Analyses of Security and Privacy Issues in Ultra-weight RFID Protocol

Jung-Tae Kim, *Member, KIMICS*

Abstract— **Radio frequency identification (RFID) tags are cheap and simple devices that can store unique identification information and perform simple computation to keep better inventory of packages. Security protocol for RFID tags is needed to ensure privacy and authentication between each tag and their reader. In order to accomplish this, in this paper, we analyzed a lightweight privacy and authentication protocol for passive RFID tags.**

Index Terms—**RFID Protocol, Security Model, Privacy**

I. INTRODUCTION

RFID have found widespread use in many commercial as well as national security applications, ranging from e-passports, contactless credit cards to supply chain management. Since RFID tags are mobile and very tiny, attached to diverse items, and often oblivious to the human user, privacy is a major concern in the design and use of RFIDs. Indeed, these tags are commonly embedded in personal devices carried around by an individual wherever he is, e.g., credit cards, e-passports, personal digital assistants (PDAs), Bluetooth devices, clothes that s/he wears, tires on his/her car, and so forth. Another issue related to the design of RFIDs is the computational effort required at the tag side. An RFID protocol consists of three flows. Typically, the first flow is a query from a server to a tag, the seconds is the reply of the tag to the server for tag authentication, and the third is the response from the server to the tag for server authentication. A server and a tag share secrets used for mutual authentication. Most RFID tags contain at least two parts. One part consists of an integrated circuit used for storing and processing information, modulating and demodulating an (RF) signal, and other specialized functions. Nowadays, RFID is one of the main technologies used to build ubiquitous systems. This is because most common tags are passive devices in the sense that they derive electrical power from the signals sent by a reader. Thus, most tags cannot be expected to perform computationally intensive operations. Peris-Lopez et al. initiated the design of the so-called ultra-lightweight RFID protocols, which involve only simple bitwise logical or arithmetic operations like exclusive-OR (XOR), OR, addition, subtraction, bit rotation, and so forth [1].

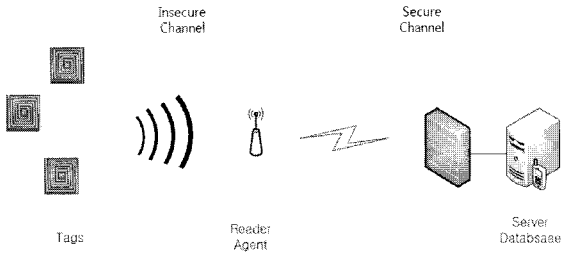


Fig. 1. Configuration of Basic RFID system.

RFID tags are categorized into two classes; passive and active. Passive RFID tags are powered by the signal received from reader. On the contrary, an active RFID tag is battery powered and has its own on-chip power source. Most RFID tags contain at least two parts [1]. One part consists of an integrated circuit used for storing and processing information, modulating and demodulating an (RF) signal, and other specialized functions. The second part consists of an antenna for receiving and transmitting the signal. Radio Frequency Identification (RFID) is widely adopted as an identification technology. While human beings are able to distinguish objects or other humans under difficult conditions, computing devices lack of this capability. From this point of view, RFID may be understood as a means of labeling objects to facilitate item automatic identification. RFID devices or tags are small chips joined to an antenna and designed to transmit data over wireless channels. By means of an RFID reader, tags are interrogated and their internal identifier or other resources, e.g. user memory, are accessed. Most RFID tags contain at least two parts. One part consists of an integrated circuit used for storing and processing information, modulating and demodulating an (RF) signal, and other specialized functions. Nowadays, RFID is one of the main technologies used to build ubiquitous systems. Recently RFID technology's potential has been recognized by ubiquitous computing researchers, in implementing physical user interfaces. It becomes evident that information security gains more importance. It would be beneficial to have a generalized threat model

Manuscript received July 22, 2011; revised August 1, 2011; accepted August 3, 2011.

Jung Tae Kim is with the Department of Electronic Engineering, Mokwon University, Daejeon, 302-729, Korea (Email: jtkim3050 @mokwon.ac.kr)

that applies to all RFID applications. Okubo et al. proposed a hash-chain based authentication protocol which protects users' location privacy and anonymity. They claimed that their scheme provides not only strong forward security but also anonymity of tags. However, Li et al. have claimed that a hash-chain calculation must be a burden on low-cost RFID tags and give back-end servers heavy calculation loads in [2].

II. RELATED WORKS

Radio Frequency Identification is a kind of object identification technology. RFID systems consist of two main components: tags and readers. Tags are small radio transponders. They contain the identification information of objects to which they are attached. Readers query these tags for the identifying information about the objects. Readers often have secure access to a back-end database. Toward these RFID security and privacy threats, many countermeasures have been suggested such as permanent tag deactivation, temporary tag deactivation (Faraday cages, sleep/wake modes), on-tag cryptographic primitives (stream ciphers, reduced AES, reduced NTRU), on-tag access control (hash locks, pseudonyms), off-tag access control (blocker tags), and tag-reader authentication (lightweight protocols, adapted air interfaces). Actually, more than hundreds of research papers were published on addressing RFID security and privacy problems. Furthermore, access control mechanisms were considered such as tag deactivation, which was standardized by the EPCglobal consortium [1, 2]

III. SECURITY AND PERFORMANCE ANALYSIS

The security design of the protocol should not impede normal operations, and should prevent a malicious adversary from getting any information. We consider the following measures:

1. Secrecy/Authentication

The cryptographic methods used (for example the keyed Hash function H) correspond to the state of the art in industry today, and reasonably guarantee the secrecy of the message. Thus, we assure the recipient that the messages originate from valid sources.

2. Indistinguishability/Tracking/Passive

Replay using a freshly generated random nonce with every message in the protocol, it is impossible to track the tag. Assume that an adversary pretends to be a genuine reader. He sends out a query, and receives a message back. Next time he sends a query, along with a fresh nonce, he receives a different message, so he cannot track the tag. Of course, with multiple tags in an area, tracking a specific tag without keys is extremely difficult if not impossible.

3. Forward Security

This means that the current key of a tag has been found, and can be used to extract previous messages (assuming that all its past conversations are recorded). Let's say the adversary somehow finds key. The tag always communicates using a hash function. The adversary cannot use the key to decode any of the tag's messages because the one-way hash function H is considered computationally un-invertible. In other words, the adversary needs to have access to the hash digest table for lookups. So, he cannot decipher/ recreate any past messages sent with previously used keys.

A. Security Analysis

Some of the security properties of the previous proposed protocols are listed as below.

- Confidentiality: This is a mechanism to guarantee a tag's privacy.
- Tag anonymity: As the ID of the tag is static, we should send it, and all other interchanged messages, in random wraps
- Tag/reader authenticity: We have designed the protocol with both reader-to-tag authentication and tag-to-reader authentication.

B. Performance Analysis

- Computational overhead:
- Storage overhead:
- Communication overhead:

C. Security and Privacy Related Goals

RFID systems may face security attacks because of the proliferation of RFID tags. Several real life applications of RFID systems require them to be secure and protective against privacy attacks. Considering those example scenarios and analyzing their security requirements the following security goals can be identified. An RFID system ensuring six elements of safety is considered to be secured and protected against all major attacks. The elements of the safety ring are as follows.

- Protect Privacy:
- Prevent Tracking:
- Deal with Denial of Service attack:
- Ensure Forward Secrecy:
- Lessen susceptibility to replay attack:
- Prevent Cloning:

D. Security Requirements of Low-cost RFID Systems

To address the fore mentioned threats and privacy concerns a low-cost RFID system should satisfy the following security requirements:

1. Anonymity-Privacy: The values transmitted by a tag must not reveal any information about the product that it is attached to.
2. Privacy Location-untraceability: The values transmitted by a tag to a reader did not allow to be traced the product or the person that is carrying this tag to an adversary.
3. Forward Security: The adversary must not be able to identify any previous transactions that a tag was involved in, even if he manages to obtain any secret values stored in the tag. This property is referred as forward traceability.
4. Protection against Tag Spoofing-cloning: The adversary must not be able to spoof or to clone a legitimate tag, unless the tag has been tampered with.
5. Availability: The reader and thus the back-end system should always be in place to identify a legitimate tag.

E. Security Threats for RFID

- Tag Cloning:
- Privacy Invasion:
- Denial/Disruption of Service:
- Location-based Attacks
- Side Channel Analysis:

F. Recent Technical Protocols

- Hash-based Protocols:
- LPN-based Protocols:
- Ultra-lightweight Protocols:
- Universal Composability Protocols:
- Multi Tag Scanning Protocols:
- Distance-bounding Protocols:
- Side channel analysis and protection on RFID:

G. RFID Threats

RFID threats can be broadly classified into following groups. a) inside supply chain b) transition zone and c) outside supply chain. Threats can also be classified into following groups depending on the type of organization/group. It affects a) Corporation b) Individuals and c) Other organizations [2].

A. Personal Privacy Threats:

Further groups the Individual privacy threats into following types

B. Association Threat: Vendors can associate a particular purchase with an individual by unsolicited reading of the RFID tags carried by that individual. RFID technology assigns unique id to each instance of the product. For example a vendor can associate a particular instance of coke bottle to an individual thereby creating a association between them.

C. Location Threat: An individuals' location can be determined by surreptitiously placing readers at specific locations. An individual carrying a unique tag can be monitored by the readers and his location revealed by correlating the unique id with the vendor database.

D. Preference Threat: A vendor/adversary can scan the RFID tags to reveal an individual's personal preference. They can use this information to push advertisements to that individual through various channels. Unauthorized person can scan items with high value to pick up a potential victim for his crime.

E. Constellation Threat: Adversaries can use "constellation" (group) of tags carried by an individual to track his location. These unique individual tags can be a "signature" for an individual. He can be tracked on basis of this "signature.

F. Corporate espionage threat: Competitors can gather data about supply chain remotely. Such data is most protected data in supply chain industry.

IV. LIGHTWEIGHT MUTUAL AUTHENTICATION

To reduce the gate count on a tag to accommodate security functions, there are a number of lightweight authentication protocols being proposed without assumptions on conventional cryptographic primitives. Weis introduced the Hopper and Blum Protocol (HB) under the RFID setting. Subsequently, Juels and Weis proposed a lightweight authentication protocol(HB+) in Reference. The security of both the HB and HB+ protocols are based on the Learning Parity with Noise problem, whose hardness over random instances remains as an open question. However, Gilbert etal, showed that HB+ is not secure against a simple MITM attack. To defend against such active attacks, Bringer et al. extended the protocols to HB++ protocol. In Ultra-Lightweight RFID Authentication Protocols, Vajda and Buttyan presented a set of extremely lightweight challenge response authentication protocols that are suitable for authenticating tags, but their protocols can be broken by a powerful adversary. So far, almost all those lightweight protocols are being attacked in a some ways, their practical deployment might be at risk unless strict security analysis is conducted. Recently Peris-Lopez et al. proposed a family of ultra-lightweight mutual authentication protocols for low-cost RFID tags: LMAP, M2AP, and EMAP, in which only simple bitwise operations are used. The protocols have some merits on its innovative design of using only ultra-lightweight primitives, but this also induces higher risk. As such, their schemes suffer from serious attacks in

which all secrets on a tag can be disclosed to an attacker either by active attacks or by passive attacks.[2] There have been several hash based solutions that create authentication for systems. These solutions are not practical for low-cost tags due to the complexity of hash functions. Furthermore, most of these solutions do not authenticate the tag, and is vulnerable to man-in-the-middle attacks. Some lightweight solutions to securing RFID systems have also been proposed, including the HB family and the MAP family of protocols, however, they have been shown to have serious security flaws. TRMA and TRMA+ tried to adhere strictly to the EPC Class 1 Gen 2 standard of tags, however, they were broken. Some protocols based on PUF have been explored. These solutions require that the back-end is preloaded with a very large amount of challenge response pairs for the reader to use to verify the authenticity of the tag. Moreover, the HB-PUF solution does not provide mutual authentication. There exist fewer solutions to the ownership transfer problem than to mutual authentication for RFID. Some of them rely on hash functions or symmetric encryption functions. A similar solution to our two-party ownership transfer protocol is mentioned, which uses similar assumptions about the security of the backwards channel. The solution depends on the tags ability to execute a cryptographic function [3].

V. OPEN ISSUES IN RFID SECURITY REQUIREMENTS

Even though many works have been done to many security threats to RFID technology, but many issues are still unsolved and some others need further investigation. Those issues include as follows.

- Functional Lightweight Cryptographic Primitives:
- Possibility of Certain Cryptographic Tasks:
- New Security Model: Multiple tags scanning:
- Effective Methods against Location-based Attacks:
- Protection against Side Channel Analysis:

Due to its open and dynamic nature, an RFID system must ensure that the legitimate tags and readers (and the backend servers) can reliably identify each other in order to recognize "self" components in face of malicious attacks. RFID tag-reader mutual authentications are required to defend against attacks such as tag and reader impersonation. There has been a great deal of lightweight cryptographic primitives and protocols designed for resource constricted RFID tags. Although a significant improvement has been achieved in security and efficiency of cryptographic ciphers suitable for low-cost devices, the design of reliable and robust protocols for secure communications and authentication remains a pending task. Since lightweight protocols can only apply simple functions such as bitwise, AND, XOR, OR, sum mod 2m , and cyclic redundancy code, security flaws have been identified in several designs of RFID authentication and communication protocols. There are two major reasons for the security flaws in those protocols: 1) poor diffusion effect of those simple functions; and 2) deficiency in protocol design. Currently, there is a lack of formal design methodology and evaluation standard, which ensures the simple function can be correctly and securely applied in developing lightweight RFID protocols for low-cost tags. This area is in need of further research [2].

The effective use of symmetric-key cryptographic primitives for privacy or authentication is effective method and implementation of these primitives. A few papers explore primitive geared at the very tightly constrained environments of RFID tag [4]. Vajda and Buttyán proposed a medley of lightweight cryptographic primitives for RFID-tag authentication. Feldhofer, Dominikus, and Wolkerstorfer proposed a lightweight hardware implementation of a symmetric-key cipher, namely, a 128-bit version of the Advanced Encryption Standard (AES). Their design requires just over 3500 gate equivalents—considerably more than appropriate for basic RFID tags, but suitable for higher cost RFID tags. Juels and Weis proposed a lightweight authentication protocol called that has security reducible to a problem called Learning Parity with Noise. To implement tags need, it only generates random bits and compute binary dot products. The key lengths required for good security are not known yet, however, and the security model is limited.

TABLE 1
COMPARISON OF DIFFERENT CIPHERS

	Model	Key size	Block size	Cycles Per block	Throughput at 100KHz	Logic Process(um)	Area (GE)
Block ciphers	PRESENT-80[1]	80	64	32	200	0.18	1
	PRESENT-80[2]	80	64	563	11.4	0.18	0.68
	DES	56	64	144	44.4	0.18	1.47
	mCrypton	96	64	13	492.3	0.13	1.71
	PRESENT-128	128	64	32	200	0.18	1.20
	TEA	128	64	64	100	0.18	1.50
	HIGHT	128	64	34	188.2	0.25	1.65
	DESXL	184	64	144	44.4	0.18	1.38
	AES-128	128	128	1032	12.4	0.35	2.17
Stream ciphers	Grain	1	1	1	100	0.13	0.82
	Trivium	1	1	1	100	0.13	1.66

We analyze the performance of some current compact algorithm where block ciphers are ordered by block and key size while hash functions are ordered by the size of the output. Table 1 shows that the hash functions available are unsuitable in practice. When we consider what we need from a hash function in an RFID tag based application, we can consider security issues. In tag based application, we do not need the property of collision resistance. Most often the security of the protocol depends

on the one way property. It is safe to use hash functions with smaller hash outputs. Applications will typically require moderate levels. Consequently 80 bit security, or even less, may be adequate [5].

We analyze the standardized cryptographic algorithms SHA-256, SHA-1, MD5, AES-128, and ECC-192 in terms of different specification. The three parameters mean are used to classify a metric of hardware implementations such as power consumption, chip area, and the number of clock cycles. The results and a comparison of the different hardware implementations are depicted in Table 2. The chip area results are based on synthesis and are given in gate equivalents [GE] [6, 7].

TABLE 2
SYNTHESES AND SIMULATION RESULTS ON 0.3UM CMOS

Algorithm	Security [bits]	I_{mean} [uA]	Chip area [GE]	Clock [Cycles]
SHA-256	128	5.86	10,868	1,128
SHA-1	80	3.93	8,120	1,274
MD5	80	3.16	8,001	712
AWS-128	128	3.0	3,400	1,032
ECC-192	96	18.85	23,600	502,000

VI. REQUIREMENTS OF SECURITY SOLUTIONS

Some of authentication protocols use hash algorithm and symmetry key algorithms due to their simplicity compared to public key algorithms. However, they fail to satisfy the mentioned basic requirements of RFID systems. It is shown that a public key cryptographic algorithm is necessary to satisfy the required properties. We evaluate the two primitives.

A. Symmetric key primitives

Symmetric key cryptographic primitives for privacy or authentication are efficient and focus on implementation of these primitives. Not many papers show primitives specifically at the tightly constrained environments of RFID tags. Vajda and Buttyan proposed a medley of lightweight cryptographic primitives for RFID tags authentication [3]. Feldhofer, Dominikus, and Wolkerstorfer proposed lightweight hardware implementation of a symmetric key cipher, namely, 1 128 bit version of the Advanced Encryption Standard (AES). Their design requires just over 3500 gate equivalents, considerably more than appropriate for basic RFID tags, but suitable for higher cost RFID tags [4].

B. Asymmetry key primitives

The task of an RFID tag is to provide information over the radio channel using minimal hardware components. This work can be supported by ECC processor for RFID tags which implements an ECDSA signature generation device. ECC is utilized to gain strong resistance against cryptographic attacks and to reduce the storage requirements. The RFID tag will provide cryptographic authentication and copy protection with the help of the digital signature. The Elliptic Curve Digital Signature Algorithm (ECDSA) provides authentication utilizing the elliptic curve discrete logarithm problem as underlying intractable operation. ECC promises the same security level for a 160 bit key as with the RSA method using 1,000 bit key [5].

VII. CONCLUSIONS

We analyzed security measurement to estimate performance and threats. Real measurements must build the basis for analyzing security protocols in order to estimate their behavior and protocol types. Additionally, we focus on the requirements of security solutions. From the crypto primitive, we evaluate symmetric key and asymmetry key primitives to acquire proper security policy.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology(grant number:2010-0024133)

REFERENCES

[1] Raphael C.-W. Phan, "Cryptanalysis of a New Ultralightweight RFID Authentication Protocol—SASI", IEEE Transaction on Dependable and Secure Computing, V.6, N.4, pp.316-320, OCTOBER-DECEMBER 2009

[2] I. Vajda and L. Buttyan, "Lightweight authentication protocols for low cost RFID tags," in Proc, 2nd Workshop on Security in Ubiquitous Computer, 2003, pp.76-82

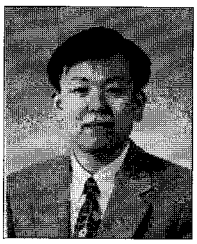
[3] M. Feldhofer, etcs, "Strong authentication for RFID systems using the AES algorithm," Cryptographic hardware and embedded systems", CHES 2004, v.3156, pp.357-370, 2004.

[4] Martin Feldhofer, "Strong crypto for RFID Tag, - A comparison of low power hardware implementation", 2007 IEEE, pp.1839-1842.

[5] Yanjun Zuo, "Survivable RFID Systems: Issues, Challenges, and Techniques", IEEE Transaction on Systems Man and Cybernetics,—PART C: Applications and reviews, V. 40, N. 4, pp. 406-418, JULY 2010.

[6] Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags. In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM 2006 Workshops. LNCS, vol. 4277, pp. 352–361. Springer, Heidelberg, 2006

[7] Andrey B,etcs, "Hash functions and RFID tags: Mind the Gap:, CHES 2008, LNCS, pp.283-299, 2008



Jung-Tae Kim
received his Ph.D. degrees in Electronic Engineering from the Yonsei University in 2001. From 1991 to 1996, he joined at ETRI, where he worked as senior member of technical staff. In 2002, he joined the department of electronic engineering, Mokwon University, Korea, where he is presently professor. His research interest is in the area of information optical security technology that includes network security system design, RFID&USN and wireless security protocol.