PROTOCOLS DEVELOPMENT FOR SECURITY AND PRIVACY OF RADIO FREQUENCY IDENTIFICATION SYSTEMS

By

Fatin Sabbagha

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Packaging - Doctor of Philosophy

2014

ABSTRACT

PROTOCOLS DEVELOPMENT FOR SECURITY AND PRIVACY OF RADIO FREQUENCY IDENTIFICATION SYSTEMS

By

Fatin Sabbagha

Radio frequency identification (RFID) is a technology that uses communication via radio waves to exchange data between an RFID reader and an electronic tag attached to an object for the purpose of identification and tracking. Although there are many benefits of adopting this technology, there are many methods of attack that can be used to compromise the system. The intent of this research is to determine how that may happen and what possible solutions can keep that from happening. With this solution, protocols were developed to implement better security. In addition, new topologies were developed to handle the problems of the key management. Most of the previously proposed protocols focus on providing mutual authentication and privacy between RFID readers and tags. However, these proposed protocols are still vulnerable to be attacked. As a result, these protocols were analyzed and the drawbacks shown for each one.

The previous works, from the beginning, assumed that the channels between readers and the servers are secured. In the newly proposed protocols, a compromised reader is considered along with how to prevent the tags from being read by that reader. The new protocols provide mutual authentication between readers and tags and, at the same time, remove the compromised reader from the system in efficient way.

Three protocols are proposed; in each one, a new idea is achieved. In the first protocol, a mutual authentication is achieved and a compromised reader is not allowed in the network. In the second protocol, the concept is similar to the first protocol, but the number of times

a reader contacts the server is reduced. Therefore, a new protocol is defined by a sharing key between the server and the tags. In this case, key leakage is prevented with the compromised reader. In the third protocol, there is another concept to provide authentication and privacy between tags and readers using a trusted third party. A session key is generated and used to encrypt and decrypt messages between the tag and the reader using symmetric key cryptography. Here also, key leakage is prevented with the compromised reader.

The developed topology is implemented using python language. The goal from this implementation is to realize and simulate work and to check the efficiency regarding the processing time. Also, the three protocols are implemented by writing codes in C language and then compiling them in MSP430. Its function the same as RFID tag. IAR Embedded workbench is used, which is an integrated development environment with the C/C++ compiler to generate a faster code and to debug the microcontroller. In summary, the goal of this research is to find solutions for the problems on previous proposed protocols, handle a compromised reader, and to solve key management problems.

To my husband Bashar Shaffo and my kids (Reeta and Matti) May God bless you with His peace

ACKNOWLEDGMENTS

The research and writing of this dissertation has been one my greatest challenges, and there is no doubt that it could not have been completed without the help and encouragement of the following people, whom I have the privilege to acknowledge here. I would like to thank Professor Robert Clarke for being my advisor, despite his many other professional commitments. I have been inspired by his wisdom, breadth of knowledge, and his commitment to the highest academic standards.

Of course, my deepest appreciation goes to my family. My loving husband Bashar has demonstrated unending devotion and sacrifice to make these pages possible. I also must thank my dear children Reeta and Matti for their endurance on this journey. I am pained by the time that we spent apart, and I am enjoying spending more time together with you now. Your consolation is that never again will you have to hear me say that I need to go work on my dissertation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

1.1 Auto ID Technologies

Automatic identification technologies (Auto ID) are very popular in many services systems. To increase the efficiency and productivity in many organizations, Auto ID can be used because it runs procedures faster, is more accurate, and it eliminates error associated with identification and data collection. Auto ID technologies can be used to provide information about numerous things, such as people, animals, goods, and so on. It can also reduce many problems related to life such as missed delivery dates, customer dissatisfaction, lower productivity, etc. There are different types of Auto ID systems based around different strategies and functions. The following sections are a brief overview of these systems.

1.1.1 Barcode Systems

This is the most common ID technology for encoding information. Some applications are inventory control, Customs control points, work in progress, security, point of sale, account receivables, marketing and business replies, time and attendance, etc. In general, there are one dimensional barcodes (1D) and two dimensional barcodes (2D). 1D is made up of parallel bars and spaces, which could be wide and narrow. Each character represented by a barcode is a series of bar and space. All barcodes contain parts; these are a quiet zone, start code,

data, stop code, and a trailing quiet zone. Also, some 1D barcodes have check digits for providing integrity. In addition, the density of the barcode can vary from low, to medium to high density. The density can be determined by the X dimension, which determines the width of the narrowest bar or space in the barcode.

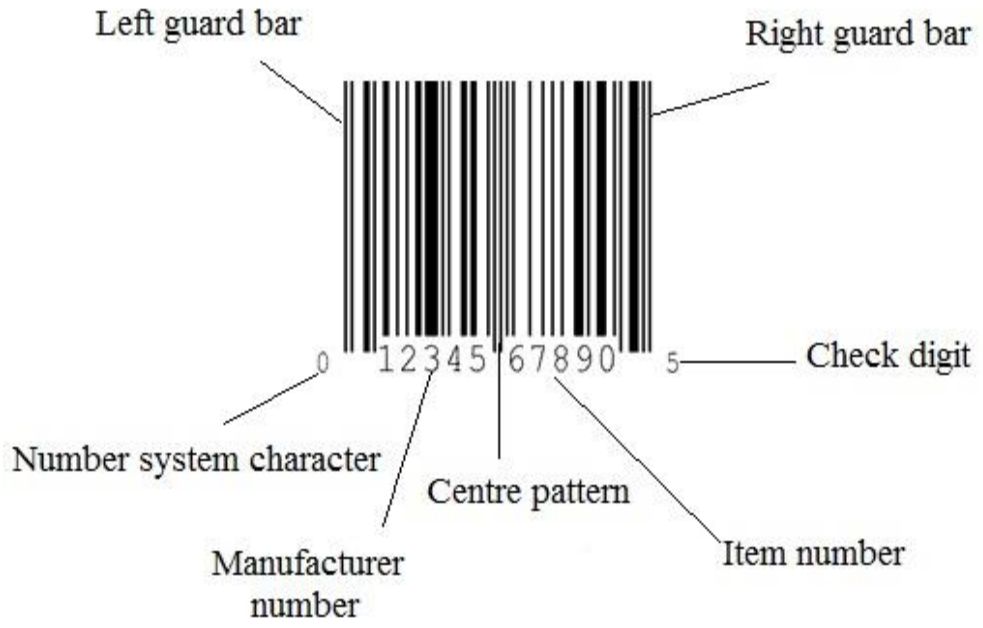

Figure 1.1: Universal Product Code type A [19, 20, 47]

Barcodes can be read by different types of scanning readers. Some are contact readers and others are non-contact, such as wands, charge coupled device (CCD), fixed focus optics (FFO), and laser. Contact scanners needs physical contact, but non-contact scanners can read items up to several inches away. Barcodes can be represented by different symbologies, such as Code 39, Code 128, Universal Product Code (UPC), European Article Number/

Japanese Article Number (EAN/JAN), Code 93, Interleaved 2 of 5 (ITF), MSI Plessey, Telepen, PosiCode A and B, Channel Code, and Coda Bar. [53] Each of these symbologies has different characteristics. Some have fixed length while others have variable length. For example, the most common barcode for retail product labeling is the UPC, which is a fixed length 12 digit numbers only code. Figure 1.1 illustrates the syntax of this code.

2D is made up of individual dots or squares and it can be printed as a square, circular or a rectangular symbol. It can be represented into two primary types: matrix codes and stacked-bar codes. A stacked-bar code is a stack of linear barcodes, which can be read by laser scanner, CCD or camera. A matrix code can be square, circular or hexagonal shape. This type can be read by a camera or CCD reader. The difference between these two types is related to the code density. Matrix codes have a higher density than stacked-bar codes with identical information. [19, 20, 35]

2D comes in different forms such as the Quick Response (QR) code that was the earliest 2D barcode, Datamatrix, and 2D color barcodes that are the newest edition of 2D barcodes. [34] The characteristics of 2D barcodes are high information density, high data capacity, and wide coding range, for example it can encode image, sound, word, signature and finger mark. [36] 2D consists of two broad areas: data areas and guide areas. The structure of Datamatrix has two parts: the finder pattern and the data. The finder pattern defines the shape of the 2D code, the size, the minimum size of the dots, and the number of rows and columns in the shape. [35]

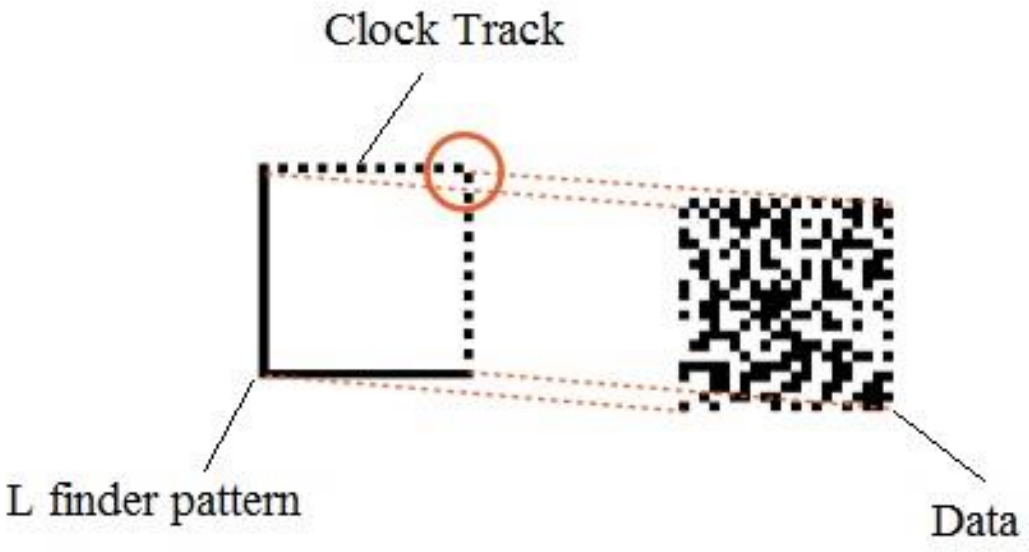

Figure 1.2: Finder Pattern and the data [35]

Figure 1.2 illustrates the shape of 2D Datamatrix. There are two parts in the finder pattern. The L finder pattern (the solid dark sides) defines the size, orientation, and distortion of the symbol. The Clock Track (the light and dark elements) defines the basic structure and also can determine the size and distortion. The maximum amount of encoded data in a square form is 2,335 alphanumeric characters and 3,116 numbers. However, the maximum amount of encoded data in a rectangular form is 72 alphanumeric characters and 98 numbers. [35]

The differences between 1D and 2D barcodes is that 1D is used as an index to a database to obtain the required information, while 2D can be a database unto itself with no need to

access as external database. 2D is used to encode more information (thousand characters) in a smaller area than would be required of 1D codes. This can make procedures move quickly and more reliably. [19, 20, 35]

1.1.2 Biometric Identification

Biometrics is a technology used to identify a person by using one of the uniquely human characteristic features and comparing it with previously stored data. It is used for providing authentication to get more sensitive information and resources. [22] There are other techniques used to provide authentication, but some of them such as passwords or documents can be stolen or lost. Biometric technology, on the other hand, cannot be forgotten, lost or stolen. [21] There are several types of biometric technologies, such as fingerprinting, hand geometry, and retinal scans. In addition, voice recognition technology is a part of biometric verification. [20] Each of these procedures can identify an individual correctly. Biometric technologies can be used in many applications, for example in time and attendance, retail, security and controlled access, computer access, couriers, banking, etc.

There can be devices installed at the secured area or entrance for getting information from an individual. Although biometric is the best technology for identifying individuals, it still has problems. It is costly compared with other technologies like card systems. That will be discussed in the next section. Some other issues that the technology faces are the degradation of biometric features over time, variance in recorded and actual biometric characteristics, and threshold values for authentication and privacy. [19, 20]. Several studies and surveys have been proposed to see how much individuals are aware of the technology and see the benefits of it. [22] Because of increasing demand of high-performance security methods, there are numerous studies about improving the image of biometric techniques. For example,

Maeva [37] introduces a newer development of the ultrasonic fingerprint imaging. Liang [38] proposed a novel video based biometric identification model based on eye tracking technique. Several visual attention characteristic are extracted from eye gaze data. Then, these features are used to identify persons.

1.1.3 Machine Vision Technology

Machine vision is defined as the automatic extraction of information from digital images. The purpose of extracting information could be for pattern recognition, part inspection, or part positioning and orientation. It is a system that uses many types of advanced hardware and software components to perform the same tasks of inspectors who work to inspect the quality of parts. However, this system provides high speed operations with greater precision. Machine vision systems improve automated technical identification, inspection, measurement, and guidance capability. [48] It can be used in many applications such as: pharmaceutical packaging, food and beverage packaging, electronics manufacturing, the Department of Defense (DOD) supply chain, and so on. It is an essential part of a manipulative task involving industrial operator (robots). The main four functions of machine vision are: measurement, counting, location, and decoding. For measurement, it is used to check the automated measurement by the machine to specified tolerances. Counting is another function of machine vision to look for a number of features on parts to see if there are missing parts. Also, it checks the absence and presence of products in one package. Machine vision is used to specify and report the position and the orientation of a part to specify tolerances. The decoding function is to interpret, for example, 1D and 2D symbologies to extract some information used later for tracking products. This information can also be used to verify the correctness of data. These four functions play a role in saving cost, reducing defects,

tracking and tracing, and complying with regulations. [48] There are four components of a machine vision system: lighting, frame grabber, image processing and analysis software, and CCD cameras. [49] Companies can rely on the machine vision to improve the quality of their products. For example, petroleum and petrochemical manufacturer Sinopec Group use this technology to maximize production output, reducing costs, minimizing waste, and saving power. [50] They used a smart camera to collect accurate data from 2D codes and text characters on the bottle labels and 1D from the secondary packaging. Another case study is when Wayne E. Bailey Company has experienced the benefits of using machine vision in packing operation. Microscan QX830 laser barcode scanner is used to confirm the product type (sweet potatoes), ensuring that each box receives the correct label. When the scanner detects the wrong code, the product is removed from the line. The benefits from using the technology are to increase labeling accuracy and traceability. [51]

Vision technology is used in packaging industries to inspect products for any defect, for example in caps, seals, labels and so on. Companies get benefits from using the system because it reduces cost and provides date and lot verification, color detection, robotic guidance, test tube cap and color inspection, error proofing, package integrity inspection, and dimensional gauging. [48]

1.1.4 Card Technologies

Card technologies demonstrate an outstanding opportunity for improving comfort and security. There are three types: magnetic stripe cards, smart cards, and optical memory cards. [39, 53] Magnetic stripe cards use a magnetic medium to encode data in binary format with the polarity of the particles determining the 0 and 1 bit. A reader then translates the code into alphanumeric characters. Magnetic stripe cards provide minimal security because data

can be read from and written to the card. In this case, the information can be stolen and duplicated. With respect to capacity, it limits the amount of data to less than 2 Kbytes. In addition, it needs contact read equipment. Because of these limitations, Magnetic stripe cards are often replaced with smart cards. [40, 53] A smart card is a plastic card that uses a microprocessor chip to store data, which is stored in binary format; the chip performs some computing functions such as encryption and decryption functions using the data. In 1968, smart cards were introduced by two German inventors, Jürgen Dethloff and Helmut Jürgen. [25] In Table 1.1, a brief outline of the evolution of the smart card is presented.

Table 1.1: Outline of the evolution of the Smart Card [26]

Year	Event
1968	2 German inventors patent combining plastic cards with micro chips
1970	Computations arise from the mathematical of Boolean logic(AND, OR..etc.)Arimura invents and patents in Japan
1974	Roland Moreno invents and patents in France
1976	French DGT initiative, Bull (France) first licenses
1977	Motorola produces first smart card microchip
1979	Motorola develops first single chip microcontroller for bank in France
1980	First trials in 3 French cities
1982	First U.S. trials in North Dakota and New Jersey
1991	AT&T declared its contact less smart card
1992	Germany uses smart card for health care
1996	First university campus deployment of chip cards in Poland

The components of this system are a smart card, reader, computer, software, and an electronic meter. The principle behind the card technology is to provide authentication and validation of the holder. There are many other advantages of using a smart card, some of

which are capacity, convenience, durability, and security. [24]

The stored information in the card can be protected from undesired access. There is a password given to the holder to use whenever the card is connected to a computer. [24] Many types of cards have been developed; these are contact based smart cards, contact less smart cards, and combinations between these two types. A contact-based card contacts with the reader to carry out functions. However, contact-less cards requires no contact with readers because it has a chip and an antenna to receive power for communication and processing the transaction. [27, 53]

Smart cards can be classified into two categories: a memory card or a processing -enabled card. A memory card can be called asynchronous because the flow of data is in one direction; data moves to the reader or to the computer system. The memory ranges from 8K- 128K bit. [41]

In addition, this type of card provides a limited capacity to secure the stored data. [26] The processor-enabled smart card or synchronous card is a more sophisticated card. It is also called a "true" smart card because it is based on semiconductor technology. [28] It contains a chip with a few hundred bytes of RAM. This type of card can perform cryptographic operations so that the information will be protected by the encryption schemes with biometric identification. The data flow is bi-directional because data can be read from and written to the card. [26] This technology can be used widely in many applications such as bank cards, ID cards, garage cards, health care cards, pre-paid cards, and hotel key cards and so on. [19, 23, 53]

Smart cards have significant advantages over magnetic stripe cards especially in health-care applications because it provides very high security and privacy; both contact and contact less smart cards provide high level of security. They protect sensitive information for trans-

actions. In addition, smart cards have higher capacity than magnetic stripe cards. [40, 41]

Optical memory cards are another technology for securing identifications. It employs a laser beam to write data to a reflective stripe of laser recording medium, composed of silver particles suspended in a matrix. A laser reader reads tiny holes that are burned into the medium; the absence and the presence of a hole represents 0 and 1 bit respectively. Optical memory cards are a write once read many (WORM) type media and the data is non-volatile, which means it is not lost when the power is removed. The storage capacity of this card is in between 4Mbytes to 6.6Mbytes of data which is higher than the other card technologies. [53] Because of the large capacity of this card, multiple features such as photographs, fingerprints, and signatures can be recorded. This card can be used in some applications that need very secure personal identification such as the US Permanent Resident Card (green card). [42]

1.1.5 Radio Frequency Identification Systems

In this section, the background of radio frequency identification systems (RFID) will be introduced. RFID is one of those newer technologies that tend to make life easier; it is a wireless device. RFID tags are small electronic devices that are used to identify objects to which they are attached. Some other references define the RFID tag as a small computer device because it has a storage unit and microcontroller. In operation, tags automatically emit their unique serial numbers when they get queries for readers. [53]

In general, the benefits of RFID systems are:

1. Improving the efficiency of production processes

2. Improving product quality and service safety or authenticity

3. Improving product track-and-trace capabilities

4. Improving asset management
5. Reducing labor costs
6. Increasing supply chain efficiencies
7. Complying with customer mandates
8. Supporting new customer-facing strategies
9. Improving supply chain visibility
10. Facilitating collaboration with business partners
11. Improving inventory management efficiencies
12. Optimizing merchandise management and reducing out-of-stocks [54]

RFID systems can be used in many applications. This technology can provide suppliers, manufacturers, distributors and retailers accurate information about their products. However, it may bring up some privacy threats. There are a set of security problems that an RFID system suffers from, and one of the most critical one is cloning. Imagine what could happen if someone successfully clones the contents of an RFID attached to a passport!

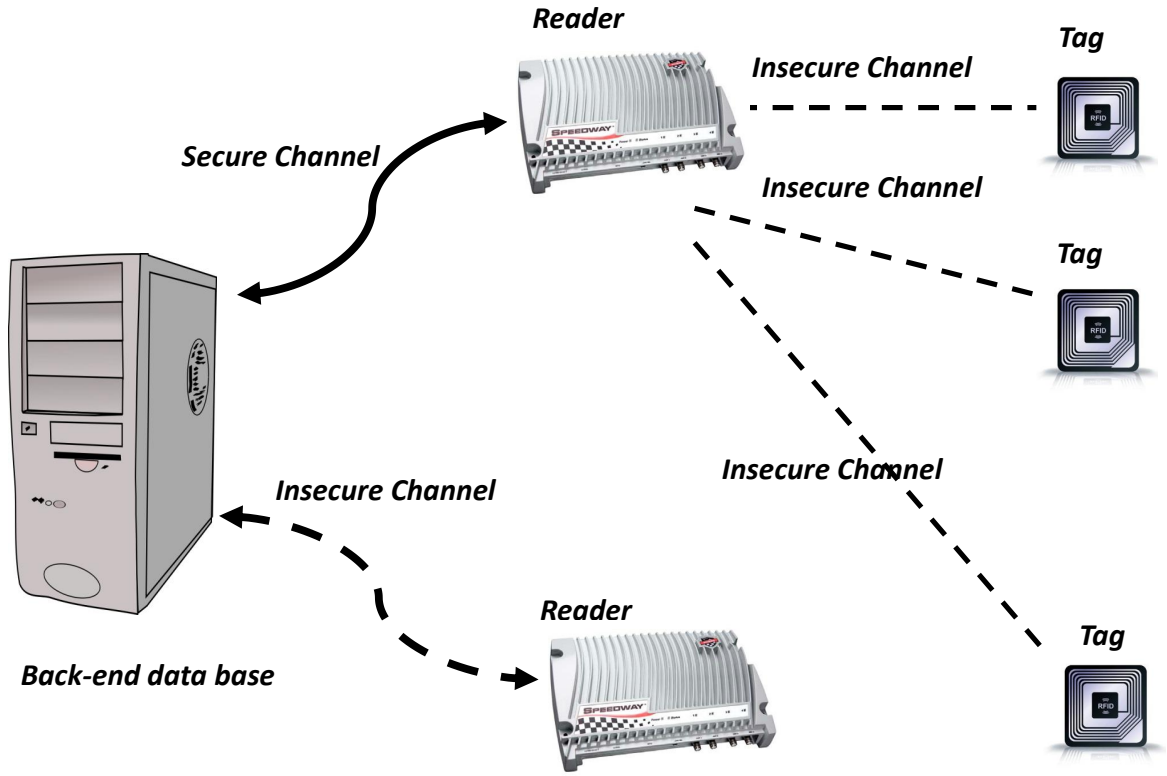

Figure 1.3: RFID System

1.1.5.1 Components of RFID devices

In general, the elements of an RFID system are a tag (transponder), a reader (transceiver), computer with software, and a back-end database. See Figure 1.3. An RFID reader is usually equipped with an RF transmitter and receiver, a control unit, and a memory unit. It is the connection between tags and the back-end database.

The role of the reader is to interrogate a tag by sending a signal to read the stored information on the tag. The tag would be then be authenticated based on the stored database information. Tags obtain, read and transmit energy from the electromagnetic field of transceivers. [16] Information is wirelessly exchanged, via radio wave, between the

reader and the tag, both of which are equipped with an antenna. In addition, a tag typically has a microchip and encapsulation or protective layers. If tag is active, it will also have an internal power supply (a battery), which boosts read capabilities. [15]

There are two types of readers. The first type is fixed (or stationary) readers, which have a fixed location in a plant and are used when tags are passing within the range of the reader. The second type is mobile readers, which can be moved around and are often used for inventory control purposes. [15, 16]

The back-end database is divided into two parts: middleware and applications. These two parts are run on computers within the network. Middleware is used to filter data and provide the interface towards the applications. [16]

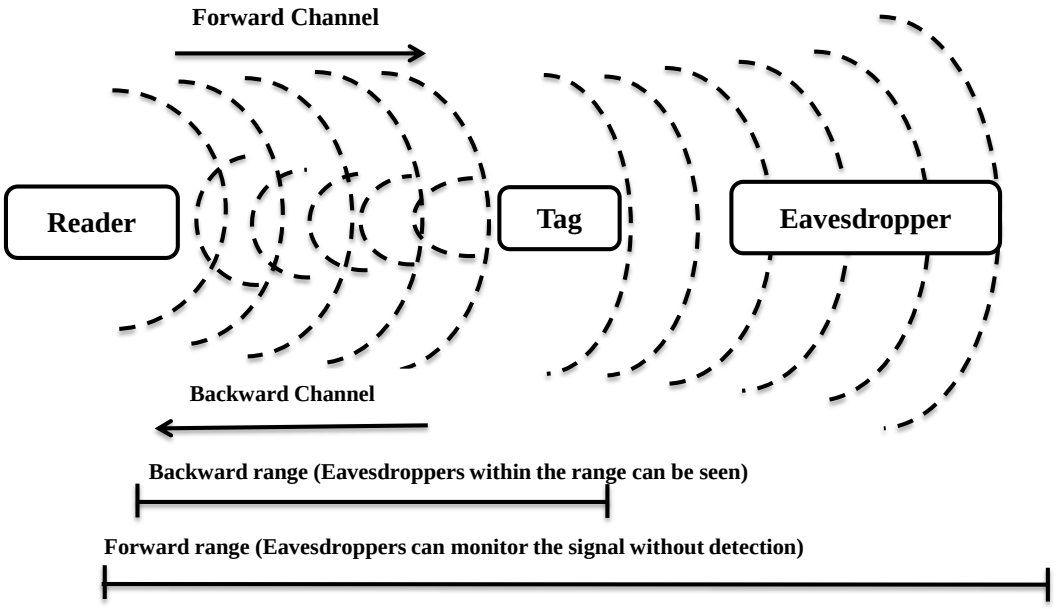

Figure 1.4: Eavesdropping range (Forward vs. backward channels) [43, 56]

Generally, it is assumed that the channel between a reader and back-end database is secure, but the channel between a reader and tag is not [1]. There are two channels between

a reader and tag, forward and backward. The forward channel is for interrogating a tag that in turn responds to a reader through the backward channel. Because a tag gets its power from the electromagnetic reader signal, the backward channel signal is much weaker than the one in the forward channel. Because of this, any passive party can eavesdrop on a message in the forward channel easier than one in the backward channel. See Figure 1.4.

1.1.5.2 Read/write capacity

RFID tags can come in many different formats. They can be read only (data cannot be changed; it is programmed once by the tag manufacture), read/write (data can be modified or rewritten over existing information), or a combination (data is stored permanently and some part of the memory will be used for other later updating). [16, 18] Some tags unwritten and then sent to packaging houses who encode the tags with some information about products. These kinds of tags can be considered as WORM, which stands for Write Once, Read Many. Others can be read only and WORM where manufacturers prewrite their information on tags and then send them to be filled in at the packaging houses. [16, 18]

The supply chain applications and the technologies can be controlled by using read/write tags. If not, new tags should be purchased in cases where the requirements are changed. Read/ write tags can have greater stored information capabilities that lead to an increase in the processing time. These tags may not be required to contact the back-end database because they can have all relevant data embedded therein. Furthermore, they can be used in different applications by erasing old information and rewriting them with new information. This can lead to cost savings and provides flexibility to adapt to future changes. [16, 18]

The reading ability typically decreases when the distance between a tag and its reader increases. Moreover, it will decrease due to differing factors. Some factors are the operating

frequency employed, type of tags, size of antennae (in both readers and tags), alignment of antennas, the environment (with local materials and conditions), and so on. Based on these factors, the reading range can be affected as well as the writing range. In this scenario, the exchange of protocols between tags and readers will be affected too. [16, 18]

The reading speed will also be affected by different factors, some of which are:

1. Number of messages to be exchanged
2. Available data rate (frequency)
3. Error correction strategy and desired reliability
4. Anti-collision algorithm and number of tags within communication range
5. Amount of data to be transmitted
6. Required time for performing calculations especially for the authentication algorithms [16]

Using low frequency (LF) and high frequency (HF) systems, 10-30 tags per second can be read. When ultra-high frequency (UHF) is used, 100-500 tags per second can be read. [1, 14, 16]

1.1.5.3 RFID tag types

Tags come in many different sizes and shapes. Some are very tiny and some have much larger dimensions. The RFID tags can be classified into three kinds based on how tags are fed with power. The first kind is active RFID tag, where a power source (battery) is located on the RFID tag and has extra memory storage so that it has more energy and a more powerful

computational ability [1]. The second kind is passive RFID tag, which implies that the tag has no internal power source (hence, it comes without a battery). There is no doubt that this type of tag needs a source of power to operate and this would be derived from the received signal energy of the reader. A passive tag has limited computational storage that can be applied. Finally, there are semi-passive tags that use some battery power to maintain their internal volatile memory. However, it gets its power from electromagnetic signals that are sent by the reader, just like passive tags. [17] This tag may also be referred to as semi-active. It can provide a longer read range than a passive tag because of the battery. In addition, a semi-passive tag can accommodate environmental sensors on-board. The environmental experience of any object will be recorded to the attached tag memory during the lifecycle of that object. This can happen because of the battery. Although the batteries in semi-passive tags have advantages, they also create a few problems such as: extra weight, larger size, higher cost, shorter life, and so on. [33]

Because of the longer range of active and semi-passive tags, they are often used for tracking high-value goods that need to be scanned over long range, such as cargo containers or railway cars on a track. However, their price is too expensive to put on low-cost items. [16, 17]

The advantages of the passive tags over active tags are low costs, smaller sizes, and lower weights. Finally, because a passive tag does not have a battery, it has an extended lifetime. In contrast, the advantage of active tags over passive is the communication will occur over longer distances (signal strength is strong and always on), greater memory capacity, and the ability to be rewritten. However, active tags have a limited life because of batteries, though a lifespan of several years is common. Both passive and active tags can be used in all environments. [16, 17]

1.1.5.4 Radio frequency classifications

Diverse frequencies ranges, which may have different characteristics, can be useful for various RFID systems applications. There are four classes of commonly used tags, based on the frequency: low frequency / LF , high frequency / HF , ultra-high frequency / UHF , and microwave /SHF. [1, 14, 16] All of these ranges are part of the frequency bands called Industrial, Scientific, and Medical (ISM) radio bands. [33, 53] Tables 1.2 and 1.3 illustrate the range of each frequency band.

Table 1.2: Type of frequency and associated bandwidth [33]

Range	LF	HF	UHF	Microwave
Frequency available	30-300 KHz	3-30 MHz	300-1000 MHz	1-6 GHz
Used for RFID	125—134 KHz	13.56 MHz	433 & 860-960 MHz	2.4 & 5.8 GHz

Table 1.3: UHF operating frequencies throughout the world [33, 44]

Country	Frequency Band (MHz)
United State and Canada	902-928
Australia	918-928
Europe	865-868
Hong Kong	865-868 & 920-925
Japan	952-954
Korea	908.5-914
New Zealand	864-929
Singapore	866-869 & 923-925

The range for LF tags is short (a few inches at best) and the data transfer rate is the

lowest. LF tags are passive tags and store a small amount of data. They can be easily read when they are attached to objects made of or holding water, wood, metal and other liquids. They are used in many applications such as animal identification, access control, asset tracking, automotive control, healthcare, and so on. LF tags have limited anti-collision capability. Thus, it is very difficult to read multiple tags simultaneously. [33] An anti-collision technique is required to ensure that tags and readers can communicate using the same shared medium without disturbing each other. There are two algorithms for this technique, probabilistic and deterministic anti-collision algorithms. Probabilistic algorithms use the ALOHA protocol, which works as follows: when the communication medium is free, a device starts to send information. If the collision occurs (several devices send data at the same time), the medium will released all the stations and then each station waits for a random time when they will start again. For the second type of algorithm, which is deterministic, the binary tree walking algorithm is used between readers and tags. This algorithm works as follows: each tag has a unique identifier; the reader controls the process by requesting all tags whose address start with 0 bit; if the collision occurs (many tags answer), the reader asks all tags whose address begins with 00. This process will continue until only one tag answers. [16, 52]

HF tags (13.56 MHz) have a short reading range (maximum range about 3 feet) and the data rate is higher than LF, but lower than UHF. HF tags can be passive or active tags. In addition, HF tags may have anti-collision capabilities, which lead to facilitate the reading of multiple tags. The cost of HF tags is lower than LF because it has simpler antenna design than LF tags. They also can be read when attached to objects made of, or holding water, wood, metal and other liquids. However, they can be affected by metal objects in the close vicinity. Because of magnetic flux, which is used to power and communicate with the tags,

HF tags can be used in many applications such as a smart shelf because it covers the entire area. HF tags are used in such different application such as credit cards, smart cards, library books, airline baggage, and asset tracking. LF and HF tags both use near-field inductive coupling to obtain power and communicate. [33, 44, 52]

UHF 433 MHz is used mostly for active tags, while UHF 860-960 MHz is used for passive, active, and semi-passive tags. The range of passive UHF, for example, is up to 135 feet. [55] UHF tags also have an anti-collision capability. They cannot be easily read when attached to objects that hold or are around water and animal tissues because water absorbs UHF waves and detuned the tag. Also, when the tags are around or attached to metal objects, they become detuned. The reading capability will be impossible when a conductive material is place between the interrogator antenna and the tags. UHF tags (passive and semi-passive) typically use far-field backscatter coupling, though newer UHF tags are available that use inductive coupling. [33, 44, 52]

Table 1.4: Comparison between RFID frequencies according to [44, 52]

Band	LF	HF	UHF	Microwave
Frequency	30-300 KHz	3-30 MHz	300 MHz- 3 GHz	2-30 GHz
Typical RFID frequencies	125-134 KHz	13.56 MHz	433 MHz or 865-956 MHz 2.45 GHz	2.45 GHz
Approximate read range [52]	Less than 0.5 meter	Up to 1.5 meters	433 MHz = up to 100 meter 865-956 MHz =0.5 to 5 meter	Up to 10 m
Typical data transfer rate	Less than 1 Kbit/s	Approximately 25 Kbit/s	433-956 =30 Kbit/s 2.45 =100 Kbit/s	Up to 100 Kbit/s

Continued on next page

Table 1.4 *(cont'd)*

Band	LF	HF	UHF	Microwave
Characteristics	Short range, low data transfer rate, read easily when they are attached to objects made of, or holding, water, wood, metal and other liquids	Higher ranges, reasonable data rate (similar to GSM phone), read when attached to objects made of, or holding water, wood, metal and other liquids	Long ranges, high data transfer rate, concurrent read of < 100 items, cannot penetrate water or metal, but can with non-water based liquids like oils	Long range, high data transfer rate, read easily with metallic objects
Typical use	Animal ID Car Immobilizer	Smart labels Contact-less Travel cards Access & security	Animal Tracking Logistics	Moving vehicle toll

Most microwave tags use 2.54 GHz. Microwave tags can be passive, active or semi-passive types. Usually, passive microwave tags are smaller than passive UHF tags, but the read range for both is the same. [45] The read range of semi-passive microwave tags is about 100 feet and 350 feet for active microwave tags. Microwave tags (passive and semi-passive tags) use backscatter coupling to communicate, but active tags use their own transmitter. Microwaves tags can work easily with metallic objects because of their shorter wavelength. [33, 52]

The read ranges for tags can be attained by different aspects. Some of these aspects are frequency, the power supply, the size and form of antennas, the alignment of antennas, the environment, and so on. [16] Table 1.4 shows the comparison between the various frequencies for RFID systems. [33, 52]

Table 1.5: Comparison between RFID and Barcode [1, 5, 12]

RFID	Barcode
RF technology	Optical technology
May not need line-of-sight	Need line-of-sight
Proceed in bulks	Proceed one by one
Identify objects at item level	Identify objects at type level
High-up to $50 per tag, averaging $0.10-$5.00 /tag	Less expensive
It can be extremely durable (internally attached)	Can be damaged (dirt, torn, etc.)
May be difficult to read when RF is passing through metal or liquid	Most can be read when it is damaged but only a very few cannot be read when they damaged
Can be read, rewritten	Can only be read
May contain high level of security (data can be encrypted, password, etc.)	Can be duplicated and counterfeited; have lower levels of security

1.1.5.5 Key differences between barcode and RFID technology

The function of an RFID tag is the same as the barcode but RFID usually has a globally unique identifier for each item on which it is attached. RFID has some significant advantages over barcodes; it may not need physical or visual contact between the reader and the RFID tag i.e., it may not need line of sight, unlike barcodes. Also, large items in crates could be scanned at the same time if the items are RFID labeled, unlike the use of barcodes where each package needs to be scanned individually. In many cases, the supply chain system benefits from this advantage of RFID tags.

In summary, Table 1.5 has the comparisons between RFID and barcode systems. [1, 5, 12]

1.1.5.6 RFID applications

As it has been mentioned above, RFID can be used in many applications in industries. The RFID components are used to identify and track objects. This system is used in many applications such as supply chain management, theft prevention, military, animal tracking, medical system, automatic payment and E-passport and so on. With a unique ID, the transportation of any cargo can be monitored in the entire value chain, from manufacture to retailer. Also, because RFID has many benefits, for example, no human intervention or being recyclable, the cost of the supply chain could be reduced and safety/security can be achieved. [1, 2] The use of this technology could result in a 90% decrease in location errors. [46] The data collection from RFID system also helps preventing errors in picking and shipping. The use of standardized assessment tools, technologies and processes are essential for improving supply chain security strategies. A track and trace system for all products throughout the domestic and foreign supply chain is a significant step for ensuring transparency and accountability of product authenticity and distribution. This could be done by using RFID, which provides a secure identification and can track a product at every point in the supply chain quickly. [7] Anti-theft security RFID labels play a key role in deterring counterfeit activity as well as detecting and monitoring the actions of would-be criminals and the movement of goods into and out of a retail establishment. This technology also has many benefits in establishing an electronic pedigree. The FDA in food defense is focusing on moving from a reactive approach to proactive approach to address the intentional and unintentional food contamination. There are four goals of this food defense. The first one is to prevent an outbreak/attack through awareness, preparedness and capacity building. The second goal is intervention through targeted inspection and sampling. The third goal is

to respond rapidly and efficiently if needed. The last goal is to recover rapidly and restore consumer confidence in the food supply. The FDA Combating Counterfeit Drugs identified several key elements for combating counterfeit crimes and securing the nation's drugs supply by providing technology and increasing criminal penalties, whereas the FDA food initiative is focusing on prevention and detection of the fraud. They both intersect in using technology (RFID and barcode) for tracking products. Also, they both can identify what products are likely to be counterfeited and entered into the legitimate supply chain, even if the prevention of that is impossible. [8, 9] In medical health, RFID can be used to obtain and track a patient's information such as ID, name, emergency contacts and so on.[1, 5] Also, RFID can be used to help surgeries in tracking surgery sponges or any tools on which RFID tags are attached. There have been cases where doctors accidently left sponges and tools inside patients, which cause damage to the patients. Therefore, a wand reader will be used on the patient after surgery to determine the location of the sponges, if any are missed in closing. [3, 4] In addition, RFID can be adopted to identify counterfeit medical drug packaging. RFID can also be used to improve the security of credit cards because of counterfeiting. So, before payment is made, a reader should authenticate the tag and card. Another example of automatic payments in which RFID can be used is the public transportation ticket system. This reduces the costs from selling tickets manually. Another example about using RFID is automatic toll readers. When cars drive along a road, tags in the cars will be read and charged a fee. This benefit increases throughput efficiency, and accuracy, and it is more convenient than collecting fees from people. [1, 2] In an E-passport, RFID tag can be embedded to record more information about the holder. This information could be related to fingerprint and more sensitive details. Information will be recorded for people who are entering and leaving the U.S. However, security should be provided to eliminate the counterfeiting, such

as having the information be encrypted. [1, 2, 6] RFID also has many benefits in animal scientific research or pet tracking. In pet tracking, this technology is used to locate and monitor the location of animals such as cows, pigs, cats, dogs or even fish, when they are lost. In some other research, it can be used to monitor animal diseases [1, 2].

The DOD uses passive and active tags within its supply chain and with all contracts. All cases and pallets that are shipped to the overseas DOD locations should be tagged. RFID can also support soldiers in their fields. [10] RFID has three main benefits for the DOD. These benefits are related to the supply chain management, asset tracking, and security. It can help to improve visibility and the efficiency of the vast DOD supply chain. The military can identify, track and manage their belongings in time. In addition, RFID systems secure suppliers, equipment, and locations. However, there are also issues related to security. These will be discussed more in Chapter Two. [11]

1.1.5.7 Standards

To deliver accurate data and information within supply chain, standards are provided by the GS1. These standards are used by businesses to operate organizations efficiently by sharing their information (location, movement and status) about their products and to speak the same language as their trading partners.

There are many standards that have been developed in RFID system for different frequencies and applications. Some of these standards are related to the communication between tags and readers and some are related to the formatting of the data or conformance between products and the standards, or applications. [29] In addition, the security of tags on products can be included in some standards. Wal-Mart and the DOD are the two largest USA drivers for using RFID technology today and to accomplish the same thing. The In-

Table 1.6: RFID Standards

ISO 14443	For Proximity Cards (A few inches)
ISO 15693	For vicinity (Out to 28 inches (from a single antenna) or 4 feet (multiple antenna))
ISO 18000 part 1	For RFID Air interface communication (Globally accepted frequencies)
ISO 18000 part 2	For RFID Air interface communication (Low frequency below 135KHz)
ISO 18000 part 3	For RFID Air interface communication (High frequency at 13.56 MHz)
ISO 18000 part 4	For RFID Air interface communication (High frequency at 2.45 GHz)
ISO 18000 part 5	For RFID Air interface communication (5.8 GHz)
ISO 18000 part 6	For RFID Air interface communication (860-930 MHz)
ISO 18000 part 7	For RFID Air interface communication (433.92 MHz)
ISO 11748/ 11785	For animal identification
ISO 11785	Define the air interface
ISO 17358	Application requirements
ISO 17363	Freight containers
ISO 17364	Returnable transport items
ISO 17365	Transport unit
ISO 17366	Product packaging
ISO 17367	Product tagging (DOD)
ISO 10374.2	RFID freight container identification
ISO 11784	Define the structure of data on tag
ISO 18047	For testing the conformance of RFID tags and readers
ISO 18046	For testing the performance of RFID tag and readers

ternational Organization for Standardization (ISO) has established standards in many areas such as in tracking cattle or goods in open supply chains. Also, the EPC Global Center has introduced the EPC (Electronic Product Code) standard to identify and track consumer goods through the international supply chain by creating their own air interface protocol.

Electronic Product Code Information Services (EPCIS) is a standard for sharing EPC-related information between trading partners. EPC is used to provide a unique identity for any item; it is a universal identifier. [17] Both Wal-Mart and DOD use the EPC standard. However, DOD uses the ISO standards for air interface. The EPC Auto-ID Center has been trying to develop protocols that can be used with different classes of tags. EPC tags are divided into five classes. Class 0 is read only and has 64 bit. Class 1 is many readable and one time writeable, and has 96 bit as a minimum. Class 2 generation 2 is read/ writes and has 96 bit as a minimum. Class 3 is read/ writes and has battery power. The last one is class 4 which is for read/ write active transmitter. The first three tags are passive and the fourth one is semi-active. For communication, class 0 and class 1 use different air interface. There are four parts of the EPC number (header which identifies the version number, EPC Manager or the manufacturer, object class, which identifies the product's type, and the serial number uniquely defines the product). [32] A second generation was developed because a global standard was needed to be more closely aligned with ISO standards. Table 1.6 summarizes the all ISO standards. [29, 30]

1.1.6 Architecture Framework

EPCglobal architecture framework is a group of standards for hardware, software, and data interfaces. Many goals are considered in the EPCglobal architecture framework to provide benefits to end users. Some of these benefits are: facilitating the exchange of data and goods between partners, developing standards for global use, the interfaces between the components of the architecture are identified in open standards, providing scalability and extensibility, all parties in end users can capture data, keep it, and share them with whom they choose to achieve their goals, and providing security and privacy to protect the information. [17, 32]

In general, there are three parts in the architecture framework: EPC physical object exchange standards, EPC infrastructure standards for data capture, and EPC data exchange standards. In the first part, all physical objects should be identified with Electronic Product Code (EPC) in end users who are the parties in the supply chain for shipping, receiving and so on. The standards are designed to ensure that all parties can access the information properly. The following standards represent all within this part of EPCglobal Architecture Framework: [17, 32]

- UHF Class 0 Gen 1 Tag Air Interface
- UHF Class 0 Gen 1 Tag Air Interface
- HF Class 1 Gen 1 Tag Air Interface
- UHF Class 1 Gen 2 Tag Air Interface v1.1.0
- UHF Class 1 Gen 2 Tag Air Interface v1.2.0
- HF Class 1 Tag Air Interface
- EPC Tag Data Standard [17, 32]

In the second part of architecture framework "EPC infrastructure standards for data capture", end users can build their internal system based on defining interface standards for gathering and recording EPC data. The following standards represents all within this part of EPCglobal Architecture Framework: [17, 32]

- EPC Tag Data Standard
- Low Level Reader Protocol

- Reader Management
- Discovery, Configuration and Initialization (DCI) for Reader Operation
- Tag Data Translation
- Application Level Events (ALE)
- EPCIS Capture Interface

In the last part of architecture framework "EPC data exchange standards", data about EPCs are shared and exchanged within the parties of end users. The standards are defined to increase the visibility of the movement of objects in any place, and to facilitate the exchanges by accessing the other EPC Network services. The following standards represent all within this part of EPCglobal Architecture Framework: [17, 32]

- Core Business Vocabulary
- EPCIS Query Interface
- Pedigree Standard
- EPCglobal Certificate Profile
- ONS
- Discovery Services [17, 32]

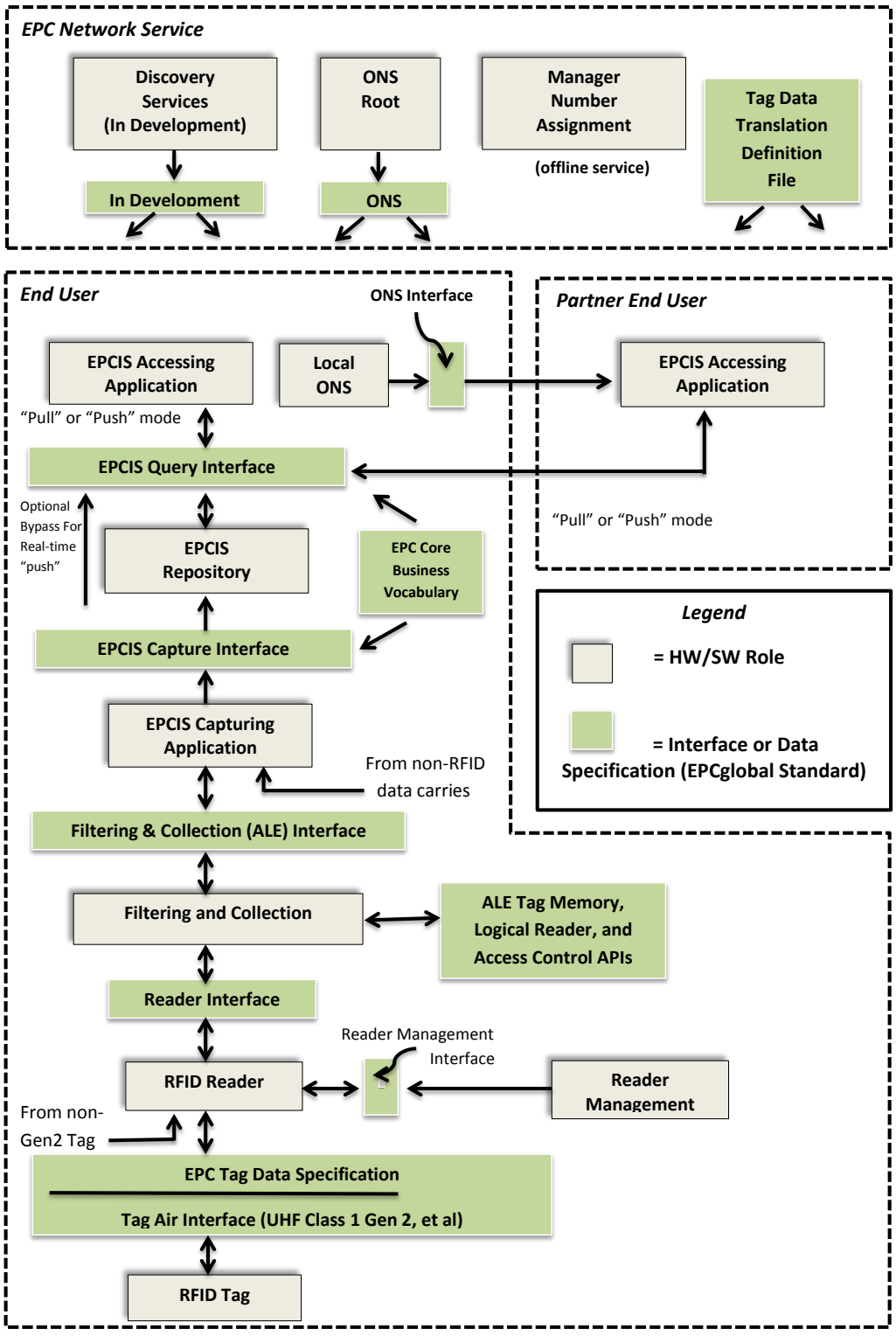

Figure 1.5: The EPCglobal Architecture Framework (Roles and Interfaces) [17, 32]

In Figure 1.5 (the EPCglobal Architecture Framework), there are three parts connected with each other: End User, Partner End User, and EPC Network Service. EPC codes on RFID tags are observed by the End user and then the data will be shared with the other End User (Partner End User). So, there will be interactions between End Users.

A EPCglobal architecture framework has interfaces that are administered by EPCglobal standards (the plain green bars), and roles that are played by hardware and software components (the shadowed boxes). The following are the definitions for the items in Figure 1.5.

RFID Tag: There are four classes of a tag. These are Class1 (identity tag), Class2 (higher-functionality tag), Class3 (battery-assisted passive tag), and Class4 (active tag). [17]

EPC Tag Data Specification: Defines the structure and the coding scheme of the EPC; the meaning of data. Also, it defines the mechanism to federate the different coding schemes, and binary representations. [31]

Reader Management Interface: Provides means to control and demand the configuration and observer the operational status of an RFID Reader. Also, if there is operational problem, this interface will notify management stations about it.

Tag Air Interface: Defines the communication of data between RFID tags and readers. In addition, it provides means to eliminate the interference between tags and readers.

RFID Reader: Gets the information from tags and sends this information to a host application via the Reader Interface. Also, it has some other features such as filtering of EPCs, aggregation reads, killing or locking and so on.

Reader Interface: Provides means to control the operation of RFID Reader. To access the all capabilities of the UHF Class 1 Gen 2 Tag Air Interface, the EPCglobal Low Level

Reader Protocol (LLRP) standard was designed. This will include reading, writing, executing other commands such as kill and lock commands, and sending reports if there are errors and handling these errors.

Reader Management Interface: Provides means to control and demand the configuration and observer the operational status of an RFID Reader. Also, if there is operational problem, this interface will notify management stations about it.

Reader Management: Controls the operational status and manages the configuration of an RFID Readers. If there are issues, Reader Management will alert management stations about them by providing mechanisms.

Filtering and Collection: If there is one or more than RFID Readers in the local area that can cause the possibility of radio frequency interference, this role manages the operations of them. Also, there are some other features such as decoding and encoding raw tag data that are read from tags.

Filtering and Collection (ALE) Interface: Provides standards to filter and collect data from Filtering and Collection role to the EPCIS Capturing Application role so that there are no duplicates in EPCs in the list. There are other means that can be provided in this interface such as to manage applications to secure client access to the ALE interface and to share data from readers for multiple client applications.

EPCIS Capturing Application: This role manages many sources of data such as filtered, collected EPC data that is received from the Filtering and Collection Interface. It controls some actions like writing RFID tags and controls other devices.

EPCIS Capture Interface: EPCIS Capturing Application generates events. This interface will provide a path for communicating these events to other roles that need them.

EPCIS Repository: When EPCIS Capturing Application generates events, these will

be recorded by this role and be made available when the EPCIS Accessing Application queries them later.

EPCIS Query Interface: When the EPCIS Accessing Application requires data from the EPCIS Repository, this interface provides means for that. Also, for mutual authentication between two parties, this interface allows this happen.

EPCIS Accessing Application: It executes some processes such as warehouse management, shipping and receiving etc. Core Business Vocabulary or Data Specification: For denoting business steps, dispositions, and business transaction types, this section provides standardized identifiers for use in EPCIS data.

Object Name Service (ONS) Interface: ONS is a research service to produce the address of an EPCIS service by using an EPC. This interface makes means available for locating the EPCIS service of the End User.

Local ONS: Provides the pointer to the EPCIS service.

ONS Root (EPC Network Service): This role identifies the local ONS service of the EPC Manager organization for that EPC. If there is no local ONS, ONS Root will accomplish the requests.

Manager Number Assignment (EPC Network Service): It issues unique EPC Manager Numbers to each organization. Tag Data Translation: It provides machine-readable files. This file is for translation between EPC encodings. This file is used by End Users to be aware of a new EPC format. [17, 32]

Although some researches proposed different methods to overcome these threats, still there are many vulnerable points in the system can be attached. For example, Divayan Konidala [32] analyzed the security threats in the components of the EPCglobal Architecture Framework and suggested some secured solutions. In this research, more details are going

to be concerned for providing security by proposing new protocols in the following chapters.

1.2 The contribution and thesis organization

The main contribution of this thesis is four chapters. Because the RFID system is one of the most widely used technologies due to its advantages, it is opened to various attacks that try to degrade the performance of the system. Therefore, a general introduction on security issues is going to be introduced in Chapter 2. Also, different types of attacks against RFID system and some proposed solutions would be reviewed in the same chapter. In addition, some suggested solutions and protocols are going to be introduced in this chapter too. Although some researches proposed different methods to overcome some threats, still there are many vulnerable points in the system can be attached. In Chapter 3, an application is addressed and new developed protocols (three protocols) are presented with different level of security to prevent some attacks and to meet both the privacy and authentication concerns. In addition, a new developed system model is going to be introduced in this chapter to solve key management problems. After explaining the details of the approaches to meet the security goals, discussion and analyzing the security and the time cost of the proposed protocols are discussed in Chapter 4.

Chapter 2

Security and Privacy

In general, the term "security" refers to the "secure" condition of a system or services. When a system has an ability to behave normally, especially when there are some efforts to make this system misbehave, this situation expresses the security of the system. As a result, the system will not suffer harm from some types of threats. [16]

2.1 Security properties

There are five goals or objectives with which any deployed system should be concerned.

- **Confidentiality**: data and resources should be accessed and shared by authorized entities. All systems should protect their information from being leaked. This can be done by protecting the communication channels within the system from unauthorized entities.

- **Integrity**: protecting data or systems from being modified, deleted or duplicated. In other words, protecting the accuracy of information and processing methods. Here, the data in an RFID systems should be protected from unauthorized modification (unauthorized readers and tags).

- **Availability**: keeping services or information available to authorized entities when required. For RFID systems, all the system components and data are available at any

time to authorized entities. The system should not be corrupted in the presence of multiple RFID readers and tags.

- **Accountability**: end users should access information in an appropriate way. Without this principle, it is impossible to ascertain who is responsible and what has happened within the system. This can be provided by an audit trail that provides more details about the events and the actions that happened within the system.

- **Non-repudiation**: proving that a particular set of data is signed by the holder; the holder cannot deny data modification and transmission. This leads to trust of one system partners and also trust of the in integrity of data. In RFID systems, this goal can be reached by providing mutual authentication between RFID readers and tags and between readers and back-end databases. [16, 17, 57]

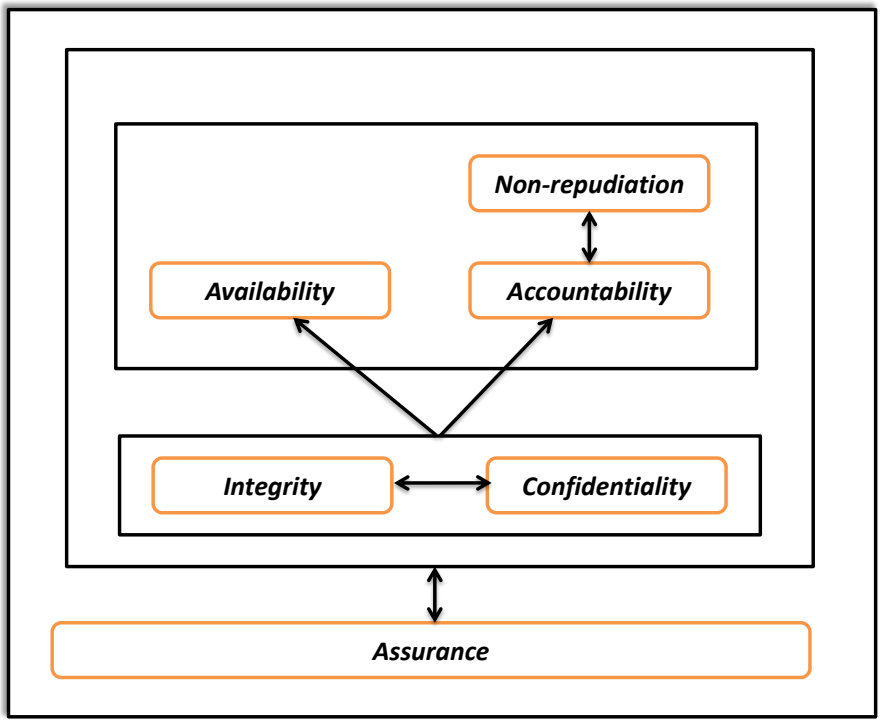

Figure 2.1: Security Objectives Dependencies adapted from[57, 58]

These five objectives are dependent on one another. It is impossible to achieve one objective without considering of the others. For example, without integrity of the system, confidentiality will not be valid. Further, all these objectives are related to another target objective which is "Assurance". It is the basis for confidence to protect the system and the information it processes; it is established as a target when designing a system. By defining all the functionality requirements of the above objectives, Assurance can be achieved and undesired actions are not going to occur. Figure 2.1 illustrates the idea of these dependent objectives. [58]

2.2 Security in RFID systems

The use of RFID is becoming more popular nowadays. So, the security of an RFID system has to be a concern. In the next sections of this chapter, the RFID security threats and some of the proposed solutions will be reviewed.

2.2.1 Issues

Opening up a system to the world or locking it down are not solutions for keeping the system safe. Security techniques are available to prevent unauthorized access of system resources. However, some issues should be taken into account first and then solutions should be proposed to eliminate some issues.

With respect to RFID security and privacy, a number of threats, such as sniffing, tracking, spoofing, replay attacks and denial of service, are classified as a high level misuse of properly formatted RFID data. The following is a brief description of some these threats with examples:

- **Malware attack**: As defined, the standard architecture of an RFID tag consists of an antenna, a microcontroller, and a storage unit. So, the RFID tag can be vulnerable to all kinds of viruses and worms that may threaten a regular computer. [61]

  RFID exploits is an example of a malicious RFID tag data corruption system. It is the same as those on the Internet, for example Structure Query Language (SQL) injection. SQL is a type of insertion attack executing SQL codes in the database to retrieve authorized data, make modifications and deletions, etc. [60, 63] Back-end RFID middleware can be exploited directly by RFID tags. One of the reasons that facilitate this kind of attack is codes should be reduced to a small number of bits to

be appropriate for tags. One example of this injection is including the following SQL command with the RFID read tag ID:

; drop table < tablename >

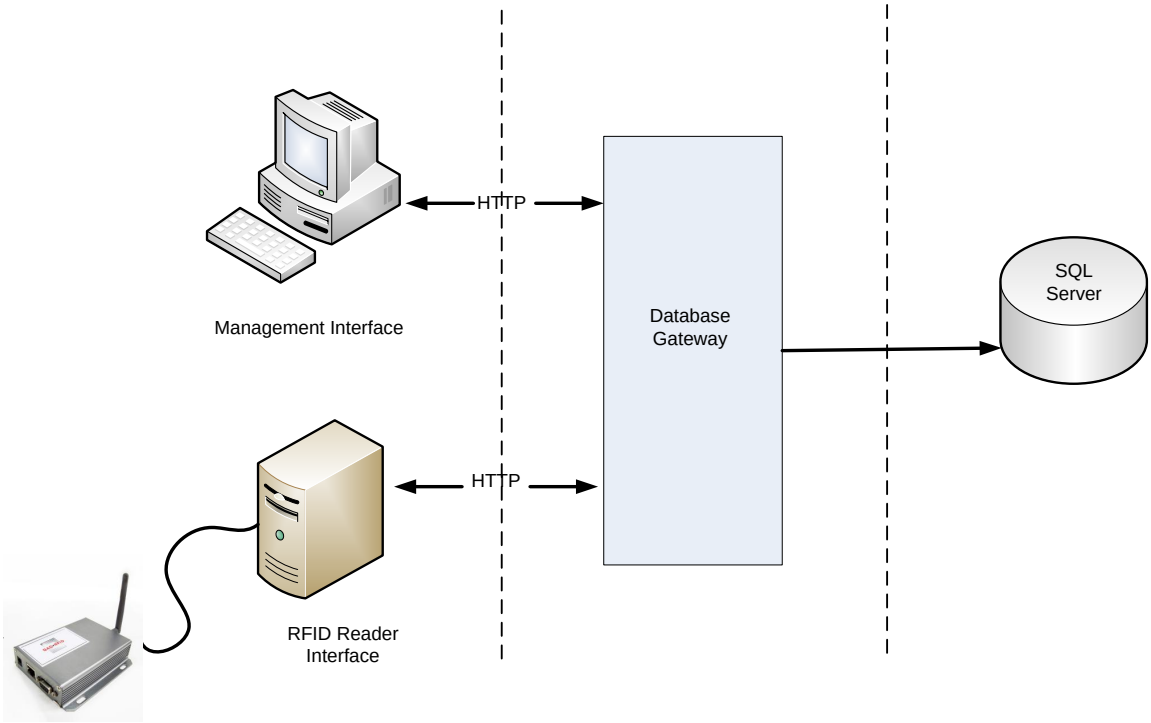

Figure 2.2: RFID Malware test platform [60]

The RFID information is usually sent to the back-end database for checking, and this is where the problem occurs. It will delete one of the database tables. This leads to corruption of the whole system. Another example is when an attacker might inject a malicious code into an application using any script language to get some information. RFID tags, which are used for tracking baggage in the airport, have a plethora of

information such as airport destination in its data field. When the tag is read, a query is sent to the back-end database system to get the information about the destination and destroy the system. Malware can infect any station within the system that is shown in Figure 2.2. [60]

Viruses and worms are another kind of threat with respect to RFID tags. On the Internet, viruses and worms can propagate into personal computers when relying on a network connection that is compromised. The same thing can happen when relying on an RFID tag and one therefore neglects the scanning mechanism of RFID.

RFID worms, which are considered a kind of malware, are downloaded from remote sites. Then upon the execution, they try to change the functionality of the RFID systems. In the case of RFID viruses, an Internet connection may not be needed as they have the capability of self-replicating. The virus can basically be located on an RFID tag, and then it propagates upon reading of the infected tag to corrupt the back-end database or any other part of the RFID system.

To make it clear about the problems faced when a hacked RFID is used, the following real-life scenario is cited. An attacker went to a supermarket and purchased some items (supermarket uses RFID tags rather than barcodes). Then, outside of the store, the attacker was able to remove the original RFID tag from items and attach fake RFID tags that carried a malicious code. After a while, the attacker went back to the supermarket to return those items with (now) fake RFID tags. This, of course, involved scanning of the infected tags by the supermarket RFID readers and the embedded malicious virus can then cause corruption of the back-end database of the supermarket. [59, 60]

Some designers have proposed techniques for making a new kind of tags that are "read only" tags with the hope that no one will be able to modify them. However, this technique still has a limited capability to solve the problem because an attacker can fake blank tags to carry his/her malicious code. Another proposed solution to resist this kind of attack is to limit the number of bits on an RFID tag. This is still not a sufficient solution because there are many SQL commands that require only a few numbers of bits such as a "shutdown" instruction that contains nine characters, or 63 bits. [59, 60]If this code is executed, the system will crash.

- **Sniffing or eavesdropping**: refers to intentionally listening to a private conversation between a reader and tag such as an ID. There are two types of sniffing attack: passive (any signal is not emitted by an attacker and not modify the message stream), and active sniffing (an attacker modifies, deletes, injects, or replaces and replays messages). [1, 6, 83] These will compromise the integrity and the confidentiality of the RFID system. Personal identities can be revealed to anybody who is equipped with a tool to get the information. Competition can find what you are shipping/ receiving. The possible distances at which an attacker can listen to the messages exchanged between a tag and a reader are categorized. [62, 63] See Figure 1.4 in Chapter 1.

  For example, when a reader sends signals to a passive tag for data exchanging, it powers the tag. In this case, the connection between them will be eavesdropped by another reader that in turn, can monitor the resulting emissions. [2, 5] This attack can be eliminated by limiting the distance between tags and readers. This can also be done by using a metal screen to shield the communication between tags and readers, and by encrypting the data. [6]

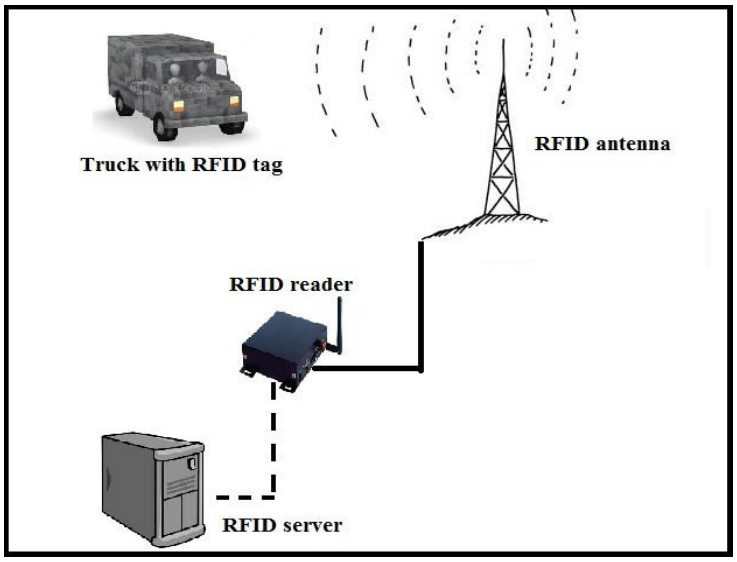

Figure 2.3: Tracking System

- **Tracking and Tracing**: when an attacker sniffs an ID of a tag, this ID can be used to track the holder of that tag and determine the location of the item. Also, this attack can be achieved when the response of the tag stays the same (the same identifier). See Figure 2.3. This attack compromises the privacy of people or assets. Imagine your glasses have an RFID tag that stores a 96 bits identifier. With this, an attacker can follow your movement and know the places that you visit. Also, the attacker can place several readers in your favorite store to learn your favorite items. Several techniques are used to combat this type of attack. Mutual authentication between readers and tags, shielding tags, killing tags after using them, and scrambling the ID of the tag are some of the ways to combat this attack. [6, 63, 65]

- **Spoofing**: attackers can imitate real RFID tags after collecting data from an eavesdropping attack. An attacker can also retag items; for example, a tag that corresponds to lower price can be replaced with one having a higher price before returning the

item on which the tag is attached. This simple switch can fool an RFID system and compromise the integrity of the system. Some researchers have proposed a solution to this problem. [1, 66]

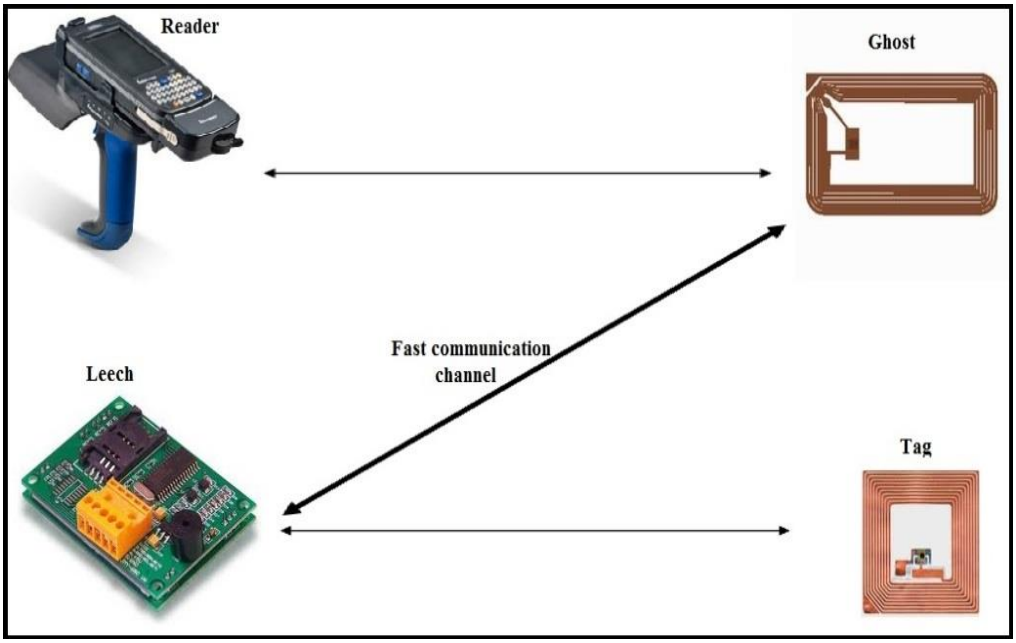

Figure 2.4: Replay Attack [63]

- **Replay attacks**: an adversary can impersonate a real reader or tag to capture some packets exchanged between two hosts, and then retransmits them at a later time. This kind of attack compromises the integrity and confidentiality of the system, for example, with garage door openers. In Figure 2.4, there are two attackers in the system (represented by "Ghost" and "Leech"). The ghost places the tool near from the door's reader and the leech places the tool near a person who has the tag. By getting the

information from the tag and making the communication between the ghost and the leech very fast, the ghost can open the door. Cryptography techniques, which are the ability to exchange information between entities in a secret way using keys to prevent an unauthorized entity from reading it [83], are not appropriate solutions to overcome this type of attack. However, some authentication techniques are required to combat this attack by using a password. [63, 64]

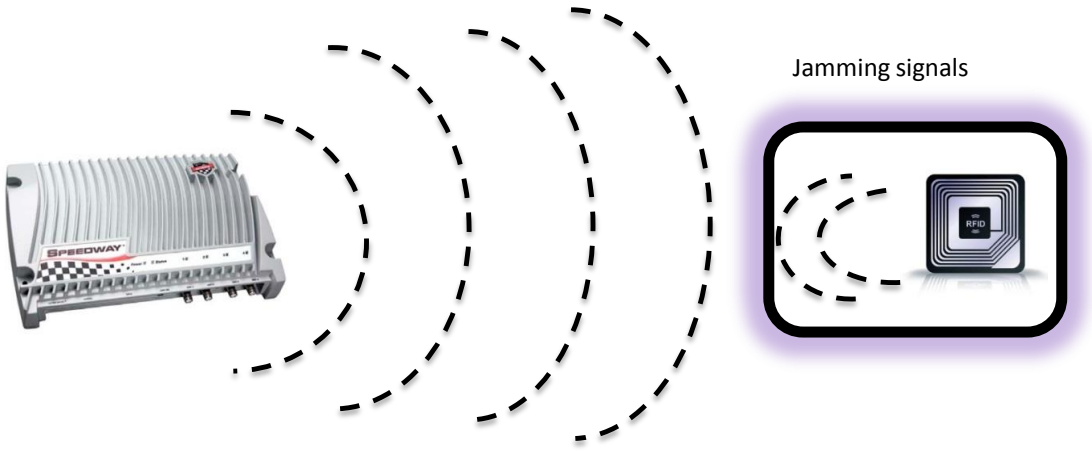

Figure 2.5: Jamming Radio Frequency

- **Denial of service (DOS)**: it denies service to valid users. This attack is easy to accomplish with a jamming frequency. See Figure 2.5. In one technique, a shoplifter carries a blocker tag, which is a passive RFID device that uses a sophisticated algorithm to send jamming signals to disrupt reader communication. When a reader tries to send a query to a tag, it cannot read the tag. In second technique, an attacker can shield the tag from being read with a Faraday Cage, which is a metal enclosure lined with

aluminum foil that prevent the reader from reading the tag. In third technique, an attacker with a powerful reader jams the reader by creating a more powerful return signal than the signal returned from the active tags. It is very easy to provoke RFID tags to communicate by an attack. In this case, the battery of the active tag will be discharged so, it can no longer communicate. Therefore, when authorized readers try to communicate with the tag, the tag is not going to respond; it will be in sleep mode. In fourth technique, attackers can remove tags from items and block RFID readers query signals. In fifth technique, they can flood the system with more information than it can handle or remove a tag from an item and put it on other item causing wrong operation in the system. These attacks compromise the availability and usability of the RFID system. [1, 66]

- **Cloning**: this is another type of spoofing. It can be tag cloning or reader cloning. In tag cloning, a tag can be duplicated, which may be similar in size or much larger than the original one, to abuse private data or to get a restricted area. In reader cloning, an attacker can duplicate an authorized reader. Authentication techniques such as fingerprint or authentication techniques are used to combat this type of attack. [1, 6]

- **Buffer overflow**: this type of attack occurres when the data exceeds the length of the memory. Some programming languages are not memory safe for example, the C and C++ languages. When a program is executed, the length of inputs is not checked. Because tags have a limited storage capacity, the buffer overflow may lead the program to execute an arbitrary code. [63]

- **Tampering with data**: this occurs when an attacker modifies, adds, deletes or re-orders data. For example, an adversary can modify the tag in a passport to contain the

serial number associated with a criminal. Also, an adversary can modify a passport tag to appear to be a citizen in good standing. Another example of modification is when an adversary changes a high-priced item to a lower priced item.

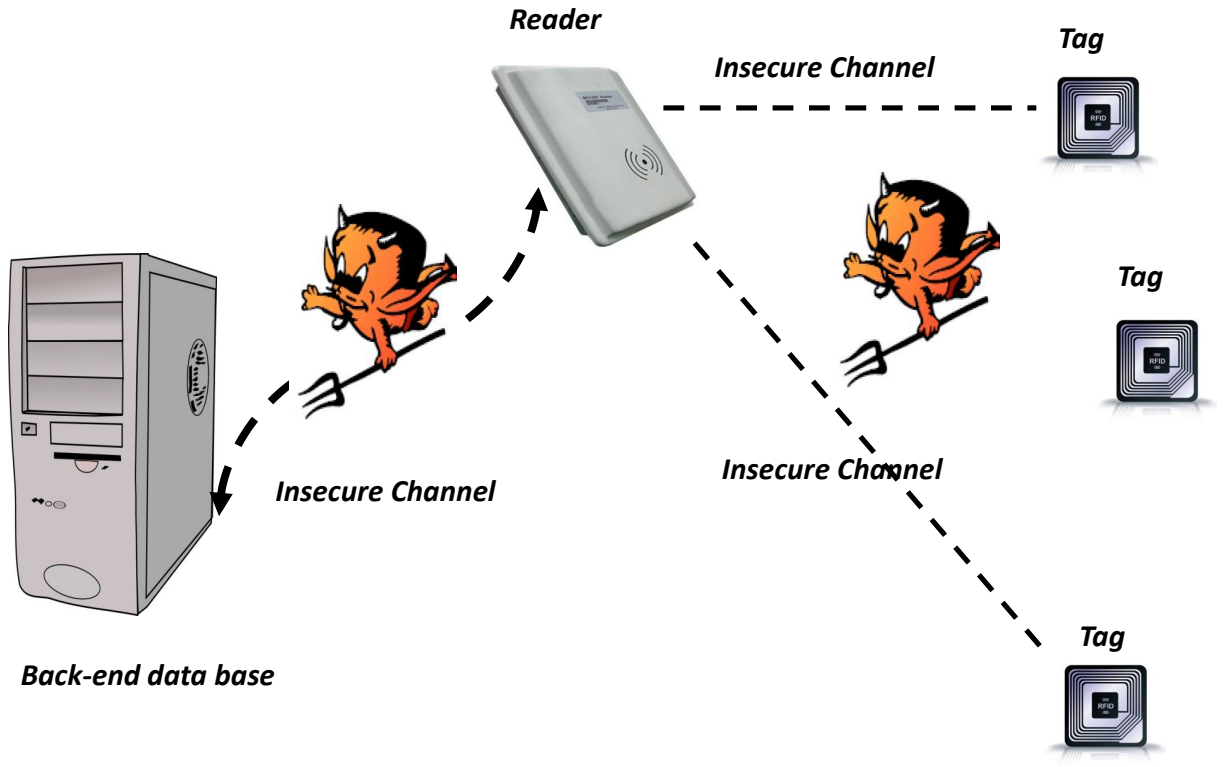

Figure 2.6: Man-in-the-middle Attack

- **Man in the middle**: attackers are able to place their devices in the middle of two hosts that are communicating and exchanging some information (i.e. a legitimate RFID reader and tag). See Figure 2.6. An attacker records and replays the information that could be changed (inserted, deleted, or modified). The main goal of this attack is to make an RFID reader think that a certain tag is in place when it is not. Some approaches have been proposed to deal with this attack. For example, a reader could

add a disturbing signal to the tone making it very difficult for the attacker to recognize the signal. [1, 6]

For adding, additional tags can be added in a shipment to make it appears to have more items than it does. For deleting, an attacker can remove or physically destroy tags attached to objects to avoid tracking. For reordering, an attacker exchanges a high-priced item's tag with a lower-priced item's tag. [63]

An RFID reader can be also compromised. There are two types of revocation: explicit and implicit. Explicit revocation is when an RFID reader is lost, stolen, or compromised. An attacker who has the compromised reader can use it to identify and track tags. Implicit revocation is when a reader certificate expires naturally. Usually, the certificate expiration of readers is checked. If the reader is compromised before the certificate is expired, the reader should be revoked from the system. So, explicit revocation is revocation before expiration and implicit revocation is certificate expiration. [67]

2.2.2 Some proposed solutions:

Many researchers have proposed providing some security, authentication and privacy between tags and readers because RFID tags are easily target for malicious attacks. This section details solutions to prevent the above attacks on RFID system.

EPCglobal [17] defined some protection methods such as Application Level Event (ALE), Reader Protocol (RP), Low Level Reader Protocol (LLRP), Reader Management (RM), and EPC Information Services (EPCIS). [17]

To prevent a sniffing attack, tags that are not used anymore should be put in a shielded

enclosure. However, this solution is not effective if the tags should always be available for legal queries. Another proposed method to enforce privacy and security on tags is the use of "kill" or "sleep" commands. 32-bit kill passwords should be supplied by an interrogator to kill a tag. However, these commands are unsatisfactory because consumers may want RFID tags to remain responsive. [17, 31, 82]

One of the drawbacks of using cryptography to prevent threats is the extra cost; it is more expensive and it needs more computational capabilities and it uses more power consumption, especially for passive tags because they don't have an internal energy source. Some designers have proposed techniques for making a new kind of tags that are "read only" tags with the hope that no one can modify them. However, this is still a limited solution because an attacker can fake blank tags to carry his/her malicious code. Another proposed solution is to limit the number of bits on an RFID tag. This is still not a sufficient solution because there are many SQL commands that require only a few numbers of bits such as a "shutdown" instruction which contains nine characters or 63 bits. [59, 60]

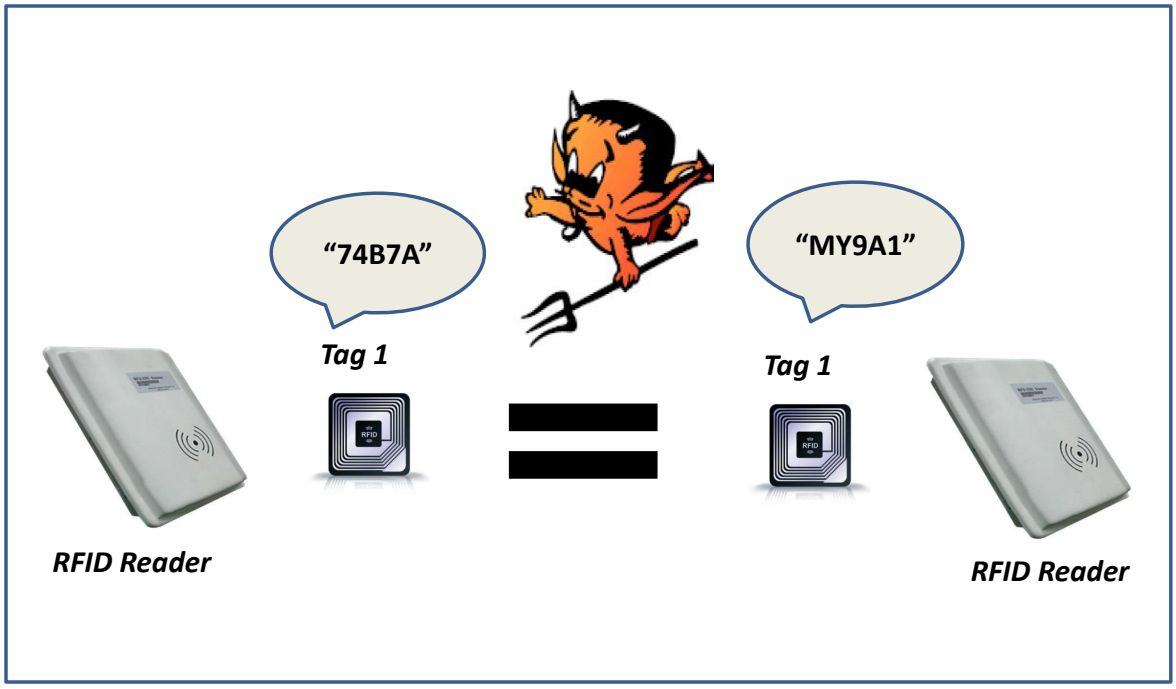

Figure 2.7: Minimalist Cryptography Technique

Juels designed a minimalist cryptography approach using a small portion of rewritable memory and very limited resources. See Figure 2.7. He proposed that each tag have a small number of pseudonyms. Then, for each query from a reader, a tag will release one of its pseudonyms and then rotate them. This makes it hard for an adversary to associate any tag with a particular object. The reader would store all the pseudonyms read from the tag for identification purposes. So, if an unauthorized reader does not have all the pseudonyms of the tag, there will be no matching between different pseudonyms of the same tag. [5, 68] Juels further proposed a method to prevent unauthorized readers from harvesting all tag pseudonyms by slowing tag's response when it is queried quickly. Minimalist cryptography

is not perfect for real world deployments, but it can improve a tag's ability and provide privacy and mutual authentication between the reader and low-cost tags. [69, 70] This design still has vulnerability compared to other approaches such as maximalist cryptography and Shoehorning security.

Minimalist cryptography approaches use limited resources so that some resources are left unused. In addition, minimum cryptographic operations are used. However, maximalist cryptography approach proves that symmetric cryptography is sufficient on an RFID tag, so security is maximized using low power microcontrollers. RC5-32/12/16, which is a symmetric block cipher used to encrypt and decrypt data, is applied on Wireless Identification and Sensing Platform (WISP) UHF RFID tag because it is simple, needs low memory and provides high security and a balance between security and performance for sensor networks. [71, 107] In addition, in this method used a T1 MSP430F1232 microcontroller-based RFID tag because of its low cost, low power consumption and it is wirelessly powered. Also, it is used for RF or battery power application. This approach calculates how much computation can be used. Smith presents in detail WISP units that consume low power. [72] This technique demonstrates that strong encryption can be performed on a tag and maximum security can be achieved.

Shoehorning is another technique for providing security. It focuses on providing an authentication protocol rather than privacy using memory as input/output for cryptographic model in a tag. [73] This method is like what Juels proposed. [69] He enhanced the using of PIN-controls for killing and read/write to provide an authentication in Class-1 Gen-2 EPC tags. However, his method can be attacked by eavesdropping attacks.

Shoehorning techniques use the same idea, but in a different way to provide a stronger protocol within the EPC standard. It uses a challenge-response protocol to prevent the

cloning of a password because when a reader sends a command, which requests the tag's password, this password can be attacked. A reader and a tag should share the same secret key. In addition, instead of sending a challenge from a reader to a tag, the tag can choose the time of day as a challenge if the tag has a real time clock. ISO Standard 7816-4 offers many commands used for authentication and accessing stored data. So, shoehorning uses an Internal Authentication command from ISO 7816-4. Also some means are used to reduce the cost by compressing ISO 7816-4. The idea of this is, if a challenge CR is implicit, that means there are some bytes that are not used in the command, so that they can be eliminated. The data field is about 512-bits; 32-bits are used for the password, so it still has space for stronger authentication. According to Bailey [73], readers can respond to a challenge for getting stronger authentication.

Most approaches are used depending on logical layer authentications. Cryptography is better than just using a password because an attacker can eavesdrop it. However, cryptography is not a suitable solution against attacks because of the problem of key management. Moreover, public key cryptography is a good solution, but it does not eliminate the fact that a tag is very cheap for applying some algorithms. Using a Challenge-Response protocol approach can eliminate an eavesdropping attack. However, the biggest problem in RFID is providing database authentication and privacy because some RFID tags can be cloned. So, a good tool needs to be provided to protect the tag. A fingerprinting approach is used for that reason because the duplication becomes very hard. However, it still has one drawback that it depends on direct optical contact, which denied the benefits of X-ray vision that RFID grants. [74]

Although many researchers have proposed protocols to provide security and privacy between RFID readers and tags, RFID tags are still exposed to cloning. One reason for this

is the limited computational capabilities of the RFID tag. For example, the contents of a tag's memory can be copied and the same data can be injected into a new (counterfeit) tag. To prevent the cloning of tags, protection techniques can be used on a tag to prevent their memory contents from being read. However, this involves extra tag cost. [76] The researchers at University of Arkansas have developed a robust method to prevent cloning of passive tags by using the fingerprint technique based on some physical attributes of a tag, then applying some applications of multi-class learning to classify the tags. An individual tag is unique because of RF and manufacturing. [75] An algorithm was used to measure the minimum power response of each tag by a sending radio frequency emitted by the reader to the tag starting with the lowest frequency and increasing it step-by-step until the tag will send a response. At a result, each tag has a unique power response for activation. This unique physical characteristic can be used in the fingerprint technique without increasing the cost of tags. RFID fingerprint data is stored in back-end database indexed by the ID of a tag or sometime stored in the tag itself. [77]

In general, anti-counterfeiting used to prevent cloning has two phases. See Figure 2.8. The first is an enrollment phase. Some trusted authority performs this phase by deriving several fingerprints and recording the response. Then, these data are signed using a secret key. All these data are printed on the product. The next phase to prevent cloning is the verification phase. The devices read all data and perform the fingerprint technique after measuring the responses to check if data has been printed by a legitimate authority, or not. [76]

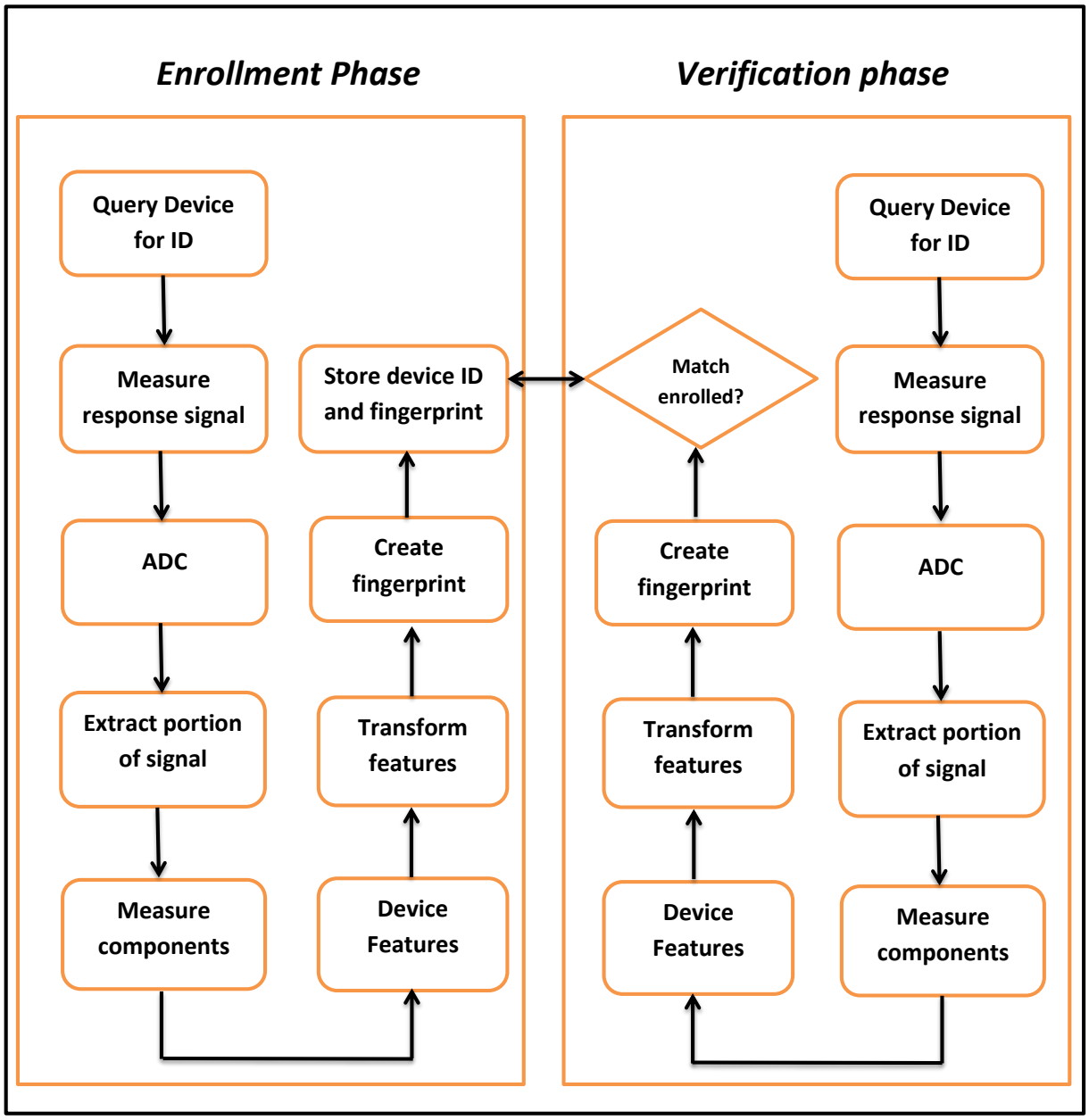

Figure 2.8: Anti-counterfeiting phases [79]

Every tag has physical-layer features which are considered as a unique identification so that they can be taken as fingerprints of tags. It is very hard to make a tag with the same fingerprint as the original one because the variations are very difficult to reproduce. Extraction techniques of the fingerprint are not expensive and it can be performed using a low-cost purpose-build reader. Moreover, there are some classification systems that are used to associate unknown RFID tag fingerprint to previously defined classes. One of these systems is neural network approaches, which is one of multi-class learning techniques. As mentioned, the fingerprints of tags are stored in either back-end database or in the chip. [78]

Some features can be used as a fingerprint: minimum power response at multiple frequencies, timing, phase or transients. An individual characteristic becomes like a secret key. [79] Some have used the transmission time of EPC, PC, and CRC to distinguish individual UHF passive RFID tags. [80] Then from the captured signals, the information was extracted using MATLAB script. The data is classified using a K Nearest Neighbor algorithm (KNN). Also, fingerprint RFID tags are based on the minimum power response which is the power required to activate tags. [77] The results prove that every tag has a unique minimum power response, which is a feature of the tags fingerprint.

There are some methods for extracting the feature of a tag. Danev'research [78] was the first study about extraction of RFID physical layer fingerprints. According to their results, the authors proved that a tag can be accurately identified; detecting of cloned tag is easy; and the extraction of the fingerprints is inexpensive and could be applied with a low-cost, purpose-built reader. They based this on the extraction of the modulation shape and spectral features of a tag's signal. A hardware setup is used to capture the signals from tags and then record them to oscilloscope. For feature extraction and matching, Principal Component Analysis (PCA) is used. With respect to the "Timing Feature", which is defined

in [78] as "the time interval within which the tag responds to a wake-up command (WUQ) and the duration of that response", it is also used to identify RFID tags.

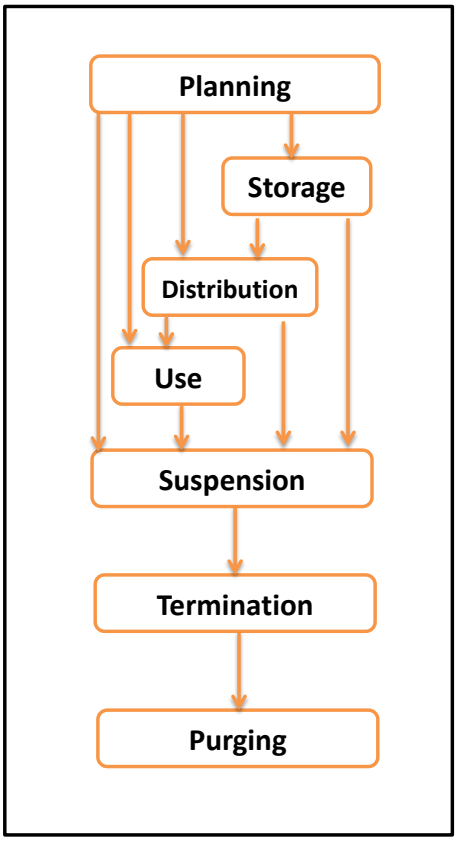

Figure 2.9: Key's life-cycle [84]

2.3 Key management

Key management is the basis of cryptography and it is an authenticated service. It is very important to secure set of operations of any cryptosystem and to sustain encrypted data with the keys during the key life-cycle. There are eight stages in the key life-cycle which are: planning, key generation, key storage, key distribution, key use, key suspension, key termination, and key purging. See Figure 2.9. [84]

The first two stages for planning and generating key are when an entity involves in an organization and becomes an authorized member. The use of the key management is to facilitate the operational availability of keying material for standard cryptographic purposes. The storage stage depends on the type and protection requirements. There are three types of storage, which are operational, backup, and archive storage. For example, operational storage is used when keying material are stored for normal cryptographic operation during the cryptoperiod of the key. The backup storage provides a source for key recovery. The key archive storage is a repository having key management of historical interest. In key termination stage, before removing a key from any organization, a reason for the termination should be determined. This includes key compromise, removal of an entity from an organization, etc. [85]

The most important part in key management is Key Management Audit because it records all the operations of the key management associated with keys. It tracks all the actions of key management, audits the conditions of using keys, and audits the changes of key life cycle state. [84] However, there are some difficulties to manage and track keys of systems. These difficulties are related to distributing keys, verifying the shared key, key storage and validity checking. So, the Key Management Service helps with the scaling problem of managing an increasing number of keys. The security of any system depends of the strength of the keys, the techniques, and the protocols that are used to protect the keys from modification by unauthorized disclosure. [81]

Distributing keys through a network should take place on secure channels. Some researches have been proposed to manage the distribution of keys between parties. A secret key is used to lock a part of the tag's memory. [17] This keeps the tag safe from tampering with the content of the memory, but does not keep the content safe from unauthorized read-

ers. Also, it can be used for killing the tags. However, it is very challenging to initialize the keys and propagate them to point-of-sale devices. [82]

There are three classes of cryptographic algorithms. These are hash functions, symmetric key algorithms and asymmetric key algorithms. Hash functions generate small hash values as an output from a large input value. This ability of hash functions is called "Compression". Adversaries cannot get the original input from the output. This function does not require keys. It has many benefits such as: generating a random number, deriving a key, compressing messages and the like. [16, 81, 83]

Symmetric-key cryptography is suitable for use in a closed system for encryption and decryption. It can provide security for RFID systems. It transforms any input data using a secret key that should be applied on the output to get the original input. A secret key should not be revealed to unauthorized entities. This kind of cryptography provides authentication, integrity and confidentiality, and generates random numbers. [16, 81]

Asymmetric key algorithm or Public-key cryptography is more suitable for open systems, since both RFID readers and tags can use their public keys to protect the security of RFID systems. It uses two keys (key pair: a private and public key). Anyone can know the public key, but the private one should be kept secure by the entity that owns that key pair. This algorithm can compute a digital signature, generate random numbers, and so on. [16, 81]

Key management should be designed in an appropriate way to eliminate the effect of a compromised a single key onto the other keys. All compromised keys should be changed and all affected keys should be replaced. [81, 83]

2.4 Other solutions

In general, attackers are becoming smarter and computers are becoming more powerful. As described in Chapter Two and with respect to the RFID security and privacy, a number of threats, such as sniffing, tracking, spoofing, replay attacks and denial of service, are classified as a high level misuse of properly formatted RFID data. In the supply chain, the transportation of cargo can be monitored in the whole chain from manufacture to retailer. Also, because RFID has many benefits as described in Chapter One, the cost of the supply chain could be reduced and safety can be achieved. [1, 2] For improving the accuracy and reducing the time of processing, RFID can be used for store level inventory down to the item level. Also, it can be used to define if a product is in the wrong location.

The use of standardized assessment tools, technologies and process is essential for improving the supply chain security strategies. A track and trace system for all products throughout the domestic and foreign supply chain are a significant step in ensuring transparency and accountability of product manufacturing and distribution. This can be done by using RFID, which provides a secure identification and can quickly track a product at every point in the supply chain. [7]

Anti-theft security devices, such as RFID labels, also play a key role (as described in Chapter One) in deterring counterfeiting activity as well as detecting and monitoring the actions of would-be criminals along with the movement of goods into and out of a retail establishment. Chapter One lists many benefits for this technology in establishing an electronic pedigree. The FDA, for food defense, is focusing on moving from a reactive approach to a proactive approach to address intentional and unintentional food contamination. The FDA Combating Counterfeit Drugs identified several key elements for combating counterfeit

crimes and securing the nation's supply of drugs by providing technology and increasing criminal penalties, whereas the FDA food side is focusing on prevention and detection of the fraud. They both intersect in using technology, which are RFID and barcode, for tracking products. Also, they both can identify what products are likely to be counterfeited and entered into the legitimate supply chain, even if the prevention of that is impossible. [8, 9] All above reasons lead to the necessity of proposing methods or protocols to provide security in RFID system.

In the next section, a brief introduction of proposed protocols is going to be introduced. These will explain how RFID can be trusted for some applications, like the DOD, which has many sensitive products that are shipped.

2.4.1 Proposed protocols

Research has been proposed to provide some security, authentication and privacy between tags and readers because RFID tags are easily targeted for malicious attacks and because a tag has both limited computational capability and limited storage. Many crypto algorithms are broken, for example, DES was broken in 1998 and SHA-1 was broken in 2005. [84] In this chapter, an overview of the related work in the field of RFID is going to be introduced for providing authentication and privacy that can be used to increase the efficiency within the supply chain.

The first approach to provide privacy on tags is the use of "killing" or "sleeping" commands. 32-bit kill passwords should be supplied by an interrogator to kill a tag. In this case, the tag cannot be read by malicious readers. However, these commands are unsatisfactory because it will eliminate all benefits of this system and consumers may want RFID tags to remain active. For example, some smart machine "microwave" needs these tags to get the

time-to-cook information. Another example is a refrigerator that informs the owner that some normally kept items are absent. Sleeping commands are used instead of killing to keep the benefit from the tag by sending the readers PIN to activate and wake the tag again. However, managing this technique in practice is difficult. [5, 14, 17, 86]

Another approach that provides privacy is shielding a tagged item. This approach uses a radio wave-blocking material or scrambling of any outgoing signals from RFID tags. For example, any container made of metal can be used to block the signals. However, this approach has limited use because some items have very large shapes that cannot fit in some containers. [5] An active jamming approach is another technique for providing privacy. This can be accomplished by a device that transmits a signal to jam the RFID readers. However, this approach is not useful because it can cause interference with nearby legitimate readers if it transmits too high of a power signal. [5, 86]

Juels proposed another approach to deal with the privacy. This approach is using a "privacy bit" in a tag. After authentication using the PIN for a tag, a reader changes the bit in the tag from 0 to 1 or 1 to 0. 0 means that the tag is inside the store and 1 means that it is about to enter places with limited access. However, there will be another tag "blocker tag" that should interact with the tag to scramble the bits of all tags within the range. This approach provides privacy only with the presence of the blocker tag. [86]

There are other approaches that provide authentication and some provide authentication and privacy together. They focus on providing mutual authentication between tags and readers. However, they presume that the channels between readers and back-end database are secured. In addition, these approaches are still vulnerable to attack. Weis provides the authentication scheme between tags and readers using a hash function. [87] Each tag has a key and its hashed function, which is known as metaID. When a reader sends a query to a

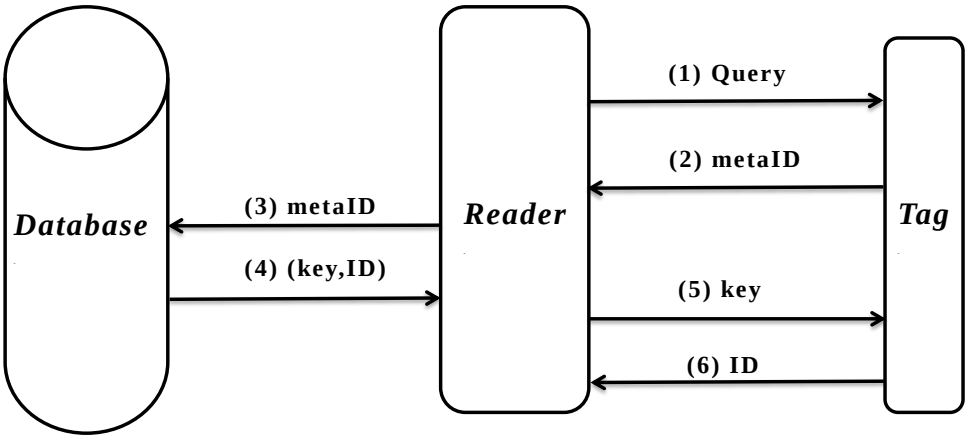

Figure 2.10: Hash-Locking: A reader unlocks a hash-locked tag [87]

tag for getting the tag's information, a tag sends metaID, which in turn will be forwarded to the database. In the database, metaID will be matched against the stored data and if there is match, the corresponding key and the ID of the tag will be sent to the reader. See Figure 2.10. The key is then sent to the tag that in turn, will apply the hash function on the received key and compare it with the stored one. If it matches, the tag will unlock itself. This scheme has three drawbacks: the metaID can be eavesdropped and copied into a fake tag. This can cause the reader to authenticate the fake tag.

The second drawback is the tag can be tracked using metaID because it is always the same. This can affect to the privacy of the holder. Third, the key and the ID are sent in a clear message that an attacker can easily obtain.

To prevent tracking the tag in the previous scheme, which is hash-locking, the same authors [87] improved the scheme by generating a random number (r) every time the tag received a query from the reader. Then, instead of sending the metaID, (ID_k, r) will be sent. So, this message will be different in every query. Then, the reader computes the hash

function for all IDs that are sent from the database with the random number r. If there is one match, there will be authentication between tags and readers. The problem in this scheme is r can still be eavesdropped with (ID_k, r) and used to make a fake tag to hold this information. Also, this scheme is inefficient because sending all IDs from the database to the reader will consume more time for calculations especially if the number of IDs is large; the computational cost for the reader will be linear. See Figure 2.11.

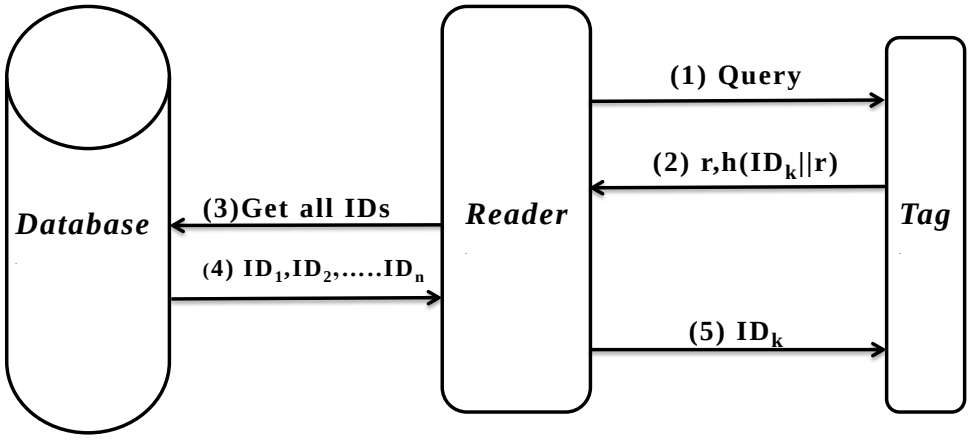

Figure 2.11: Randomized Hash-Locking: A reader unlocks a tag whose ID is k in the randomized hash-lock scheme [87]

A Privacy and Authentication Protocol for Passive RFID Tags (PAP) is another protocol that deals with a privacy and authentication for passive tags. [14] This protocol provides computation that can be applied in passive tags. The authors present four protocols used in four locations: inside a store, at a checkout counter, at a return counter, and outside the store. They used the random number and privacy bit concepts. Also, they assumed that there will be no malicious readers inside a store and an attacker cannot connect to the database to get the information of the tag.

The in-store and out-store protocols are very simple. The other protocols (checkout and return) have more steps to be applied between readers and tags. Each tag has a secret key (k), an ID, a privacy bit (0 means inside a store, and 1 means outside a store), and a generic name. In the checkout protocol, see Figure 2.12, the reader gets the shared secret key of the tag from the database by using tag's ID. Then, the reader and the tag will authenticate each other by computing the hash function between the random number and the key. If it matches with what they already have, the mutual authentication will be satisfied and the privacy bit will be changed from 0 to 1.

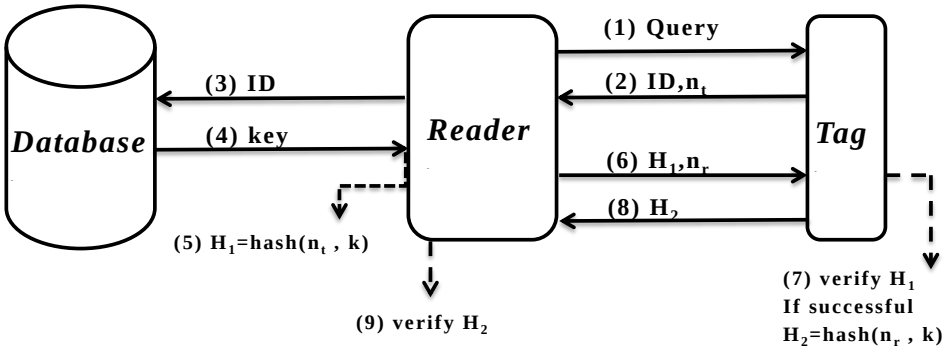

Figure 2.12: The checkout protocol in PAP [14]

The idea of the return protocol is the same. But, the privacy bit will be changed from 1 to 0 after satisfying the mutual authentication between tags and readers.

Still, these protocols are vulnerable to attack. Kim [88] proposed Improved Privacy and Authentication Protocol for Passive RFID Tags (IPAP) method for improving the PAP protocols because he found that each protocol in the PAP scheme is vulnerable. For example, for the in-store protocol, there is a possibility for an attacker to sniff the information. An

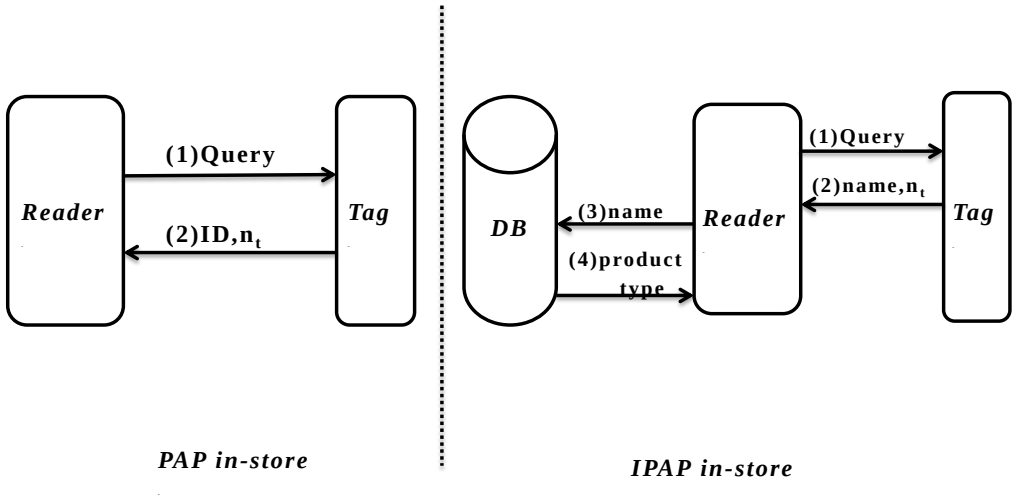

Figure 2.13: Comparison between PAP and IPAP in-store protocol [88]

attacker can get the information of the tag without connecting with the back-end database because a tag sends its ID when it receives a query. In this case, the attacker keeps the ID and compares it with the scanned one during the checking out. If they match, the attacker can obtain the information that is related to the purchased product of the consumer. So, the IPAP scheme for the in-store protocol does not transmit any information about the product in order to keep the privacy of the product. The name, which is not a unique identifier, will be sent instead of the ID. See Figure 2.13. However, the name, which represents the numeric representation of the product type, can be eavesdropped.

In addition, the return protocol in PAP has one significant issue, which is the tag sends its name to the reader that, in turn, will communicate with the back-end database to get the secret key of that tag. The problem is the name (or product type), which is the same for all identical products, and it is not the serial number. In this case, the reader performs a brute-force search to get the secret key of the tag.

IPAP provides a different concept. In this protocol, the first two steps are the same as

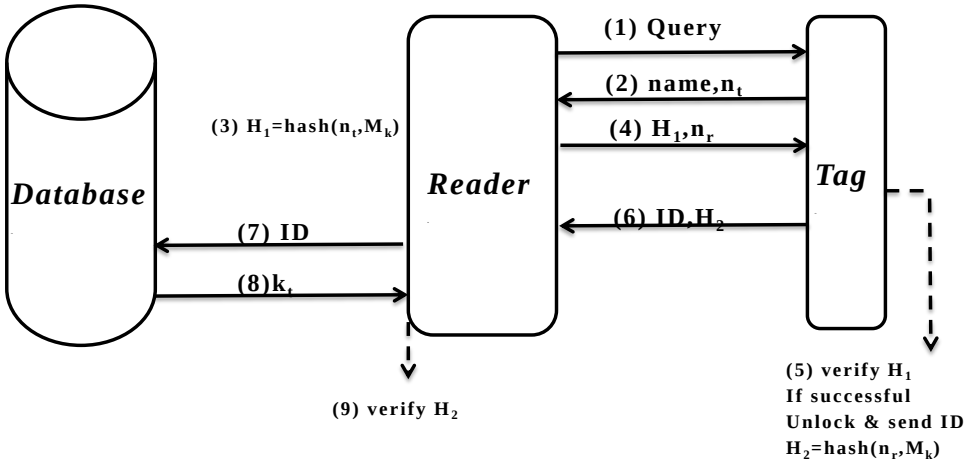

Figure 2.14: The checkout protocol in IPAP [88]

the IPAP in-store protocol. The difference is in the next steps. See Figure 2.14. A reader has the secret shared key of that tag and it computes the hash function and sends it to the tag that, in turn, verifies the results. After the verification step, the tag now sends it's ID. However, this is also vulnerable because an attacker can eavesdrop product IDs. All the previous methods to provide privacy and authentication have weak points and the channel between back-end database and readers are assumed to be secured.

A man-in-the-middle attack can be applied on this protocol to obtain the ID between tags and readers, and between readers and the backend database.

There are other solutions for providing security to an RFID system, but they are not suitable for passive tags because of the tags limited computational capability. To avoid that, one proposed solution uses external device to be carried during the day to provide security, but this is impractical. [89]

Another approach for eliminating the drawbacks of PAP protocol is RFIDGuard. [90] A kind of pseudonym challenge-response protocol is proposed in this approach. This research

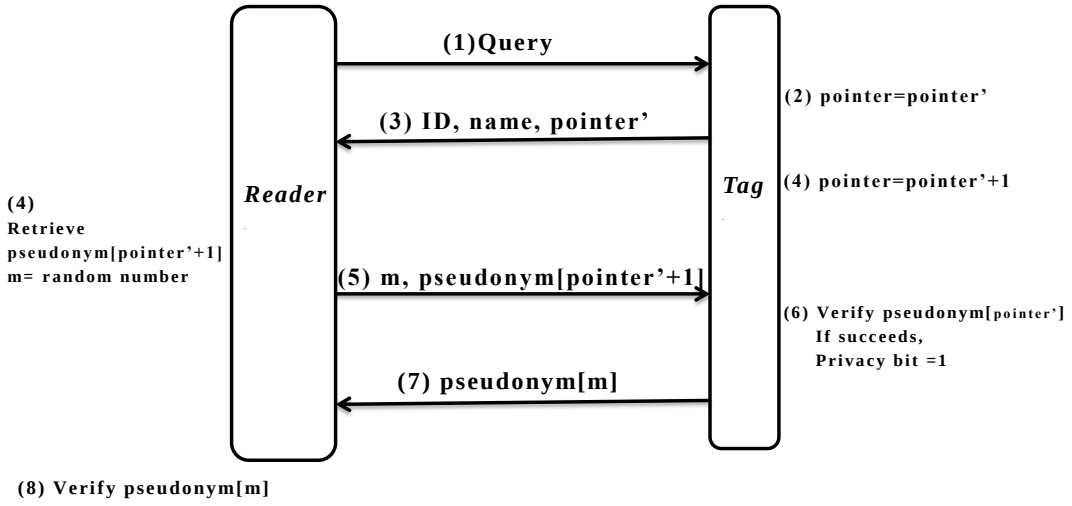

Figure 2.15: The checkout protocol in RFIDGuard [90]

uses the same idea of PAP, which has four protocols, but with procedures that provide more security while eliminating some drawbacks of PAP. Almost the same assumptions are used in this approach. One of these assumptions is an attacker cannot hide himself easily between the authorized readers and tags. Also, a privacy bit, a same list of pseudonyms for both a tag and reader, and a pointer for this list are used in this approach. When a tag receives a query from a reader, the tag sends the pointer of the list and ID of the tag. [90] See Figure 2.15.

Although this approach requires the passive tag to do a very small amount of computation and deals with privacy and authentication at the same time, still it has drawbacks. First, a malicious reader may exist within the range of interaction. Second, how many pseudonyms can a passive tag carry? Also, there are no details about the list of pseudonyms for example: if the pointer is at the end of the list, what does the tag do? Third, replay and man-in-the-middle attacks can be applied in the checkout and return protocols. An attacker can get the

information from the tag and forward it to the reader, and vice versa, until the attacker gets the ID of the tag in the last step of these protocols. In spite of sending the pseudonyms after XORing (XOR is a logic operation) with the random number that is established and shared between readers and tags, the IDs are not going to be XORed with the random number. They are sent in clear text. Fourth, in the checkout protocol, the tag sends its ID to the reader. In this case, an attacker eavesdrops and keeps the ID and compares it with the scanned one during the checking out. If they match, the attacker can obtain the information that is related to the purchased product of the consumer. This problem is the same as the problem in PAP. Fifth, the tag can be cloned by getting the list of pseudonyms. Although there will be difficulties in aligning the pseudonyms with their pointer, this approach can be vulnerable.

Hakeem proposed a novel key management protocol, which is Hacker Proof Authentication Protocol (HPAP), for providing mutual authentication between readers and tags and securing tags 'information. [95] He used time stamp, random number, hash function, encryption key, and Linear Feedback Shift Register (LFSR), which is a shift register its input bits is linear function of its previous state with using XOR. He simulated his protocol using C#.NET. However, this protocol has drawbacks, which are changing a key of a tag every time a reader sends a query to the tag, needs more computation in the tag and in the server, and require a number of time consuming arithmetic operations in LFSR. In addition, the key of the tags and the timestamps are updated using LFSR. Because LFSR has a finite number of possible states, it must eventually enter a repeating cycle.

Most of the proposed approaches focus on providing privacy and authentication between readers and tags. Also, they focus on how to avoid the counterfeiting of a tag. A major question is what to be done about the readers whether they are safe and whether they can be

compromised. Most of the above approaches assume from the beginning that the channels between readers and the back-end database are safe. RFID readers can be lost, stolen, compromised by an attacker, or decommissioned. In all of these cases, a reader should be revoked correctly and effectively from the system before an attacker gets the compromised reader so that he can identify and track tags.

As described in Chapter Two, there are two types of revocation: explicit and implicit revocation. The explicit revocation is when RFID reader is lost, stolen, or compromised. An attacker who has the compromised reader can use it to identify and track tags. The implicit revocation is when a reader certificate expires naturally. So, the explicit revocation is revocation before expiration and the implicit revocation is certificate expiration. [43]

Very few solutions are proposed to find a compromised reader, reader revocation, and expiration checking. [91] Some solutions for reader revocation techniques are: date register and time stamp, internal clock, on-line revocation, and so on. [93] The most important challenge is the way for revocation and expiration checking of the RFID reader certificate to be handled. Some approaches use Certificate Revocation Lists (CRLs), but these approaches are weak in public key-enabled RFID systems. [92] One of the reasons that make this approach weak is a passive tag has no clock. In this case, a tag cannot make sure that a reader's public key certificate (PKC) is expired or revoked. In addition, if a passive tag has an internal clock, it also cannot be used because the clock needs uninterrupted power to be sustained. Even for an active tag, it leads to problems such as: battery cost, clock synchronization, and battery replacement. So, it is difficult to manage the system without error. [93]

Public key cryptography infrastructure is used [94] to provide authentication between readers and tags. It uses also a digital signature that tags have for validating a product.

However, this approach is not suitable for an RFID system because it is complicated and needs high run-time complexity. Also, the disadvantages for using a public key cryptography infrastructure are the speed and it may vulnerable to impersonation after successfully attacking on a certification authority. In this case, using public key cryptography infrastructure is not necessary and using secret key cryptography can be sufficient. This can be done by monitoring and managing all keys in closed system by an appropriate authority. Threats on products are increasingly becoming prevalent because of huge financial motives. At any stage of a supply chain management from manufacturers to retailers, threats can be introduced. Using an RFID system is a suitable solution for eliminating some of the threats in different means. In next the chapter, a new approach is developed to provide privacy and authentication in the RFID system by addressing an application that is based on an electronic lock. This can be used to provide security for freight passing through customs and in international airports. In addition, this approach focuses on handling a compromised reader, not just providing security between readers and tags. Also, it handles key management and manages distributing the keys, and tries to eliminate some problems that can be found in distributing the keys. This developed model aims to provide security (privacy and mutual authentication between readers and tag) in the closed system with low computational requirements. Also, this model aims to detect and revoke a compromised reader from the closed system by an effective model.

Chapter 3

Methodology

3.1 The Application

Radio frequency identification (RFID) systems can be used in many applications such as supply chain management, theft and counterfeiting prevention, Department of Defense measures, passport control, Customs, and so on. Every entry in the supply chain is vulnerable to be attacked. It is necessary to develop solutions against possible attacks, which are discussed in Chapter three, in international ports and customs control points for incoming containers from land, sea or air.

Customs inspections at borders can lead to delays and additional logistics costs. The processes of container transportation are vulnerable to security threats such as counterfeiting. In this case, an RFID system can provide physical and contents security by using an electronic seal (eSeal). [104] It is used to guarantee the authenticity and the integrity of freight containers. Also, it is used to not just provide physical security but also to store information and different data for supply chain management. This information could be the seal ID number, the container ID number, an alarm function to inform in real-time, sensors to indicate the environmental status of the container content, etc. When any container moves from one port to another, there is no need to have a physical inspection where eSeals are used. This leads to increased efficiency of the whole process including reducing logistics costs, decreasing inventory stocks and increasing customer service levels. [101]

One type of eSeal, developed by Confidex, is used by Container Centralen (CC) on its fleet of 3.5 million CC containers to improve the quality of the CC Container pool, their capacity to detect counterfeit products, and to provide transparency in the supply chain. [102, 103]

For international cargo transportation, the cargo is loaded into some type of container and transported to a border customs control point like Hong Kong custom. At the border, the cargo will be inspected and cleared to enter the country. After inspecting the cargo, a decision will be made if the cargo is going to be rejected or accepted. [97] The above process needs to be accomplished quickly and accurately.

The application that is addressed by this research is based on an electronic seal that can be used, as mentioned above, to provide security for freight passing through customs. This can help to ensure that the cargo is kept safe (tamper free) and need not be opened for inspection at numerous border control points. In this scenario, either active or passive tags can be used.

RFID technology can improve the security and visibility of the customs process and also reduce the amount of time required for clearing each container through customs. In addition, an agency can record the path of the containers and the place and time of each inspection. This type of system is currently being used in the Hong Kong customs process and it can be expanded to cover other border control points because of the benefits that can be gained from the eSeal system. [97]

At each country border crossing, this application allows a number of readers to inspect the cargo seals. This will also be the case for international airports. The tagged goods are moved through different customs control points where an eSeal will be interrogated by the customs agency. The eSeal consists of a physical lock activated by a built-in RFID tag,

which allows the lock to be opened or kept closed by means of receiving a signal from a reader. The eSeal will be attached to the cargo container at the time when the container is filled and sealed. Then, ID numbers of the eSeal will be read from the tags via readers. The data are saved in the custom's database. This data includes a unique ID, key and other information. The system stores the eSeal ID number linked to the vehicle ID. Before the container can be unlocked, the eSeal must be unlocked via an electronic key, which is received from the back-end database. In addition, truck drivers cannot unlock the container because they don't have access to the electronic keys.

In 2011 the Hong Kong Customs and Excise Department (C & ED) used this technology to increase the speed of all processes of checking on cargo in their customs. In 2012, C & ED proved that using RFID system is an effective solution to provide security in freight passing through customs. They estimate that the RFID system reduced the time required to clear the containers in customs from 2-3 hours to 5 minutes because the containers have not been opened between their inspection at the border control points and their arrival at the airport. Also, the information about where the cargos have been is recorded during the transportation, as is and the time for the inspection. The custom officials know that the cargo containers are not opened during the transportation and the inspection at the border control points. To facilitate this custom inspection process, RFID readers can be installed at border control points and also international airports. A total of 38 readers are installed in the Hong Kong C&ED. [97]

ESeal provide a high level of tamper resistance. However, the security of the eSeal itself must be ensured. There are many possible attacks against the integrity and authenticity of eSeals. For example, a malicious party can generate a fake alarm to deceive the interrogator, sniff information about an eSeal by intercepting radio signals between eSeals and readers,

clone an eSeal and creating a device that cannot be discerned from a legitimate eSeal, and disrupt the communication channel by jamming or shielding. Currently, RFID eSeals do not provide any robust solution to these problems. [104, 105]

3.1.1 An attack scenario

There was a particularly extensive vulnerability assessment for eSeals in early 2005. Spoofing and cloning attacks were identified as potential data integrity threats to eSeals. [104]

Imagine two port terminals (A and B), each of which has many interrogators to read tags attached to cargo containers. See Figure 3.1.

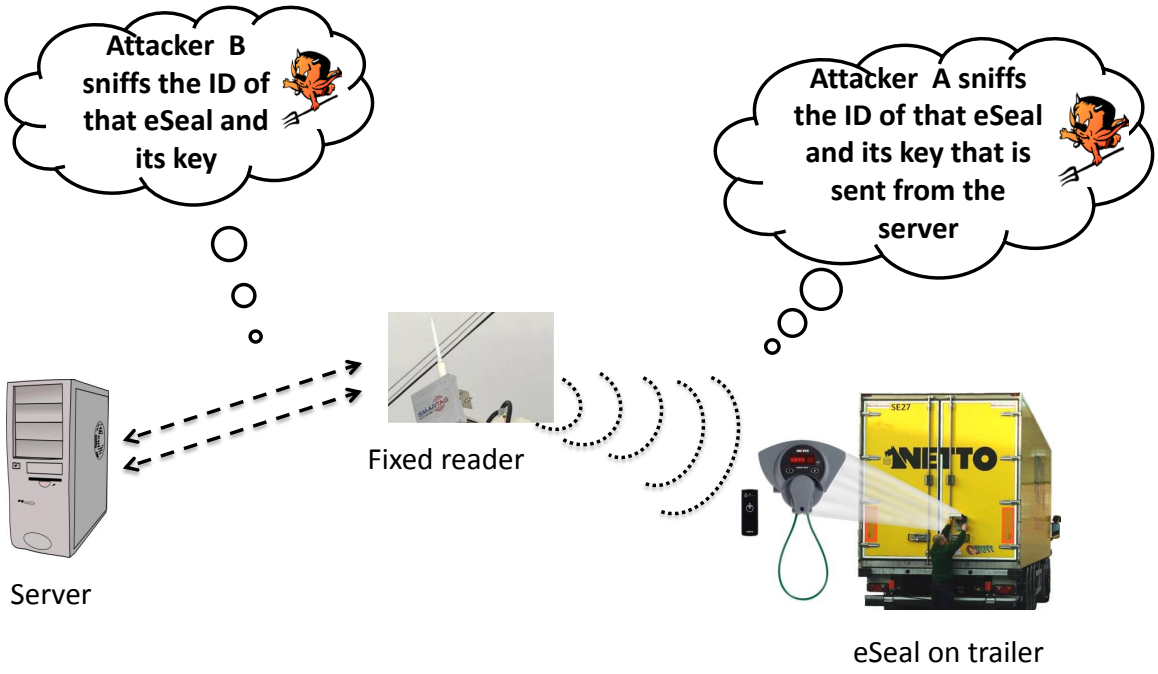

Figure 3.1: An Attack Scenario in Port A

When the cargo reached port A, the ID will be read from the tags via readers and then the ID will be sent to the database by the reader to get the key of that tag to unlock the tag. An eavesdropper with an antenna and some basic receiving equipment can gather the same RFID tag ID that is compiled by the reader at the port because the ID is sent in a clear message. After sniffing the ID, the key of that tag can also be sniffed because it is sent in a clear message. In this case, the cargo now will be tracked to know its location and also can be opened using the sniffed key. An adversary can steal large numbers of RFID data and then place the real data onto counterfeit RFID tags. This way, both the real and fake RFID tags contain legitimate information.

In Figure 3.1, the IDs and keys can be stolen. In addition, one of the readers installed at a border control point can be compromised, or lost as a result of some attacks. In order to solve the above problems and make the system secured by preventing counterfeiting, a communication protocol between an eSeal and an interrogator should guarantee the following security functions:

- Mutual authentication between an eSeal and readers
- Data confidentiality and data integrity
- Immunity to denial of service
- Replay protection
- Revoking a compromised reader

This can be done by developing a topology and three protocols for providing a suitable network and secured methods. [104, 105]

In summary, RFID systems can be used in customs control points because it has advantages such as anti-smuggling, improving cargo movement security, improving efficiency of customs clearance, getting real time information on the activities, and savings of cost and time. [98] In the remainder of this chapter, a developed system model is going to be introduced to manage the generation, exchange, storage, use, and replacement of keys. Also, new proposed protocols will be presented to provide mutual authentication between tags and readers and between readers and back-end database, to revoke a reader when it is compromised, and to add a new reader in the system.

3.2 System modeling

In total, there are four levels in the system: enterprise, facilities, reader and supply level. The enterprise level is the organization wide communication network that runs from the server down to all the readers. At this level, all tags are created and each tag has a unique ID and key. Also, it is the repository for all the information. The facilities level could be a node in the distribution system or the border crossing. The readers are the devices by which eSeal or tags can be read and they are directly connected back up to the facilities and the supply level that flow tags.

The eSeal system architecture (The governing information control system) consists of a main server (enterprise level) and a set of sub-servers (facilities level). Each sub-server is connected to a number of RFID readers. Further, every reader may read thousands of tags inside the network. The goal for the system is to provide mutual authentication between servers-readers and readers-tags. Because all tags in this system have a unique key, the whole keys should be stored in the main server and then any authenticated reader in the system

can get a key of a read tag from the main server. In addition, if there is a compromised reader, it will be revoked in an efficient way from the whole system without affecting the rest of the system by developing a model to manage this problem.

Before starting to explain the developed protocols, a system model should be designed to solve what computer scientists refer to as "key management problems" and to manage the communication function between servers and RFID readers by providing privacy, integrity, and authentication. As seen in Figure 18, a tree key graph model can be used to implement the RFID system in customs control points because a compromised reader may need to be revoked from the system or a new reader may need to be added in the system. [96] New keys will be created and shared to facilitate the process.

3.2.1 The Tree Key Graph

The system is designed based on the concept of a tree key graph because it is scalable to large groups. [96] Their secure group system consists of a set of users (U), a set of keys (K), and R which is the binary relation between U and K (user-key relation which means that the (user, key) is in R). See Figure 3.2. Each user has an individual key which is shared only with the main server; for example: u_1 has the key k_1. Also, there is the main key, which is k_{1-9}, and the group keys, such as k_{123}, k_{456}, and k_{789}. When the server sends a message to the first group, it will be encrypted using k_{123}. In the border customs scenario, the main key would be the government master key, the group key would be the individual custom station key and the user keys would be the readers keys used at each customs stations. The advantage of the group keys is to reduce the number of messages that the server sends because each message sent adds time to the encryption and decryption functions and therefore slows the system down.

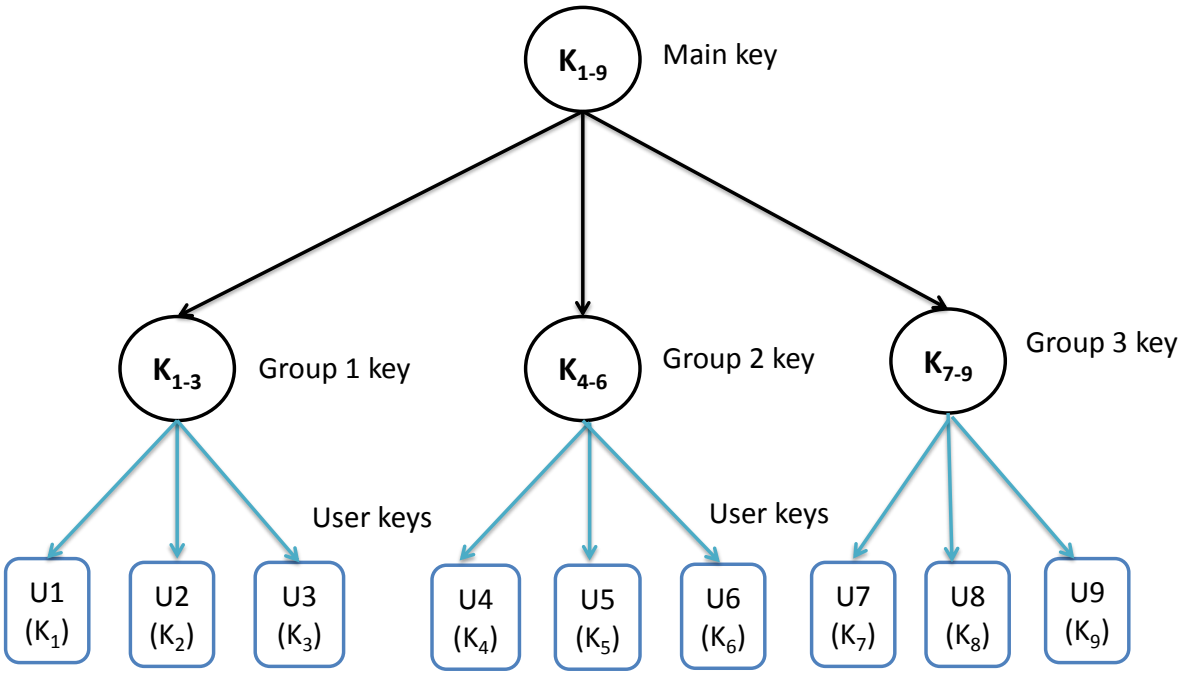

Figure 3.2: A tree key graph [96]

Every time a user joins or leaves, new keys are created and sent to the client. The number of messages that the server sends depends on the number of users the system has. For example, if u_9 is revoked from the system, the server creates a new group key instead of k_{789} and main key instead of k_{1-9}. Then, these keys will be encrypted before sending them. In Figure 3.2, when u_9 leaves the system, the server will send the following messages: a new group key k_{78} to the u_7 and u_8 encrypted by using their individual keys (k_7 and k_8), and a new main key k_{1-8} to the first group (1,2,3) and second group (4,5,6) encrypted by k_{123} and k_{456} respectively. Then, it will send another message which has the main key (k_{1-8}) to the third group (7,8) encrypted by a new k_{78}. The same above process will be applied when

a new user joins the system.

To construct and send the rekey messages within the system, three different approaches are considered [70].

1. **User Oriented Rekeying:** The idea of user oriented rekeying is that for each user, the server constructs a rekey message that contains the new keys needed by the users and encrypts them using a key already held by the users.

   For joining the system, if a user u_{10} is added to the system with the group (7, 8, 9), the following messages are going to be sent by the main server:

   - The server sends to the users (1-6) the message (k_{1-10}) encrypted by k_{1-9}
   - The server sends to the users (7,8,9) the message (k_{1-10}, k_{78910}) encrypted by k_{789}
   - The server sends to the user (10) the message (k_{1-10}, k_{78910}) encrypted by k_{10}

   For a user leaving the system, for example u_9, the following messages are going to be sent by the server:

   - The server sends to the users (1,2,3) the message (k_{1-8}) encrypted by k_{123}
   - The server sends to the users (4,5,6) the message (k_{1-8}) encrypted by k_{456}
   - The server sends to the user (7) the message (k_{1-8}, k_{78}) encrypted by k_7
   - The server sends to the user (8) the message (k_{1-8}, k_{78}) encrypted by k_8

2. **Key Oriented Rekeying:** Each new key is encrypted individually. The server constructs multiple rekey messages as per the needs of each subgroup. The users of each group receive a rekey message containing precisely the new keys that each group needs.

For joining the system, if a user u_{10} is added to the system with the group (7,8,9), the following messages are going to be send by the server:

- The server sends to the users (1-9) the message (k_{1-10}) encrypted by k_{1-9}
- The server sends to the user (10) the message (k_{1-10}) encrypted by k_{10}
- The server sends to the users (7,8,9) the message (k_{78910}) encrypted by k_{789}
- The server sends to the user (10) the message (k_{78910}) encrypted by k_{10}

For a user leaving the system, for example u_9, the following messages are going to be sent by the server:

- The server sends to the users (1,2,3) the message (k_{1-8}) encrypted by k_{123}
- The server sends to the users (4,5,6) the message (k_{1-8}) encrypted by k_{456}
- The server sends to the user (7) the messages (k_{1-8}) encrypted by k_{78}, and (k_{78}) encrypted by k_7
- The server sends to the user (8) the messages (k_{1-8}) encrypted by k_{78}, and (k_{78}) encrypted by k_8

3. **Group Oriented Rekeying:** Here the server constructs a single rekey message containing all new keys. This rekey message is then multicast to the entire group. This technique has a number of advantages compared to the other techniques. One, there is no need for a subgroup multicast. Second, with fewer rekey messages, the number of messages are reduced. Also, the total number of bytes transmitted by the server per join/leave request is less than those of the other approaches. [96]

For joining the system, if a user u_{10} is added to the system with the group (7,8,9), the following messages are going to be sent by the server:

- The server sends to the users (1-9) the messages (k_{1-10}) encrypted by k_{1-9}, and (k_{78910}) encrypted by k_{789} - The server sends to the user (10) the message $(k_{1-10}$,$k_{78910})$ encrypted by k_{10}

For a user leaving the system, for example u_9, the server sends to the users (1-8) only one single rekey message $(k_{1-8})_{k_{123}}, (k_{1-8})_{k_{456}}, (k_{1-8})_{k_{78}}, (k_{78})_{k_7}, and (k_{78})_{k_8}$

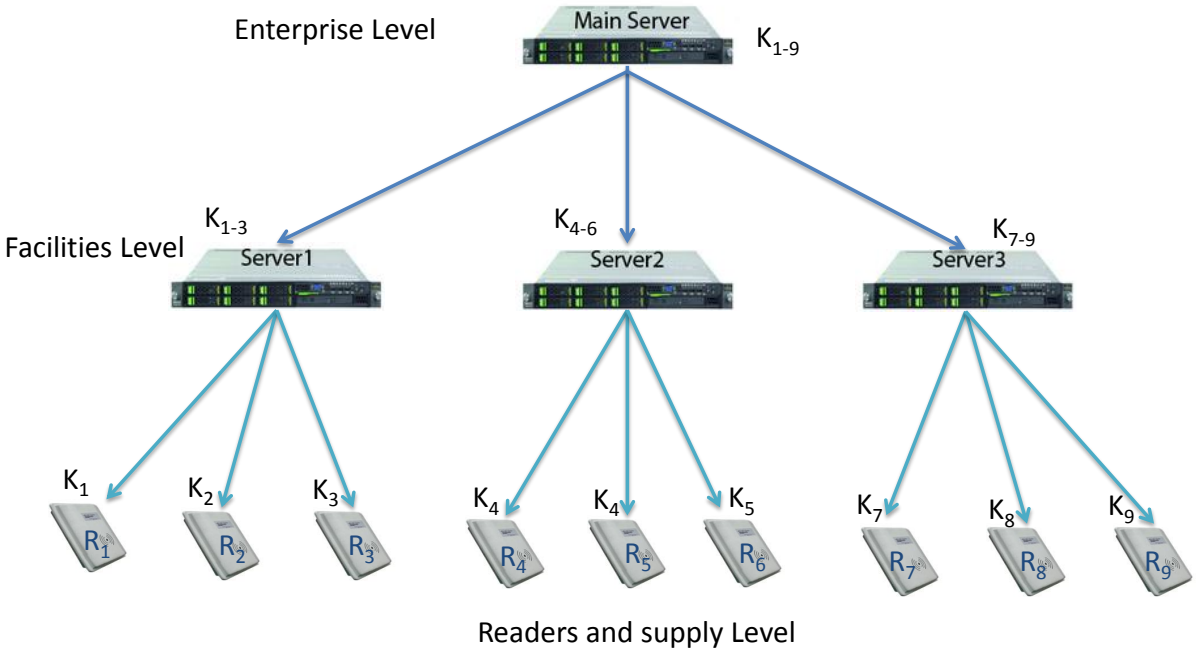

Figure 3.3: Developed RFID System Model

3.2.2 The Developed System

The newly developed system in this work is designed based to the concept of the tree key graphs described above. The system consists of a main server (enterprise level) and set of subservers (facilities level). Each subserver is connected to a number of RFID readers. In this application, every customs control point at a border has a subserver that controls a number of readers. Every reader may read thousands of tags inside the network. It is possible to add new readers to the server and remove existing or compromised readers from the server. This is mainly done by using the concept of shared keys within the network. Earlier, this situation was discussed. The border customs has the government master key (the main key), and the individual custom station key (the group key). The main server has the main key, which is shared between the subservers. For example, in Figure 3.3, the main key is k_{1-9}. In addition, a shared key (k_{123}) is the group key between the subserver and readers R_1,R_2 and R_3. Also, each reader and tag has their own unique key that helps to identify them. The technique that is used in this application is group-oriented rekeying for three reasons. One, there is no need for a subgroup multicast. Second, with fewer rekey messages, the numbers of messages are reduced. Also, the total number of bytes transmitted by the server per join/leave reader is less than those of the other approaches.

When new readers are added to the system or when existing readers are removed from the system, the security within the system should not be compromised. This is achieved by effectively changing the keys at each and every point in the network. To securely distribute the new keys within the network, the server sends the rekey messages to the readers. A rekey message contains one (or more) encrypted new keys that the readers use to decrypt with appropriate keys in order to get the new keys.

As mentioned earlier, there are four levels in the system: enterprise, facilities, reader and supply level. The goal for the system is to provide mutual authentication between servers-readers and readers-tags. Because all tags in this system have a unique key, the whole keys should be stored in the main server and then any authenticated reader in the system can get a key of a read tag from the main server. There are three scenarios on which the system can be applied. These three scenarios can be described and applied in the system.

1. A good reader reading a good tag
2. A good reader reading a bad tag
3. A bad reader reading either a good tag or a bad tag

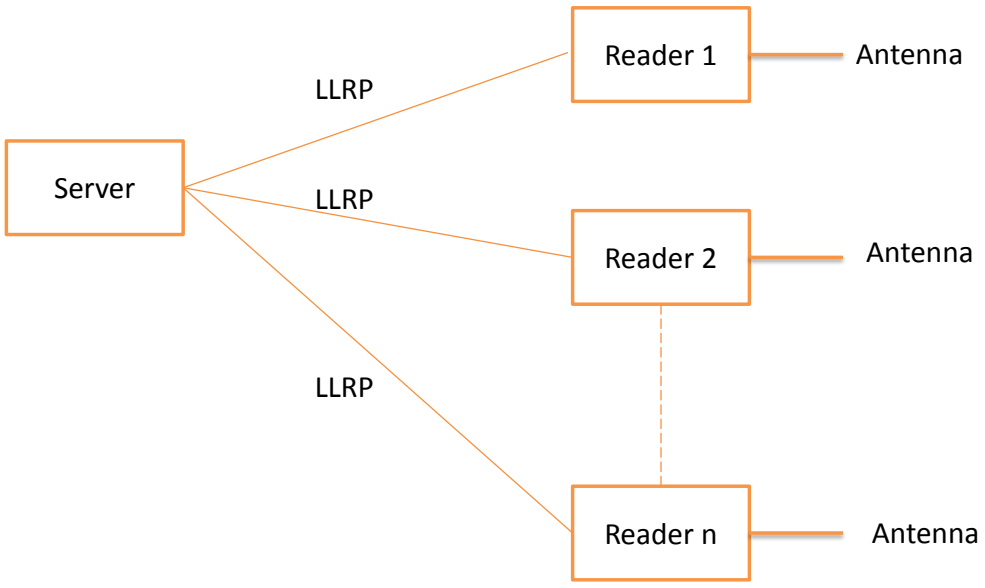

Figure 3.4: LLRP endpoint [99]

As described in Chapter One, the Low Level Reader Protocol (LLRP) provides authenticated communication between the server and the reader. [99] See Figure 3.4. It provides the format and procedures for communication between them. In addition, the LLRP provides

control of RFID air protocol operations timing and access to air protocol command parameters. There will be messages (used by LLRP) from the server to the readers for managing, controlling and updating the operations at the readers. Also, there will be messages from the readers to the server for sending the status of the readers as a report. After receiving reports from the readers, the server configures the readers to enable or disable some other events such as buffer overflow.

3.3 The Communication Between Readers and Servers

Therefore, there will be an interchange of message between readers and the server to check the health of the readers in the system. For example, GET_READER_CONFIG is a command that is issued by the server to the reader to get the information related to the reader's configuration. This command has some interested parameters that the reader will return. If there is an error, some codes will be sent to the server. Also, ReaderEventNotificationData and ReportBufferOverflowErrorEvent are parameters sent by the reader to notify the server about the connection establishment (Transmission Control Protocol and Internet Protocol (TCP/IP connection)) or some critical events like fault-detection and buffer overflow. Another parameter sent by the reader is ReaderExceptionEvent, which is sent if an unexpected event has occurred on the reader. In addition, if an antenna has an issue (connected or disconnected), the reader will send a report (AntennaEvent Parameter) to the server telling about this issue. [99]

Another aspect for the communication between the reader and the server is there will be two channels between the server and the reader: an alarm channel and command channel. The server issues requests and sends them by the command channel to the readers and also

receives a response from the readers. This is done to monitor the health of the readers. The response will be either a normal or an error response. The alarm channel carries messages issued by the readers to inform the server about the health of the reader. For example, if the server asks the reader to get the serial number of the reader, and the reader cannot find it, the error message "ERROR_UNKNOWN" is sent by the reader. [100]

There are two types of errors: communication errors and command execution errors. The communication errors can occur when the server tries to issue a command to the reader, but the reader is not responding, or the reader sends a notification to the server. However, the command execution errors occur as a response to commands sent from the server to the reader in the event of errors. These errors could be parameter_missing, parameter_length_extended, parameter_invalid_format, and so on. If errors happen in a reader such as a buffer overflow, the reader will send a notification to the server. [100]

In the above cases, when the enterprise server receives the error notification, it will determine if the issue that happened to the reader is critical, or not. If it is critical, this reader will be revoked from the entire system. If not, it will handle and maintain the errors.

In the next section, three proposed protocols that provide mutual authentication and handle a compromised reader are going to be introduced briefly.

3.4 The Developed Protocols

3.4.1 First Protocol

In this protocol, each reader has an individual key and also a shared key with their servers. Every RFID system consists of a database (the server), which holds the information about all the authenticated tags and readers under that network. All RFID tags have a unique ID,

which is the numeric representation of the individual item, name (item type), and a secret key (K_t). The tag memory is logically separated into four distinct banks: reserved memory (at least 32 bits for storing the EPC information such as password), EPC memory (at least 496 bits for storing EPC information), TID memory (at least 32 bits storing tag identifier), and user memory (for storing information related to the application of a tag).

The main server (enterprise level) might have a number of subservers (facilities level) based on the capacity and the size of the network. All RFID readers (authenticated ones) are connected to the subservers via a group key (which is the common key between the readers and the server in a particular network).

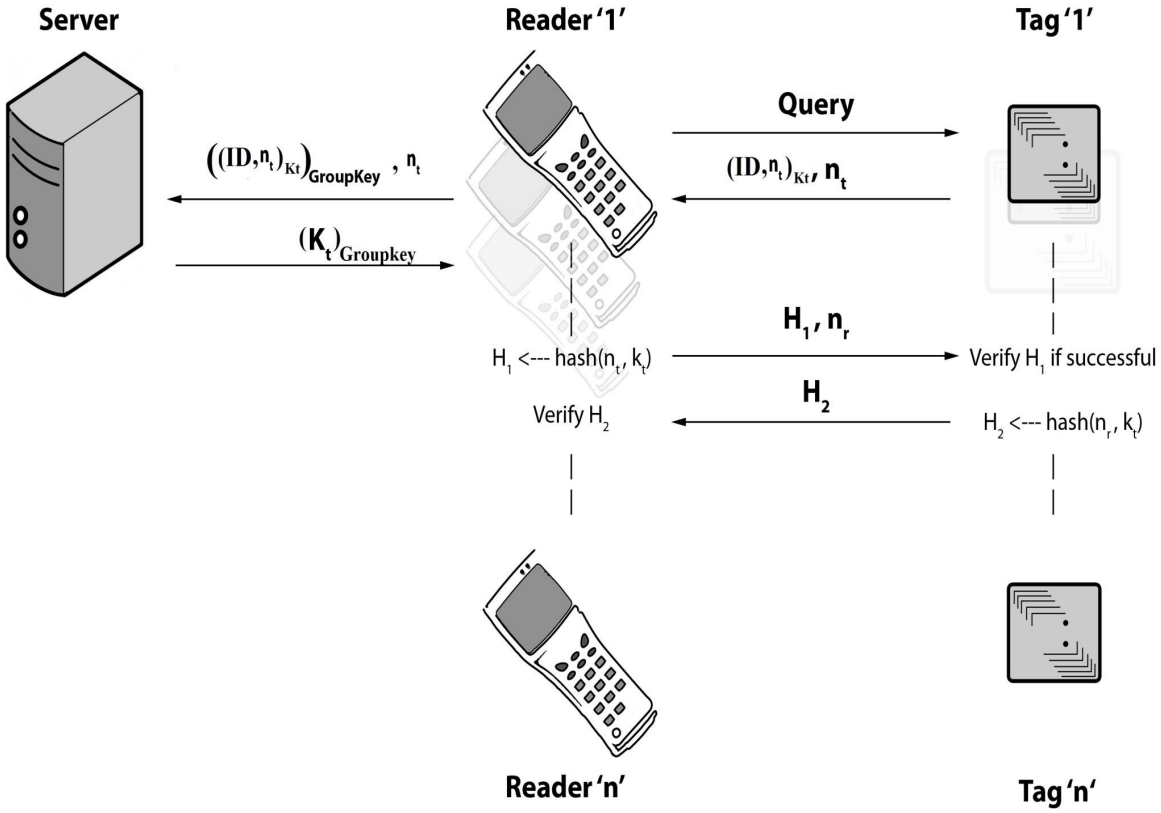

Figure 3.5: First Protocol

When a reader sends a query to a tag for getting that tag's information, the tag sends its ID, encrypted with a random number, generated from the tag, using its key. The reader in turn communicates with the subserver in the network and sends the encrypted message using the group key to get the key of the tag. The subserver contacts the main server by using the shared key and validates the tag and finds out the corresponding matching key for the tag from its database. This key is encrypted by using the group key and then sent to the reader, that can now read the information on the tag. See Figure 3.5.

Only an authenticated reader can get the key of a tag. This way, compromised readers cannot access the tags. When such a compromised reader tries to access the database, it fails because it does not have a valid key to communicate with the main database. By using keys, both the tags and readers are authenticated, and compromised readers are not allowed in the network.

This method makes sure that compromised readers cannot read the tag information and also provides mutual authentication between readers and tags and between readers and the back-end database in the system. A tag comes in contact with a reader; the reader validates the tag by sending a query to the tag. Now the tag generates and sends a random nonce number (n_t) to the reader. Also, it sends its unique ID which is encrypted with the random number by using its key K_t. Before the reader sends the tag-encrypted ID, which is $(ID, n_t)_{K_t}$, to the server, it will encrypt the message using the group key $((ID, n_t)_{K_t})_{groupkey}$. Also, it sends the random number of the tag (n_t) along with the $((ID, n_t)_{K_t})_{groupkey}$. The server has all information about the tags and even their ID. So, the server first will decrypt the message by using the same shared group key that validates the reader. Then, it will search in database to find the key of the tag and then encrypts the key of the tag by using the shared group key. If the reader is genuine, the server will send the encrypted key of the tag

to the reader, which is $(K_t)_{Groupkey}$. The reader in turn decrypts the message to get the key Kt and sends the hash of the nonce number and the key [*i.e.*, $H_1(n_t, K_t)$] along with its random number (n_r) to the tag. Because the tag knows the key K_t, it can verify that the hash result received from the reader is valid. The tag will then send H_2, which is the hash of (n_r, K_t) to the reader. The reader authenticates the tag by verifying the validity of the hash result [$hash(n_r, K_t)$] received from the tag. See Figure 3.5.

When a reader is compromised on the network, the group key and the main key will be changed by using one of the rekeying strategies; the enterprise server will change the keys and then distribute them to the facilities level. In case a compromised reader tries to connect with the server to get the key of the tag, it encrypts the tag's ID with its old group key (since the compromised reader does not have the new group key) and sends it to the server. However, the server will not be able to decrypt the message because there is a mismatch of the group keys between the server and reader.

Table 3.1: The Steps For The Authenticated Reader in the first protocol

Server	**Reader**	**Tag**
	1) - Send query to the tag - Encrypt (ID, n_t) using K_t - Send $(ID, n_t)_{K_t}$ and n_t	2) - Generate n_t
	3) - Encrypt (ID, n_t) using the group key - Send $[(ID, n_t)_{K_t}]_{groupKey}$ to the server	
4) - Using the group key for that reader - Decrypt the message $[(ID, n_t)_{K_t}]_{groupKey}$		

Continued on next page

Table 3.1 *(cont'd)*

Server	**Reader**	**Tag**
- Add n_t with all stored ID - Encrypt the results with the keys for each tag - If the result matches the received one o Get the key K_t o Decrypt (K_t) using group key o Send $(K_t)_{groupKey}$		
	5) - Decrypt $(K_t)_{groupKey}$ - Generate n_r - Calculate hash for K_t and n_t - Send the hash along with n_r to the tag	
		6) – Calculate hash for K_t and n_t - Compare the result with the one received - If not the same: o The reader is not authenticated o Abort - If the same: o Calculate hash for K_t and n_r o Send $hash(K_t, n_r)$ to the reader
	7) Calculate hash for for K_t and n_r - Compare the result with the received one - If the same: o The tag is authenticated o Getting more information from the tag - If not the same: o The tag is not authenticated	

Continued on next page

Table 3.1 *(cont'd)*

Server	**Reader**	**Tag**
	o Abort	

Table 3.2: The Steps For The Compromised Reader in the first protocol

Server	**Reader**	**Tag**
	1) - Send query to the tag - Encrypt (ID, n_t) using K_t - Send $(ID, n_t)_{K_t}$ and n_t	2) - Generate n_t
	3) - Encrypt (ID, n_t) using the group key (old one) - Send $[(ID, n_t)_{K_t}]_{groupKey}$ to the server	
4) - Using the group key (new one) for that reader - Decrypt the message $[(ID, n_t)_{K_t}]_{groupKey}$ - The server cannot do that because of is matching o Abort		

Tables 3.1 and 3.2 shows the steps for the two situations (a compromised reader and a genuine one) explained above.

3.4.2 Second Protocol

In this protocol, the concept is similar to the first protocol, but the number of times a reader contacts the server is reduced. See Figure 3.6. Therefore, the second protocol is defined by sharing the key between the server and the all tags. Also, the server will send an encrypted

message, from which a reader cannot get the information. The result is that only the system tags will receive the information.

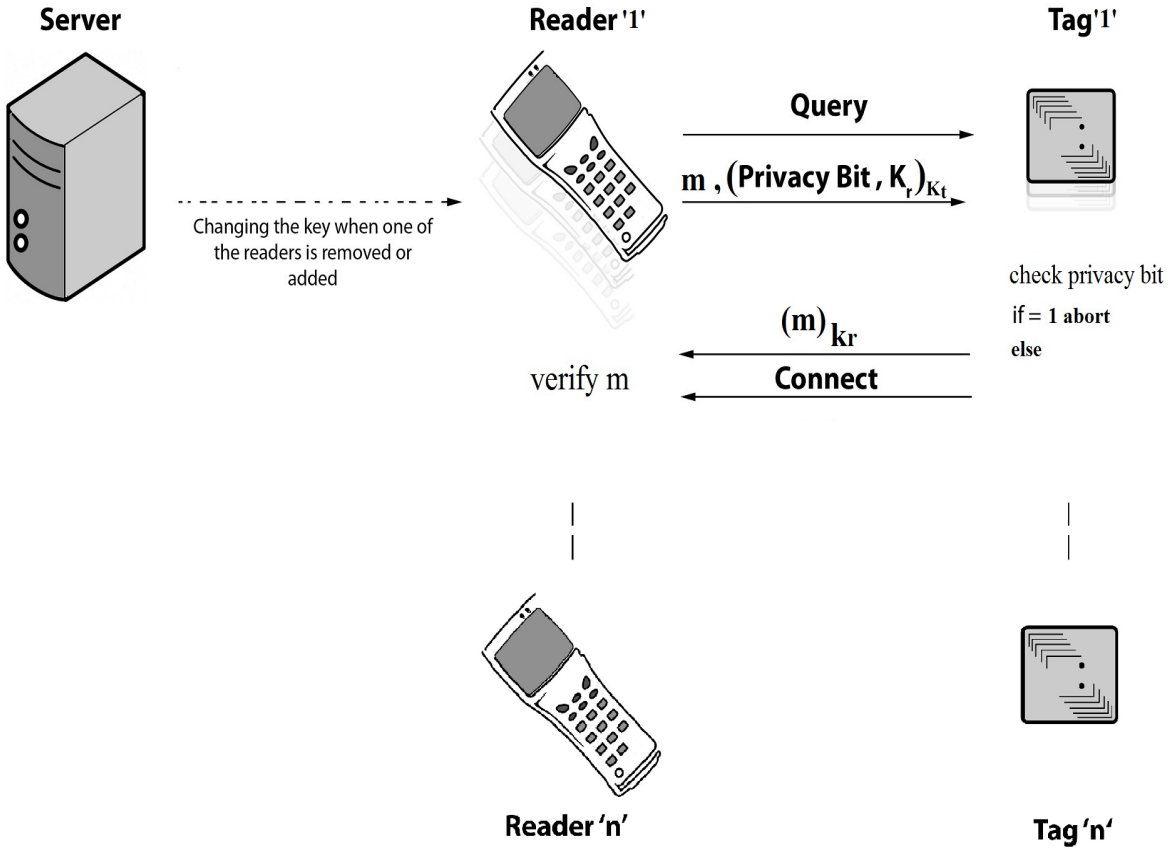

Figure 3.6: Second Protocol

Initially, all the tags have a shared key (K_t) between the server and the tags. In addition, every reader has a privacy bit (either 0 or 1) assigned by the server. The privacy bit 0 indicates the reader is not compromised and 1 indicates the reader is revoked. When a tag is read by the reader, the reader will send a random number (m) and the encrypted message (using K_t) that is received from the server, which has the privacy bit and the unique key of the reader K_r. This message will be changed only when one of the readers is added to or revoked from the system.

Then, the tag checks the privacy bit of the reader after decrypting the message using the key Kt. If the privacy bit is zero, then the tag will send the encrypted random number (m) received from the reader using the key of the reader which is K_r. After verifying the (m) by the reader, the tag will communicate with the reader using the key of the reader K_r that is sent inside the decrypted message. If the privacy bit is one, the tag will not send any more information to the reader. However, when one of the readers is compromised, the server will change the message that has the privacy bit and the key of the reader, and will send this new massage. The server will also change the privacy bit of the revoked reader to 1 to prevent the revoked readers from reading the tags again.

As shown in Figure 3.6, when a tag receives a query from the reader, the reader sends out the message $(privacy\_bit, K_r)_{K_t}$ along with the random number (m). The tag checks the privacy bit first after decrypting the message using Kt. There are two cases:

1. If the privacy bit is 1, the tag finds that the reader is revoked from the system and the tag will stop sending its information to the revoked reader.

2. If the privacy bit is 0, the tag will encrypt the random number (m) using K_r, $(m)_{K_r}$ and then the reader will verify the m.

The advantage of this protocol is that readers avoid contacting the server every time a tag is read, which increases the efficiency of the system. The server is contacted only when new readers are added or existing readers become compromised. This increases the overall efficiency of the system as it reduces the number of times the servers are contacted. The tag calculates only one encryption function and one decryption function to check the authenticity of the reader, which means reduced cost and timed compared to the other protocols. In addition, in the closed-system, a reader doesn't have a shared key with a tag.

(This is different from what is usually assumed by the research community where a reader is often assumed to have a shared key with a tag). This is reasonable; considering a terminal reader in the Airport customs process, there is no way for a reader to have shared keys with the RFID passports of travelers from different places/countries.

Table 3.3: The Steps For The Authenticated Reader in the second protocol

Server	**Reader**	**Tag**
	1) - Send query to the tag	
	2) - Generate random number (m) - Send $(privacybit, k_r)_{k_t}$ which is received from the server	
		3) - Decrypt the message to get privacy bit and k_r - Check the privacy bit, If bit=0 - Encrypt (m) using k_r
	4) - Verify m by decrypting $(m)_{k_r}$	

Table 3.4: The Steps For The Compromised Reader in the second protocol

Server	**Reader**	**Tag**
1) It changes the shared key for the group of readers and change the privacy bit to 1 for the compromised reader		
	2) - Send query to the tag	
		3) - Generate random number (m)

Continued on next page

Table 3.4 *(cont'd)*

Server	**Reader**	**Tag**
		- Send $(privacybit, k_r)_{k_t}$ which was received from the server after it is revoked from the system
		4) - Decrypt the message to get privacy bit and k_r - Check the privacy bit, If bit=1 - The connection is aborted

Table 3.3 and 3.4 show the steps for the connection between the authenticated reader with the tag and the compromised reader with the tag, respectively. When the system finds a compromised reader, the server will change the privacy bit of that reader from 0 to 1. Also, it encrypts a message again that includes the privacy bit and the key to that reader and stores it to the compromised one.

3.4.3 Third Protocol

In this protocol, there will be another concept to provide authentication and privacy between tags and readers using a trusted third party. Man-in-the-middle attacks and the symmetry in the authentication protocols can be avoided with this protocol. In addition, a session key is established in this protocol. A session key that is generated by the server will be used to encrypt and decrypt messages between the tag and the reader using symmetric key cryptography.

When the reader sends a query and random number nr to the tag, the tag will send the following: its ID with the random number n_t encrypted by using its key, which is K_t, the

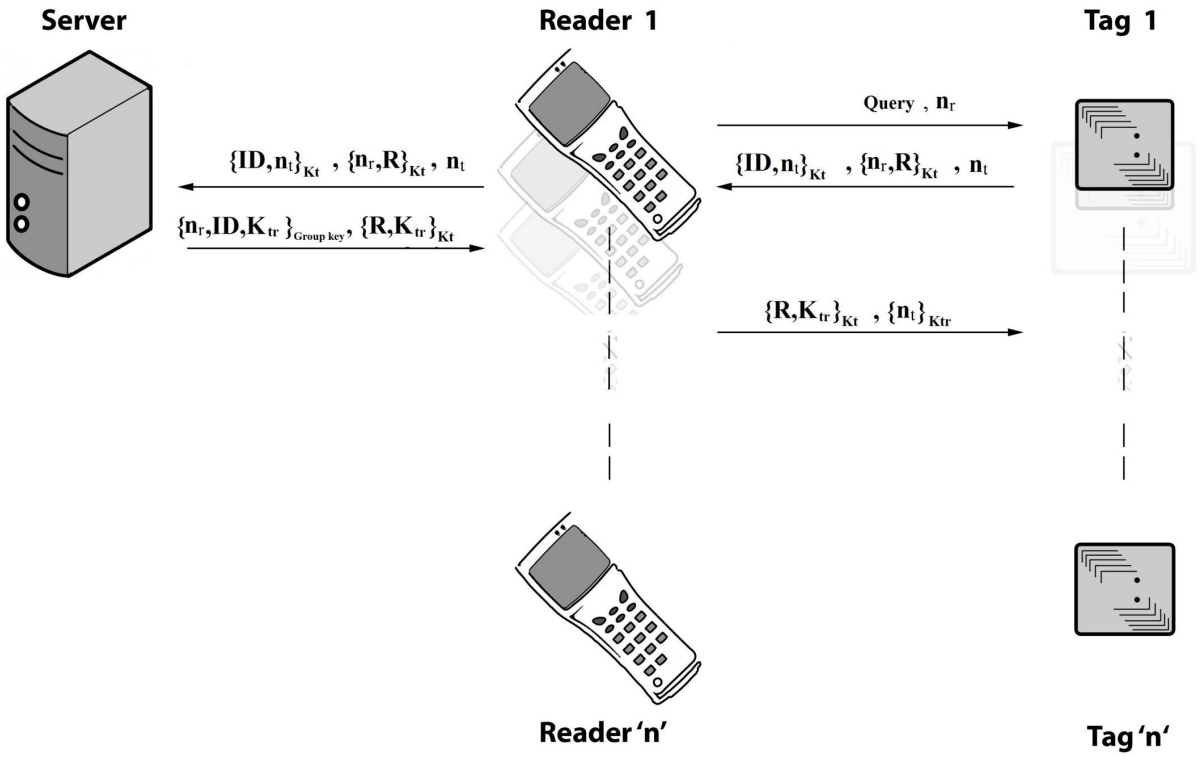

Figure 3.7: Third Protocol

encrypted message of n_r with reader's name (R) using the key of the tag $(n_r, R)_{k_t}$, along with the random number (n_t). In turn the reader will forward the received messages $((ID, n_t)_{k_t}$ and $(n_r, R)_{k_t})$ to the server, sending the random number (n_t) too. Because the server knows the K_t of the tag, it will decrypt the message to get n_r and R. See Figure 3.7.

The server will then reply to the reader with two messages. The first one has n_r, ID and K_{tr}, which is the session key used between the tag and the reader, $(n_r, ID, K_{t_r})_{groupkey}$. These three entries are encrypted using a group key that is shared between the subserver and the readers in that server. The second message has R, and K_{tr} is encrypted using K_t, $((R, K_{tr})_{k_t})$. When the reader receives these two messages from the server, it will decrypt

the first message, which is $(n_r, ID, K_{tr})_{groupkey}$, because it has already the group key to get the session key and also to authenticate the tag. The reader will forward the second message, which is $(R, K_{tr})_{K_t}$, to the tag. Also, when the reader gets the session key from the first message, it will encrypt the random number (n_t), which is received from the tag, and send it to let the tag authenticate the reader, using the session key K_{tr}.

Therefore, the tag will receive two messages $(R, k_{tr})_{k_t}$ and $(n_t)_{k_{tr}}$. The tag will decrypt the first message to get the session key and verify the reader. Then, it will decrypt the second one using the session key to verify and authenticate the reader. In this protocol, the authentication and privacy will be provided with higher security. As a benefit, the reader will never know the tag key. As a result, this prevents key leakage from a compromised reader. Table 3.5 illustrates the steps for the connection between a reader, tag and the server in authenticated situation.

Table 3.5: The Steps For The Authenticated Reader in the third protocol

Server	**Reader**	**Tag**
	1) - Send query to the tag - Send random n_r	
		2) - Generate random number (n_t) - Encrypt ID and n_t using its key k_t - Encrypt R and n_r using k_t - Send them to the reader
	3) - Forward the received two encrypted messages to the server	
4) - Decrypt ID_{k_t}		

Continued on next page

Table 3.5 *(cont'd)*

Server	**Reader**	**Tag**
- Decrypt $(n_r, R)_{k_t}$ - Create two encrypted messages: o $(n_r, ID, k_{tr})_{groupkey}$ o $(R, k_{tr})_{k_t}$ - Send them to the reader		
	5) - Decrypt the message $(n_r, ID, k_{tr})_{groupkey}$ to get the session key - Encrypt (n_t) using the session key K_{tr} - Forward $(R, k_{tr})_{k_t}$ to the tag	
		6) - Decrypt $(R, k_{tr})_{k_t}$ to get the session key - Decrypt $(n_t)_{k_{tr}}$ to verify m

Chapter 4

Security and Time Analysis with Conclusion and Future works

RFID tags have limited memory capacity. Hence, there is a strong need for new lightweight cryptographic primitives that can be supported by low-cost RFID tags. The speed and simplicity of an algorithm are usually qualifying factors; low complexity of the primitives has a first place importance in this research. It also determines how attacks may happen in an RFID system and what possible solutions can keep that from happening. After developing and implementing the three protocols and the topology, security analysis and time analysis are explained in this chapter.

4.1 Security analysis

In the three proposed protocols, there are no assumptions like the previous proposed solutions. Two situations have been handled: a compromised reader and a compromised tag by providing a mutual authentication and privacy between them and the server. The following subsections provide security analysis for each protocol.

4.1.1 Analyzing the first protocol

This protocol makes sure that compromised readers have no way to get the information of the tag and also provides mutual authentication between readers and tags in the system. A tag generates and a random nonce number (n_t) to the reader. In this way, replay attacks cannot be applied because $(ID, n_t)_{K_t}$ is different in each communication. The reader will be authenticated when it encrypts the message using the group key $((ID, n_t)_{K_t})_{groupkey}$ because this key is changed when one of the reader is revoked from the system. If the reader is genuine, the server will send the encrypted key of the tag to the reader, which is $(K_t)_{Groupkey}$. The mutual authentication between readers and tags can be achieved by verifying the two hash functions H_1 and H_2.

In this protocol, mutual authentication and privacy have been achieved. Also, readers will be verified. So, if there is a compromised reader, it will never get the private information from the tag.

Security Analysis

- **Mutual authentication** The mutual authentication is achieved between readers and tags and between readers and the server. The authentication between readers and tags is achieved by verifying hash functions $hash(n_t, K_t)$, $hash(n_r, K_t)$. Also, the reader has another opportunity to authenticate the tag (before verifying the hash function) by getting the key of that tag from the server encrypted using the group key. The reader is authenticated by the server from the message $((ID, n_t)_{K_t})_{groupkey}$.

- **Integrity** The integrity of this protocol can be achieved in all the steps. The integrity of communication is ensured by generating random numbers and encrypting the contents of the messages between reader, tags, and the servers. So, even if an attacker

gets all the transferred messages, the real messages cannot be revealed.

- **Replay** Attackers can record the messages between readers and tags and between the server and readers. They can use later these messages for communications. However, because tags generate random number (n_t) and readers generate also random number (n_r), this attack can be prevented. In this case, attackers cannot replay previous messages for communication.

- **Man-in-the-middle** An attacker can modify the messages or inject new messages into the channels. This kind of attack is prevented in this protocol because mutual authentications are achieved and random numbers are generated.

- **Compromised readers** A compromised reader is prevented to get the private information in the system by revoking it from the system and updating the main and group keys. So, when a compromised reader gets the message $(ID, n_t)_{K_t}$) from the tag, it will encrypt the message using the old group key not the updated one. Then, the server will know if this reader is an authenticated one or not by decrypting the message $((ID, n_t)_{K_t})_{groupkey}$ using the updated key. In this case, the server will not send the message $(K_t)_{Groupkey}$ to that reader.

4.1.2 Analyzing the second protocol

The number of times a reader contacts the server is reduced in this protocol. This is achieved by sharing the key between the server and the all tags. Also, the server will send an encrypted message, from which a reader cannot get the information. Just the tags can get the information. This is different from what is usually assumed by other research where a reader is often assumed to have a shared key with a tag. When one of the readers is compromised,

the server will change the message $(privacy\_bit, K_r)_{K_t}$, which has the privacy bit and the key of the reader, and then it will send this new massage. The server will also update the privacy bit of the revoked reader to 1 to prevent the revoked readers from reading the tags again.

Security Analysis

- **Mutual authentication** The mutual authentication is achieved between readers and tags and between readers and the server. The authentication between readers and tags is achieved by verifying the message $(privacy\_bit, K_r)_{K_t}$ and $(m)_{K_r}$. so, when the tag receives the message $(privacy\_bit, K_r)_{K_t}$, it will decrypt it and checks the privacy bit to see if this reader is authorized by the server or not. If yes, then the reader can verify the next message received from the tag, which is $(m)_{K_r}$.

- **Integrity** The integrity of this protocol can be achieved. The integrity of communication is ensured by generating random numbers and encrypting the contents of the messages between reader and tags. So, even if an attacker gets all the transferred messages, the real messages cannot be revealed. The key leakage from a compromised reader is prevented in this protocol because the reader never knows the key of the tags.

- **Replay** Attackers can record the messages between readers and tag. They can use later these messages for communications. However in this protocol, readers generate a random number (m). In this case, attackers cannot replay previous messages for communication because of the random number.

- **Man-in-the-middle** An attacker can modify the messages or inject new messages into the channels. This kind of attack is prevented in this protocol because mutual authentications are achieved and random numbers are generated.

- **Compromised readers** A compromised reader is prevented from getting the private information in the system by revoking it from the system and updating the message $(privacy\_bit, K_r)_{K_t}$. In this case, the tag will never send private information to the compromised reader when it checks the privacy bit and sees that it is 1.

4.1.3 Analyzing the third protocol

Without a trusted third party, readers and tags share a secret key. However, with a trusted third party, a reader and a tag share a secret key with the third party. The third protocol is developed with this idea. There are many threads such as: inject a new message into a channel, modify or delete a message in a channel, or replay and old message. The idea of using trusted third party is to reduce the number of keys. The message $(n_r, R)_{k_t}$ is send to the reader by the tag. Using R is for preventing $(n_r)_{k_t}$ from being reused by attacker. The message $((ID, n_t)_{k_t}$ is to prevent sniffing the ID of the tag for tracking that tag. Also, the message $(n_r, ID, k_{tr})_{groupkey}$, which is sent by the server, is to make the reader authenticate the tag, which in turns will authenticate the reader when receiving the two messages $(R, k_{tr})_{k_t}$ and $(n_t)_{k_{tr}}$. In addition, the message $(n_r, ID, k_{tr})_{groupkey}$ is used to make sure that the compromised reader cannot decrypt it because it does not have the updated group key. After providing the mutual authentication between the reader and the tag with the server, the transferring messages between the tag and the reader will be encrypted using the session key that is established by the server. This is used to ensure the security of the communication between the tag and the reader. This key is used for both encryption and decryption.

In this protocol, the mutual authentication and privacy have been achieved. Also, readers will be verified. So, if there is a compromised reader, it will never get the private information

from the tag.

Security Analysis

- **Mutual authentication** In third protocol: the tag-to-reader authentication is achieved when the reader verifies the value of $(n_r, ID, k_{tr})_{groupkey}$, which includes the random number sent by the reader (n_r), the ID of the tag , and the session key (K_{tr}) that will be used for the communication between the reader and the tag. When the server sends the ID of that tag, it means that this tag is an authenticated one. The reader-to-tag authentication is achieved by receiving these two messages $(R, k_{tr})_{k_t}$ and $(n_t)_{k_{tr}}$. The first message includes the R, which represents the reader, and the session key. So, when the tag receives these two messages, it will know that the reader R is an authenticated one. Then, the tag will use the session key to verify its random number (n_t). In addition, the readers can be an authenticated by the server by sending R to the server, which in turn send the message $(n_r, ID, k_{tr})_{groupkey}$. If the reader is authenticated one, it can use the group key to decrypt the message and to get the information. If not, it cannot decrypt the message $(n_r, ID, k_{tr})_{groupkey}$ using the old key because after revoking the compromised reader from the system, the server will update the group key.

- **Integrity** The integrity of this protocol can be achieved in all the steps. The integrity of communication is ensured by generating random numbers and encrypting the contents between reader, tags, and the server. In addition, the integrity of this protocol can be completed by using the session key that is established by the third party. This key will be used between the reader and the tag after the mutual authentication is satisfied to encrypt all the messages that are transferred between them. By using a

session key, the key leakage from a compromised reader is prevented with this protocol.

- **Replay** An attacker can record the messages between readers and tag and between backend database and readers. They can use later these messages for communications. However, because both tags and readers generate the random numbers (n_t) and (n_r) respectively, this attack can be prevented. In this case, an attacker cannot replay previous messages for communication.

- **Man-in-the-middle** An attacker can modify the messages or inject new messages into the channels. This kind of attack is prevented in this protocol because mutual authentications are achieved and random numbers are generated. Also, symmetry of the transferred messages in this protocol is avoided.

- **Compromised readers** A compromised reader is prevented in this protocol from getting the private information in the system by revoking it from the system and updating the group key. In this case, the compromised reader cannot decrypt the message $(n_r, ID, k_{tr})_{groupkey}$ using the old key because after revoking the compromised reader from the system, the server will update the group key.

Table 4.1: The goals of the three developed protocols that have been achieved

Goal / **Protocol**	**Mutual authentication**	**Integrity**	**Replay**	**Man-in-the-middle**	**Compromised reader**
First	√	√	√	√	√
Second	√	√	√	√	√
Third	√	√	√	√	√

Table 4.1 summarizes the goals that have been achieved in each developed protocol, but

in different ways.

4.2 Time analysis of the topology

A program for implementing the topology was written in Python language. A main server and three sub servers are implemented to check the time consumed in deleting a compromised reader from the system. The time is calculated in seconds. Figures 4.1 and 4.2 show the results of deleting a reader from the system.

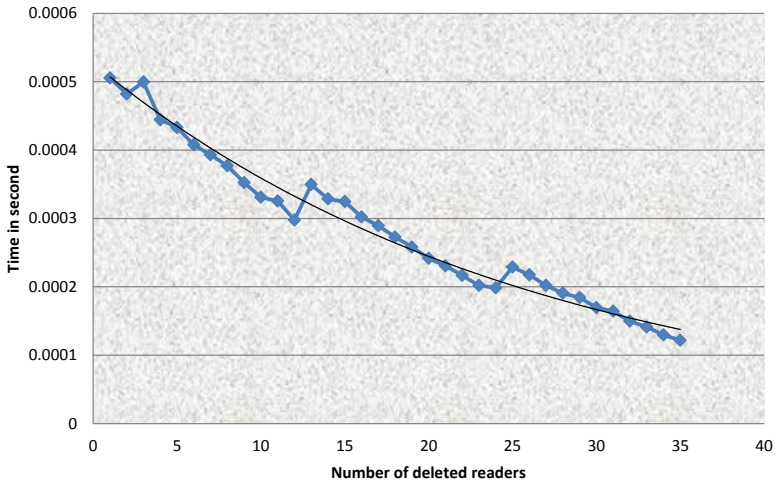

Figure 4.1: The execution time for deleting a compromised reader form the system

Figure 4.1 shows the execution time for deleting a reader sequentially. The execution time decreases every time one of the readers is deleted form the system. The readers were deleted from the first sub server and then from the second and so on.

In the second case, the readers are deleted from the system randomly. In Figure 4.2, the execution time for deleting a reader decreases every time one of the readers is deleted from the system. In this case, also, the time decreases similar to the first case.

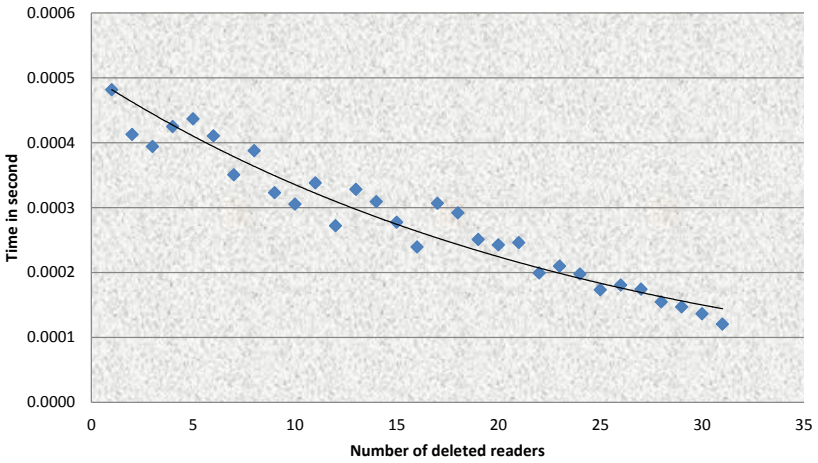

Figure 4.2: The execution time for deleting a compromised reader form the system randomly

4.3 Operations in an RFID tag

A tag in each protocol applies some steps for providing privacy and mutual authentication. The number of steps is different in each protocol. In this section the operations that are executed by a tag are defined: The operations that are executed in the first protocol by the tag:

1. Generating random number
2. Applying encryption function
3. Applying hash function

4. Making compassion

5. Applying another hash function

The operations that are applied in the **second protocol** by the tag:

1. Applying decryption function

2. Applying encryption function

3. Checking the privacy bit

The operations that are applied in the **third protocol** by the tag:

1. Generating random number

2. Applying encryption function

3. Applying another encryption function

4. Applying decryption function

5. Applying another decryption function

6. Checking random number

Based on the above operations that are applied by the tag, the time is calculated in each protocol as described in the next section.

4.4 Time analysis

In each protocol, the time is calculated in the tag to check how fast it is to execute operations for providing privacy and mutual authentication with readers. The time is calculated in micro seconds. MSP430-P2274, which is a mixed-signal microcontroller from Texas Instruments, is used to calculate the time. MSP430-P2274 is used for low cost and low power consumption embedded applications. [108] Its function the same as RFID tag. In addition, IAR, which is an integrated development environment with C/C++ compiler is used in this research to generate faster codes and to debug the microcontroller. It is powerful with the shortest possible execution times. It is user friendly; it incorporates a compiler, an assembler, a linker and a debugger in one integrated development environment (IDE). This gives an uninterrupted workflow. Three codes for each protocol are written in C programming language. In each code, the time is calculated for the all operations that are run in the 'tag'. The following sections provide more details about the time in each protocol:

4.4.1 The time calculated in the first protocol

A tag performs five operations, as described above, in the first protocol. These are:

1. Generating random number
2. Applying encryption function
3. Applying hash function
4. Making compassion
5. Applying another hash function

For each operation, the time is calculated. Figure 4.3,4.4,4.5, and 4.6 show the results.

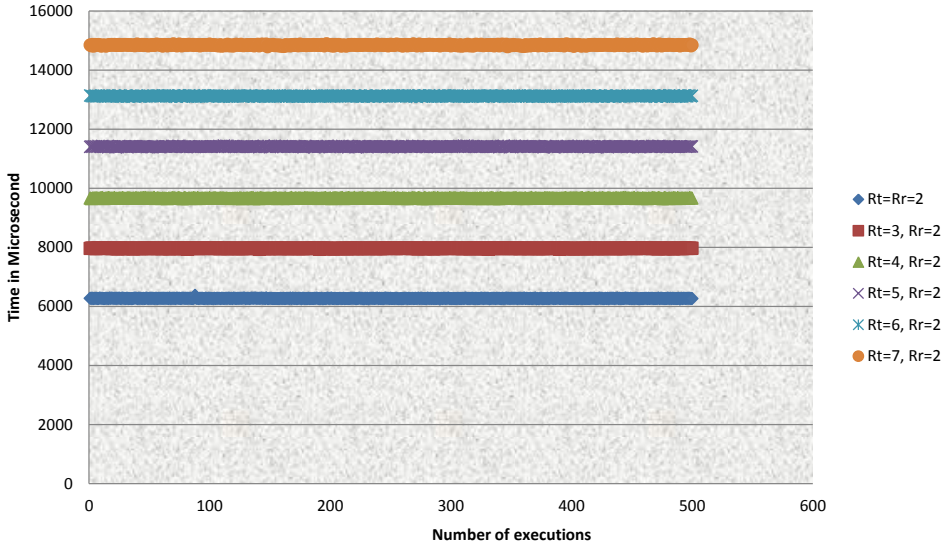

Figure 4.3: Times, while increasing the number of digits in RFID tags only in the first protocol

Figure 4.3,4.4,4.5, and 4.6 show six cases based on the number of digits in generating the random number. Every time the number of digits increases, the time to run the calculation also increases. In this protocol, two random numbers are generated, one by a tag (R_t) and the other one by a reader (R_r).

In Figure 4.3, the random numbers started with two digits and then increased the number of digits in the random number that is generated by the tag only in each case. The code for the first protocol was run 500 times to check the stability of it.

In Figure 4.4, the number of digits in the random number generated by the reader is increased, but not for the tag. Both random numbers started with two digits. The code for the first protocol was also run 500 times to check the stability of it.

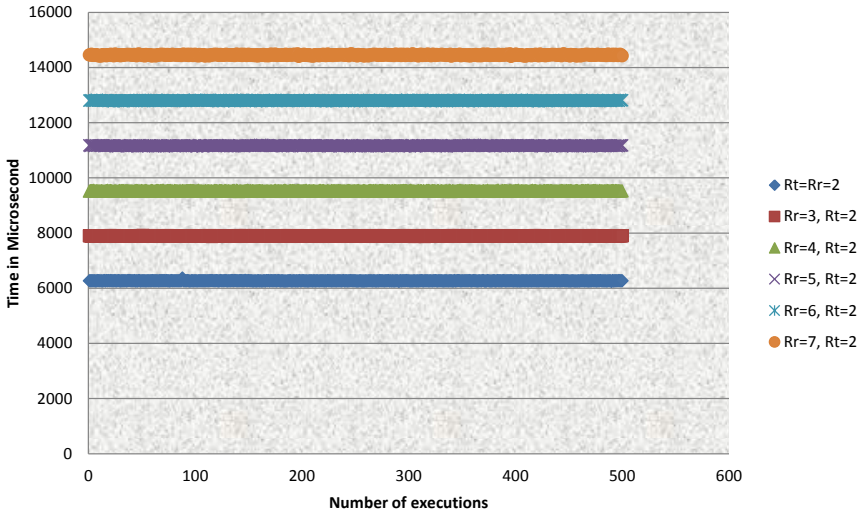

Figure 4.4: Times, while increasing the number of digits in RFID readers only in the first protocol

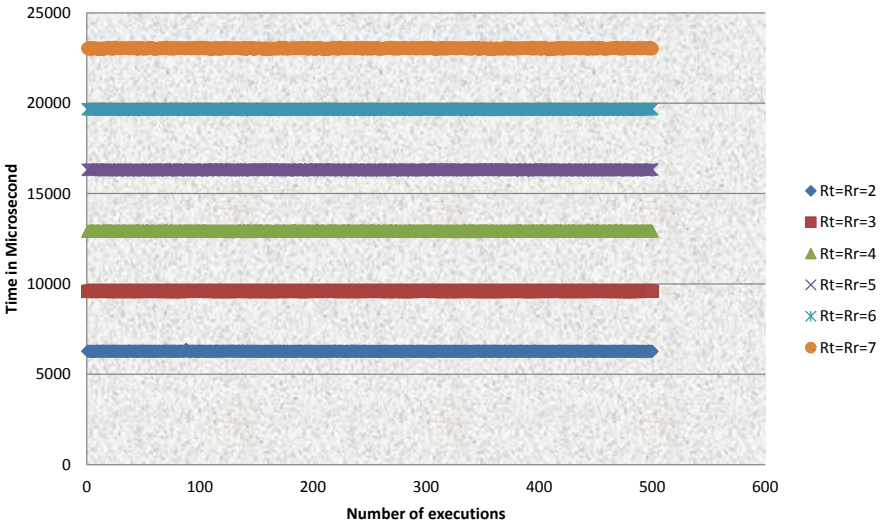

Figure 4.5: Times, while increasing the number of digits in both RFID tags and readers equally in the first protocol

In Figure 4.5, the number of digits in the random number is increased equally in both of the tag and the reader. Both random numbers started with two digits. The code for the first protocol was also run 500 times to check the stability of it.

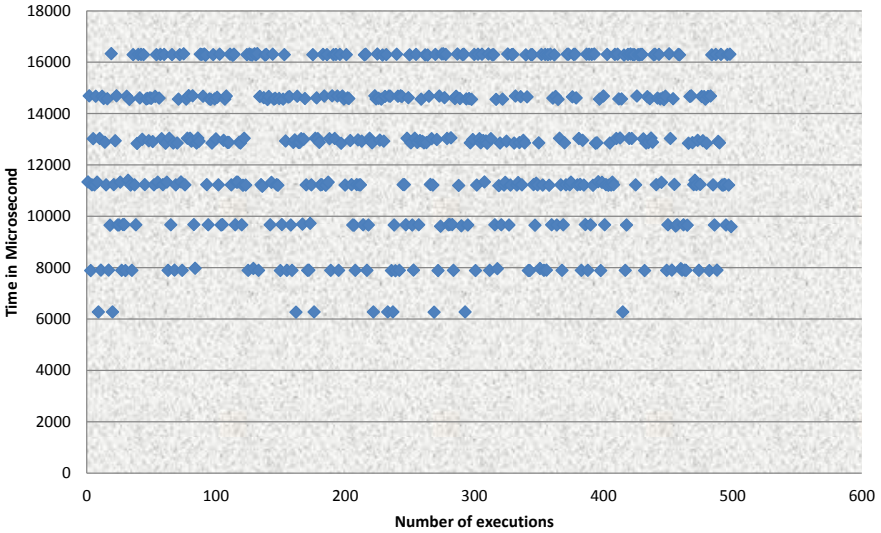

Figure 4.6: Times,with random digits in both RFID tags and readers in the first protocol

In Figure 4.6, the number of digits in the random number generated by the tag and the reader were generated randomly. The code for the first protocol was also run 500 times. The times in the figure are random, based on the number of digit in the random number that is generated by the tag and by the reader in every run.

4.4.2 The time calculated in the second protocol

A tag performs three operations, as described above, in this protocol. These are:

1. Applying decryption function
2. Applying encryption function
3. Checking the privacy bit

For each operation, the time is calculated. Figure 4.7 and 4.8 show the results.

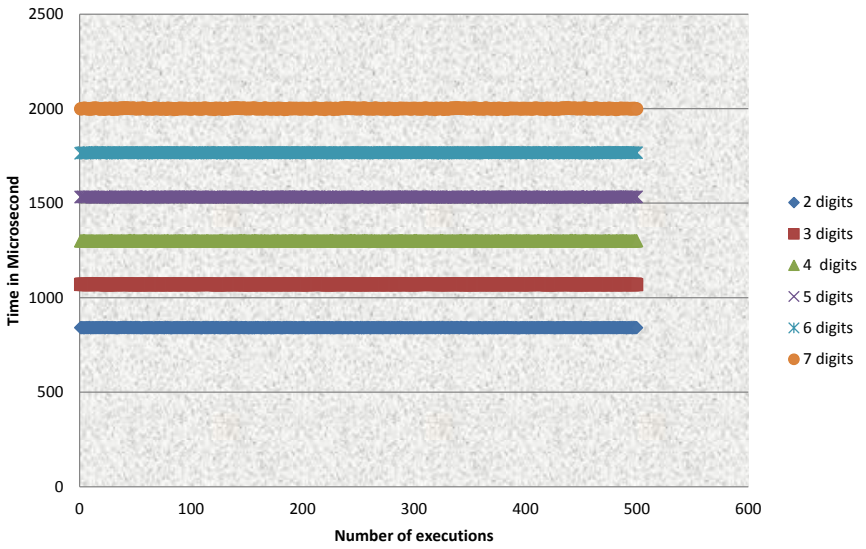

Figure 4.7: Times, while increasing the number of digits of the random number in RFID readers in the second protocol

Figure 4.7 and 4.8 show six cases based on the number of digits in the random number. Every time the number increases, the time also increases. In this protocol, only one random number is generated by the reader. In Figure 4.7, the number of digits in the random number was increased by one, starting with two digits. The code for the second protocol was run 500 times to check the stability of it.

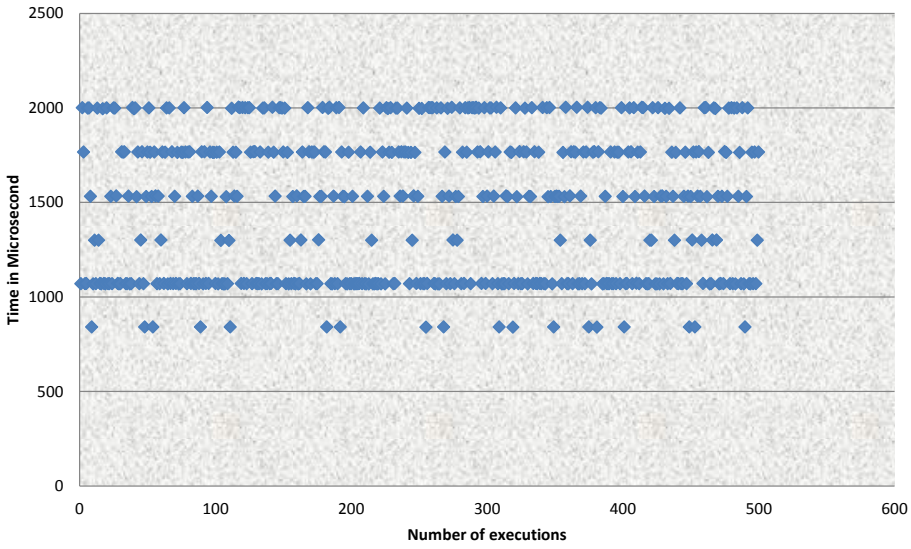

Figure 4.8: Times, while generating random numbers with random digits in RFID readers in the second protocol

In Figure 4.8, the number of digits in the random number generated by the reader is generated randomly. The code for the second protocol was also run 500 times. The times in the figure are random, based on the number of digit in the random number that is generated by the reader in every run.

4.4.3 The time calculated in the third protocol

A tag performs six operations, as described above, in this protocol. These are:

1. Generating random number

2. Applying encryption function

3. Applying another encryption function

4. Applying decryption function

5. Applying another decryption function

6. Checking random number

For each operation, the time is calculated. Figure 4.9,4.10,4.11, and 4.12 show the results.

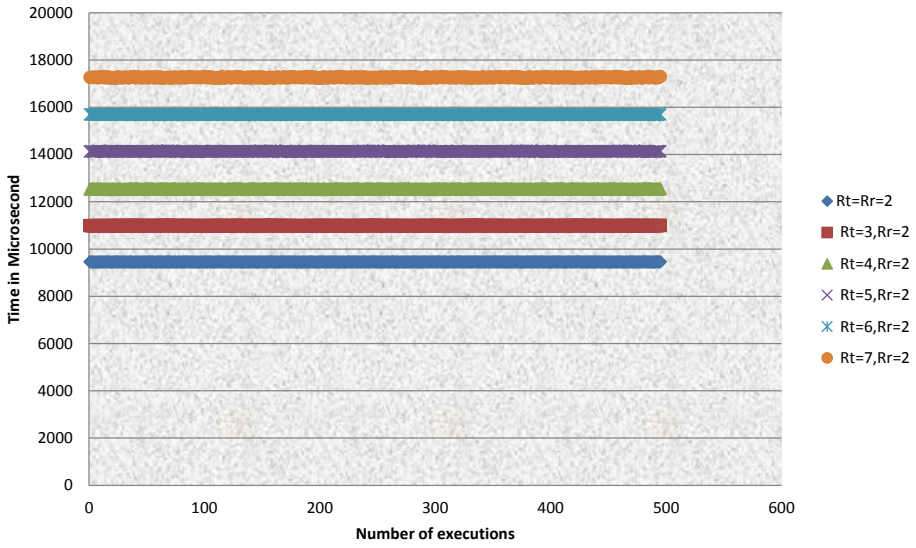

Figure 4.9: Times, while increasing the number of digits in RFID tags only in the third protocol

4.9,4.10,4.11, and 4.12 show six cases based on the number of digits in the random number. Every time the number increased, the time also increased. In this protocol, two random numbers were generated, one by the tag (R_t) and the other one by the reader (R_r). In Figure 4.9, the number of digits in the random number generated by the tag is increased, but not for the reader. Both random numbers started with two digits and then increased

them by one in every run. The code for the third protocol was run 500 times to check the stability of it.

In Figure 4.10, the number of digit in the random number generated by the reader is increased, but not for the tag. Both random numbers started with two digits and then increased them by one in every run. The code for the third protocol was also run 500 times to check the stability of it.

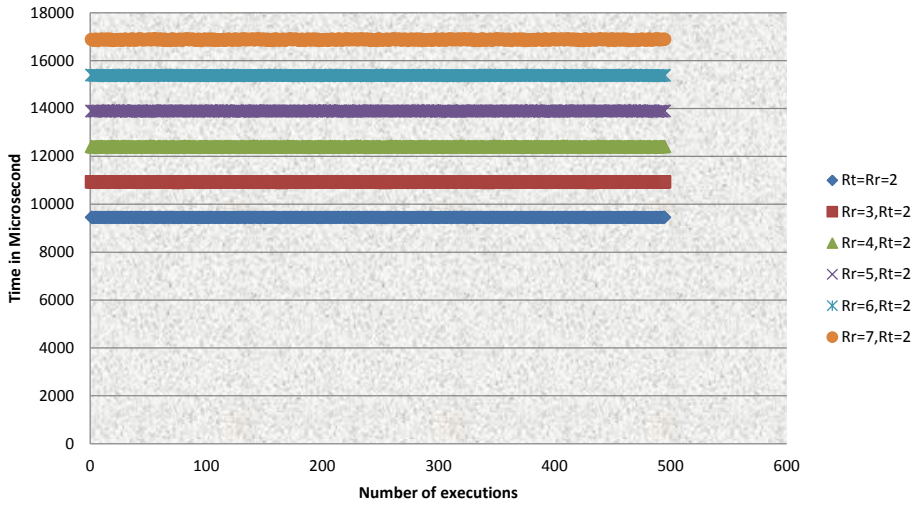

Figure 4.10: Times, while increasing the number of digits in RFID readers only in the third protocol

In Figure 4.11, the number of digits in the random number was increased equally in both of the tag and the reader. Both random numbers started with two digits. The code for the third protocol was also run 500 times to check the stability of it.

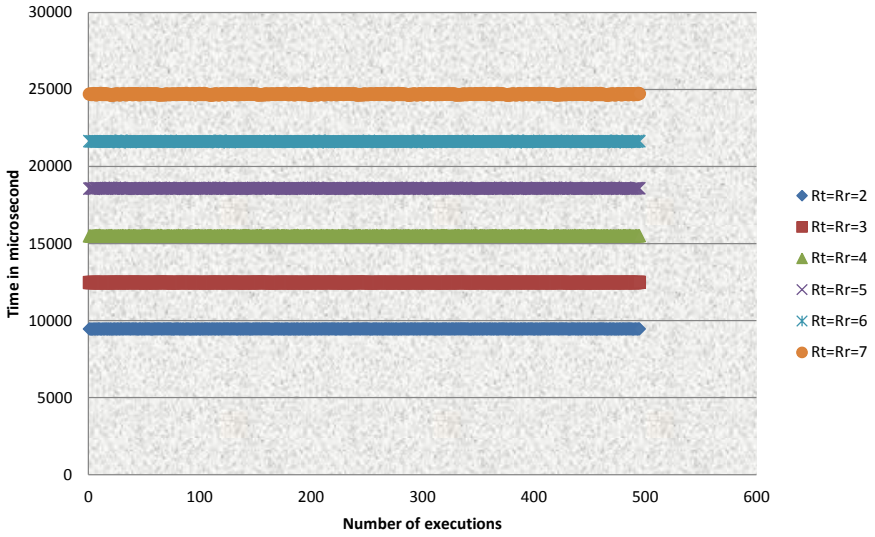

Figure 4.11: Times, while increasing the number of digits in both RFID tags and readers equally in the third protocol

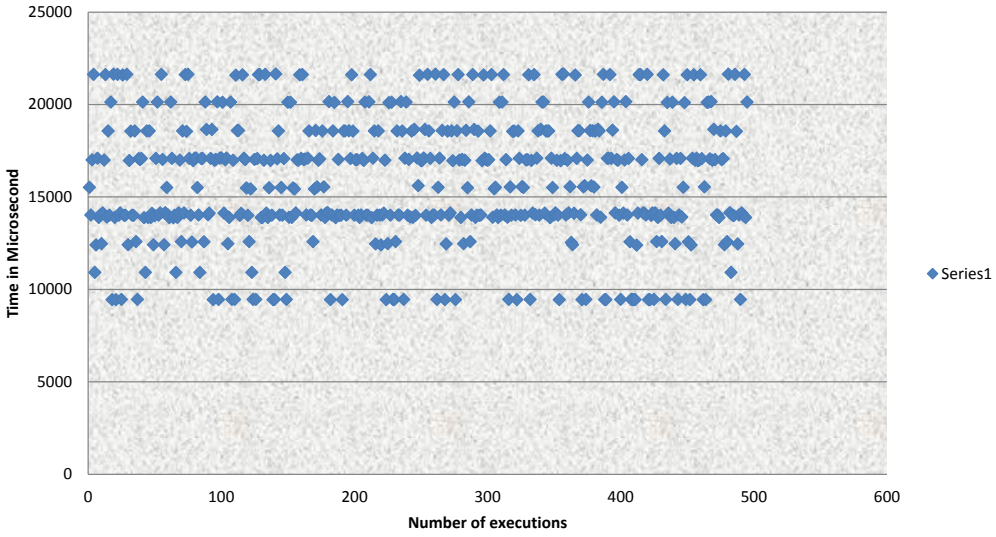

Figure 4.12: Times, with random digits in both RFID tags and readers in the third protocol

In Figure 4.12, the number of digits in both random numbers (R_t and R_r) was generated randomly. The code for the third protocol was also run 500 times. The times in the figure are random based on the number of digits in the random number generated by the tag and

by the reader in every run.

In summary, there are discrete time variables based on the number of steps and the number of digits in the random number. As random numbers increase, the time to read increases. Therefore, the number of communication transactions will be bounded within a short time period by the number of tags in the field.

Table 4.2 shows the time range in microseconds of the second protocol; a reader generated the random number for this protocol. Tables 4.3 and 4.4 show the time range in microseconds of the first and the third protocols in two situations (the number of digits in a reader increased without increasing the digits in a tag, and the number of digits in a tag increased without increasing the digits in a reader) respectively. Table 4.5 shows the time range in microseconds of the first and the third protocols when the number of digits in the random number of a tag and reader were equal.

Table 4.2: The time duration in microseconds of the second proposed protocol

Protocol	2 digits	3 digits	4 digits	5 digits	6 digits	7 digits
2nd	840-842	1068-1071	1298-1302	1528-1535	1763-1768	1995-2004

Table 4.3: The time duration in microseconds of the first and third proposed protocols when the number of digit in a reader increases

Protocol	R_t=2, R_r=3	R_t=2, R_r=4	R_t=2, R_r=5	R_t=2, R_r=6	R_t=2, R_r=7
1st	7871-7906	9499-9549	11134-11192	12771-12826	14398-14492
3rd	10903-10934	12384-12430	13865-13926	15350-15399	16834-16910

Table 4.4: The time duration in microseconds of the first and third proposed protocols when the number of digits in a tag increased

Protocol	R_r=2, R_t=3	R_r=2, R_t=4	R_r=2, R_t=5	R_r=2, R_t=6	R_r=2, R_t=7
1st	7939-7971	9638-9682	11379-11437	13088-13141	14786-14879
3rd	10970-11002	12516-12565	14102-14160	15660-15711	17217-17296

Table 4.5: The time duration in microseconds of the first and third proposed protocols when the random number of a tag and a reader were equal

Protocol	R_t=2, R_r=2	R_t=3, R_r=3	R_t=4, R_r=4	R_t=5, R_r=5	R_t=6, R_r=6	R_t=7, R_r=7
1st	6246-6366	9565-9603	12892-12952	16267-16340	19604-19686	22964-23083
3rd	9433-9456	12445-12483	15468-15525	18531-18610	21574-21657	24623-24732

4.5 Conclusion

The developed topology, security requirements for the eSeal system, and proposed the eSeal protection protocols are identified in this research. The security analysis shows that the proposed protocols satisfy the security requirements, which are preventing man-in-the-middle and reply attacks, providing integrity and mutual authentication, and revoking a compromise reader from the system. The processing time in an eSeal requires several microseconds using MSP430-P2274, which is used for a low cost and low power consumption embedded application. In each protocol, the execution time is measured based on the number of operations that are performed by an RFID tag and the number of digits in random numbers. As a result, the execution time in the second protocol is less than the execution times in the other protocols because the tag performs just three operations. Also, the execution time in the first protocol is less than the execution times in the third one because the tag in

the first protocol performs five operations including one encryption function and two hash functions. However, the tag in the third protocol performs two encryption functions and two decryption functions. In all cases, the time jump was linear based on the number of digits in the random number.

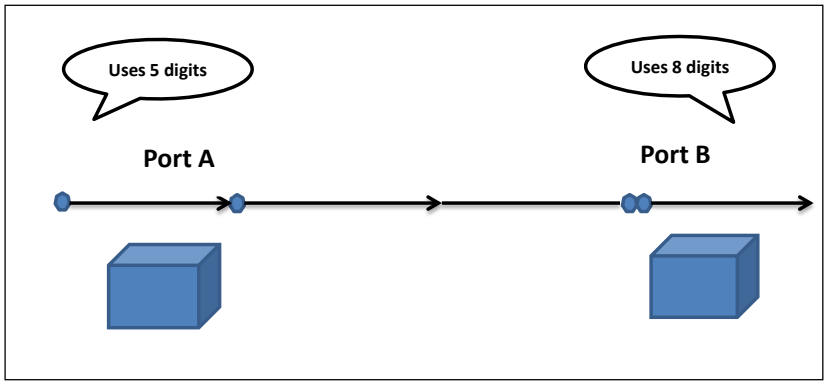

Figure 4.13: Customs using RFID system with secured protocols

The execution time for the tag depends on how many operation it performs. In addition, it depends on the number of digits of the random number. As found, when the number of digits of the random number increases, the execution time of the tag also increases. However, changing the number of digits of the random number gives another benefit of security in the system. After changing the number of digits in every run, the outputs from the tag are also changed. For example, in Figure 4.13 port A and port B can have the same program but different number of digits. If an attacker sniffs the output between the tag and the reader in port A, s/he cannot match this output with the sniffed output in port B. Remember that the real data are the same in both ports, but after applying the functions (encryption or

hash) the output is different. If an attacker acquired a suitable antenna, an RF receiver, and a method to sample and record the data, s/he cannot execute an eavesdropping attack. So, a tracking attack between ports is prevented. This means that the protocols provide another benefit of security in customs application. When there is a shipment coming in to a warehouse, the tag will be scanned and operate with this security protocol to designate whether the shipment is legitimate, or not.

Hong Kong customs may use a lower number of random digits. Because there is counterfeiting, Hong Kong customs might require higher security. Therefore, they use a higher number of random digits.

If enterprises, such as ports, are looking for lowest cost and high speed operations, they can choose the second protocol.If they are looking for highest security and irrespective of cost, they can choose the third protocol. If they are looking for the middle ground, with low cost and medium security,they can choose the first protocol.

In summery, the following table 4.6 demonstrates the applicability of the three developed protocols

Table 4.6: The differences between the three developed protocols

1st protocol	**2nd protocol**	**3rd protocol**
A tag performs five operations	A tag performs three operations	A tag performs six operations
It is selected when enterprises are looking for the middle ground, with low cost and medium security	It is selected for lowest cost, high speed operations	It is selected for highest security, irrespective of cost

Continued on next page

Table 4.6 *(cont'd)*

1st protocol	**2nd protocol**	**3rd protocol**
It provides integrity by generating random numbers and encrypting the contents of the messages between reader, tags, and the server using the key of a reader and a tag	It provides integrity by generating random numbers and by using the shared key between tags and the server to encrypt the contents of the messages between reader, tags, and the server	It provides integrity by using the session key that is established by the third party to encrypt all the messages that are transferred between them
It handles a compromised reader because the server sends an encrypted message using an updated group key	It handles a compromised reader because the server updates the message that has a privacy bit from 0 to 1 after finding a compromised reader	It handles a compromised reader because the server sends an encrypted message that has a session key using a valid and an updated group key
It prevents man-in-the-middle attack because mutual authentication was achieved between readers and the server; readers and tags, and random numbers were generated	It prevents man-in-the-middle attack because mutual authentication was achieved and random numbers were generated	It prevents man-in-the-middle attack because mutual authentication was achieved and random numbers were generated. Also, symmetry of the transferred messages in this protocol is avoided
It prevents replay attack because attackers cannot replay previous messages for communication	It prevents replay attack because attackers cannot replay previous messages for communication and because of the random number	It prevents replay attack because attackers cannot replay previous messages for communication and because of the random number
Authorized readers knows the key of the tag	Authorized readers cannot know the key of the tag	All readers cannot know the key of the tag. They use a session key
The server does not generate a session key used between readers and tags. It sends the key of a tag	The server does not generate a session key. It uses the shared key between the server and the tags	The server generates a session key. It does not use the keys of readers and tags
The tag performs one encryption and two hash functions	The tag performs one encryption function and one decryption function	The tag performs two encryption functions and two decryption functions

Continued on next page

Table 4.6 *(cont'd)*

1st protocol	**2nd protocol**	**3rd protocol**
There is a connection between the server and readers every time readers contact tags	The number of times a reader contacts the server is reduced. Only when one of readers in the system is compromised does the server contact the reader	There is a connection between the server and readers every time readers contact tags
A reader performs one encryption function, one decryption function, and two hash functions	A reader performs one decryption function only	A reader performs one decryption function and one encryption function
If there is a compromised reader, the reader can get the encrypted messages even if it cannot decrypt them	If there is a compromised reader, the reader cannot get any information from the tags and servers even if they are encrypted	If there is a compromised reader, the reader can get the encrypted messages even if it cannot decrypt them

4.6 Future Works

Ports worldwide, like Hong Kong, need to be monitored for security requirements based on increased counterfeiting or increased shipments movement. In this research, encryption, decryption, and hash functions are used for providing security. There are many types of algorithms for these functions. Therefore, different algorithms for these functions can be applied in the system to figure out the calculated time and compare them with the group of time that are calculated in this research. Also, the results from this research can be compared with other research, such as Chiew's works in evaluating the time cost using different types of encryption, decryption, and hash functions. [106] The calculation times are gotten when the functions are applied within the tag. In future works, this should be expanded to include all units (readers and servers) in order to analyze the time for the whole system. The path

way to do this has been created in this research.

REFERENCES

REFERENCES

[1] Bing Liang, *Security And Performance Analysis For RFID Protocols*,2010.

[2] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. *The Evolution of RFID Security*, IEEE Pervasive Computing, 5(1):62?69, January?March 2006.

[3] Alex Macario, MD, MBA; Dean Morris, MBA; Sharon Morris, RN, BSN, CNOR , *Initial Clinical Evaluation of a Handheld Device for Detecting Retained Surgical Gauze Sponges Using Radiofrequency Identification Technology*, 2006.

[4] Timothy Hay, *Using RFID To Track Surgical Sponges Left In The Body*, August 31,2010.

[5] Ari Juels. *RFID Security and Privacy: A Research Survey*, IEEE Journal on Selected Areas in Communications, 24(2):381?394, February 2006.

[6] Pawel Rotter, *A Framework for Assessing RFID System Security and Privacy Risks*, IEEE Pervasive Computing, 7(2):70?77, June 2008.

[7] Michael O. Leavitt, *An integrated strategy for protecting the nation?s food supply*, Department of Health and Human Services/ Food and Drug Administration, Nov. 2007.

[8] Rudolf, P. M. and I. B. G. Bernstein, *Counterfeit Drugs*, New England Journal of Medicine Volume 350:1384-1386, Number 14,2004.

[9] Acheson, D., *Food Protection, Food Safety and Food Defense*, Association of Food and Drug Officials (AFDO) Annual Conference. San Antonio, Texas, Association of Food and Drug Officials (AFDO), 2007.

[10] Mark Roberti, *DOD Releases Final RFID Policy*, 2005.

[11] Defense Industry Daily staff, *RFID Technology: Keeping Track of DoD?s Stuff*, Jul 13, 2010.

[12] 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, ACM, ACM Press, October 2004.

[13] Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum, *The Evolution of RFID Security*, IEEE Pervasive Computing, 5(1):62-69,January-March 2006.

[14] Liu, A. and Bailey, L., *PAP: A Privacy and Authentication Protocol for Passive RFID Tags*, 2005.

[15] Michael Grimalia, *RFID Security Concerns*, ISSA Journal, Feb 2007.

[16] Dirk Henrici, *RFID Security and Privacy: Concepts, Protocols, and Architectures*, Volume 17, pp 7-56, 2008.

[17] Ken Traub, Felice Armenio, *The EPCglobal Architecture Framework*, Dec 2010.

[18] Intermec, *The Write Stuff: Understanding The Value of Read/ Write RFID Functionality*, 2004.

[19] Klaus Finkenzeller, *RFID HANDBOOK: Radio Frequency Identification Fundamentals and Applications*, 2000.

[20] Genn W. Lee, *The Auto ID Book: Bar Coding and Automatic Identification Technologies*, Informatics, Inc, 1998.

[21] Chris Riley, David Benyon, Graham I. Johnson and Kathy Buckner, *Security in context: investigating the impact of context on attitudes towards biometric technology*, BCS '10 Proceedings of the 24th BCS Interaction Specialist Group Conference Pages 108-116 , Sept 2010.

[22] Alexander P.Pons and Peter Polak, *Understanding User Perspectives on Biometric Technology*, Communication of the ACM, Volume 51, Issue 9, Sept 2008.

[23] Won J. Jun, *Smart Card Technology Capabilities*, July 8, 2003.

[24] Daniel Kouril, Ludek Matyska, and Michal Prochazka, *Improving Security in Grids Using the Smart Card Technology*, IEEE Computer Society, September 2006.

[25] Husemann, D. The smart card: don?t leave home without it, IEEE Concurrency 7, 2, 24?27 (April?June 1999).

[26] Katherine M. Shelfer, and J. Drew Procaccino, *Smart Card Evolution*, Communications of the ACM , Volume 45 Issue 7, July 2002.

[27] Thomas Roder, *Smart Cards Solutions: Bringing Value to Citizens*, May 2012.

[28] Fletcher, P. , *Europe holds a winning hand with smart cards*, Electronic Design 47, 1 , 106, (Jan. 11, 1999).

[29] *A Summary of RFID Standards*, RFID Journal, Inc, 2005.

[30] *RFID Standards*, RFID in Europe, 2012.

[31] EPCglobal, *EPCglobal Tag Data Standards Version 1.5*, EPCglobal Ratified Standard, August 2010, `http://www.gs1.org/gsmp/kc/epcglobal/architecture/architecture_1_4-framework-20101215.pdf`

[32] Divyan M. Konidala, Woan-Sik Kim, and Kwangjo Kim, *Security Assessment of EPCglobal Architecture Framework*, April 2006.

[33] Mark Brown, Sam Patadia, and Sanjiv Dua, *Mike Meyer?s Certification Passport/ RFID+Certification*, McGraw-Hill Professional Publishing, 1st edition, 2007.

[34] Parikh, D. and Jancke, G., *Localization and Segmentation of A 2D High Capacity Color Barcode*, IEEE , 2008.

[35] GS1 DataMatrix, *An Introduction and technical overview of the most advanced GS1 Application Identifiers compliant symbology*, 2011.

[36] Bo Chen , Xiao-hui Qiang , and Ling Yu, *A lightweight color barcode algorithm and application in mobile e-commerce*,Computer Science and Education (ICCSE), IEEE 8th International Conference on , 2013.

[37] Maeva, A. and Severin, F., *High Resolution Ultrasonic Method for 3D Fingerprint Recognizable Characteristics In Biometrics Identification* , IEEE International, 2009.

[38] Zhen Liang , Fei Tan , and Zheru Chi, *Video-based biometric identification using eye tracking technique*, Signal Processing, Communication and Computing (ICSPCC), 2012 IEEE International Conference , p (728-733), 2012.

[39] Taherdoost, H. and Masrom, M., *An examination of smart card technology acceptance using adoption model* , Information Technology Interfaces, 2009. ITI '09. Proceedings of the ITI 2009 31st International Conference on , p (329-334), 2009.

[40] Smart Card Alliance, *Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications*, 2011-2012.

[41] Smart Card Alliance, *Smart Card Technology in U.S.Healthcare:Frequently Asked Questions*, A Smart Card Alliance Healthcare Council Publication, Sept 2012.

[42] Christopher J. Dyball and Terri Lichtenstein, *Optical memory cards provide secure identification*, LaserFocusWorld, International Resource for Technology and Applications in the Global Photonics Industry, Nov 2001.

[43] Yu-Yi Chen and Meng-Lin Tsai, *The Study on Secure RFID Authentication and Access Control*, Current Trends and Challenges in RFID, Prof. Cornel Turcu (Ed.), ISBN: 978-953-307-356-9, InTech, DOI: 10.5772/20750, 2011.

[44] Robinson, G. and Clarke R., *Effects of Radio Frequency Noise on Communication Capabilities of Ultra-High Frequency Passive Transponder*, Master thesis, Michigan State University, Packaging, 2010.

[45] Thamae, L.Z. , Wu, Z. and Konrad, W, *Propagation characteristics of a 2.45 GHz microwave radio frequency identification system* ,IET Journals, vol 3, issue 1, 2009.

[46] S.P. Singh, M. McCartney, J. Singh, and R. Clarke, *RFID research and testing for package of apparel, consumer goods and fresh produce in the retail distribution environment*, Packaging Technology and Science, P 91-102,2008.

[47] *GS1 General specification*, version 13.1, Issue 2, Jul 2013.

[48] MICROSCAN, *Machine Vision and Auto ID/ Track, Trace and Control Solution*, 2013.

[49] Yud-Ren Chen, Kuangkin Chao, and Moon S Kim, *Machine vision technology for agricultural application*, Computers and Electronics in Agriculture,Vol 36, Issues 2?3, Pages 173?191, November 2002.

[50] Sinopec group, *Industrial Lubricant Manufacturer Relies on Machine Vision for Product Quality and Traceability* , Food and Beverage Packaging, 2013.

[51] Wayne E. Bailey, *Fourth-Generation Sweet Potato Supplier Incorporates Traceability System in its Packing Line for PTI Compliance*, Food and Beverage Packaging, 2013.

[52] Ward, M and Kranenburg, R., *RFID: Frequency, standards, adoption and innovation*, JISC Technology and Standards Watch, May 2006.

[53] AIM Inc., *Linear Symbologies*, `https://aimglobal.site-ym.com/?page=Linear_symb`.

[54] *RFID Adoption and Implication*, A Sectoral e-Business Watch study by IDC / Global Retail Insights, study report, No. 07 /Sept 2008.

[55] The RFID Network, *Omni-ID Unveils The Ultimate Passive Tag with 135 foot Read Range*, `http://rfid.net/product-listing/reviews/183-omni-id-unveils-the-ultimate-passive-tag-with-135-foot-read-range`,Oct 2011.

[56] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, *Security and Privacy Aspect of Low-Cost Radio Frequency Identification Systems*, Security in Pervasive Computing, Vol 2802, 2004, pp 201-2012.

[57] Smart Border Alliance, *RFID Security and Privacy* , RFID Security and Privacy white paper, `http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachE.pdf`

[58] Gary Stoneburner, *Computer Security*, Underlying Technical Models for Information Technology Security, NIST, Dec 2001.

[59] M. Rieback, *RFID Malware: Truth vs myth*, IEEE Computer Society, 2006.

[60] Rieback, M.; Simpson, P.; Crispo, B. and Tanenbaum, A., *RFID Malware: Design Principles and Examples*, IEEE PErCom, 2006.

[61] Rieback, M.; Simpson, P.; Crispo, B. and Tanenbaum, A., *Is Your Cat Infected with a Computer Virus*, IEEE PErCom, 2006.

[62] Michael Grimalia, *RFID Security Concerns*, ISSA Journal, Feb 2007.

[63] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda, *Attacking RFID Systems*, in Wireless Networks and Mobile Communications Series: Security in RFID and Sensor Networks, CRC Press, ch. 2, pp. 29-48, 2009.

[64] Alexei Czeskis, Karl Koscher, Joshua R. Smith, and Tadayoshi Kohno, *RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications*, ACM, Oct 2008.

[65] Chia-hung Huang, *An Overview of RFID Technology, Application, and Security/Privacy Threats and Solutions*, Spring 2009.

[66] *RFID Security*, The Government of Hong Kong Special Administrative Region, Feb 2008.

[67] Rishab Nithyanand, Gene Tsudik, and Ersin Uzun, *Readers Behaving Badly/ Reader Revocation in PKI-Based RFID Systems*, Cryptoloy ePrint Archive, Report 2009 / 465, 2009.

[68] Juels, A., *Minimalist Cryptogarphy for Low-Cost RFID Tags*, RSA Laboratories. Bedford, 2005.

[69] Juels, A, *Strengthening EPC tags against Cloning*, Proceedings of the 4th ACM workshop on wireless security, 67-76, Sept 2005.

[70] Peris-Lopez, P.; Hernandez-Castro, J.; Estevez-Tapiador, J. and Ribagorda, A., *A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags*, Academic Press, Inc, 2006.

[71] Rivest, R., *The RC5 Encryption Algorithm*, Proceedings of the Second International Workshop on Fast Software Encryption, 1994.

[72] Smith, J; Sample, A.; Powlwdge, P.; Roy, S. and Mamishev, A., *A Wirelessly-PoweredPlatform for Sensing and Computation*, Springer-Verlag Berlin Heidelberg ,2006.

[73] Bailey, Daniel, and Juels, Ari, *Shoehorning Security into the EPC Standard*, International Conference on Security in Communication Networks - SCN 2006, p. 303-320, 2006.

[74] Juels, Ari, *Vision of RFID security*, Proceedings of the IEEE 95(8): 1507-1508. August, 2007.

[75] University of Arkansas, Fayetteville (2009, November 19). *Fingerprinting' RFID tags:Researchers develop anti-counterfeiting technology.* Science Daily. Retrieved January 14, 2011.

[76] Yao, Y.; Marcialis, G; Pontil, M.; Frasconi, P. and Roli, F., *A New Machine Learning Approach to Fingerprint Classification*, Advances in Artificial Intelligent, 2001.

[77] Chinnappa Gounder Periaswamy, S.; Thompson, D.; Di, J., *Fingerprinting RFID Tags*, IEEE Computer Society, October 2010.

[78] Danev, B.; Heydt-Benjamin, T. and Capkun, S., *Physical-layer Identification of RFID Device*, Proceeding SSYM'09 Proceedings of the 18th conference on USENIX security symposium, 2009.

[79] Saparkhojayev, N and Thompson, D.R., *Matching Electronic Fingerprints of RFID Tags Using the Hotelling's Algorithm*, Sensors Applications Symposium, IEEE, February 2009.

[80] PERIASWAMY, SCG.; THOMPSON, D. and ROMERO, H., *Fingerprinting Radio Frequency Identification Tags Using Timing Characteristics*, 2010.

[81] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, *Computer Security/ Recommendation for Key Management*, NIST, July 2012.

[82] Ari Juels, Ravikanth Pappu, and Bryan Pamo, *Unidirectional Key Distribution Access Time and Space with Applications to RFID Security*, Proceedings of the 17th conference on Security Symposium, July 2008.

[83] Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security/ Private Communication in a Public World*, Second Edition, 2008.

[84] Matt Ball, *Key Management Summit*, IEEE Computer Society, slides show and videos hosted by MSST, May 2010.

[85] *Key Management Lifecycle*, National Institute of Standards and Technology, U.S. Department of Commerce, `http://csrc.nist.gov/groups/ST/toolkit/documents/kms/lifecycle\%20slides\%20\%28b-w\%29.pdf`.

[86] A. Juels, R. L. Rivest, and M. Szydlo, *The blocker tag: Selective blocking of RFID tags for consumer privacy*, In Proceeding of the 10th ACM conference on Computer and Communication security, page 103-111, 2003.

[87] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, In Security in Pervasive Computing, volume 2802 ,pages 201?212, 2004.

[88] Sung-Ho Kim, Hong-Jin Lee, Han-Wool Jung, Beom-Ki Maeng, and Yongsu Park, *IPAP: Improved Privacy and Authentication Protocol for Passive RFID Tags*, Network Infrastructure and Digital Content, IEEE, 2010.

[89] A. Juels, P. Syverson, and D. Bailey, *High-Power Proxies for Enhancing RFID Privacy and Utility*, Privacy Enhancing Technologies (PET) Workshop, pp. 210-226. 2005.

[90] Alex X. Liu, LeRoy A. Bailey and Adithya H. Krishnamurthy, *RFIDGuard: a Lightweight privacy and authentication protocol for passive RFID tags*, Security and Communication Networks, page 384-393, 2010.

[91] A. Juels, D. Molnar, and D. Wagner, *Security and privacy issues in e-passports*, In Security and Privacy for Emerging Areas in Communications Networks ? SECURECOMM, 2005.

[92] R. Housley, W. Ford, W. Polk, and D. Solo. *RFC 2459: Internet X.509 public key infrastructure Certificate and Certificate Revocation List (CRL) Profile*, Network Working Group, April 2002.

[93] R. Nithyanand, G. Tsudik, and E. Uzun, *Readers behaving badly: reader revocation in PKI-based RFID systems*, ESORICS'10 Proceedings of the 15th European conference on Research in computer security, page 19-36, 2010.

[94] Pearson, J., *Securing the pharmaceutical supply chain with RFID and public key infrastructure (PKI) technologies*, in Texas Instruments White Paper, 2005.

[95] Hakeem, M., Raahemifar, K., and Khan, G., *A Novel Key Management Protocol for RFID System*, IWCMC, page 1107-1113, IEEE, 2013.

[96] Chung Kei, Mohamed Gouda, and Simon Lam, *Secure Group Communications Using Key Graphs* ,2000.

[97] Claire Swedberg, *Hong Kong Customs Moves Forward With E-Lock Plans*, May 4, 2012.

[98] Asia-Pacific Economic Cooperation (APEC), *Using RFID for customs control transit containers*, submitted by Chinese Taipei, Feb 2009.

[99] *EPCglobal: Low Level Reader Protocol (LLRP)*, ver 1.1, Oct 13, 2010, `http://www.gs1.org/gsmp/kc/epcglobal/llrp/llrp_1_1-standard-20101013.pdf`

[100] *EPCglobal: Reader Management (RM) ver 1.0.1*, May 31, 2007, http://www.gs1.org/gsmp/kc/epcglobal/rm/rm_1_0_1-standard-20070531.pdf

[101] Kateryna Daschkovska and Bernd Scholz-Reiter, *Electronic Seals for Efficient Container Logistics*, Dynamics in Logistics, Springer Berlin Heidelberg , pp 305-312, 2008.

[102] *Confidex supplies the EPC Gen2 compliant RFID e-seal in multi-million dollar contract*, Jan 11,2011, IT reseller, http://www.itrportal.com/articles/2011/01/11/6319-confidex-supplies-the-epc-gen2-compliant-rfid-e-seal url-in-multi-million-dollar

[103] World Customs Organization, *Customs capacity to fight counterfeits strengthened by WCO/GS1 cooperation agreement*, Brussels, Sept 6 2012, http://www.wcoomd.org/press/?v=1&lid=1&cid=14&id=316

[104] Dong Kyue Kim, Mun-Kyu Lee, You Sung Kang, Sang-Hwa Chung, Won-Ju Yoon, Jung-Ki Min, and Howon Kim, *Design and Performance Analysis of Electronic Seal Protection Systems Based on AES*, ETRI Journal, vol. 29, no. 6, pp. 755-768, Dec. 2007. http://dx.doi.org/10.4218/etrij.07.0107.0068

[105] T. Drake and J. Reinold, *ISO Study: Vulnerabilities and Threats for Container Identification Tags and e-Seals*, 2005.

[106] Chiew, K., Yingjiu Li, Tieyan Li, Deng, R.-H., Aigner, M., *Time Cost Evaluation for Executing RFID Authentication Protocols*, Internet of Things (IOT) , vol., no., pp.1,8, Nov. 29 2010-Dec. 1 2010.

[107] Chae, H.-J., D. J. Yeager, J. R. Smith, and K. Fu, *Maximalist cryptography and computation on the WISP UHF RFID tag*, in The Conference on RFID Security 2007 (RFIDSec 07), Malaga, Spain, Jul. 11?13, 2007.

[108] *MSP430-P2274 development board, Users Manual*, Olimex,July 2009.