A Survey of RFID Authentication Protocols

Yawer Yousuf, Vidyasagar Potdar
Digital Ecosystems and Business Intelligence Institute, Curtin Business School, Curtin University of Technology, Perth, Western Australia
v.potdar@curtin.edu.au, yawer_yousuf@yahoo.com

Abstract

RFID are small wireless devices which can be used for identification of objects and humans as well. Their acceptance has grown in past years and is expected to grow further. Due to reduction in cost of production RFID devices are being deployed in large numbers in supply chains (by Wal-Mart, etc.) In this paper we provide a comprehensive survey of various RFID authentication protocols proposed in the literature and classify them in different categories. We then study RFID authentication protocols having minimalist technique namely EMAP, LMAP and M2MAP.

1. Introduction

RFID (Radio Frequency IDentification) is a technology used for the identification of objects. RFID has gained popularity in past few years. RFID technology started to replace the more tradition system of barcodes mainly due to the efforts of Wal-Mart, Procter and Gamble, etc.

A RFID system is basically composed of a RFID Transponder (tag) and a RFID Interrogator (Reader). The RFID tag is microchip connected to an antenna. This tag can be attached to an object, which needs to be uniquely identified, e.g. it can be used in a storehouse to track the entry and exit of goods. This tag contains information similar to the barcode, which stores the unique properties of the object to which it is attached. A RFID reader can access this information. The RFID reader communicates with the RFID tag using radio waves. The main advantage of RFID tags over barcode system is:

1. RFID system uniquely identifies the object "e.g. 114119201 is a bottle of jam of X company."
2. RFIDs do not require line of sight. The objects (tags) should be in a range much larger than barcodes would allow, and there is no need to individually scan each product.

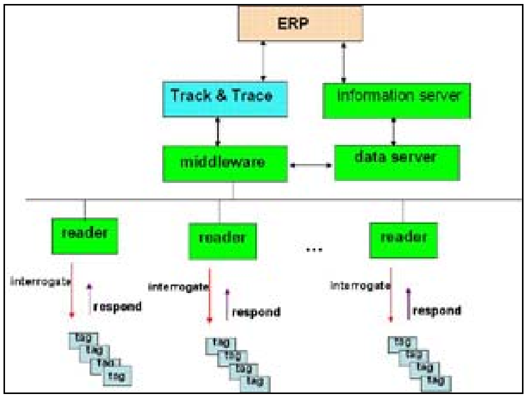

Figure 1:RFID Architecture [8]

RFID tags can be a *passive* tag which does not have any power source; they derive their power from the radio frequency generated by the reader. Tags that derive their own power are *semi-passive* tags in which batteries supply power when tags are interrogated by a reader and *passive* tags whose batteries provide power for transmission.

Within the RFID technology there are several security issues, which need to be tackled in order to make this technology more robust and reliable. The key security properties like confidentiality[1], integrity[2], availability, authentication and anonymity[3] need far more attention.

These security issues can be explained by the following scenario. Let us consider a storehouse, a malicious reader can eavesdrop the communication between tag and reader, thus *confidentiality* and *anonymity* is lost. A malicious reader can tamper the data stored in the tag, thereby compromising the data

[1] confidentiality in communication between the tag and the reader.
2 reliability of the information on the RFID tag.
3 Anonymity to undesired and anonymous scanning of items or people.

978-0-7695-3096-3/08 $25.00 © 2008 IEEE
DOI 10.1109/WAINA.2008.214

integrity. In some cases a message jamming attack or a Denial of Service attack can hamper the communication between a reader and a tag which can bring system to a halt by which current status at the storehouse cannot be made *available* at a moment. A malicious *authentication* can make a fake tag to impersonate the real one which can result in serious security issues.

In this paper we heavily focus on authentication issues and will provide a generic classification of various authentication protocols.. Authentication basically provides a certain level of trust amongst the reader and the tag such that the identity of the tag is verified and *vice versa.*

Each year quite a large number of RFID authentication protocols are published in scientific literature [2]. Some of these protocols are well-suited for only one particular solution, others are found to be fallacious and later corrected; and finally some proposals are trivial and are subsequently discarded. This induces us to give a proper classification of all the RFID authentication protocols. But attributes of a protocol such as its structure, or some complex cryptographic function may make classification difficult. Conceptually speaking classification means distinguishing on the basis of general prototypes which can cover various fundamental protocols. The author's in [1] stated that classification of authentication protocols is based on three points

1. Underlying algorithm used in the protocols.
2. Procedure of message exchange.
3. Secure combination of above two.

The concentration on message exchange has helped in abstracting away from cryptographic mechanism. There are few definitions which must be deduced from [1], these are discussed in detail in section 2 under preliminary concepts.

In section 3 we will explain the basic process of classification and the prominent prototypes of protocols. In section 4 we will discuss recent authentication protocols on RFID and analyze various security & privacy protection and integrity related issues. In the end we will conclude the paper in section 5.

2. Preliminary Concepts

Definition 1.*Forced Challenge (F):* If the fresh data is a random nonce generated by the verifier and then delivered as a plaintext or a ciphertext to the prover, then we say that the protocol uses a forced challenge to authenticate the prover.

Self Challenge(S): If the fresh data is generated by the prover himself the protocol is said to use self challenge.
No Challenge (Ø): When there is no challenge value exchanged in the protocol, we say that the protocol has no challenge.

Definition 2. *Origin Authentication (OA):* If a protocol contains a message which is generated by application of private key on cryptographic particles. i.e. the message is of the form $APriKey\{\bullet\}$ then we say the protocol provides origin authentication of the entity.

Destination Authentication (DA): If a protocol contains a message which is generated by application of public key on cryptographic particles. i.e. the message is of the form $APubKey\{\bullet\}$ then it provides destination authentication of the entity A.

Implicit Authentication (**IA**): If a protocol contains no message of the form $APriKey\{\bullet\}$ or $APubKey\{\bullet\}$, but still requires entity A to compute a value of the form $APriKey\{\ \bullet\}$, then we say that the protocol provides implicit authentication of A.

3. Protocol Classification

As discussed earlier as well as in [1], classification of authentication protocols implies distinguishing them on the basis of fundamental prototypes. However, the inclusion of extraneous information may make classification difficult. Therefore, the basic requirement is to identify the essential elements in the authentication protocols and the way they are combined and used. The authors have recognized the basic elements as the type of authentication and the types of challenge values. So the basic steps of classification are:

Step 1: Identify the type of authentication used in a given protocol. Is it Implicit Authentication (**IA**), Origin Authentication (**OA**) or Destination Authentication (**DA**)?

Step 2: Identify the type of challenge values used between two identities (i.e. sender and receiver) in a given protocol. is it forced challenge (**F**), self challenge (**S**) or no challenge (∅)?

Step 3: In case of DA with forced challenge, if there is responses by prover then the protocols are further classified into $DA_{F,\ No\ Ack}$ (No Acknowledgment) and $DA_{F,\ Ack}$.(Yes, Acknowledgment).

There are eight different prototypes for the classification and are summarized below as well as in Table 1:

3.1. Implicit Authentication

Implicit Authentication with no challenge (**IA$_{Ø}$**): If the message does not contain any message of the form *APriKey*{•} or *ApubKey*{•}, but still requires entity *A* to compute a value of the form *ApriKey*{ •}. And no challenge value is exchanged between the identities. Then it is called Implicit Authentication with no challenge.

Implicit Authentication with forced challenge (**IA$_{Ø}$**): If the message does not contain any of the form *APriKey*{•} or *APubKey*{•}, and requires entity *A* to compute a value of the form *APriKey*{ •}. In addition to that, the verifier computes random nonce generated by the verifier(through public or private key) and then sends it as a plaintext or cipher text. Then it is called Implicit Authentication with forced challenge.

3.2. Origin Authentication

Origin Authentication with no challenge (**OA$_{\varnothing}$**): If the message contains the message of the form *APriKey*{•}, that is message is generated by applying private key and no challenge value is exchanged between the identities. Then it is called Origin Authentication with no challenge.

Origin Authentication with self challenge (**OA**$_S$): If the message contains the message of the form *APriKey*{•}, and the data is generated at the prover end, then it is called Origin Authentication with self challenge[1].

Origin Authentication with forced challenge (***OA$_F$***): If the message contains the message of the form *APriKey*{•}, and the data is generated by the verifier then it is called Origin Authentication with forced challenge.

3.3. Destination Authentication

Destination Authentication with no challenge (**DA**$_{□}$): If the message contains message of the form *APubKey*{•},and no challenge values is exchanged between the identities then is it called Destination Authentication with no challenge.

Destination Authentication with forced challenge (**DA$_F$**): If the message contains message of the form *APubKey*{•}, and the verifier produces the random nonce then the authentication is called Destination Authentication with forced challenge. It can be further divided into two types.

1. *With Acknowledgment(***DA$_{F,\ Ack}$***):* If the prover responds to the forced challenge by the verifier then the authentication is called Destination Authentication with forced challenge and acknowledgment.

2. *No Acknowledgment(***DA$_{F,\ No\ Ack}$**): If the prover does not respond to the forced challenge by the verifier then the authentication is called Destination Authentication with forced challenge and no acknowledgment.

Table 1 – Protocol Classification

Authentication Type		**Example**
Implicit Authentication (IA)	IA$_{Ø}$	A : *ApriKey*{ *B* }
	IA$_F$	A $\leftarrow$B : r_B *A:*Ap*riKey* { *B*, r_B }
Origin Authentication (OA)	OA $_{\varnothing}$	A $\rightarrow$B : *APriKey*{ *B* }
	OA$_S$	A $\rightarrow$ B : TS_A , *APriKey*{ *B*, TS_A }
	OA$_F$	A $\leftarrow$B : r_B A$\rightarrow$B : *APriKey* { *B*, r_B }
Destination Authentication (DA)	DA$_{\varnothing}$	A $\leftarrow$B : *APubKey*{ *B* }
	DA$_{F,\ NoAck}$	A $\leftarrow$B : *APubKey*{ *B*, r_B }
	DA$_{F,\ Ack}$	A $\leftarrow$B : *APubKey*{ *B*, r_B } A $\rightarrow$B : r_B

3.4. Mutual Authentication

There should not be more than 8^2 = 64 prototypes for mutual authentication by counting exhaustively. But the protocols in which, the responder entity B, act as an initiator can be regarded as *illegal.*

This condition rules out many prototypes which are mirror images of each other. The authors have identified 17 prototypes which come under illegal prototypes, so in all there are 47 (64-17) prototypes, which can be used for classification. The prominent protocols are summarized below in the Table 2.

Table 2

Prototype	Example
$IA_{F\text{-}\varnothing}$	1. $A \rightarrow B$: r_A B: $BPriKey\{ r_A \}$
$DA_{\varnothing}–\varnothing$	1. $A \rightarrow B$: $BPubKey\{ A \}$
$IA_{\varnothing}–IA_{\varnothing}$	A: $APriKey\{ B \}$ B: $BPriKey\{ A \}$
$IA_F\text{-}IA_F$	1. $A \rightarrow B$: r_A 2. $A \leftarrow B$: r_B A: $APriKey\{ B, r_B \}$ B: $BPriKey\{ A, r_A \}$
$IA_F\text{-}OA_S$	1. $A \rightarrow B$: r_A , TS_A , $APriKey\{ B, TS_A \}$ B: $BPriKey\{ r_A \}$
$OA_F\text{-}OA_F$	1. $A \rightarrow B$: r_A 2. $A \leftarrow B$: $BPriKey\{ A, r_A \}, r_B$ 3. $A \rightarrow B$: $APrikey\{ B, r_B \}$
$OA_F\text{-}DA_{F,NoAck}$	1. $A \rightarrow B$: r_A 2. $A \leftarrow B$: $APubKey\{B, r_B , BPriKey\{ A, r_A \} \}$ or, 1. $A \rightarrow B$: r_A 2. $A \leftarrow B$: $BPriKey\{ A, r_A , APubKey\{B, r_B \} \}$
$DA_{F,NoAck}\text{-}OA_S$	1. $A \rightarrow B$: $BPubKey\{A, r_A , TS_A , APriKey\{ B, TS_A \} \}$ or, 1. $A \rightarrow B$: TSA , $APriKey\{ B, TS_A , BPubKey\{A, r_A \} \}$
$DA_{F,Ack}\text{-}OA_F$	1. $A \rightarrow B$: $BPubKey\{ A, r_A \}$ 2. $A \leftarrow B$: r_A , r_B 3. $A \rightarrow B$: $APriKey\{ B, r_B \}$
$DA_{F,NoAck}\text{-}DA_{F,NoAck}$	1. $A \rightarrow B$: $BPubKey\{ A, r_A \}$ 2. $A \leftarrow B$: $APubKey\{ B, r_B \}$
$DA_{F,Ack}\text{-}DA_{F,Ack}$	1. $A \rightarrow B$: $BPubKey\{ A, r_A \}$ 2. $A \leftarrow B$: $APubKey\{ B, r_B \}, r_A$ 3. $A \rightarrow B$: r_B

4. Discussion

4.1. Implicit Authentication with forced challenge- Implicit Authentication with forced challenge (IAF-IAF)

Minimalist cryptography approach: The real light-weight protocols were proposed by Pedro Peris-Lopez *et al.* namely, Lightweight Mutual Authentication Protocol (LMAP) [3] and Minimalist Mutual-Authentication Protocol (M2AP)[4] and Efficient Mutual Authentication Protocol (EMAP) [5]. In all three of the protocols simple binary operations like XOR, OR, AND, mod 2^m are used. Costly operation such as multiplication was not included. All the protocols are based on *index-pseudonyms* (96-bits) which is a row of a table to store all information related to the tag. It also uses a 480 EEPROM and a 96-bit key divided into 4 parts updates after each message cycle. Mutual Authentication is as follows:

Tag Identification: The reader sends a hello message to which tag responds by giving its IDS.

Reader Authentication: The reader generates random numbers n1 and n2 which are used to generate sub-messages A, B and C by using IDS and sub-keys K1, K2 and K3 respectively. The message A || B || C is transmitted to the tag where tag generates n1 and n2 which it uses to generate D. By the sub-messages A and B, the tag will authenticate reader.

Tag Authentication: Tag sends the sub-message D in case of LMAP and D and E in case of M2AP and EMAP containing the Static Identifier which in turn authenticates the tag. The whole authentication process is summarized in the table.

Reader Authentication	**Tag Authentication**
LMAP **Tag Identification Reader □ Tag:** ***hello*** **Tag □Reader: IDS**	
Reader □Tag: A||B||C $A = IDS^{(n)}_{tag(i)}$ **XOR** $K1^{(n)}_{tag(i)}$ **XOR** n1 $B = (IDS^{(n)}_{tag(i)}$ **OR** $K2^{(n)}_{tag(i)}) +$ n1 $C = IDS^{(n)}_{tag(i)} + K3^{(n)}_{tag(i)} +$ n2	Tag □Reader: D $D = (IDS^{(n)}_{tag(i)} + ID_{tag(i)})$ **XOR** n1 **XOR** n2
M2MAP **Tag Identification – Similar to LMAP**	
A and C are same as LMAP $B = (IDS^{(n)}_{tag(i)} \wedge K2^{(n)}_{tag(i)})$ **OR** n1	Tag □Reader : D||E $D = (IDS^{(n)}_{tag(i)}$ **OR** $ID_{tag(i)}) \wedge$ n2 $E = (IDS^{(n)}_{tag(i)} + ID_{tag(i)})$ **XOR** n1
EMAP **Tag Identification – Similar to LMAP**	
A is same as LMAP $B = (IDS^{(n)}_{tag(i)}$ **OR** $K2^{(n)}_{tag(i)})$ **XOR** n1 $C = IDS^{(n)}_{tag(i)}$ ***XOR*** $K3^{(n)}_{tag(i)}$ ***XOR*** $n2$	Tag □ Reader : D||E $D = (IDS^{(n)}_{tag(i)} \wedge K4^{(n)}_{tag(i)})$ ***XOR*** $n2$ $E = (IDS^{(n)}_{tag(i)} \wedge n1$ ***OR*** $n2)$***XOR***$ID_{tag(i)}M^{4}_{I=1}KI^{(n)}_{tag(i)}$

4.2. Vulnerability of EMAP, LMAP and M2AP:

However, vulnerability of these protocols was identified by Tieyan Li *et al.* [5, 6, 7]. They showed the protocols were susceptible to attacks such as De-synchronization Attack such that they can not authenticate each other in any following protocol run and Full-Disclosure attack which can cause disclosure of all the information present in the tag including tag's ID. The countermeasures were proposed by build bit level error correcting mechanisms at the database and by sending a message Ď from tag irrespective of the authentication of reader. Both the cases will provide additional computation costs.

5. Conclusion

In this paper we studied several different RFID authentication protocols and focused on the three main researches i.e. EMAP, LMAP and M2MAP. We assert that other protocols can also be classified according to [1] to provide a more standardized study of RFID Authentication Protocols.

6. References

[1] DongGook Park, Colin Boyd, and Ed Dawson, "Classification of Authentication Protocols: A Practical Approach", *Proceedings of Information Security Workshop (ISW 2000), Springer-Verlag, LNCS Vol.1975*, pp.194-208

[2] Ari Juels, “RFID Security and Privacy: A research Survey”, September 2005, *Manuscript, RSA Laboratories*, 2005.

[3] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan and Ribagorda, Arturo, “LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags*” Printed handout of Workshop on RFID Security -- RFIDSec 06*, July 2006.

[4] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan and Ribagorda, Arturo,”M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags”, *Lecture Notes in Computer Science, 912--923, Springer-Verlag,* Sep-2006.

[5] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan M. and Ribagorda, Arturo, “EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags”, *OTM Federated Conferences and Workshop: IS Workshop -- IS'06, 2006, 4277 Lecture Notes in Computer Science*, P-352--361, November Springer-Verlag.

[6] Li, Tieyan and Wang, Guilin “Security Analysis of Two Ultra-Lightweight {RFID} Authentication” Protocols *IFIP SEC 2007*.

[7] Li, Tieyan and Deng, Robert H., “Vulnerability Analysis of {EMAP} - An Efficient RFID Mutual Authentication Protocols” *Second International Conference on Availability, Reliability and Security -- AReS 2007* April 2007 Vienna, Austria

[8] RFID Architecture Available Online - http://www.simtech.a-star.edu.sg/events/images/rg_RFID_BigSafe2.jpg Accessed on Friday, December 28, 2007

A Critical Analysis of RFID Security Protocols

Atif Sharif, Vidyasagar Potdar
Digital Ecosystems and Business Intelligence Institute, Curtin Business School, Curtin University of Technology, Perth, Western Australia
atifet97@yahoo.com v.potdar@curtin.edu.au

Abstract

RFID, Radio Frequency Identification Systems, have gains its popularity for automated identification and supply chain applications. This paper describes the technical fundamentals of RFID systems, recent technical research on the problems of privacy/security and some security proposals are presented for this new radio technology i.e. RFID.

1. Introduction

Tiny integrated circuits equipped with radio antennas are fast becoming one of the most controversial technologies ever to enter the consumer marketplace. These so-called Radio Frequency Identification tags—better known as RFID—could help stamp out drug counterfeiting, trace contaminated beef products to the very shelves where they reside, and eliminate supermarket checkout lines.

Yet, despite the technology’s current widespread use and significant future potential, most popular press coverage of RFID tags has centered on the technology’s potential for tracking consumers without their knowledge or consent. Typical of this coverage is a Wired News article that erroneously reported clothing giant Benetton’s plans “to weave radio frequency ID chips into its garments to track its clothes worldwide” [1].

For RFID manufacturers, these tiny chips are the 21st Century replacement for the Universal Product Code bar codes developed in the 1970s. RFID tags offer an improved enumeration system, giving each tag at least a 96-bit number that is both globally unique and not reusable. But, unlike barcodes, RFID tags can be read at a distance without a person’s knowledge. As a result, tags placed in consumer items for one purpose might be covertly used to track people as they move through the world. This is especially true of RFID tags that might be embedded in items such as shoes and clothing.

Some industry insiders discount such privacy concerns. Others say they can be trivially addressed using technologies that “kill” RFID chips when tagged items are sold to consumers. We believe that privacy concerns are real and will only be solved by combining technical and policy approaches. We also believe that RFID can offer powerful benefits for businesses and consumers alike. If industry fails to address privacy concerns, however, these benefits might well be stymied by restrictive legislation or a public backlash.

2. Characteristics of RFID Systems

RFID systems always consist of three major components shown in fig 1:

1. Reader/transceiver including antenna which communicates with the tag.
2. Tag/RFID label or Transponder which is placed on the object to be identified.
3. Application systems

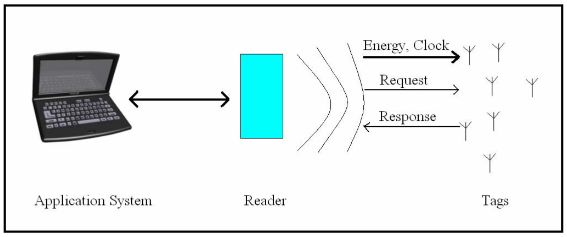

Figure 1 Components of an RFID system

Generally, an RFID label consists of a small microchip with some data storage and limited logical functionality, and an antenna. The antenna allows the label to couple to an electromagnetic (EM) field to obtain power or to communicate with the reader or to do both.

RFID labels can be distinguished based on their frequency of operation (HF or UHF), or on powering techniques (active, passive, or semi-passive). Passive labels have no power source of their own and therefore must rely on the EM field created by a reader. Passive labels normally communicate information to a reader by modulating the reader’s RF signal (load modulation or backscatter). Hence, these labels fall on to the low cost end of the RFID labels.

978-0-7695-3096-3/08 $25.00 © 2008 IEEE
DOI 10.1109/WAINA.2008.212

The data stored on the label may contain an Electronic Product Code (EPC) [2], which is a unique item identification code. An EPC typically contains information that identifies the manufacturer, the type of item and the serial number of the item. This information is also referred to as a label ID. There are four fields in the Electronic Product Code. They are, in order, a header, defining the variety of EPC among a number of possible structures; a domain manager number (effectively a manufacturer number); an object class (equivalent to a product number); and a serial number.

The readers communicate with the labels using a radio frequency interface. Either a strong energy storage field near the reader antenna, or radiating EM waves, establishes the RF interface. Communication between a reader and a label process may involve interrogating the label to obtain data, writing data to the label or beaming commands to the label so as to affect its behavior. The readers consist of their own source of power, processing capability and an antenna. The readers are generally connected to a back end database (as outlined in Fig 1).

The application systems are used to collect data aggregated through readers and the electronic database software uses the data for various purposes.

3. Frequencies and Regulations

Most RFID systems operate in the Industrial, Scientific and Medical (ISM) bands designated by the ITU [4]. The most commonly used High Frequency (HF) ISM band in Europe and America is centered at 13.56 MHz and the UHF band in the US is 902-928 MHz [5, 6].

The 13.56 MHz band has a 14 KHz powering bandwidth while signaling occupies a greater bandwidth but is implemented by shallow and infrequent reader modulations, producing low amplitude sidebands. For this band typical reading ranges of RFID labels are around 30cm to 50 cm because they operate in the near field.

The 902-928 MHz band, under US regulations, allows multiple readers to label communication choices. The regulations allowing the longest communication range require the reader to change its communication frequency every 400 milliseconds. The reader may hop between a stipulated numbers of channels, however the maximum bandwidth of a channel cannot exceed 500 kHz [6]. The technique is referred to as frequency hopping. Because they operate in the far field, because a radiated power of 4W is allowed and because antenna impedances are suitable for matching to the IC circuits, passive UHF RFID labels have reading distances of around 3m to 5m.

4. RFID Security and Privacy Problems

RFID technology poses unique privacy and security concerns because humans cannot sense the RF radiation used to read tags, and the tags themselves typically maintain no history of past readings. As a result, tags are promiscuous: they can be read by entities other than their owners and without their owners' knowledge. Further, both tags and readers can be covertly embedded in the environment; short-range readers can be small enough to fit into a cell phone [3]. In terms of RFID, security refers to one or a combination of the following:

4.1. Confidentiality

Confidentiality or message content security: The communication between reader and tag is unprotected in most cases (with the exception of some high-end ISO 14443 systems). Eavesdroppers may thus listen in if they are in immediate vicinity. The forward channel from the reader to the tag has a longer range and is more at risk than the backward channel [8]. Furthermore, the tag's memory can be read if access control is not implemented.

4.2. Integrity

Integrity of message content With the exception of high-end ISO 14443 systems which use message authentication codes (MACs), the integrity of transmitted information cannot be assured. Checksums (CRCs) are often employed on the communication interface but protect only against random failures. Furthermore, the writable tag memory can be manipulated if access control is not implemented.

4.3. Authentication

Authentication of the Sender and Recipient the authenticity of a tag is at risk since the unique identifier (UID) of a tag can be spoofed or manipulated. The tags are in general not tamper resistant.

4.4. Anonymity

Anonymity - The unique identifier can be used to trace a person or an object carrying a tag in time and space. This may not even be noticed by the traced person. The collected information can be merged and linked in order to generate a person's profile. A similar problem occurs in supply-chain applications where undesired product scans are possible. The automated reading of tags permits the counting of objects (e.g. banknotes with attached tags) which may be undesired.

4.5. Availability

Availability - Any RFID system can easily be disturbed by frequency jamming. But, denial-of-service attacks are also feasible on higher communication layers. The so called "RFID Blocker" [9] exploits tag singulation (anti-collision) mechanisms to interrupt the communication of a reader with all or with specific tags.

The privacy aspect has gained special attention for RFID systems. Consumers may carry objects with silently communicating transponders without even realizing the existence of the tags. Passive tags usually send their identifier without further security verification when they are powered by electromagnetic waves from a reader. The ID information can also be linked to other identity data and to location information. Consumers might employ a personal reader to identify tags in their environment but the large number of different standards may render this difficult. Companies are facing customer fears and the privacy issues may become a major obstacle to further RFID proliferation. There are suggestions for a policy framework (e.g. the "RFID Bill of Rights" [7]).

5. Various RFID Security Protocol Proposals

Active attacks and eavesdropping attacks may violate individual privacy as well as leak sensitive inventory data. Traffic analysis attacks also present a threat, particular to an individual's location privacy and to organizational logistics data. Denial of service may also be a potentially expensive and disruptive attack.

Active querying attacks may be addressed by limiting who is permitted to read tag data through access control. Eavesdroppers may be dealt with by ensuring that tag contents are not broadcast in the clear over the forward channel.

Effective RFID Security Protocols can provide protection against the described threats. Although RFID is a cheap and automated identification technology but still numerous good RFID security protocols hard to fit in the said domain because of the complexity of protocols against the limited/tight computational tag resources.

Hash Lock a low cost solution: Hash lock is a simple access control mechanism based on one-way hash functions. Tags, equipped with a hash function, will have a portion of memory reserved for a temporary metaID and will operate in either a locked or unlocked state. A tag owner locks tags by computing the hash value, metaID, of some random key then stored in tag and toggle it into a locked state. Writing the metaID may occur either over the RF interface or over a physical contact channel for added security. A locked tag responds to all queries with only its metaID and offers no other functionality. Finally, the tag owner will store the key and metaID in a back-end database, indexed on the metaID.

To unlock a tag, the owner first queries the metaID from the tag and uses this value to look up the key in a back-end database. The owner transmits this key value to the tag, which hashes the received value and compares it to the stored metaID. If the values match then the tag unlocks itself and offers its full functionality to any nearby readers. This scheme prevents unauthorized readers from reading tag contents. Spoofing attempts may be detected under this scheme, although not prevented. Hash locks can be extended to provide access control for multiple users or to other tag functionality, such as write access.

Yong Ki Lee and Ingrid Verbauwhede [11] propose two protocols SRAC and A-SRAC. The first protocol SRAC (Semi-Randomized Access Control) is designed using only a hash function as security primitives in tags. In spite of very restricted functionality, SRAC resolves not only security properties, such as the tracking problem, the forward secrecy and the denial of service attack, but also operational properties such as the scalability and the uniqueness of metaIDs. The second protocol A-SRAC (Advanced SRAC) resolves the replay attack in the cost of a random number generator in tags. Moreover, these schemes have significantly reduced the amount of tag transmissions which is the most energy consuming task.

Another invention is a 'RFID blocker tag' [9] which exploit tag singulation (anti-collision) protocols in order to interrupt the communication with all tags or tags within a specific ID range. The blocker works for the most relevant anti-collision protocols (tree walking and ALOHA) and may be used for privacy protection but it can also be misused for mounting denial-of-service attacks.

The Danish company RFIDsec recently announced their first commercial launch of a secure RFID system, aptly called "RFIDsec". The RFIDsec Secure Protocol implements following features:

- Compliant with EPC Gen-2 specifications operating in the standard protocol custom command space.

- Strong encryption – all communications can be encrypted, making “listening in” a useless activity.
- One-step authentication- the tag can remain silent, and hence unnoticed, until the reader that emits the “wake up” signal has been authenticated.
- Support for advanced access management – making it possible to “partition” the chip memory and define different access rights for different parties for different parts of that memory. It is essential to mention here that a “master key” is part of this functionality, making it possible to transfer full access control of the tag and all data on it to the customer at the POS when a tagged item is bought by him.

Another Security proposal, Asymmetric Key Agreement, in which Readers may take advantage of the asymmetry of the forward and backward channels to transmit sensitive values such as keys. Suppose a reader needs to transmit the value v to a singulated tag. That tag can generate a random value r as a one-time-pad and transmit it in the clear on the backward channel. The reader may now send $v \oplus r$ over the forward channel. If eavesdroppers are outside the backward channel, they will only hear $v \oplus r$, and v will be information theoretically secure.

In another scheme the tag emits only an ‘Anonymous Electronic Product Code (EPC)’ [12]. A back-end security centre then delivers the clear text EPC over a secure channel to authorized entities. In an extended version, the readers can send a reanonymising request to the security centre which generates a new ‘Anonymous Electronic Product Code (EPC)’. The tag is then updated with this ID.

Need of encrypted communication in RFID? Data Sniffing (passive) and Hijacking (active) are the possible feasible attacks that can be realized in RFID system. To avoid these attacks among many proposals cryptography (SSL, SSH, WEP) act as defensive techniques and in RFID the choice of cryptographic solutions to encrypt communications are must. RFID systems adopt symmetric algorithms (the key to encrypt and decrypt messages is same), also because asymmetric solutions (two different keys Kpub and Kpri exists, that execute the inverse function of the other) require much more computational and supply power.

Cryptography is needed to implement authentication and to prevent eavesdropping. The Design goals proposed by A. Poschmann et-al [13] for RFID ciphers (to implement the cipher in a serialized fashion, value chip size over execution time, DESL) have small gate count, low power consumption and high security. The resulting DESL implementation has low gate count ~ 1848 GE, smaller than several eStream ciphers, low current draw (0.89 µA @ 100 KHz), seems to be secure against LC/DC attacks.

In RFID systems, privacy and security are of critical importance to avoid potential tracking abuse and privacy violations. Physical attacks receive few considerations from the current research. Through physically attacks, attackers can get the secret identification-related information stored on RFID tags, and can later use the obtained information to impersonate legitimate readers for illegal tracking. Zhaoyu Liu and Dichao Peng [14] propose a secure identity reporting protocol to address these threats. In this case, the tag responds to readers with pre-stored one-time tokens. The tokens contain the tag's encrypted ID that can only be decrypted by a legitimate reader. The reader sends back dynamically created new tokens to the tag. The new tokens are encrypted by a one-time pad, which is also dynamically updated by the reader. Their security and performance analysis show that the proposed protocol can defeat physical attacks, in addition to other security threats, and scale well to large RFID systems.

The proposed protocol has light-weighted hardware complexity and good scalability, but with lower system reliability. Also In their approach, the item-related information can be stored in cipher text within each token which can provide confidentiality of the data.

Roberto Di Pietro and Refik Molva [15] proposed an identification and authentication protocol for RFID tags with two contributions aiming at enhancing the security and privacy of RFID based systems. First, they assume that some of the servers storing the information related to the tags can be compromised. In order to protect the tags from potentially malicious servers, they devise a technique that makes RFID identification server-dependent, providing a different unique secret key shared by each pair of tag and server. The proposed solution requires the tag to store only a single secret key, regardless of the number of servers, thus fitting the constraints on tag’s memory. Second, they provide a probabilistic tag identification scheme that requires the server to perform simple bitwise operations, thus speeding up the identification process. The proposed tag identification protocol assures privacy, mutual authentication and resilience to both DoS and replay attacks.

Conto et-al [16] proposed a new RFID identification protocol: RIPP-FS based on hash chains and it enforces privacy and forward secrecy. Also is resilient to a specific DoS attack, in which the attacker attempts to exhaust the hash chain the tag is programmed to spend. The computations required on the tag side are very limited, just three hash functions; on the reader side RIPPFS allows to leverage pre-computations, in such a way that tag identification resolves to a lookup in pre-computed tables, speeding up the identification process.

HB and HB+ [17] are two shared-key, unidirectional authentication protocols whose extremely low computational cost makes them potentially well-suited for severely resource-constrained devices. Security of these protocols is based on the conjectured hardness of learning parity with noise; i.e., learning a secret s given "noisy" dot products of s that are incorrect with probability ".

Although the problem of learning parity with noise is meaningful for any constant $\xi < 1/2$, existing proofs of security for HB and HB+ only imply security when $\xi < 1/4$. In this note, we show how to extend these proofs to the case of arbitrary $\xi < 1/2$.

Dang Nugyen et-al [18] proposed a synchronization-based communication protocol for RFID devices. Focus is on EPC Global Class-1 Gen-2 RFID tag which supports only simple cryptographic primitives like Pseudo-random Number Generator (PRNG) and Cyclic Redundancy Code (CRC). The protocol is secure in a sense that it prevents the cloned tags and malicious readers from impersonating and abusing legitimate tags, respectively. In addition, the protocol provides that each RFID tag emits a different bit string (pseudonym) when receiving each and every reader's query. Therefore, it makes tracking activities and personal preferences of tag's owner impractical to provide the user's privacy.

The proposed protocol achieves desirable security features of a RFID system including: implicit reader-to-tag authentication, explicit tag-to-reader authentication, traffic encryption and privacy protection (against tracking).

Sindhu et-al [19] proposes an efficient RFID tag identification algorithm that incorporates reader-authentication. The proposed algorithm is secure against the anticipated threats to RFID systems and does not require computationally expensive cryptographic mechanisms; it relies on rather simple matrix multiplication. To further enhance the utility of algorithm they suggested a scheme that allows for the algorithm to carry out secure identification of multiple tags simultaneously.

Hyunrok Lee and Kwangjo Kim [20] propose a secure RFID reader protocol which can be satisfied with the security requirements for the reader protocol based on SLRRP. The requirements of reader protocol satisfied from confidentiality to replay attack prevention, proposed secure RFID reader authentication protocol, key agreement and message format. For supporting secure communication in basic SLRRP, the establishment of secure communication channel should be provided first. In the setup phase, the authentication will be performed by Proxy certificate [21] based authentication protocol. This authentication mechanism can reduce efficiently cost of issuing official certificate. After finishing the authentication and key agreement protocol, the negotiation step of cipher suite is followed for selecting designated symmetric cipher. In the sequel phase signaling is passed to establish a secure channel between the reader and back-end server. Due to including own security mechanism into the reader protocol, one can achieve secure RFID reader protocol which not only provides various communication channel, but also satisfies security requirements of reader protocol.

6. Conclusions

RFID is an emerging technology which will replace lots of the existing Auto-ID technologies. Security is a very important issue of RFID Systems and it must be kept in high consideration during the design phase of the whole system. The security functions to be adopted in a system, strongly depend on the application contest. It means that the optimal solution doesn't exist; instead it consists in the right trade-off among costs and claimed security levels.

7. Reference

[1] E.Batista, "What Your Clothes Say About You", Wired News, March 12, 2003; www.wired.com/news/wireless/0,1382,58006,00.html/wn_ascii.

[2] Cole, P. H., and Engels, D. W., "Auto-ID 21st century supply chain technology", Proceedings of AEEMA Cleaner Greener Smarter conference, October 2002.

[3] "Nokia Unveils RFID Phone Reader", RFID J., 17 March 2003; www.rfidjournal.com/article/view/834. http://www.simson.net/clips/2002/2002.TR.10.RFID_Bill_Of_Rights.htm

[4] International Telecommunication Union (ITU) http://www.itu.int/ITU-R/terrestrial/.

[5] Cole, P.H., Level 4 Electromagnetic Compatibility lecture notes, 2003, http://www.eleceng.adelaide.edu.au/Personal/peter/peter

[6] FCC regulations Part 15, 2003. http://www.fcc.gov.

[7] Garfinkel. S. : RFID Bill of Rights. Technology Review 10, 35, 2002

[8] Weis, S.; Sarma, S.; Rivest, R,; Engels, D.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Security in Pervasive Computing, Lecture Notes in Computer Science, Volume 2802, p. 201-212, Berlin 2003

[9] Juels, A.; Rivest, R.L.; Szydlo,M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. CCS'03, October 27-30, 2003, Washington http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf

[10] ISO/IES 14443: Identification cards – Contactless integrated circuit(s) cards- Proximity cards. Parts 1 to 4, Geneva 2000

[11] Yong Ki Lee and 2Ingrid Verbauwhede "Secure and Low-cost RFID Authentication Protocols" 1University of California, Los Angeles and 2Katolieke Universiteit Leuven

[12] Ishikawa, T.; Yumoto, Y.; Kurata, M.; Endo,M.; Kinoshita, S.; Hoshino, F.; Yagi, S.; Nomachi, M.: Applying Auto-ID to the Japanese Publication Business, 2003. http://www.autoidlabs.com/whitepapers/KEI-AUTOID-WH004.pdf

[13] A.Poschmann, G.Leander, K.Schramm, C.Paar "An Efficient Block Cipher for Lightweight Cryptosystems" Ruhr-Universitat Bochum, Germany 2006

[14] Zhaoyu Liu and Dichao Peng, "A Secure RFID Identity Reporting Protocol for Physical Attack Resistance", Department of Software and Information Systems University of North Carolina at Charlotte, Charlotte, USA. JOURNAL OF COMMUNICATIONS, VOL. 1, NO. 4, JULY 2006

[15] Roberto Di Pietro and Refik Molva, "Information confinement, privacy, and security in RFID systems", Dipartimento di Matematica Universita di Roma Tre L.go S. Murialdo, 1 - 00149 Roma, Italy, Institut Eur´ecom 2229, route des cretes Sophia-Antipolis, France

[16] Conti, Pietro, Mancini, Spognardi, "RIPP-FS: An RFID Identification, Privacy Preserving Protocol with Forward Secrecy.," percomw, pp. 229-234, Fifth IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07), 2007

[17] Jonathan Katz, Adam Smith Analyzing the HB and HB+ Protocols in the "Large Error" Case

[18] Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning Dang Nguyen Duc, Jaemin Park, Hyunrok Lee, Kwangjo Kim, SCIS 2006

[19] Sindhu Karthikeyan, Mikhail Nesterenko. RFID Security without Extensive Cryptography. (SASN, November 2005)

[20] Hyunrok Lee, Kwangjo Kim "A Secure RFID Reader Protocol based on SLRRP", SCIS 2007 The 2007 Symposium on Cryptography and Information Security Sasebo, Japan, Jan. 23-26, 2007

[21] IETF, "X.509 Public Key Infrastructure – Proxy Certificate Profile", http://www.ietf.org/rfc/rfc3820.txt.