technology to identify objects or people automatically and has received many application in recent years. Few decades ago, barcodes and magnetic strips on items or cards was a common practice. RFID has become superior due to bulk reading and high efficiency. RFID products contain more memory and can be read from a distance which leads to its biggest disadvantage. Transmitting over a wireless channel is never secure and since RFID is mostly used in application to enforce security this is a great concern. The protocols by which the transmission is done needs to be highly secure.

Over the years many protocols have been researched and developed some easily broken but some still standing the test of time. This shows that the world of RFID is still evolving. In the field of information security it is known that nothing can always be secure one day or the other it will be broken and the more research done in a field on its security enhances its chances of being secure for a longer time.

This thesis is also focused on enhancing the security of an RFID system. After some research we have selected an RFID protocol that claimed security from different attacks. Our main objective will be to find out any weakness if that protocol has and to improve its security by removing those vulnerabilities.

Key Words: *RFID, Smartcards, RFID Protocols, Barcode, Information Security, Identity Theft*

Table of Contents

List of Figures

CHAPTER 1: AIMS / OBJECTIVES

1.1 Problem Statement

1.1.1 Identity theft

Wireless ID theft / **contactless ID theft** or **RFID theft**, is can be described as compromising Identity information using radio frequency mechanics. The theft relies on RFID tags basic features. When a tag comes in to the coverage radius of a reader it responds with a signal that contains identifying information. Once this information is captured (harvesting) an attacker can program other cards to transmit the same information (cloning). Instructions for performing this attack are easily available on the internet.

In 2006 a group of researchers in their report "Vulnerabilities in First-Generation RFID enabled credit cards", mentioned some interesting findings about wireless ID thefts.

- Some Cards revealed the owners name, card number and expiration date.
- Scanning distance could be increased from a few inches to couple of feet.
- Ever one of the 20 cards tested were vulnerable to at least one attack they were exposed too.
- The vulnerabilities were not only limited to credit cards but the electronic passports were prone to these as well.

The most popular and widely used application of RFID technology has been mentioned in section 1.4. Let's take an example of the electronic ID cards. These cards are not only used to provide access to secure areas but might also contain other identity information that should be kept confidential. It is common human nature that we rely so much on technology that we trust it blindly. An attacker who is able to extract the information from a card will be able to clone a new one and could potentially access any restricted area. Since the system would recognize it as an authentic card it would not raise an alarm and the attacker can then freely perform his malicious attack without the fear of getting caught or stopped. A cloned national id card or a security card for a military installation is a great risk for any government or military organization. But the threat does not stop here, in the near future we would soon be moving to a

concept of single card identity which would mean that just one card would be our national ID card, credit or debit card and even our driver's license.

The literacy rate of our country is very low and even fewer people have a general understanding of an RFID technology. A region where people do not understand the risks of a technology is a gold mine for cyber thieves and criminals. Technology should be a reason for people to feel secure not to aid attackers to exploit others.

A survey was conducted to find out the level of knowledge that the people had about RFID technology. The questionnaire that was distributed is provided in Appendix B. Number of people that participated in the survey were twenty. The participants were mainly family member or colleagues. A brief introduction about RFID technology was given to each individual before the survey.

1.1.2 Results

Out of twenty people that participated in the survey following are the results according to the questions asked.

- **8** had the Smart Id Cards (40%)
- **12** had NHA Tags (60%)
- **2** have heard of RFID technology (10%)
- **1** knew how RFID System Works (5%)
- **1** Knew the drawback of an RFID system (5%)
- **2** Knew how someone can steal information from RFID cards or tags. (10%)
- **19** people would prefer a single card that would replace all other cards. (95%)

It was widely clear from the results of the survey that majority of the people had been using RFID technology without even knowing how their data and identity can be compromised. In the future the number of people, who will have either a smart id card or an NHA tag, will increase making more and more people prone to cybercrimes.

The aim of this thesis is to patch up the vulnerabilities in the current RFID system. In such a vast field it is not possible to completely remove all the threats in an RFID system but by picking up

one RFID protocol, analyzing it and reshaping it to become much more resistant could be the few steps that eventually lead us to achieving a perfect system.

1.2 Objectives

The thesis will focuses on the passive tags with ultra-light-weight protocol, specifically protocol introduced by Yung-Chen Lee in their paper "Two Ultra-Light Weight Protocols for Low Cost RFID [1]", which are mostly used with them. It will also focus on two of the many applications of passive tags, Inventory Management and Vehicle identification systems. In both of the applications the RFID tag is used to uniquely identify a product or a vehicle.

The objectives of the thesis are:

- To discover the different vulnerabilities that exists in the existing protocol, how these vulnerabilities affect the protocol and how these vulnerabilities could be removed.
- To improve the security of existing RFID protocol so that they can withstand different types of attacks which were previously not detected?
- Test the protocol under different scenarios to ensure that they remain secure under these conditions.

CHAPTER 2: INTRODUCTION

2.1 RFID Background

RFID stands for radio frequency identification. It is a technology that uses wireless Electromagnetic fields to send and receive data.

2.1.1 History

The history of RFID technology can be traced back to World War 2. After the discovery of Radar by Scottish physicist Sir Robert Alexander Watson in 1935, The Germans, Americans, British and the Japanese had been using this technology to monitor and warn of approaching aircraft. Although the Radar could detect aircraft in a given airspace there was no way of establishing the identity of the aircraft in question.

German pilots discovered that if they when approaching the base if the roll their aircraft it would change the radio signal that is reflected back to the radar station, alerting the station crew that it's a friendly aircraft. The British started working on the first Friend or Foe system, by putting a transmitter on each friendly aircraft which would transmit a return signal every time it approached the base station, the British were able to identify its own aircraft. Radar and RF Systems continued to see advancements through the 50s and 60s. The first commercial use of RFID was in anti-theft systems that could detect if the item in a store has been paid for or not. The tags relied on a 1 bit tag that could represent 0 for if an item has been paid for and 1 for not paid.

The first RFID device was patented in 1973 invented by Mario Cardullo. It was an active RFID tag with rewritable memory. Charles Walton received a patent for a passive transponder, capable of unlocking a door without a key, in the same year.

In 1970 the energy department requested national laboratory of Los Alamos to develop a system for tracking nuclear material. The system worked by attaching a transponder to the truck and reader at the gates. The system was capable of identifying data such as driver id and other information.

2.1.2 Architecture

A basic RFID system consists of an RFID tag, an RFID reader a database and a controlling application. An RFID tag is a label that can be used to uniquely identify an object in an RFID system. RFID tags can be divided into three types which are as follows: -

Passive Tag: A tag without any power source is called a passive RFID tag. It operates by using the energy of the radio signal from the reader that is interrogating it. As they are not dependent on a power source these type of tags have a long life, are cheap but with the drawback of being more prone to interference and a limited area of transmission.

Battery assisted passive Tag: These tags are hybrid tags which mean that they contain some of the features of passive and some features of active tags. They have a power source but only transmit when they are queried by a reader.

Active Tag: A tag with a power source that continually transmits is called an active tag. Due to their dependence on battery life they cannot operate as long as a passive tag and are expensive but on the other hand they have a greater range.

Figure 01: RFID Tags

In an RFID system the tags are separated from the reader, the database and the controlling application by an unsecured wireless channel. The readers also known as interrogator are used to supply power to the tags in case of passive tags and also to retrieve the information and pass it on to the controlling application and the database. In the scope of this thesis we will assume that the channel connecting the readers, database and the controlling application is secured at all time.

Figure 02: RFID Readers

A database contains all record of the objects identified by each tag. It also maintains the inventory of all the tags registered in the system. The database could be a separate module or integrated within the controlling application, the implementation may vary from situation to situation.

The controlling application is the main governor of an RFID system. Using information from the readers, tags and the database it provides access control functionality to the whole system. The application also manages the addition, removal of tags and readers from the system as well as providing update and real time information to the users allowing them to respond immediately in case of any emergency situation.

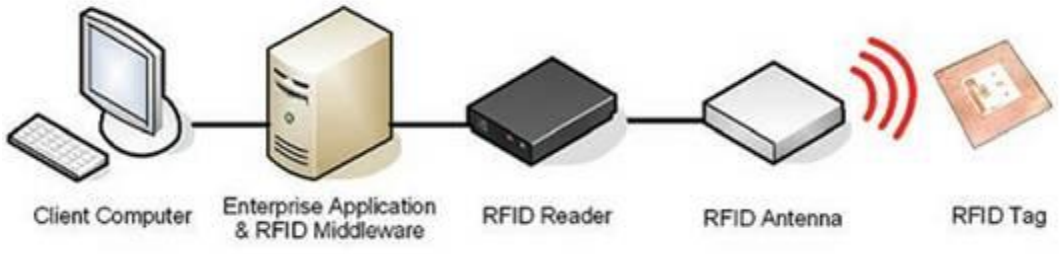


Figure 03: RFID System

2.2 RFID vs. Barcodes

Developed in the 1960s' by General Telephone and Electronics barcodes can be described as the predecessor to RFID technology. Barcode technology gained commercial success when they were successfully used to automate supermarket checkouts.

Barcodes used lines of varying widths and spacing to represent data. These types of barcodes were called 1D but the technology later incorporated other geometric pattern to evolve into 2D barcodes.

Figure 04: A Barcode

2.2.1 RFID-Barcode Comparison

RFID	*Barcode*
No need of Line-of-sight	Need Line-of-sight
No human-intervention	Need human-intervention
Proceed in Bulks	Proceed one by one
Identify objects in item-level	Identify objects in type-level
Wireless	closely scanned
Low cost 5 cents, recycled	Low cost, unrecycled
People unconsciously scanned	People consciously scanned

Figure 05: RFID Vs Barcode

Some of the disadvantages of barcode as are as follow:

- To keep the inventories up to date every barcode needs to be scanned individually
- Bar code is a read-only technology, meaning that it cannot send out any information.

2.2.2 RFID Applications

RFID tags are an improvement over bar codes because the tags have read and write capabilities. Data stored on RFID tags can be changed, updated and locked. This also expands the list of scenarios where RFIDs can be used.
Following are a few examples where RFID technology is being used.

- **Travel**

Electronic passports contain an RFID chip which allows border officials to scan a passport of a passenger quickly and avoid long lines at customs. It is also easy to maintain a blacklist and counter any threat before it can materialize.
Electronic Toll lanes require drivers to have an RFID Tag which can deduct the fare directly from the tag.
Subway / bus passes work similarly to electronic toll lanes. The passes can store information about the money in the card and can make addition or deductions according to the situation.
Some hotels have started embedding RFID tags in the linens to prevent travelers from stealing.

- **Agriculture**

RFID Technology is used in agriculture to monitor and track the movement of animals. Farm management system can be automated with the help of RFID technology.

- **Retail**

Real time asset management, warehouse management and supply chain visibility are some of the examples of RFID use in retail. Products can be easily tracked from raw material to the final product.

- **Smart Plates & Edible RFID**

NutriSmart is a company that is using printable RFID tags on food products with the purpose of making sure that people are taking the right medicine and food. The technology can also track the food through the body's digestive system and notify any problems.

- **Navigation Systems for visually impaired**

RFID technology is being used to assist people with disabilities. A common example is that of a visually impaired person with rfid tags strategically placed around a building. The tags relay information about the surrounding to the visually impaired persons stick equipped with an RFID reader. The information is then relayed to the person through an earpiece.

- **Waste Disposal**

In 2006 an RFID based waste management system, BinBug was introduced in UK. An RFID tag was embedded in the waste bin. The tag was tracked by the trash truck and the information such as weight and location were recorded.

- **Defense**

Access Control is the main application of RFID technology in defense sector. RFID enabled tags / cards along with road blockers and turnstiles make sure that only authorized personnel are allowed to visit a highly sensitive area. The area can also be divided into security zones depending on the security level.

- **Smart Dust**

This is one of the future applications of RFID technology that is still in its development stages. As the size of RFID tags become smaller they would eventually reach the size of nano particles. Vast amount of areas can be covered with the RFID tags acting as wireless sensor network providing information about a particular environment in real time.

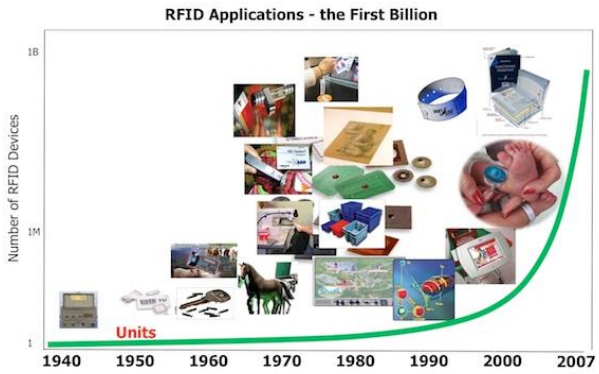


Figure 06: Application- the first billion

2.2.3 Other RFID Technologies

Optical RFID is an RFID technology that is based on optical readers; This technology operates in the Electro-magnetic spectrum between a frequency band of 333THz / 380 THz and 750Thz. The reader is able to read the tags information when the incoming signal is filtered by the tag and reflected back to the reader. This type of technology claims more security that the normal RFID as it requires an attacker to maintain a line of sight in order to attack a system.

Chip less RFID: In this RFID technology the RFID tags do not contain a microchip. It utilizes the following communication techniques.

- Time Domain Reflectrometry / Frequency Signature
- Chemical Based (Self Generating ceramic Mixtures, Biocompatible ink, CrossID nanometric ink)
- Magnetism Based (Programmable magnetic resonance, Magnetic Data tagging, surface acoustic waves)

2.2.4 Future Innovations

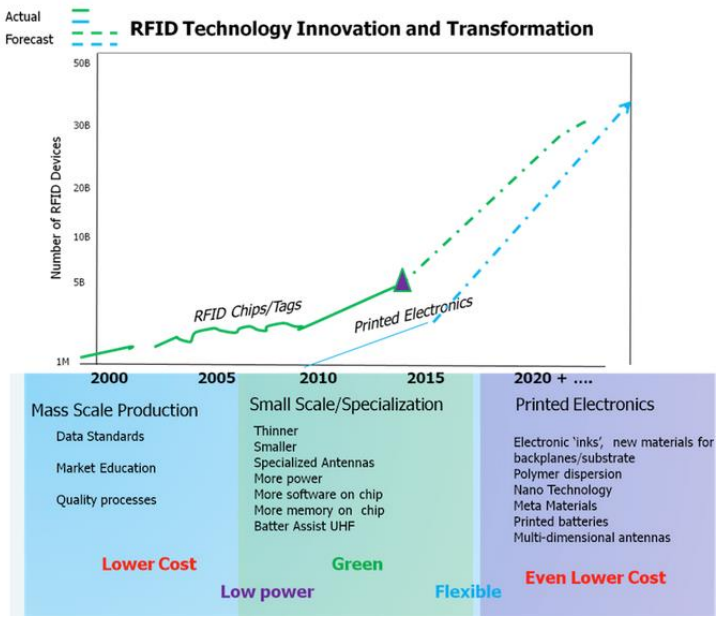


Figure 07: Transformation

The future of RFID technology is expected to evolve at a faster rate due to the innovations in technologies such as organic polymers, Nano technology and meta materials. A new era of cheaper, flexible and more secure products will start to appear in the markets.

2.3 Applications in Pakistan

2.3.1 Electronic Passport

In 2004 National Database and registration authority started issuing multi-biometric electronic passports to Pakistani citizens. Till now more than 7 million passports have been issued.

Figure 08: E-Passports

The electronic passports had the following features:

- Biometrics such as facial and fingerprints
- 2D Barcode
- Machine readable Zone
- Watermark Paper
- Security Ink
- Micro lettering

Design Architecture

- End to End Data Capturing
- Verification
- Backend processing and printing
- High end Network connectivity
- Modular and fully functional data capturing facilities

2.3.2 Smart ID Cards

In 2009 Pakistan Army started the SecureVision project with the aim of providing every army personnel with an RFID / Smart Card. RFID tags were issued to the vehicle while RFID cards were issued to the personnel which ensured access control for any vehicle or person entering a military installation.

Figure 09: SmartCard

In October 2012 NADRA started issuing Smart National identity cards. The cards contains a data chip similar to the ones issued for the SecureVision project and claimed to contain up to 36 security features.

2.3.3 E-Toll

Pakistan also has an electronic toll collection solution deployed on its Peshawar-Islamabad-Lahore motorways commonly known as M-1 and M-2. The solution allows the tagged enabled vehicles to pass through the toll booths without stopping to pay the fare, instead the amount is automatically deducted from the tag account.

Figure 10: E-Tag Lane

Features

- Real time control and Management
- Rechargeable credit
- Time saving
- Automated Report Generation

2.4 RFID Frequency Bands

RFID Technology operates in different frequency bands. The band frequency and its applications are listed in the following table.

Band	Regulations	Range
120-150 Hz (Low Frequency)	Unregulated	10cm
13.56 Mhz (High Frequency)	ISM Band	10cm to 1m
433 MHz (Ultra High Frequency)	Short Range	1m to 100m
865-868 / 902-928 (UHF)	ISM Band	1m to 12m
2.45 – 5.8Mhz (microwave)	ISM Band	1m to 2m
3.1-10 Ghz (microwave)	Ultra Wide Band	200m

2.5 RFID Standards

ISO 14223	Animal Identification
ISO 14443	HighFIDs, RFID enabled passports, near field communication
ISO 15693	Non contact smart payment and credit cards
ISO 18000	Item Management
ISO 18092	Near Field Communication (NFCIP-1)
ISO 18185	Electronic Seals
ISO 21481	Near Field Communication (NFCIP-2)
ASTM D7434	Test Method for performance on Palletized or unitized loads

ASTM D7435	Test Method for performance on Loaded Containers
ASTM D7580	Test Method for determining readability on Palletized or unitized loads
ISO 28560-2	Encoding standards

2.6 Security Problems in RFID Systems

RFID Readers: An attacker can take the identity of a legitimate reader. Using this technique the attacker is able to steal the secret information contained in the tag. If the tag is not write protected the contents of the tag can be rewritten according to the attackers will.

RFID Tags: Tags that are not protected enough can be cloned by an attacker. Cloning can not only provide access to an attacker but also reveal the secret keys which might compromise other tags in the systems as well.

Channel: Man in the middle attacks are the common issues in a wireless channel since the sender and receiver are generally not visible to each other.

2.7 Attacker Levels

In a basic RFID System attackers can be simplified in to the following three categories

Passive Attackers: These types of attackers are able to intercept messages without interfering with normal workings of a system.

Active attack: These types of attackers are able to communicate with a legitimate tag or a reader and disrupt the normal workings of the system.

Active attack with compromising secrets: These types of attackers are able to extract the secret key of the tag using different methods.

2.8 EPC Specifications

In 1990s a joint venture was created between GS1 and GS1 US called the EPC Global with the aim of simplifying the RFID protocols. Their main focus was on the use of Passive RFID and Electronic Product Codes. The EPC Gen 2 standard was approved in 2004 it had the following features:

- Working frequency of 860 Mhz to 960 Mhz
- Four memory blocks (user block, reserved block, EPC block and TID block)

User specific data could be stored in the user block, reserved block contained the kill or access password, TID blocks contained manufacturing data and the EPC block contained the tags unique ID.

2.9 RFID Protocol Types

The processes by which RFID tags and readers communicate with each other are called RFID protocols. Although RFID technology has become quite popular in the last few years there is still no universally approved and agreed protocol. As a result new and improved protocols emerge every year claiming to be more securing then the last. All this research is actually an advantage in the field of this technology as vulnerabilities are constantly wiped out and more and more secure algorithms are being invented. Hopefully before a single protocol has been universally approved it would be secure enough to counter and threats against it thereby protecting the privacy of the system it was meant to do.
RFID protocols can be classified in to many different types depending upon their computation power and the level of security they can provide.

The full-fledged class: The top most class in the security chain. Applications that require high level of security employee these types of protocols. An example is electronic passports. Full-fledged class uses cryptographic functions such as one way hash or public key encryption.

The Simple class: A little less secure then the full-fledged class using pseudo random number or one-way hash functions for security.

The light-weight class [22]: Pseudo random number generator or CRC checksum are used in this class to provide security. As a result this class requires less computational power then the above mentioned classes but low in the security chain.

The ultra-light-weight class: The simplest of all the types using bitwise operations to enforce security. Those operations are XOR, AND, OR etc.
The thesis will focus on ultra-light weight class which will be described in detail latter in the thesis.

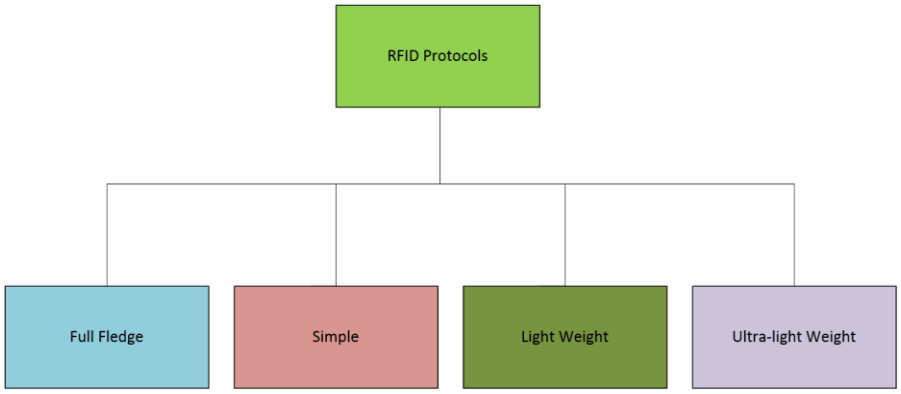


Figure 11: Protocols Classification

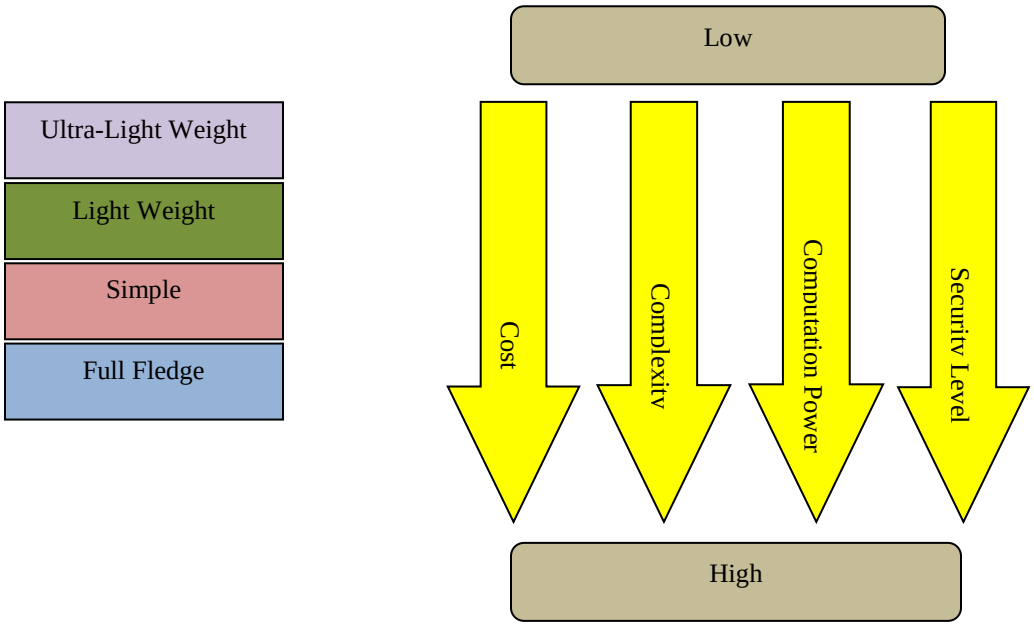


Figure 12: Protocols Comparison

2.10 Performance Management of an RFID

The performance of an RFID system can be measured in two different ways.

Search Cost: The time it takes for a database to locate a tag in its inventory is called the search cost of a tag. This might not be an issue with a small database that contains hundreds or thousands of tags but a database that contains million records it might take a long time for a tag to be located. Since rest of the operations is dependent on the identity of the tag, a high search cost might not make the RFID solution suitable for real time environments.

Operations Cost: All cryptographic functions that are performed to ensure that the secrets of a tag or a reader are not revealed to the attacker is called the operations cost. Higher the complexity of the functions, higher the requirement of space and processing power required by the tag.

Chapter 3 RELATED WORK

3.1 Previous Work

Passive RFID tags have memory and computational restraints which mean that the protocols that work with them need to be extremely light-weight as well. It has to use minimum resources and at the same time protect the privacy and integrity of the system involved. Over the years many protocols have emerged but researches have also proven that most of the protocols are vulnerable to different types of attacks.

In 2006 Peris-Lopez et al. [2-4] introduced ultra-light-weight protocols named as Minimalist Mutual-Authentication Protocol (M2AP), Efficient Mutual-Authentication Protocol (EMAP) and Light weight Mutual-Authentication Protocol (LMAP). These protocols used simple bitwise operations making them light weight. These protocols however were proved to be vulnerable to different types of attacks by Tieyan Li and Guilin Wang [8] in "Security analysis of two ultra-light weight RFID authentication protocols"and by MihalyBarasz et al [7] in "Breaking LMAP".

In 2007 Chien's [13] Strong authentication and strong integrity protocol (SASI) was introduced. It also worked on the principal of bitwise operations. This protocol was also proved vulnerable to attacks by Sunet al [5] in "On the security of Chien's Ultra-light-weight RFID authentication".

Similarly many other protocols [9-10] exist as well as researches proving that they can be breached.

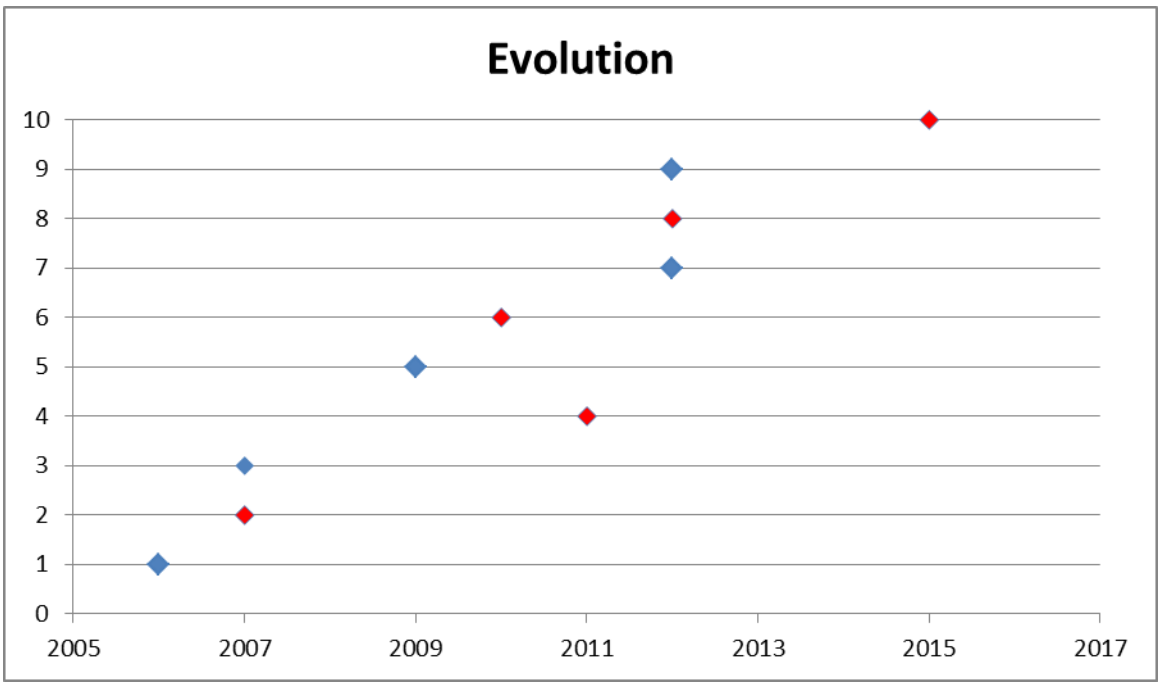


Figure 13: Evolution

The graph above shows the evolution of different protocols through time. Y-axis represents an event such as introduction (blue) or proof of vulnerability (red) of a protocol, while the X-axis represents the year in which the event occurred. Different events from 1 to 8 are described below.

1. Protocol Introduced by Peris-Lopez et al (M2AP, LMAP, EMAP) [2-4]
2. Protocol proved vulnerable by M. Barasz et al and T. Li et al [7]
3. Protocol Introduced by H.Y. Chen (SASI) [13]
4. Protocol proved vulnerable by H.M Sun et al [5]
5. Protocol Introduced by M.David et al [14]
6. Protocol proved vulnerable by Peris-Lopez et al [6]
7. Protocol introduced by Y.C Lee et al [11]
8. Protocol proved vulnerable Y. Farzanaeh et al [27]

9. Protocol introduced by Y.Tian et all [28]

10. Protocol proved vulnerable by Z.Ahmadian and Da-Zhi [29-30]

3.2Protocol Working

Yung Chen's protocol consists of two phases the authentication phase and the key updating phase.The reader and the tag share two values the dynamic identity (DIDT) of the tag and the secret key (K). Both these values are updated after authentication to avoid different attacks. In order to prevent desync attacks two different values of DIDT and the Key, (DIDT(x),K(x)) and (DIDT(x+1), K(x+1)) are stored in the memory where x is an authentication session.

3.2.1 Authentication Phase

When a tag comes into a range of the reader it transmits its dynamic identity (DIDT) to the reader. The reader then locates the tags secret key in the database, generates a random number (R) and transmits two messages A and B.

$A = K(x) \oplus R(x)$

$B = Rot [K(x), K(x)] \oplus Rot [R(x), R(x)]$

Rot (a,b) is a left rotation function on "a" of w(b) bits, where w(b) is the hamming weight of "b". The tag upon receiving the two messages calculates its own version of message B by obtaining random number from message A. If the tags version of B matches that of the reader the reader is authenticated. The tag then generates a message C:

$C = Rot [K(x), R(x)] \oplus Rot [R(x), K(x)]$

Now it's the reader's time to authenticate the tag so it receives the message C and calculates its own version. The tag is authenticated if the two versions are a match.

3.2.2 Key updating

Once both the tag and the reader are authenticated the process of key and identity updation are initiated. On both the reader and the tag sides the new DIDT and K are calculated by the following formulas.

$DIDT(x+1) = Rot[R(x), R(x) \vee K(x)] \oplus Rot[K(x), R(x) \wedge K(x)]$

$K(x+1) = Rot[R(x), R(x) \wedge K(x)] \oplus Rot[K(x), R(x) \vee K(x)]$

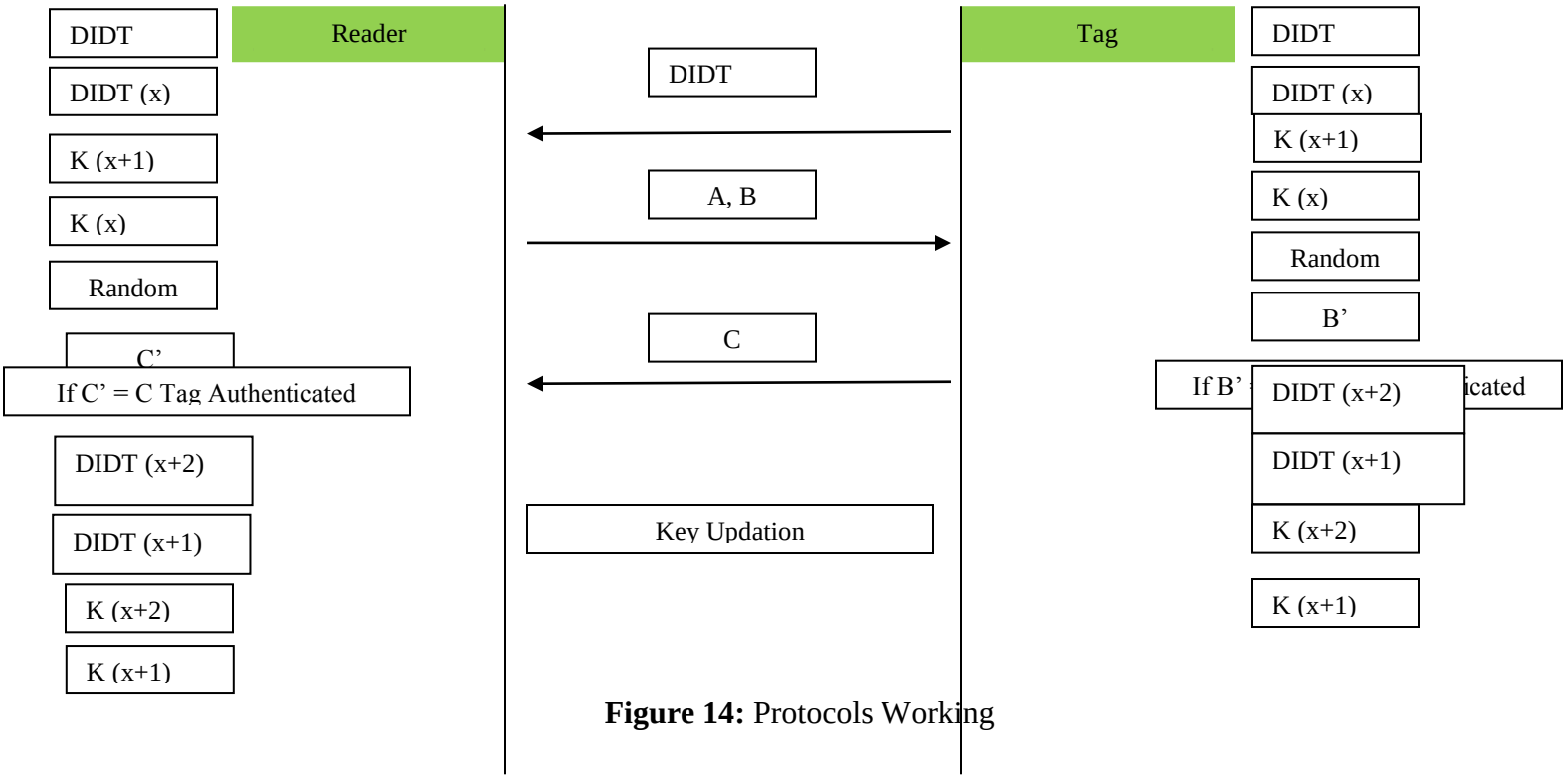


Figure 14: Protocols Working

Chapter 4: ATTACKS

4.1 DeSync Attacks

A desynchronized attack or desync for short happens when the reader no longer recognizes a legitimate tag. This could happen when the value of DIDT and K no longer matches in the tag and the reader.

Let the values of in the tag and the reader are as follows:

	Reader	**Tag**
DIDT old	DIDT[0]	DIDT[0]
KEY old	K[0]	K[0]
DIDT New	DIDT[1]	DIDT[1]
KEY New	K[1]	K[1]

When the tag comes into the range of the reader it is queried and responds with its DIDT[1]. The reader after checking against the records in the database extracts the tags K[1] and generates it messages A and B. The tag after verifying the message B will respond with its own message C. The attacker prevents the message C from reaching the reader. The attacker also records all the messages to be used further. Now since the reader has not received the tags verification it does not update the values while the tag does so the values now become

	Reader	**Tag**
DIDT old	DIDT[0]	DIDT[1]
KEY old	K[0]	K[1]
DIDT New	DIDT[1]	DIDT[2]
KEY New	K[1]	K[2]

The tag is again queried by the reader and this time it's DIDT[2] is not recognized by the reader which asks for an old ID DIDT[1].

The protocol is again started with the old DIDT[1] and K[1].

The values now become

	Reader	Tag
DIDT old	DIDT[1]	DIDT[1]
KEY old	K[1]	K[1]
DIDT New	DIDT[3]	DIDT[3]
KEY New	K[3]	K[3]

Now the attacker using an attacking reader query the tag which would respond with its DIDT[3]. The attacker then transmits no DIDT found message forcing the tag to use DIDT[1]. Since the attacker has captured the A and B messages from the previous sessions, the protocol continues with the tag returning its message C. The tag then updates its values

	Reader	Tag
DIDT old	DIDT[1]	DIDT[3]
KEY old	K[1]	K[3]
DIDT New	DIDT[3]	DIDT[4]
KEY New	K[3]	K[4]

Now the tag and reader have different value in their memory and have become out of sync which means that although the tag was found legitimate by the reader in one session it now has become a tag which is no longer recognized by the system.

4.2 Key revealing attack

A key revealing attack is an attack which aims to recover all the bits or most part of a secret key shared by the reader and the tag. In order to assist in this attack a simple application in c++ was developed. The code is written using visual studio 2010. The complete code can be found in appendix A.

1) $A = K(x) \oplus R(x)$

2) $DIDT(x+1) = Rot[R(x), R(x) \vee K(x)] \oplus Rot[K(x), R(x) \wedge K(x)]$

3) $K(x+1) = Rot[R(x), R(x) \wedge K(x)] \oplus Rot[K(x), R(x) \vee K(x)]$

XOR		
0	0	0
0	1	1
1	0	1
1	1	0

AND		
0	0	0
0	1	0
1	0	0
1	1	1

OR		
0	0	0
0	1	1
1	0	1
1	1	1

Figure 15: Gate Comparison

From the above mentioned information we can see that the AND function behaves like a compliment of XOR function with a probability of ¾, whereas the OR function behaves like an XOR function with a probability of ¾.
So the equation 2 and 3 can be rewritten in terms of equation 1 as follows:

4) DIDT (x+1) = Rot [R(x), A(x)] ⊕ Rot [K(x), A'(x)]

5) K (x+1) = Rot [R(x), A'(x)] ⊕ Rot [K(x),A(x)]

The code developed for the thesis will be using the above mentioned equations to verify how much of the original bits can be recovered.

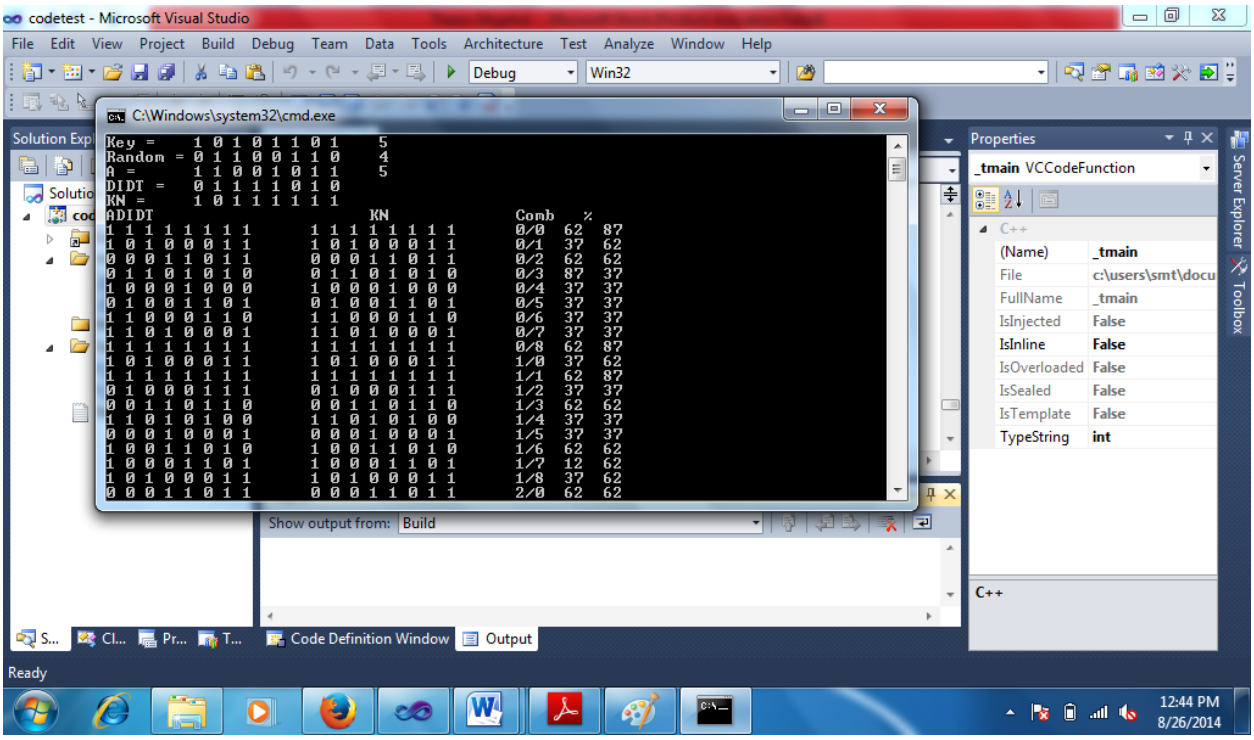


Figure 16: Code Snapshot

Chapter 5: ANALYSIS OF THE RESULTS

5.1 Analysis

From the working of the code it was observed that we get different values of DIDT and Key some very closer to the actual value. Although the percentage of similarity would not be known to the attacker the percentage and the values keep repeating which reduces the key space significantly. The results can be classified into two groups.

Same Hamming weight: When the Hamming weight of the key and the random number are similar the DIDT and the Key are the same. This could be great vulnerability if unchecked as it could reveal all the bits of a key without any computation or effort. In order to find out if the hamming weights are the same a simple look at the messages A and B would tell whether if there is any similarity. If same, B would be a rotation of A.

Different Hamming weights: The task to find the key becomes a little difficult when the hamming weights are different. The code written for this thesis can be used to estimate values for DIDT and key. By testing different values for key and random number a value very close to the original value was obtained.

The process to find the key can be defined as

1) Check for similar hamming weight vulnerability i.e. A and B test
2) If true DIDT is the same as the key. (Secret Found)
3) If first test fail use the code to calculate closest values for DIDT and KEY
4) Perform brute force attack on the closest values to find the real key.

5.2 Suggested Enhancements

The key revealing attacks were dependent on the probability of the AND, XOR and OR functions. Since the probability of this function cannot be changed. The thesis recommends to further add some functionality in the key updation phase to make the results more random.

DIDT (x+1) = Rot [R(x), R(x) ∨ K(x)] ⊕ Rot [K(x), R(x) ∧ K(x)]⊕Rot [R(x)+k(x), R(x) ∨ K(x)]

K (x+1) = Rot [R(x), R(x) ∧ K(x)] ⊕ Rot [K(x), R(x)∨ K(x)]⊕Rot [R(x)+k(x), R(x) ∨ K(x)]

This would increase the key space that we predicted from the code and make it harder for the attacker to extract the original key.

Chapter 6: CATEGORIZATION

6.1 Categorization of RFID Protocols

RFID protocols are categorized upon the basis of security levels. Our work is simple than the previous one. Vaudenay's [15] work is the most systematic and important and referred by most of the previous researchers. A comparison will be given between Vaudenay's work and ours.

6.2 Previous Work on Categorization

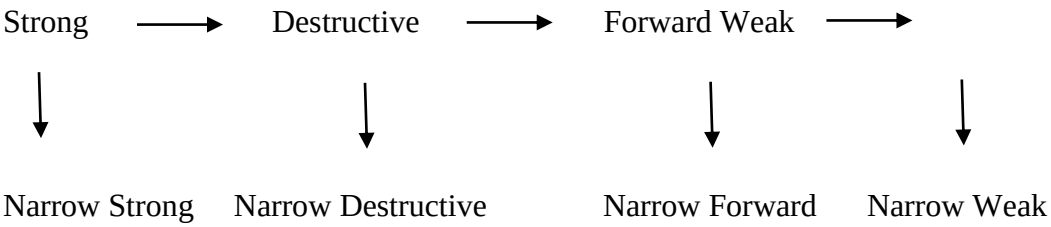


Figure 17: Vaudenay's Model

A lot of categorization works have been done up to now. There are two groups according to CCS'09 Ma et.al [27] categorization:

a) INP {Indistinguishability-Based Privacy}
b) UNP {Unpredictability-Based Privacy}

According to INP it is not possible for attacker to differentiate between tags having higher probability than the random guess.
Whereas according to UNP prediction cannot be made by the attacker that whether the message is an output of the protocol or a random one. Therefore, we say that this work is not reliable and authentic.

Vaudenay's model was another theoretical categorization [15] consists of eight different categories also known as eight different abilities. In this model, an adversary can simulate seven oracles:

a) Createtag (ID)
b) Draw (distr)
c) Free (vtag)
d) Launch
e) Sendreader (m; ¼)
f) Result (1/4)
g) Corrupt (vtag)

The adversary that can access all the oracles, we can call that a strong adversary. Forward adversary is one that can only access corrupt oracle after the target tag is being corrupted. Weak adversary is defined as the adversary that cannot access corrupt oracle. In Fig 17 second line the Narrow adversary cannot access result(1/4) oracle, which returns 1 for protocol complete protocol whereas 0 for incomplete.
Therefore, there are eight privacy models:

a) Strong
b) Destructive
c) Forward
d) Weak
e) Narrow-Strong
f) Narrow-Destructive
g) Narrow-Forward
h) Narrow-Weak

The Fig 17 explains the relationship of all these forces. After that this model of eight was given extension into mutual authentication models in ASIACCS'08 [16]. The eight RFID privacy model was further simplified into three categories [17]. Still we can find arguments about standards of classification. Vaudenay's work is the most systematic and widely cited one among the previous works.

Another category Narrow-Strong is to be carried out by public key cryptography (PKC) [16] but it is not a light-weighted solution. Since public key cryptography is not suitable for low cost RFID systems. Moreover, all three methods described by Vaudenay's and Ng are mere theoretical rather than practical. We have re-categorize the existing RFID protocols in terms of previous references but our main focus in upon existing RFID symmetric.

6.3 Typical Protocols& Categorization:

The categorization of RFID protocols like Vaudenay's scheme is also based upon anti-tracing and forward secrecy properties. In anti-tracing property tag's response to reader changes is observed. Tag's internal state updates give the measurement of forward secrecy property.
Our categorization of existing RFID protocols in attacker's point of view consists of six classes in terms of whether a tag's response changes and whether the internal state of tag updates once the tag is queried. Tag's response is divided into three situations:

a) Unchanging plain
b) Unchanging Meta ID
c) Changing response

On the basis of changing responses, for an attacker it is not possible to distinguish between two tags with a probability of higher than the random guess. For the first two cases, the tags can be traced with unchanging responses. In this categorization, it not possible for adversary to distinguish between two tags before corruption with a probability of higher than fifty percent in case of corruption of one or two of tags after updates.

1. EPC protocol:

Internal state is not updated by a tag in this protocol. Every time the tag responds its EPC code in plain text when it is interrogated by a reader, therefore EPC protocol can guarantee neither forward secrecy nor anti-tracing. EPC is the weakest protocol. It only uses two passwords to protect RFID tags: one is the kill password used for destruction of tag and the second is the access password used for prevention of malicious readers from writing into a tag arbitrarily.

2. Tracing Protocols:

It is better than the EPC protocol. The tag with tracing protocol does not respond its EPC code directly to a reader, conversely the tag gives response with unchanging MetalD back to reader. So it protects the tag's privacy. However, for same MetalD (e.g. pseudoname) attackers can trace the same tag. Moreover, while tracing protocols, a tag was not able to update its internal state. So it cannot achieve forward secrecy i.e. if a tag is corrupted with internal state is extracted by a malicious reader. In this case the tag's previous internal states can be retrieved by the malicious reader successfully.

3. Strong Anti-tracing Protocols:

By comparing with previous two categories, this category is blessed by functions like PRF (Pseudo random function) in tags, tags can respond with different values every time when reader interrogates them. Consequently, an adversary cannot distinguish two tags having a probability of higher than a random guess. Moreover, this protocol cannot guarantee forward secrecy without updating internal state. It consists of Random Hash-loch [18], Big Brother [19], MW Tree [20], Dual Mode protocols [21] etc.

4. Weak Anti-tracing, Weak Forward Secrecy Protocols:

This category and next two categories acquire forward secrecy on different levels. These types are included in Category IV protocols. In this class only specific authorized parties can update tag's internal states and tag's responses.

5. Strong Anti-Tracing, Weak Forward Secrecy Protocols:

In this class with the help of PRFs in tags, tags respond with changing, unlikable messages every and acquire strong anti-tracing all the time rather than partial tracing in class IV. So Like previous category a tag can only updates its internal states after successful authentication of authorized parties in this category. This class includes SM protocol [23], Revised SM [24].

6. Strong Anti-Tracing, Strong Forward Secrecy Protocols:

This class consists of strongest security property properties in our categorization. In this type, a tag automatically updates not only its response but also its internal states also every time, without considering either the querying reader is legitimate or not. In this way this type can acquire strong anti-tracing as well as strong forward security. Examples are OSK [25], RFIDDOT [26], narrow-destructive protocol [16].

Chapter 7: CONCLUSIONS AND FUTURE RESEARCH

This thesis focuses upon security and enhancement of RFID Light weight protocols.
First we conducted a short survey (Appendix B) to find out how much people actually know about the RFID technology because if someone does not have a working knowledge of a system he can be an easy target for an attacker. Our survey revealed that although many people were using RFID technology most of them had no clue how much they were vulnerable to a cybercrime.
Secondly we selected an ultra-light weight RFID protocol and developed a c++ application (Appendix A) to see how it worked and also how it can be attacked.The vulnerabilities were found because the protocol was dependent on the AND, XOR and OR functions. By increasing the complexity of the protocol we managed to reduce the effects of the vulnerability found in the existing protocol.
Next, Existing RFID protocols were categorized into six categories by their anti-tracing and forward secrecy properties. All these six classes include EPC protocols, tracing protocols, Strong Anti-Tracing protocols, Weak anti-tracing and weak forward secrecy protocols, strong anti-tracing and weak forward secrecy protocols, strong anti-tracing and strong forward secrecy protocols.
Only EPC and tracing protocols were described in the previous classification works. But these categories are especially relevant to practice. Therefore, the new categorization model is more relevant to practice than the previous models.
For administrator point of view, a lot of options are available according to different security requirements. The implications of trade-off for that higher security are worse performance. Performance is analyzed for two perspectives: search cost of a tag in a reader's database and tag-related cost. This tag related cost consists of cost of cryptographic operations cost and communication cost between tag and reader.
The one perspective of our investigation is to investigate security and search cost by category with the help of database complexity analysis. There are certain circumstances higher security requires heavy cost. On the other hand security properties are not affected by the cost.

Sometimes we discuss security and tag-related cost upon the basis of experimental results. The time related cost of any RFID protocol is measured with help of general formula in each category. Best performers are selected as standards for checking performance of other protocols. With the help of different comparisons, redundant operations in a couple of existing RFID protocols are discovered for revision.

Finally, Proposals are given for the design of future protocols to get the better trade-off between tag-related cost and search cost. The significance of this work is that both High and low cost tags are provided with higher level of security as compare to the earlier ones.

In near future, we will be able to design protocols having higher performance with low cost.

APPENDIX A: CODE

A.1 Functions

In C++ code a function is a set of procedures or subprograms that are performing a specified task. The advantages of using functions in a code is that instead of writing the code again for a task that is repeatedly used in a program, we can just call the function, reducing the length of the code and making it more efficient and faster to use. The names of the functions are given by the programmer and are not universally used. For the purpose of the thesis I have named the function according to the task that they are performing which makes it easier for the reader to understand.

A.1.1 Compliment

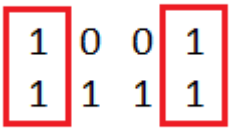
```
int* arrayinv(int a4[])
{
	int * d4 = newint[8];

	for (int m4=0; m4<8; m4++)
	{
		if (a4[m4]==0)
		{d4[m4] =1;}

		elseif (a4[m4]==1)
		{d4[m4] =0;}

	}
	return d4;}
```

The compliment function provides the compliment of an input array. In our application an array could be the secret key or the random number. Although the key or random number are of 96 bits, for easy of testing we have declared an array of 8 bits. A logical compliment is an inverse of another function meaning compliment of 0 is 1 and compliment of 1 is 0

A.1.2 Comparison

```
intarraycomp ( int a6[],int b6[])
{
        int n6=0;
        for (int m6=0; m6<8; m6++)
        {
                if (a6[m6] == b6[m6])
                {n6++;}
        }
        int o6 = (n6*100)/8;
        return o6;}
```

The comparison function is used to compare the percentage of similarity between two arrays. For example the percentage of similarity between the following two arrays can be calculated as:



Percentage of similarity = 2/4* 100 = 50 percent

A.2Main

The main function is the starting point of any c++ application.

A.2.1Variable declaration

The following variables have been declared in the main function. These are the same variables that are used in the protocol. Since this is a complete code even the attack variables are defined.

```
int key[]    = {1,0,1,0,0,0,0,1};    // Key I
        int random[] = {0,1,0,0,0,1,1,0};    // Random I

        int* A  = newint [8];              // A I
        int* DIDT  = newint [8];           // DIDT I+1
        int* KN    = newint [8];           // Key I+1
        int* ADIDT = newint [8];           // Attack DIDT
        int* AKN   = newint [8];           // Attack Key
```

A.2.2 Equation 1,2& 3

```
A = arrayxor(key,random,8);
```

```
DIDT =
arrayxor(arrayrot(arrayor(key,random,8),hamming(random)),arrayrot(arrayand(key,random,8),ha
mming(key)),8);
```

```
KN =
arrayxor(arrayrot(arrayand(key,random,8),hamming(random)),arrayrot(arrayor(key,random,8),ha
mming(key)),8);
```

A.2.3 Displaying Values

```
cout<<"Key =    ";
printarray(key, arraylen(key));
cout<<"   ";
cout<<hamming(key);
cout<<'\n';

cout<<"Random = ";
printarray(random,arraylen(random));
cout<<"   ";
cout<<hamming(random);
cout<<'\n';

cout<<"A =      ";
printarray(A,arraylen(A));
cout<<"   ";
cout<<hamming(A);
cout<<'\n';

cout<<"DIDT =   ";
printarray(DIDT,arraylen(DIDT));
cout<<'\n';

cout<<"KN =     ";
printarray(KN,arraylen(KN));
cout<<'\n';
```

Until now the code only displays the original values as described by the original algorithm. The following starts the test scenarios i.e equation 4 and 5. Since the hamming weights of the secret

keys and random number is not known on the attacker side. The thesis uses a brute force attack. We know that in most rfid systems the secret keys is 96 bits long so the brute force attack displays all the combinations of random number and the key between 1 and 96. For ease of display in the thesis the counter and length of the keys and random number have been set to 8. The code also shows the percentage of similarity of all the combinations.

A.2.4 Test Values Scenario

```
for (int a5 = 0; a5<9; a5++)
        {
                for (int b5=0; b5<9; b5++)
                        {
                                ADIDT = arrayxor(arrayrot(A,a5),arrayrot(arrayinv(A),b5),8);
                                AKN   = arrayxor(arrayrot(arrayinv(A),a5),arrayrot(A,b5),8);
                                printarray(ADIDT, arraylen(ADIDT));
                                cout<<"     ";
                                printarray(AKN, arraylen(AKN));
                                cout<<"     ";
                                cout<<a5;
                                cout<<"/";
                                cout<<b5;
                                cout<<"  ";
                                cout<<arraycomp (DIDT,ADIDT);
                                cout<<"  ";
                                cout<<arraycomp (KN,AKN);

                                cout<<'\n';
                }
```

APPENDIX B: RFID SURVEY

RFID stands for Radio frequency identification. It is a wireless technology that as many applications in our day to day life. The most common use of RFID technology is the CNIC cards issued by Nadra to every Pakistani citizens. If you ever have travelled from Islamabad to Lahore through motorway ou would also be familiar with the NHA tags that are used to access the e-tag Lane.

This survey is designed to analyze the knowledge a normal citizen has about RFID technology.

Q1) Do you have an RFID based CNIC Card. (RFID based cards would have a metallic box like structure on the top left corner).

a) Yes
b) No

Q2) Do you have an NHA e-tag

a) Yes
b) No

Q3) Do you frequently use the Cards or tags ?

a) Yes
b) No

Q4) Have you heard of RFID Technology before ?

a) Yes
b) No

Q5) Do you know how an RFID System Works ?

a) Yes
b) No

Q6) Do you know the drawbacks of an RFID System?

a) Yes
b) No

Q7) Do you know how someone can steal information from RFID Cards or Tags?

a) Yes
b) No

Q8) If there is option of using one RFID card for all services in your country e.g (debit / Credit card, CNIC, License), would you use this card ?

a) Yes
b) No

One of the most common threats of an RFID system is identity theft. Identity theft is when criminals steals the identity information of another person and then use this information for criminal purposes. Since RFID is a wireless technology the card / tag holder is not aware of when his information is being stolen.

Q8) Would you be interested in a short article on how to protect yourself from Identity theft?

a) Yes
b) No

APPENDIX C: BIBLIOGRAPHY

[1] Two Ultra-light Weight Authentication Protocols for Low-Cost RFID Tags by Yung-Cheng Lee

[2] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags. Procedings of UIC'06, LNCS 4159, (2006), 912-923.

[3] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags. Proceedings of the OTM Federated Conference and Workshop: IS Workshop, (2006), 352-361.

[4] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador and A. Ribagorda, LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags. Proceedings of the Second Workshop RFID Security, (2006).

[5] On the Security of Chien's Ultra-light weight RFID Authentication Protocol by Hung-Min Sun et al

[6] J.C. Hernández Castro, P. Peris-Lopez, R.C.W. Phan, J.M. Estévez-Tapiador, Cryptanalysis of the David-Prasad RFID Ultralightweight Authentication Protocol. Procedings of the 6th International Workshop on Radio Frequency Identification: Security and Privacy Issues, (2010), 22-34.

[7] M. Bárász, B. Boros, P. Ligeti, K. Lója and D.A. Nagy, Breaking LMAP, International Conference on RFID Security 2007, Malaga, Spain (2007).

[8] T. Li and G. Wang, Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. Proceedings of the 22nd IFIP TC-11 International Information Security Conference, (2007).
[9] M. David and N.R. Prasad, Providing Strong Security and High Privacy in Low-Cost RFID Networks. Procedings of Security and Privacy in Mobile Information and Communication Systems, Springer Berlin Heidelberg, (2009), pp.172-179

[10] A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity by HY. Chien

[11] A New Ultralightweight RFID Protocol with Mutual Authentication by YC. Lee et al

[12] Security Flaws in an Efficient Pseudo-Random Number Generator for Low-Power Environments by Peris-Lopez et al

[13] H.Y. Chien, SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing, Vol.4, No.4, (2007), 337-340.

[14] M. David and N.R. Prasad, Providing Strong Security and High Privacy in Low-Cost RFID Networks. Procedings of Security and Privacy in Mobile Information and Communication Systems, Springer Berlin Heidelberg, (2009), pp.172-179

[15] Serge Vaudenay. On Privacy Models for RFID. In Advances in Cryptology - Asiacrypt 2007, volume 4833 of Lecture Notes in Computer Science , pages 68–87, Kuching, Malaysia, December 2007. Springer Verlag.

[16] Radu-IoanPaise and Serge Vaudenay. Mutual Authentication in RFID: Security and Privacy. In Masayuki Abe and Virgil D. Gligor, editors, Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security – ASIACCS'08, pages 292–299, Tokyo, Japan, March 2008. ACM, ACM Press.

[17] Ching Yu Ng, Willy Susilo, Yi Mu, and ReihanehSafavi-Naini. Rfid privacy models revisited. In ESORICS , pages 251–266, 2008.

[18] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Dieter Hutter, Gunter Muller, Werner Stephan, and Markus Ullmann, editors, International Conference on Security in Pervasive Computing – SPC 2003, volume 2802 of Lecture Notes in Computer Science, pages 454–469, Boppard, Germany, March 2003. Springer-Verlag.

[19] TassosDimitriou. A secure and efficient RFID protocol that could make big brother (partially) obsolete. Pervasive Computing and Communications, IEEE International Conference on, 0:269–275, 2006.

[20] David Molnar and David Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In Birgit Pfitzmann and Peng Liu, editors, Conference on Computer and Communications Security – ACM CCS , pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.

[21] ShaoyingCai, Tieyan Li, Yingjiu Li, and Robert H. Deng. Ensuring dual security modes in RFID-enabled supply chain systems. In ISPEC '09: Proceedings of the 5th International Conference on Information Security Practice and Experience , pages 372–383, Berlin, Heidelberg, 2009. Springer-Verlag.

[22] TassosDimitriou. A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm, Athens, Greece, September 2005. IEEE.

[23] Boyeon Song and Chris J. Mitchell. RFID Authentication Protocol for Low-cost Tags. In V. D. Gligor, J. Hubaux, and R. Poovendran, editors, ACM Conference on Wireless Network Security, WiSec'08, pages 140–147, Alexandria, Virginia, USA, April 2008. ACM Press.

[24] ShaoyingCai, Yingjiu Li, Tieyan Li, and Robert Deng. Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions. In David A. Basin, SrdjanCapkun, and Wenke Lee, editors, Proceedings of the 2nd ACM Conference on Wireless Network Security – WiSec'09, pages 51–58, Zurich, Switzerland, March 2009. ACM, ACM Press.

[25] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags. In RFID Privacy Workshop, MIT, Massachusetts, USA, November 2003.

[26] TassosDimitriou. RFID-DOT: RFID Delegation and Ownership Transfer made simple. In 4th International Conference on Security and Privacy for Communication Networks – SecureComm 2008, Istanbul, Turkey, September 2008.

[26] Changshe Ma: RFID privacy: relation between two notions, minimal condition, and efficient construction, Proceedings of the 16th ACM conference on Computer and communications security, Pages 54-65

[27] Vulnerability Analysis of Two Ultra Light Weight RFID Authentication Protocols – The international Arab Journal of Information technology 2015 (Y. Farzanaeh)

[28] A new ultralight weight RFID Authentication protocol with permutation – IEEE Communications Letter 2012

[29] Desynchronization attack on RAPP ultralight weight authentication protocol – Information Processing Letters 2013 (Z. Ahmadian)

[30] Analysis and Enhancement of Desynchronozation attack on an Ultralight weight RFID Authentication Protocol (Da-Zhi) 2015