MUTUAL AUTHENTICATION PROTOCOL MODEL FOR LOW-COST RFID SYSTEMS BASED ON SHELLED RANDOM VALUE

by

MU'AWYA NASER SALAM AL-DALA'IEN

Thesis submitted in fulfillment of the requirements

for the degree of Doctor of Philosophy

Jun 2011

DEDICATION

To my parents and family who offered me unconditional love and support throughout the course of this thesis.

بسم الله الرحمن الرحيم

ACKNOWLEDGMENTS

The praises are due to Allah, The Lord of the Worlds, and may the prayers of blessing of Allah be upon Prophet Muhammad, the chosen, the trustworthy, and upon his family and all of his companions.

This research project would not have been possible - after blessing of Allah - , without the support of many people. I wish to express my gratitude to my supervisor, Assoc. Prof. Dr. Rahmat Budiarto who was abundantly helpful and offered valuable assistance, support and guidance. Deepest gratitude are also due to the members of the supervisory committee, Assoc. Prof. Dr. Muhammad Rafie Hj. Mohd. Arshad, Dr. Wafaa Ali Alsalihy and Dr. Pedro Paris-Lopez without whose knowledge and assistance this study would not have been successful. Special thanks also to all of school staff, especially Mrs. Noor Azlina Yusoff and Mr Mohd Redzuan Asmi for their assistance.

I wish to express my love and gratitude to my beloved family and my fiancée Najlaa Abu-Adhmah; for their understanding & endless love, through the duration of my studies.

I must also acknowledge my friend Mohammad Al-Majali who I appreciate his vast knowledge and skill and his assistance in writing my thesis. Also my friends Dr. Yazan Wrekat and his daughter Balqees, Dr. Ahmad Al-Shabatat , Dr. Esaa Al-Khutaba, Dr. Hussein Al-Bazar, Dr. Mohammad Al-Betar. Eng Mr. Mahmoud Al-Hasanat, Mr. Ali Al-Bdour, Mr. Mohammad Al-Habahbeh, Mr. Mohammad Al-Khresat, Mr. Sdam Al-Widyan, Mr. Ibrahem Al-Khasaba, Mr. Hammam Al-Matarneh, Mr. Rafi Al-Njadat and Mr. Masha'al Al-Qudah.

I would also like to convey thanks to the school of computer sciences, institute of postgraduate studies (IPS) and the USM fellowship scheme for providing financial support and laboratory facilities.

To each of the above, I extend my deepest appreciation.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ALE	Application Level Events
AtSe	CL-Based Attack Searcher
AVISPA	Automated Validation of Internet Security Protocols and Applications
CBC	Cipher Block Chaining Mode
CRC	Cyclic Redundancy Code
EMAP	An Efficient Mutual-Authentication Protocol For Low-Cost RFID Tags
EPCglobal	Electronics Product Code Global Incorporated
EPCIS	EPC Information Services
FC	Faraday Cage
GEN 2	EPC Class 1 Generation 2
GEN1	EPC Class 1 Generation 1
HF	High Frequency
HLPSL	High-Level Protocol Security Languages
IDS	Index Pseudonym
ISO	International Organization For Standardization
LF	Low Frequency

LMAP	A Real Lightweight Mutual-Authentication Protocol For Low-Cost RFID Tags
M2AP	A Minimalist Mutual-Authentication Protocol For Low-Cost RFID Tags
OFMC	On-The-Fl Model Checker
ONS	Object Name Service
PRNG	Pseudo-Random Number Generator
RFID	Radio Frequency IDentification
RP	EPC Reader Protocol
SASI	Strong Authentication and Strong Integrity Protocol
SATMC	SAT-Based Model-Checker
SHA1	Standard Hash Function1
SLRV	Shelled Lightweight Random Value Protocol
SRV	Shelled Random Value Model
SURV	Shelled Ultralightweight Random Value Protocol
TA4SP	Tree Automata-Based Protocol Analyzer
TBD	To-Be-Done Queue
TDS	Tag Data Standard
TID	Tag IDentifier
TP	EPC Tag Protocol
UHF	Ultra-High Frequency

MODEL PROTOKOL PENGESAHAN BERSAMA BAGI SISTEM RFID BERKOS RENDAH BERDASARKAN NILAI RAWAK BERPETALA

ABSTRAK

Mereka bentuk sebuah protokol kos rendah yang boleh dipercayai dan selamat untuk mengenal pasti frekuensi radio (RFID) adalah amat sukar. Piawai primitif kriptografik boleh menjadi suatu kekangan untuk tag berkos rendah memandangkan ia memerlukan kos yang agak besar dan mahal dari segi saiz litar, penggunaan kuasa, dan saiz ingatan. Oleh itu, kriptografi ultra-ringan dalam mereka bentuk protokol RFID berkos rendah yang mampu melaksanakan sesi komunikasi data dengan cekap dan berkesan amat diperlukan bagi menangani masalah bebanan pangkalan data, serangan pasif, penyahlarasan dan masalah kos pengkomputeran yang tinggi. Tesis ini memperkenalkan model (SRV) untuk mereka bentuk protokol keselamatan berkos rendah yang cekap, dan mencadangkan dua protokol RFID berkos rendah yang selamat (SURV dan SLRV) berdasarkan pengesahan bersama antara ultra-ringan dan ringan dengan menggunakan gabungan primitif keselamatan konvensional dan bukan konvensional.

Penilaian kualitatif dan kuantitatif yang menyeluruh telah dijalankan ke atas protokol yang telah direka bentuk. Kedua-dua protokol telah dianalisis secara kualitatif dari aspek keupayaannya menyediakan kerahsiaan data, anonimiti tag, pengesahan bersama dan integriti data, keupayaan mengendalikan keselamatan ke hadapan dan serangan yang dimainkan semula, penyahlarasan, dan serangan manusia-di-tengah dan serangan pendedahan. Kedua-dua protokol telah mencapai prestasi keselamatan yang ketara positif dalam semua aspek berbanding dengan semua protokol dalam literatur yang dikaji sebelum ini. Begitu juga, kedua-dua protokol telah dinilai secara kuantitatif terhadap serangan pasif dengan menggunakan alatan Diehard dan ENT, yang telah membuktikan tahap keselamatan yang tinggi menerusi mesej yang sangat rawak, dan terhadap beban pangkalan data dengan menggunakan tiga algoritma carian yang berbeza ke atas tiga set data yang saiznya berbeza mengikut pilihan. Selain itu, pelaksanaan yang dicadangkan telah dikemukakan untuk memperlihatkan kecekapan kos bagi protokol yang dicadangkan. Penilaian ini juga merangkumi pengesahan keselamatan dengan menggunakan alat AVISPA. Walau bagaimanapun, keputusan terhadap keupayaan AVISPA mengesahkan protokol RFID umumnya dan protokol kami khususnya, membuahkan hasil yang negatif.

MUTUAL AUTHENTICATION PROTOCOL MODEL FOR LOW-COST RFID SYSTEMS BASED ON SHELLED RANDOM VALUE

ABSTRACT

Designing a reliable secure low-cost protocol for radio-frequency identification (RFID) is difficult, standard cryptographic primitives can become a limitation for low-cost tags due to their costly large requirements in terms of circuit size, power consumption, and memory size. Therefore, ultralightweight cryptography in designing low-cost RFID protocols capable of executing data communication sessions efficiently and effectively are needed to solve database loading, passive attacks, desynchronization and high computational cost problems. This thesis presents a model (SRV) for designing efficient low-cost security protocols, and proposes two low-cost RFID secure protocols (SURV and SLRV) based on ultralightweight and lightweight mutual authentication using a combination of conventional and unconventional security primitives.

Comprehensive qualitative and quantitative evaluations were performed on the designed protocols. Both protocols have been analyzed qualitatively for its ability to provide data confidentiality, tag anonymity, mutual authentication and data integrity, capability to handle forward security and replay attacks, desynchronization, and man-in- the-middle and disclosure attacks. Both protocols achieved significant positive security performance in all aspects compared to all protocols in the studied literature. Similarly, both protocols have been evaluated quantitatively using Diehard and ENT tools for passive attacks, which proofed high security through highly randomized messages, and against database loading using three different search algorithms on three datasets with different sizes alternatively. Furthermore, proposed implementations have been put forward to illustrate the cost efficiency for the

proposed protocols. The evaluation also included security verification using the AVISPA tools. However, the results on the capability of AVISPA to verify RFID protocols in general and our protocols in particular, came out negative.

Chapter 1

INTRODUCTION

1.1 Introduction

Before the advent of electronic communication and data transfer, preserving data security was simpler in some ways. Records were produced by hand and stored on paper, and physical access to them was limited by keeping valuable documents in a safe. This minimized the risk of altering or destroying the data. Electronic communication aimed to mimic the whole process by electronically storing, securing, and exchanging data. Methods to grant access only to authorized entities (e.g., encryption) were also invented. The more important and sophisticated the system (hardware and software), the more challenging and innovative the attack. Therefore, several initiatives were taken to protect data depending on the communication model measures and the relative importance of the data, while most studies focused on minimizing the cost of these measures to widen the security primitives a system holds.

Radio Frequency IDentification (RFID) technology is a promising data communication tool for wide adoption due to its simplicity, relatively low cost, and wide range of data volume capacity and implementation models, especially in identity verification, supply chain, and asset management (Weinstein, 2005). The promised benefits of RFID include authentication-based access, productivity gains in the warehouse, better product visibility in the distribution channel, improved inventory accuracy, less shrinkage, reduced number of transaction errors, better asset tracking and utilization, and easier detection of counterfeit products, such as fake identity cards (Michael and McCathie, 2005, Want, 1991). Despite these factors, the adoption rate of RFID technology has significantly stalled in recent years, mainly due to security and privacy reasons, especially in low-cost RFID. The use of RFID technology has engendered considerable controversy and even product boycotts by consumer privacy advocates in some countries because using low-security primitives might enable sensitive data gathering about an individual without consent, which jeopardizes the holder's privacy.

RFID is defined as a technology that uses communication via electromagnetic waves to exchange data between a terminal and an object, such as a product, animal, or person, for the purpose of identification and tracking. Some tags can be read from several meters away and beyond the line of sight of the reader. The RFID system components principally consist of tags, readers, and backend databases. The RFID system transmits data embedded in wave signals over an open wireless channel. These waves can be transmitted and received by almost anyone with the right gear, and thus, data encryption and entity authentication play huge roles in implementing a secure RFID technology.

Several approaches have been taken to accommodate different implementations. Nevertheless, a large gap exists in the trade-off between the cost and the security level offered. Most of these approaches significantly correlate the two factors by linking the increase of security levels to the dramatic increase in cost, which in this case follows a categorization in the RFID technology binding low-cost RFIDs to low-security primitives. For this reason, this thesis attempts to reduce the aforementioned gap by providing low-cost and high-security level RFID solutions using different methods to enable various implementations of utilizing the underlying algorithms. The solutions include introducing RFID technology with a new notion of shelled data under two protocols, namely, Shelled Ultralightweight Random Value (SURV) and Shelled Lightweight Random Value (SLRV).

The rest of this chapter is organized as follows. The next section portrays the background for the technology, and the security concerns and solution standards within the security protocols. Section 1.3 shows the problem statements. 1.4 lists the thesis objectives. The motivation behind the research and its significance are illustrated in Section 1.5. The scope of the research is shown in Section 1.6. We conclude with the organization and outlines for the rest of the thesis in Section 1.7.

1.2 Background of the research

RFID systems produce methodologies that offer data portability by embedding data in small devices (tags) that can be mobile and held within other objects. These data may include identification to grant access authentication for several transactions or entry passes through secured checkpoints in different locations. The security and privacy issues for these data are vulnerable to various threats (Shih et al., 2005, Kim et al., 2007, Knospe and Pohl, 2004, Sarma et al., 2002). Recent studies in RFID attempted to find solutions for several applications within the field. However, the solutions offered are often hindered by the fact that, in most cases, different RFID deployments do not meet required security specifications and needs (Kim et al., 2007, M. Naser, 2008, Rotter, 2008). These solutions could also be hindered by other implementation obstacles, such as cost and compliance with existing RFID standards.

RFID technology implementation represents a wireless network where data transfer or exchange is mainly secured by encrypting the data over the open channels and decrypting the data at the authorized entities when received. Any security protocol designed to fulfill the needs and special requirement of this technology should conform to the implantation specifications and standards. We give an overview of development environment components, such as network security, security protocols, and cryptography, and define the RFID system and its relative importance in the foreseen implementations.

1.2.1 Network Security and Protocols

Computer networks are defined as a collection of computers and devices interconnected by communications channels that facilitate communication among users (businesses, government agencies, individuals, and machines) and allow them to share resources. Networks may be classified into public (open access) or private (controlled access) based on the utilizing users. Networks mainly consist of nodes, servers, and/or host computers. Nodes refer to “client” terminals (e.g., individual user PCs).

All procedures, processes, and actions performed to ensure network usability, integrity, sustainability, privacy, and value of data and operations are acknowledged as Network Security. Measures, characterized as short programs used to protect computer data and communication in transit over a network, are called network security protocols (Kaufman et al., 2002). The primary tool used to protect information as it travels across a network is cryptography (see Section 1.2.2). Cryptography performs data encryption via algorithms to render data readable only by authorized users. In general, cryptography for delivering a secure data transfers through a set combination of procedures or protocols that manage the exchange of data between networks and devices. Furthermore, any effective network security strategy requires the identification of possible threats, and accordingly, the most effective combination of procedures, tools, and protocols to defend against the identified threats is chosen.

Common threats to network security include threat tools (e.g., Viruses, Trojan horse programs, and Vandals) and threatening actions (e.g., Data Attacks, Data Interception, and Social Engineering). The latter can use one or more tools in achieving its purpose. The following are brief descriptions for these threats:

- **Viruses:** Computer programs written by devious programmers and designed to replicate themselves and infect computers when triggered by a specific event

- **Trojan horse programs:** Delivery vehicles for destructive codes that appear to be harmless or useful software programs such as games

- **Vandals:** Software applications or applets that cause destruction

- **Data Attacks:** Reconnaissance attacks (information-gathering activities to collect data that are later used to compromise networks), access attacks (exploits network vulnerabilities to gain entry to e-mail, databases, or the corporate network), and denial-of-service attacks (prevents access to a part of or the entire computer system)

- **Data Interception:** Involves eavesdropping on communications or altering data packets being transmitted

- **Social Engineering:** Obtaining confidential network security information through nontechnical means, such as posing as a technical support person and asking for people's passwords

In this context, security protocols are gaining increased importance in almost any data transaction activity in all networks domains, especially in organizational and business transactions. Security protocols aim to provide confidentiality, authenticity, privacy, anonymity, and fairness, among many others. Moreover, we argue that theories should provide integrity when coupled with applications. In the sense of network security applications, the vulnerability of any protocol can be found in an application even after the protocol is accepted as a standard. A popular example is the Needham-Schroeder protocol (Needham and Schroeder, 1978), in which Lowe discovered a flaw 17 years after the protocol's publication (Lowe, 1996, Lowe, 1995). This proves that using a strong security solution does not necessarily protect against all possible threats. Again, proper network security strategy and consideration of different variables play huge roles in securing any network. Figure 1.1 provides proof for this notion.

1.2.2 Cryptography

The notion of cryptography has been in use for centuries for civilian and military purposes (e.g., cipher wheels or marks on papers in World War I, and Purple machine and Enigma in World War II) . Cryptography has significantly developed with the help of technology to provide a high level of security for data exchanged in daily essential communications, such as Internet communications, banking transactions, and wireless communication. It has helped introduce new communication models and has radically reshaped some existing communication methods.

Cryptography can be defined as the art of protecting information by converting (encrypting) data into scrambled, unreadable, and/or unmeaningful code (cipher-text) that can be sent across public or private unsecured network channels to be understood only by the intended recipient. Cryptography reverses these data into the original form (decryption). It is generally designed to provide confidentiality, authentication, integrity, and accessibility services (Stallings, 2010).

Confidentiality service is used to ensure that messages are accessible only to authorized recipients. **Authentication** is normally used to authenticate the identity of the connected parties. Preventing eavesdroppers from changing the content of the messages sent from source to destination is basically provided by the **integrity** service. Lastly, **accessibility** is designed to allow only authorized parties to use available information resources.

There are two main styles or forms for data encryption in cryptography: symmetrical and asymmetrical. Symmetrical encryption algorithms use a secret key shared by both sides of the communication for encrypting the data on one side and decrypting it on the other side. Hence, this method is referred to by different studies as secret-key, shared-key, and private-key encryption. In this method, the encryption and decryption keys can be exact copies or, for an enhanced level, loosely related to each other.

Asymmetrical encryption, on the other hand, does not dictate a secure initial exchange between both sides of the transaction for one or more secret keys. Asymmetric algorithms create a mathematically related key pair, a published public key and a secret private key. The former is used to encrypt a message which can only be decrypted using the private key. This helps protect the confidentiality and integrity of a message. Similarly, private key encryption creates a digital signature for a message, which can be verified by the public key to preserve the message's authenticity.

The process of breaking the encryption protocol or algorithm (code breaking) aimed at obtaining the hidden information and/or preventing the communication session from successfully completing is known as cryptanalysis. Methods of avoiding security measures for exchanging data in a protocol include understanding how the system works and finding a way to get around it through obtaining the secret key to decrypt data, misleading the receiver by injecting false data, or revoking the authenticity capability for futuristic communication. The definition of cryptanalysis implies the performing of logical attacks via mathematical perception and standards, excluding physical attacks such as bribery, physical coercion, burglary, keystroke logging, and social engineering because these attacks are independent from the security model set by the cryptography scheme.

In cryptographic taxonomy, both cryptography and cryptanalysis are part of one science under the name of Cryptology, which intends to acquire a better understanding of the methods of securing information and communication technologies. The sciences of Cryptology and its cryptographic primitives are depicted in Figure 1.2.

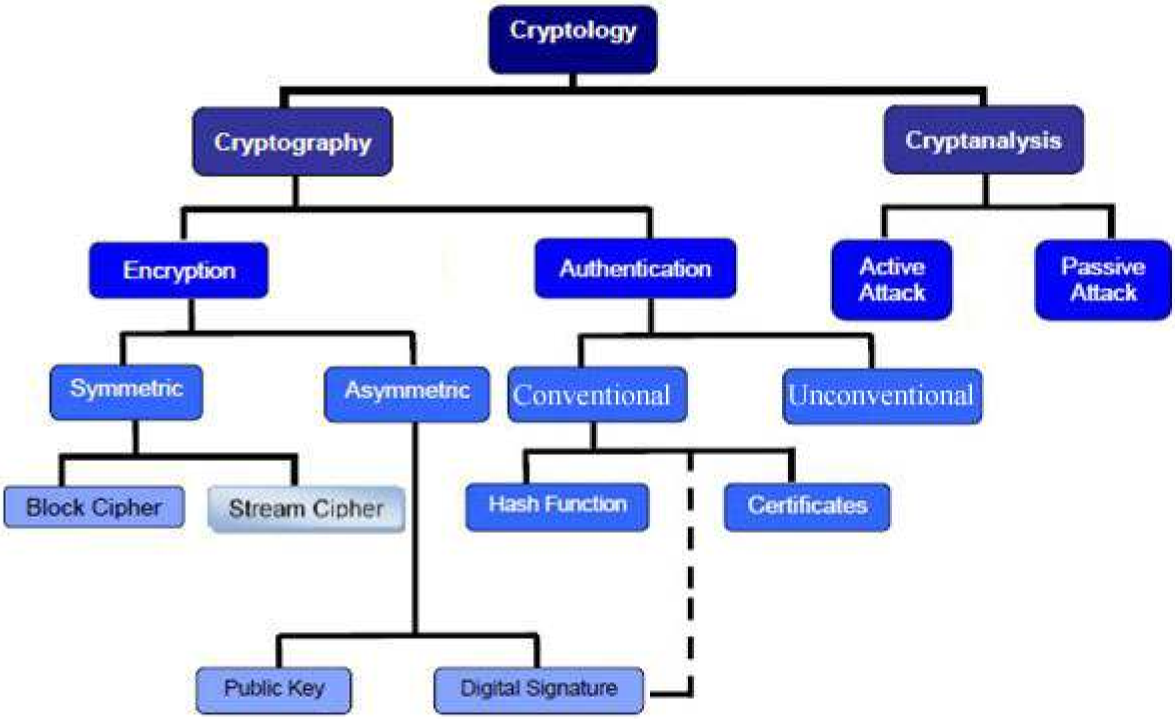

Figure 1.1: Taxonomy of Cryptology

Figure 1.2 illustrates the categories and sub-categories of cryptosystems, where cryptology science is divided into a Cryptanalysis category and a Cryptography category. The former is further classified into passive attacks aiming to obtain the confidential data and active attacks aiming to alter the exchanged messages' data, and the latter is further classified into two sub-categories: Authentication and Encryption. Authentication is comprised of hash functions and certificates authentication, and Encryption is comprised of the aforementioned symmetric and asymmetric cryptosystems. In this research, we only focus on mutual authentication, which falls under cryptography.

Data security is a mathematical definition based upon the application of a given encryption. From a cryptography perspective, although symmetric and asymmetric cryptosystems share the same goal of successfully encrypting and decrypting users' messages, the principal deviance between those cryptosystems is the use of an additional key in the asymmetric cryptosystems. Conversely, the fundamentals defer from a cryptanalysis perspective, where symmetric cryptosystems are vulnerable to plain-text attacks and linear cryptanalysis, usually characterizing high risk by being simple to decode. Careful planning for the cryptographic process coding and functions is therefore necessary to reduce this risk. Asymmetric encryption is considered relatively harder to break and has proved to be secure against intruders with computationally limited resources because it requires much more complicated mathematical processes to bypass the security and, in particular, because the private key cannot be derived from the public key. A common method of asymmetric encryption is using a random key generated by the public key of the sender. This method varies in application depending on the encryption protocol and its intended use.

1.2.3 Radio Frequency IDentification (RFID)

Radio Frequency IDentification (RFID) is basically a technology for wireless information exchange over short distances (Riedl et al., 2007). RFID technology uses radio waves to identify and track animals, objects, products, and even humans. It was originally meant to replace traditional barcode systems and overcome their limitations because optical barcodes suffer from several drawbacks, such as the need for human intervention to scan the barcode, required physical manipulation of the object to be scanned to align the barcode with scanners or the other way around, limited data storage on barcodes, and worst of all, the compromised readability of the barcode as a result of dirt, moisture, abrasion, or packaging contours (Shih et al., 2005). These limitations, which confine the performance of the traditional barcode system, can be overcome by RFID.

The benefit of RFID over the barcode system is that RFID does not require direct contact (line of sight scanning). RFID uses radio waves which can pass through objects and automatically identify the object holding the tag. In this case, less human intervention is needed, which, in turn reduces operation costs. Furthermore, the tag is embedded inside the object, which reduces the possibility of the tag from being susceptible to water, dirt, and similar materials that can easily damage the barcode.

Radio frequencies were first used by the Allies during World War II to identify enemy or unfriendly aircrafts. However, at the time, its use was not widespread. However, later on and to date, due to the continuous decrease in the cost of its equipment and tags, and the increased reliability and establishment of international standard, RFID technology started to expand and is now widely used in many applications, beginning with animal tracking and identification, inventory applications, healthcare system (Kuo et al., 2007), and industries (Al-Kassab and Rumsch, 2008). Another important reason is the adaptation of RFID technology for identification at case-level of the supply chains by major retailers, such as Wal-Mart, Albertsons, and Target. Similarly, the U.S. Department of Defense ordered that all shipments to its armed forces be equipped with RFID tags.

Recently, research has been conducted regarding the usage of RFID technology for human-centric applications, such as Islamic Pilgrimage identification (Mohandes, 2008), crowded event management (Yamin et al., 2009), crowd management (Yamin and Ades, 2009), and security consideration in embedding RFID in "Hajj" systems (Naser et al., 2010b). To accommodate the various possible applications, RFID had broadened protocol development into several categories and sub-categories. In our research, we focus on low-cost mutual authentication sub-categories, such as lightweight and ultralightweight protocols under several standards like Gen-2.

Despite the many advantages of RFID, the main concern remains to be the privacy and security of the RFID systems. The information stored in an RFID tag is considered crucial when it involves identification, money transactions, critical circumstances involving RFID devices in military missions, or failures of RFID-based healthcare systems during major surgeries, which could be life threatening. Lei et al. listed some security properties in their research, such as information leakage, intractability, forward security, and mutual authentication(Lei et al., 2010) . Meanwhile, common types of attacks in the RFID system, such as Man-in-the-Middle, Malicious tracking, Denial-of-Service (DoS), Replay, and Attack against forward security, will be discussed in detail in Chapter 2.

Many studies have been conducted in the attempt to overcome some of these security issues. Nevertheless, no standard currently exists to evaluate the overall security performance of these protocols. Further research needs to be done for standardization efforts in RFID protocol designing framework. Nonetheless, although most studies in securing RFID share common grounds and are based on cumulative work, they do not follow an obvious RFID-consistent protocol development framework.

1.3 Problem Statement

In previous studies, the RFID tag has several types and a variety of applications which lead to diverse options for solving the security issues of these applications. Meanwhile, the low-cost RFID tag has its own limitation and security concerns, whereby the main goal for its protocols is to find a strong trade-off method between good security and low-cost implementation. The main problems faced when designing efficient and effective protocols are to solve Desynchronization, Database Loading, Tag Computations, and Passive Attacks. This research focuses on solving these problems; where detailed description for these concerns can be found in section 4.2.1.

1.4 Research Objectives

The aim of this thesis is not only to develop low-cost RFID protocols but also to show that these protocols can outperform other protocols in terms of performance and security level it provide for low-cost RFID systems published in the literature. Thus, new alternatives for solving security problems are provided.

The key objectives of the research presented in this thesis are as follows:

1. To provide a critical review and analysis for significant protocols in the low-cost RFID mutual authentication field and identify weaknesses and misuses of the involved security primitives.
2. To propose a RFID protocol based on Lightweight mutual authentication conforming to EPC Class-1 Generation-2 standard.
3. To propose a RFID protocol based on Ultraightweight mutual authentication.

4. To provide an effective evaluation for the proposed RFID protocols under a suitable structure.

1.5 The Research Motivation

RFID is expected to play an important role in future ubiquitous computing. According to ABI research in 2008, the total RFID revenue will amount to more than $5.6 billion in 2009, the global RFID industry will be valued at $9.7 billion by 2013, and the compound annual growth rate will be about 15%. The total volume of tags used worldwide will reach 10.6 billion pieces in 2011, 80% of which will be UHF passive tags.

Recently, IDTechEx forecasted that the entire RFID market value will be $5.63 billion in 2010, up from $5.03 billion in 2009. This includes tags, readers, software, and services for RFID cards, labels, fobs, and all other form factors. The $3.27 billion of the total $5.63 billion is spent on non-carlike structures: from RFID labels to active tags. In retail, RFID is facing rapid growth for apparel tagging. In 2010, this application alone demanded 300 million RFID labels. In the same year, RFID in the form of tickets used for transit demanded 380 million tags, while a substantial 178 million tags were used in the tagging of animals (such as cow, sheep, and pets), which has become a legal requirement in many territories. This phenomenon is happening in regions such as China and Australasia. In total, 2.31 billion tags were sold in 2010 versus 1.98 billion in 2009. Most of the growth is from passive UHF RFID labels.

At the same time, RFID systems also need security methods that can prevent several attacks. Prevention of attacks leads to increased readability of the RFID system. The increasing demand for securing the RFID system motivates this research, especially in the area of low-cost RFID tag, where the demand is huge and increasing rapidly.

There are many proposed solutions for securing RFID technology under different categories and standards. Thus far, none of these protocols have proven to be a universally secured protocol for a given category or standard. The limitations and multiple assumptions of these protocols hinder their widespread application and utilization.

In this thesis, we seek to point out where previous proposals failed and which threats they failed to address. We do this by focusing on previously proposed protocols in one of the RFID standards, namely, Class-1 Generation-2 tags under the lightweight category to identify their strengths and weaknesses. We aim to utilize these protocols as basis for creating better protocols capable of providing a high security level, especially in terms of continuous functionality and preserved privacy.

The expected outcome of the research in the form of two lightweight RFID protocols and their experimental results may generate new significant scientific and practical knowledge in their possible implementations.

1.6 Scope of the Research

Although this thesis will review different standards, it would not be possible to conduct a comprehensive survey of all of them, and/or create one solution fitting all standards due to manufacturing and implementation primitives based on the intended purposes of application. Therefore, the scope of this thesis will be RFID systems implementing lightweight and ultralightweight protocols conforming to Class-1 Generation-2 tags, which fall under low-cost tag category.

1.7 Thesis Organization

The organization of this thesis is as follows:

First, a comprehensive explanatory platform of RFID technology literature review is stated in Chapter 2. This chapter comprises six sections which review RFID Technology, RFID standards, RFID security, RFID Privacy, RFID Attacks, and an overview of RFID solution categories.

Next, an extensive literature review of low-cost mutual authentication protocols is provided in Chapter 3. This chapter comprises two sections reviewing two categories in low-cost RFID protocols, namely Lightweight mutual authentication protocols and Ultralightweight mutual authentication protocols, where each section reviews and analyze a set of significant protocols for each respective category and indicates weaknesses in each of the discussed protocol.

Chapter 4 demonstrates the methodology followed by the researcher in an attempt to employ a state of the art method that involves using a Shelled Random Value (SRV) model as a development tool for two RFID low-cost mutual authentication protocols. The chapter also presents the evaluation framework for the proposed protocols with respect to the implementation restrictions.

The first protocol named Shelled Ultralightweight Random Value (SURV) protocol is presented in chapter 5, which is designed based on lightweight security primitives on the tag side and standard cryptography primitives on the reader's side. Deep dissection for performance and security analysis of SURV and comparison with existing protocols are presented in this chapter.

In Chapter 6, we continue with the proposed protocols and present a Shelled Lightweight Random Value (SLRV) Protocol, conforming to RFID EPC Class-1 Generation-2 standard and designed based on lightweight security primitives on the tag side and standard cryptography primitives on the reader’s side. Deep dissection for performance and security analysis of SURV in comparison with existing protocols are presented in this chapter.

The proposed protocols are evaluated in chapter 7 along with the implementations and testing results. In this chapter, four main considerations are covered. The first is evaluating the proposed protocols’ ability to protect against passive attacks. The second consideration is security protocol verification. The third consideration is evaluating the suitability and benefit of using binary search algorithm in the proposed protocols to reduce the time consumed for data retrieval from the database, and to minimize database loading. The fourth consideration is evaluating the proposed protocols in terms of cost efficiency and illustrating their logical schemes and dataflow to prove that they reduce the tag computations and thus are low-cost RFID security protocols.

Finally, Chapter 8 summarizes and concludes the research that has been carried out to achieve this thesis. In addition, the chapter includes the summary of contributions, which presents the areas of contributions made and the products of the research which have been realized and named as SURV and SLRV. The chapter also highlights that both protocols have been thoroughly tested using several methods for evaluation against well-known published RFID security concerns, for the standards identified in the scope of the thesis, compromising the completion of successful communication sessions without jeopardizing the incorporated private data. Thereafter, the chapter suggests futuristic research prospects.

Chapter 2

FUNDAMENTALS OF RADIO FREQUENCY IDENTIFICATION

2.1 Introduction

This chapter explains Radio Frequency IDentification (RFID). The characteristics and standards of RFID technology are presented in Sections 2.2 and 2.3, respectively. Security concerns within the RFID technology are discussed in Section 2.4. In Section 2.5, the significance of including privacy as a design objective is described. Details on possible attacks on RFID networks are presented in Section 2.6. Finally, an overview of RFID solution categories is given in Section 2.7.

2.2 RFID Technology

RFID technology is a complement to the invention of Guglielmo Marconi in 1901. He was the first person to transmit radio signals over the Atlantic. Since then, this technology has continuously developed. In 1935, radar was invented by the Scotsman, Alexander Watson-Watt. Despite the limitation of the radar at that time, a huge application for the technology was discovered in the Second World War. Identification Friend or Foe was created by the British to distinguish between their airplanes and German aircrafts. This was considered the first RFID application. The first patent for this domain was the "Portable radio frequency emitting identifier" in 1983, and the first paper was published in 1984 by Harry Stockman (Stockman, 1984). Since the time of the IFF, the development of RFID has accumulated in areas of price reduction, performance improvement, enhanced security, and new application domains. The Massachusetts Institute of Technology Auto-ID Centre

1999 was one of the most significant organizations that helped make RFID research recognizable.

The extension of using the barcode for identification purposes opened possibilities for developing new technology to overcome limitations in barcodes, such as the need for direct line-of-sight within a short distance from the reader to the printed barcode and the long processing speed (one item at a time). RFID tags do not need direct line-of-sight, they can read from a long distance. RFID readers are also much faster (able to read several tags at a time). Furthermore, barcodes do not have a read/write capability and could not be reused, whereas RFID tags could be reused and their data overwritten.

In general, there are three main components in RFID systems: the tag, the tag reader, and the backend database (Chen et al., 2010). These three components communicate with one another in order to identify, track, or monitor objects using radio frequency waves between the tag and the reader, which uses an ordinary network connection with the application server (backend database). Figure 2.1 depicts a general architecture for the RFID system.

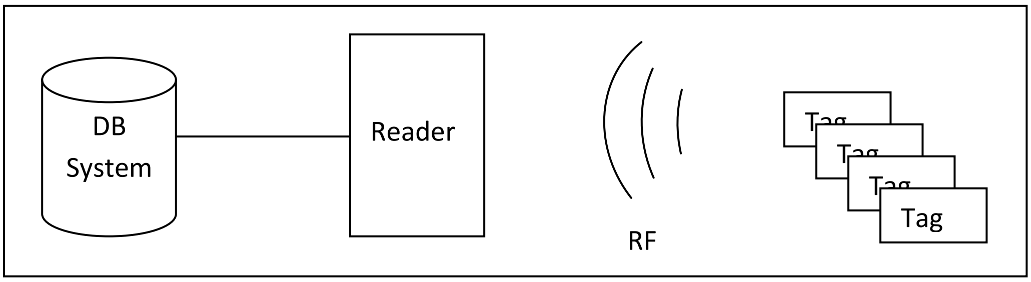

Figure 2.1: RFID System Architecture

The tag is basically a combination of an antenna used for transmitting and receiving radio frequencies and an integrated circuit that processes and stores data. Data can be the tag's ID, the tag's manufacturer, and other details related to the tagged item (i.e., the tag's holder). Tags can be classified into three different groups:

active, passive, and semi-passive. Active tags and semi-passive tags have internal batteries which aid in longer transmission ranges. Passive tags gain electricity through radio waves to receive and send back the necessary data to the reader(Yeh et al., 2010) .

The reader retrieves any data sent by the tag and then processes these data in the backend database server. The reader acts as an interpreter between the tag and the backend database. The backend database server is responsible for the authentication processes and other available services (Lei et al., 2010). Often, the reader and the backend database server are treated, in most literature, as a single entity because the communication between these two components is considered secure. On the other hand, the open wireless communication between the tag and the reader is generally the main concern.

The types of tags, readers, and even the connection with the backend database vary depending on the application model. In this research, we focus on the data communication algorithm which depends mainly on the tag type. As for the reader and the backend database, they are considered as one entity representing standard types with no special requirements. Therefore, we only illustrate different types of tags in RFID systems in the next sections.

2.2.1 RFID Tags

Basically, a RFID tag is a device that can be attached to any object in order to identify it. RFID tags can be classified based on their memory type, power source, price, and radio wave frequency range. Each of these aspects in terms of RFID systems are described below:

Tag memory: a tag may contain either a writable or a non-writable (read-only) memory, where the data can be programmed in the tag either on manufacturer level (non-writable) or in the application level (writable). Another special tag is the Write-Once-Read-Many kind, where the tag can also be read an unlimited number of times but its memory is written only once to enable writing customized data.

Tag power source: a tag can gain its power from several sources based on its type. Tags can recharge itself either from radio waves sent by the reader or from an embedded battery inside it. According to the power source, a tag can be classified as one of the following three sub-categories:

- ***Passive tags***: the tag will be active while it is in the reading range of the reader, where the reader supplies the tag with the needed power. Due to limited power source, this tag usually has a small memory and a low price.
- ***Active tags***: the tag is active all the time and has its own battery for power supply. Active tags can support higher memory capacity and more computational capability. They are usually very expensive compared to passive tags.
- ***Semi-passive tags***: this tag has a battery, but it only uses the battery to provide power for other functions when no readers are available to recharge the tag.

For the rest of the thesis, we refer to passive RFID tags as RFID tags because the scope of the thesis will only be limited to passive tags. Figure 2.2 depicts RFID Tag types based on their power source and their relation with other manufacturing aspects.

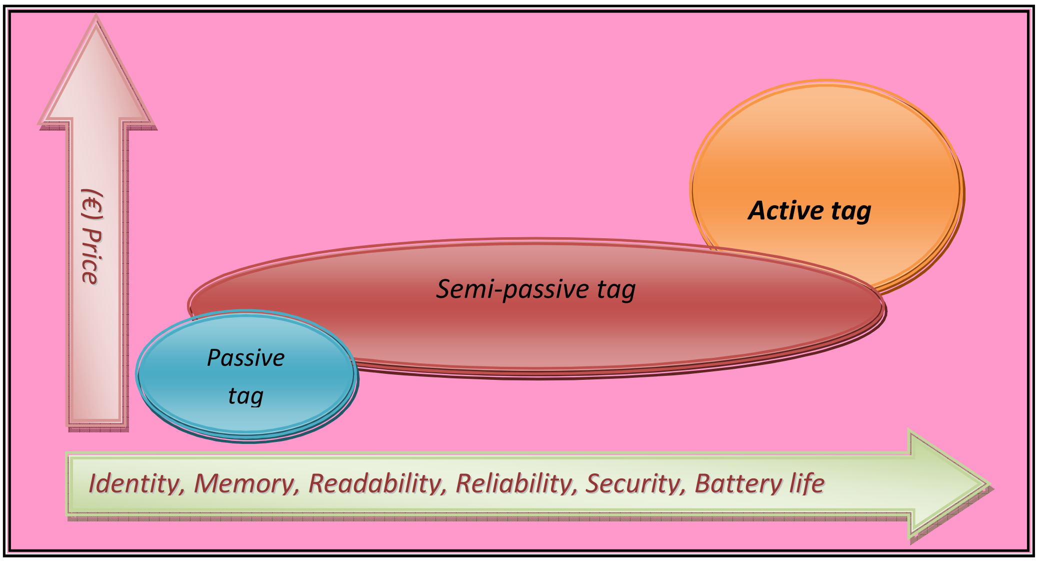
(€) Price
Active tag
Semi-passive tag
Passive tag
Identity, Memory, Readability, Reliability, Security, Battery life

Figure 2.2: RFID Tag types based on power source

Tag price: In terms of cost, RFID tags could be divided into two main sub-categories, namely, low-cost RFID tags and High-Cost RFID tags. The price differences in RFID tags are due to variation in capabilities and manufacturing requirements between the two sub-categories. Low-cost tags have very limited computational capabilities (in terms of storage, circuitry, and power consumption), which makes the tag unable to perform any cryptography primitives. High-cost RFID tags have a microprocessor capable of performing different kinds of cryptography primitives. Table 2.1 shows a summary of tag features in terms of their cost categorization with respect to current commercial RFID tags.

Table 2.1 illustrates that the security aspects for high-cost RFID tags are very much different than those for low-cost RFID tags. Circuitry located for security purposes in low-cost RFID tag cannot exceed 4000 logical gates. In contrast, high-cost RFID tags can implement standard cryptography primitives, except Asymmetric cryptography which is too expensive. Note that the smallest hash-function proposed so far is the Universal Hash Function (1700 logical gates and only 64-bits of output). Nevertheless, this function performs around 232 operations and, therefore, does not guarantee acceptable security due to the “Birthday paradox” and the ease of finding collisions. The rest of the cryptography functions require more than 4000 logical gates. For example, Standard Hash Function (SHA1) needs 8100 logical gates and 1228 clock-cycle, and MD5 needs 8400 logical gates and 612 clock cycles, which are far from the specifications of low-cost tags. Furthermore, low-cost RFID tags are not resistant to physical and active attacks, unlike high-cost tags which are tamper resistant and secure against passive and active attacks.

Table 2.1: Low-cost Versus High-cost RFID Tag (Peris-Lopez, 2008)

	Low-cost	**High-cost**
Standards	EPC Class-1 Generation-2 ISO/IEC 18006-C	ISO/IEC 14443 A/B
Power Source	Passively powered	Passively powered
Circuitry (security processing)	250 – 4000 gates Standard cryptographic primitives cannot be supported	Microprocessor Implemented 3DES, SHA-1, cannot support RSA
Reading Distance	Up to 7 m	10 cm
Price	0.05–0.1 €	Several Euros
Physical Attacks	Not resistant	Tamper resistance EAL 5+ security level
Resistance to Passive Attacks	Yes	Yes
Resistance to Active Attacks	No	Yes
[52, 111, 118, 158]		

Radio wave frequency range: RFID systems also differ by the radio wave frequency they use. There are several available and practical frequencies for RFID tags [e.g. LF (low frequency), HF (high frequency), or UHF (ultra-high frequency)]. The frequency for RFID systems is in the myriametric range below 135 KHz through short wave and ultrashort wave, or in the microwave range with the highest frequency being 24 GHz. Wave frequency does not affect the security protocol to be proposed; therefore, this aspect would be excluded in the rest of this thesis.

2.3 RFID standards

There are many approved and proposed RFID standards that describe how tags and readers communicate with each other using air interface protocols. These are also known as security protocols in terms of data format, conformance, and usage of standards in applications. These standards are defined by several known groups such as the International Organization for Standardization (ISO) and the Electronics Product Code Global Incorporated (EPCglobal).

ISO has created several RFID standards for different applications (e.g., the standards for animal tracking and item management). These standards differ in their description. For example, in animal tracking, ISO 11784 defines how data are structured on the tag. Meanwhile, ISO 11785 defines the air interface protocol for the same application. Moreover, ISO has also standardized the air interface protocol of RFID tags used in payment systems and contactless smart cards in ISO-14443, and for vicinity cards in ISO 15693. ISO has also established standards for testing the conformance of RFID tags and readers in ISO-18047, and even the performance in ISO-18046.

Similarly, EPCglobal also created many standards for RFID. The Electronic Product Code (EPC) standard is particularly well known, and its platform, the EPCglobal Architecture Framework(Auto-ID-Center, 2003). Figure 2.3 illustrates the EPCglobal Architecture Framework.

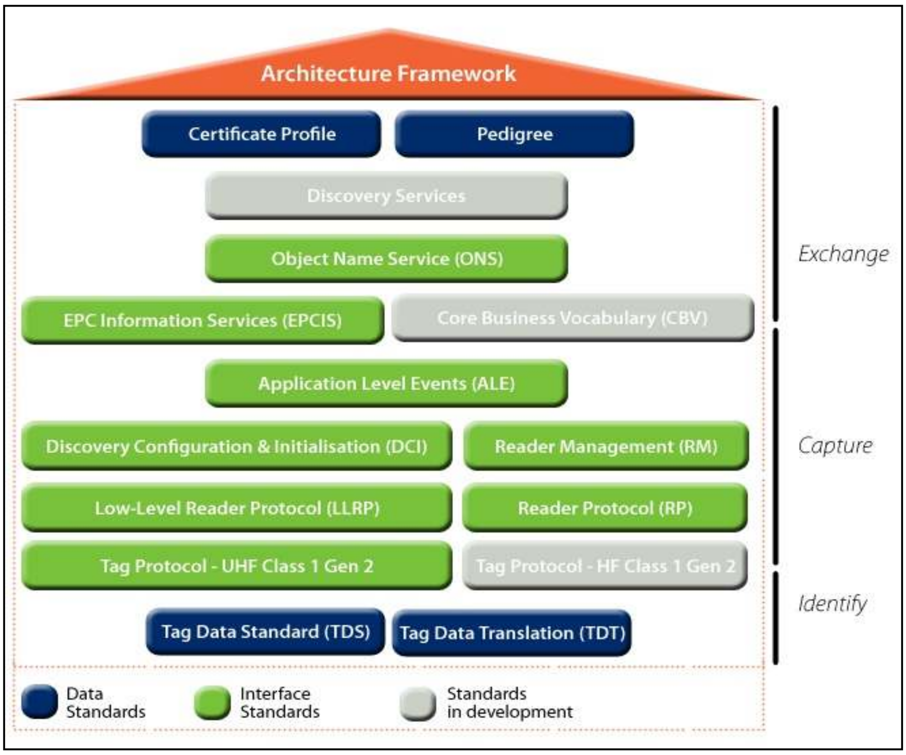
Architecture Framework
Certificate Profile
Pedigree
Discovery Services
Object Name Service (ONS)
EPC Information Services (EPCIS)
Core Business Vocabulary (CBV)
Application Level Events (ALE)
Discovery Configuration & Initialisation (DCI)
Reader Management (RM)
Low-Level Reader Protocol (LLRP)
Reader Protocol (RP)
Tag Protocol - UHF Class 1 Gen 2
Tag Protocol - HF Class 1 Gen 2
Tag Data Standard (TDS)
Tag Data Translation (TDT)
Exchange
Capture
Identify
Data Standards
Interface Standards
Standards in development

Figure 2.3: EPCglobal Architecture Framework(Auto-ID-Center, 2003)

The framework is a collection of standards, which include Discovery Services, Object Name Service (ONS), EPC Information Services (EPCIS), Application Level Events (ALE), EPC Reader Protocol (RP), EPC Tag Protocol, and EPC Tag Data Standard (TDS). The EPCglobal also defines four classes of RFID tags (EPCglobal, 2007):

Class-1: Identity Tags: Passive tags with the minimum features of an electronic product code (EPC) identifier, a Tag identifier (Tag ID), a function that renders a tag permanently non-responsive, and provides optional decommissioning or re-commissioning of the tag, optional password-protected access control, and an optional user memory.

Class-2: Higher-Functionality Tags: Passive tags holding Class-1features as well as an extended Tag-ID, an extended user memory, an authenticated access control, and an additional feature of a To-Be-Done (TBD) queue.

Class-3: Semi-passive tags holding Class-1features with a power source that may supply power to the tag and/or to its sensors, and/or sensors with optional data logging.

Class-4: Active Tags: Active Tags with the minimum features of an electronic product code (EPC) identifier, an extended Tag-ID, authenticated access control, a power source, an autonomous transmitter for communications, an optional user memory, and optional sensors with or without data logging.

Within these classes, every higher EPC tag class is compatible to the preceding class. Each higher class maintains the previous class' capabilities and characteristics, and adds new features. In general, low-cost RFID tags are considered Class-1 with two main protocol models, Generation 1 (the basic model) and Generation 2 (Gen-2). Gen-2 is an enhancement of the first model. In this research, we consider low-cost tags conforming to the EPC Class-1 Generation-2 standard. To justify our choice, we compare the characteristics and details of the two generations of Class-1.

2.3.1 EPC Gen-2

EPC Class 1 Generation 2 Standard is one of the important standards in passive RFID tags. It was developed by EPCglobal (EPCglobal, 2008) and adopted with minor modifications as ISO 18000-6C in 2006 (Razaq et al., 2008). Gen-2 characteristics define physical and logical requirements for a passive-backscatter, Interrogator-talks-first (ITF), RFID system operating in the 860–960 MHz frequency range. The tag's power is triggered by the readers. The tag's memory is insecure and susceptible to physical attacks, i.e., tags could not be trusted to store global, long-term secrets, when left in isolation. A kill command with a 32-bit PIN is used to