http://dx.doi.org/10.6109/ijice.2011.9.6.701

Analyses of Security, Privacy Issues and Challenges for RFID System

Jung-Tae Kim, *Member, KIICE*

***Abstract*— RFID is a widely adopted in the field of identification technology these days. Radio Frequency IDentification (RFID) has wide applications in many areas including manufacturing, healthcare, and transportation. Because limited resource RFID tags are used, various risks could threaten their abilities to provide essential services to users. A number of RFID protocols have done by researcher in order to protect against some malicious attacks and threat. Existing RFID protocols are able to resolve a number of security and privacy issues, but still unable to overcome other security & privacy related issues. In this paper, we analyses security schemes and vulnerability in RFID application. Considering this RFID security issues, we survey the security threats and open problems related to issues by means of information security and privacy. Neither a symmetric nor an asymmetric cryptographic deployment is necessarily used with light weighted algorithm in the future.**

***Index Terms*— Security, Privacy, RFID Protocol, Ultra-weight algorithm**

I. INTRODUCTION

RFID is expected to be the basic technology for ubiquitous network or computing, and to be associated with other technology such as telemetric, and wireless sensors. Recently, the wide deployment of RFID systems in a variety of applications has raised many concerns about the privacy and the security issues. RFIDs have applied widespread use in many commercial product as well as national security applications, ranging from e-passports, contactless credit cards to supply chain management. Since RFID tags are wireless 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. Another issue related to the design of RFID is the computational performance required at the tag side. These days many systems applicable to ubiquitous surroundings use wireless communications. Within such environments the majority of devices have limited computing resources, small storage and low power supply. It needs light-weight protocol to implement [1].

As shown in Fig. 1, basic RFID system consists of six main components [2].

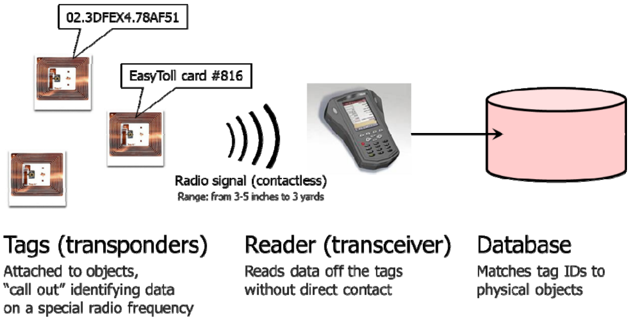

02.3DFEX4.78AF51
EasyToll card #816
Radio signal (contactless)
Range: from 3-5 inches to 3 yards
Tags (transponders)
Attached to objects, "call out" identifying data on a special radio frequency
Reader (transceiver)
Reads data off the tags without direct contact
Database
Matches tag IDs to physical objects

Fig. 1. Basic Configuration of RFID System.

A basic RFID infrastructure consists of 3 major components: (1) tags, (2) a reader and its antenna, and (3) middleware application software. RFID tags are transponders that contain a chip and an antenna. The antenna receives radio signals from the readers while the chip is used to respond to the signals and to store information. Current tags are small enough to be embedded into physical objects for identification and tracking. Tags can be read only, write once/read many times or read/write capable. RFID readers are electronic interrogators that emit and receive radio signals through their antennas. They capture data stored and may over write the data on the tags. They are also responsible for the information flow between the tags and the host system via the middleware. Typically, there are three types of players in an RFID system—RFID tags, readers, and the backend databases. A tag is physically attached to an item with a unique identification. The radio frequencies at which a tag transmits and receives signals include low frequency (LF, e.g., 124–135 kHz range), high frequency (HF, e.g., 13.5 MHz), ultrahigh frequency (UHF, e.g., 860–960 MHz), and microwave bands. Particular fixed frequencies can be assigned to an RFID application to avoid or reduce the effects of radio interference. As a tag's operating frequency increases its signals are able to carry more data. The communication between tags and reader uses a defined radio frequency and protocol [3].

Manuscript received October 23, 2011; revised November 24, 2011; accepted November 30, 2011.

Jung Tae Kim is with the Dept. of Electronic Eng., Mokwon University, Korea (Email : jtkim5068@hotmail.com)

II. RELATED WORK

Privacy and security solutions can be divided into two groups: hardware solutions and software solutions. Hardware solutions are related to some controls of process variations in each integrated circuit, killing a tag or blocking a tag. As consumers use some readers to scan their own tags, a technique to protect context of tag is kill the tag. Indeed, a kill command can be used to destroy a tag. However, a killed tag is truly dead and can never be reactivated. This is a key disadvantage for the "killing tag" technique. Different from the "killing tag" technique, the blocking tag method involves no modification to the consumer tag. Based on the "tree walking" method, a blocking-capable tag creates an RF environment to prevent unauthorized scanning of consumer items in order to "spam" misbehaving readers, i.e. there is no way to locate the protected tag's ID. Generally, the bit used to "spam" misbehaving readers is one of 28-bit EPC management. Software solutions are based on the exchange of messages to establish authentication between two entities. Although s mutual authentication without any hash function is used, most software solutions use general hash functions (like MD4 and SHA-1) to support access control and authentication. A number of security researchers have published papers on security solution. Most of the sources of security and privacy issues arise from the violation of the air interface between a tag and its reader [4].

A. Performance Analysis

In general, memory cost depends on digital logic gate counts. Normally, logic gates to be used for security are from 250 to 3000 in a tag. In conventional scheme, a tag store one key and two binary matrices. A tag need not store the implementation of low-cost cryptographic primitives which can be constructed with 6 to 13 K gates. It results in the usage of less memory than previous scheme. The conventional scheme requires a lightweight bitwise operation both in a tag and a reader. It reduces the burden on database in process of searching a tag ID as well as on a tag to operate. Communication cost can be counted number of protocol and memory size in a tag. If the bit length of R and the number of rows on memory and the bit length of each row on memory and the length of ID are respectively 16, 128, 7, and 128. By using complement rows, communication overhead is reduced as keeping strong security. Following overhead should be estimated [5].

- Computational overhead
- Storage overhead
- Communication overhead

B. Security Requirements of RFID Systems

Threats and privacy concerns with a low-cost RFID system should satisfy the following security requirements [6]:

a. Anonymity-Privacy: The values transmitted by a tag must not reveal any information about the product that it is attached to.

b. 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.

c. 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.

d. 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.

e. Availability: The reader and thus the back-end system should always be in place to identify a legitimate tag.

C. Threat of RFID

Some well-known threats are presented as follows [20]

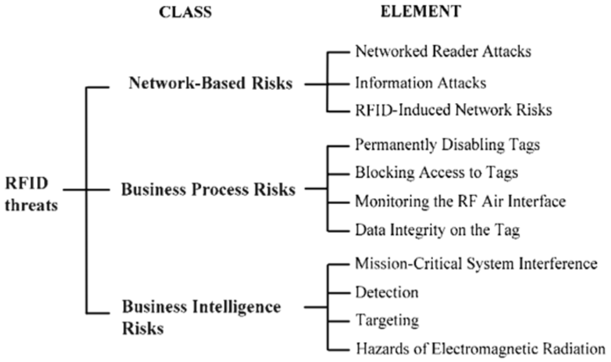

CLASS
ELEMENT
RFID threats
Network-Based Risks
Networked Reader Attacks
Information Attacks
RFID-Induced Network Risks
Business Process Risks
Permanently Disabling Tags
Blocking Access to Tags
Monitoring the RF Air Interface
Data Integrity on the Tag
Business Intelligence Risks
Mission-Critical System Interference
Detection
Targeting
Hazards of Electromagnetic Radiation

Fig. 2. Karygiannis's Taxonomy Model.

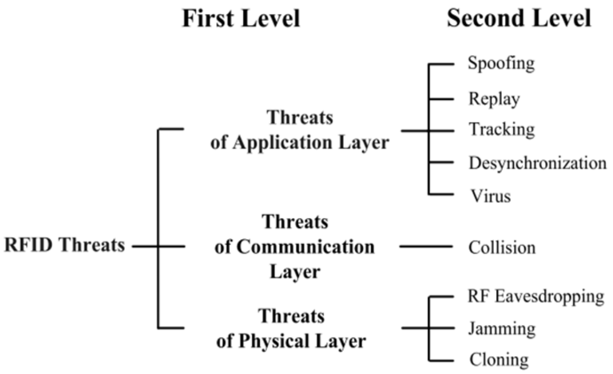


Fig. 3. Taxonomy Model of RFID Security Threats.

D. Attacks of RFID

Some well-known attacks are presented below [11, 12].

a. Physical Attacks: Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others.

- Secure network and access points (firewalls, intrusion detection systems)

b. Denial of Service (DoS): A common example of this type of attack in RFID systems is the signal jamming of RF channels.

c. Counterfeiting: There are attacks that consist of modifying the identity of an item, generally by means of tag manipulation.

d. Spoofing: When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.

- Mutual authentication and data encryption, digital signatures
- Appropriate placement of tags and readers.

e. Eavesdropping: In this type of attacks, unintended recipients are able to intercept and read messages.

- Data encryption
- Proper placement of RF equipment
- Limit RF transmission power
- Authentication for reader access
- Physical access control

f. Traffic analysis: Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even though the messages are encrypted and cannot be decrypted.

g. Relay (man in the middle) attacks

- Enforce strict time requirement limit for a tag to respond to a reader's query

h. Replay attacks

- Hash-based schemes with challenges

Even though many works have been done for many security threats with RFID technology, but many issues are still unsolved and some others need to be investigated. 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:

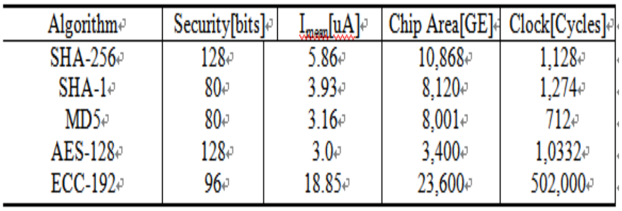
III. SECURITY REQUIREMENTS

A. Hardware based on Crypto algorithm

A few papers explore primitive geared at the very tightly constrained environments of RFID tag [5]. 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 3,500 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 needs, 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 [8].

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 I. The chip area results are based on synthesis and are given in gate equivalents [GE] [9, 10].

TABLE I
SYNTHESES AND SIMULATION RESULTS ON 0.3UM CMOS [9, 10]



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
AES-128	128	3.0	3,400	1,0332
ECC-192	96	18.85	23,600	502,000

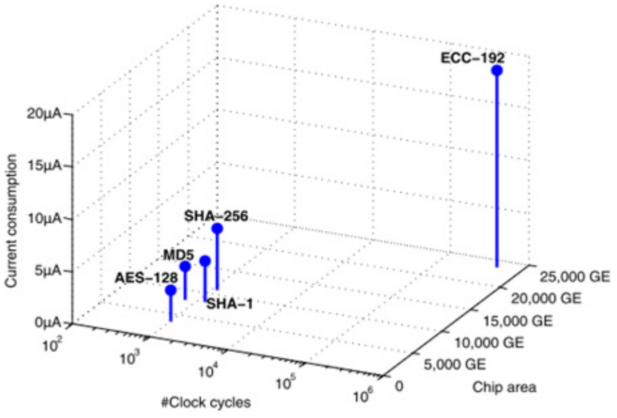


Fig. 4. Comparison of Low-power Implementation of Crypto Algorithms.

B. Research Directions for RFID Survivability

Survivability can only be achieved by the use of preventive, reactive, adaptive, and recovery approaches together. The following outlines the research thrusts to be pursued that could significantly improve the survivability of an RFID system. Although some research has been conducted, there are still no complete solutions, which is a readily applicable to enhance RFID survivability as given in the following [6, 11, 12].

1) Continuously developing efficient software and hardware authentication and communication mechanisms suitable for low-cost RFID tags.
2) Developing advanced physical security of RFID system.
3) Building agile, adaptive, robust, and resilient RFID systems.
4) Developing fault tolerance, recovery, intrusion and detection techniques or RFID systems.

C. Threat of RFID Protocol

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

- 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 oracle.
- Tag/reader authenticity: We have designed mutual protocol with both reader-to-tag authentication and tag-to-reader authentication.

Privacy threats can be classified into several types as follows.

- Action threat: n individual's behavior is inferred by monitoring the action of a group of tags.
- Association threat: individual's identity can be associated with the purchased items containing the RFID tag.
- Location threat: individuals carrying unique tags can be monitored and their location revealed.
- Preference threat: the individual's preference can be exposed by identifying the tag on an item he purchases.

D. Vulnerability of RFID Protocol

Security design of the protocol should not impede normal operations, and should prevent a malicious adversary from getting any information [13, 14, 15, 16, 17, 20]. 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.

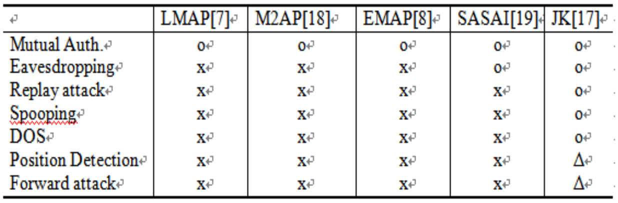
2) Indistinguishableness/Tracking/Passive Replay

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

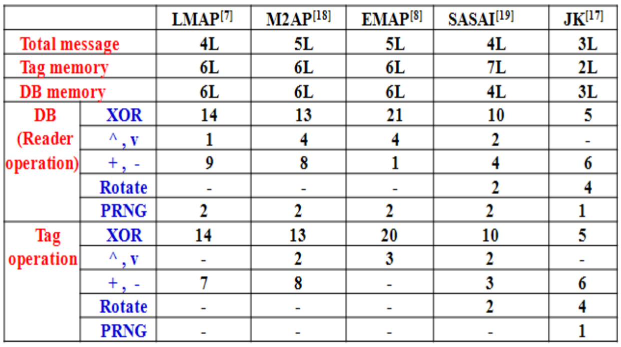
This means that the current key of a tag has been found, and can be used to extract previous messages (assuming that all its past conversations are recorded). Let's say the adversary somehow finds keys. The tag always communicates using a hash function. The adversary cannot use the key to decode any 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. There are a number of solutions proposed so far to solve the security problems and threats associated with the use of RFID systems [11].

TABLE II
COMPARISON OF SECURITY ANALYSES FOR DIFFERENT PROTOCOLS [10]



	LMAP[7]	M2AP[18]	EMAP[8]	SASAI[19]	JK[17]
Mutual Auth.	o	o	o	o	o
Eavesdropping	x	x	x	o	o
Replay attack	x	x	x	x	o
Spooping	x	x	x	x	o
DOS	x	x	x	x	o
Position Detection	x	x	x	x	Δ
Forward attack	x	x	x	x	Δ

TABLE III
COMPARISON OF STORAGE AND OPERATION ANALYSES FOR DIFFERENT PROTOCOLS [10]



		LMAP[7]	M2AP[18]	EMAP[8]	SASAI[19]	JK[17]
Total message		4L	5L	5L	4L	3L
Tag memory		6L	6L	6L	7L	2L
DB memory		6L	6L	6L	4L	3L
DB (Reader operation)	XOR	14	13	21	10	5
	^ , v	1	4	4	2	-
	+ , -	9	8	1	4	6
	Rotate	-	-	-	2	4
	PRNG	2	2	2	2	1
Tag operation	XOR	14	13	20	10	5
	^ , v	-	2	3	2	-
	+ , -	7	8	-	3	6
	Rotate	-	-	-	2	4
	PRNG	-	-	-	-	1

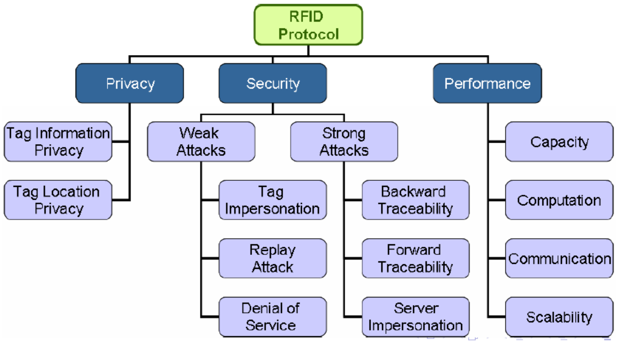


Fig. 5. Consideration of Requirement for RFID Protocols

IV. CONCLUSIONS

We analyzed security issues to estimate performance, threats and performance of security related to issues by means of information security and privacy. Neither a symmetric nor an asymmetric cryptographic deployment is necessarily with light weighted algorithm. Advantages and disadvantages and their relative suitability will depend on the application. In future work, we will develop test bed for RFID system to estimate performance and related problems.

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:2011-0026950)

REFERENCES

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

[2] George Poulopoulos, Konstantinos Markantonakis, Keith Mayes, "A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems", pp.706-p.711, 2009 International Conference on Availability, Reliability and Security

[3] Dong-liang Wu, "A brief Survey on Current RFID Application", Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009, pp.2330-2335

[4] S.A.Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", In Security in Pervasive Comp., volume 2802 of LNCS, pages 201-212, 2004.A

[5] M. Feldhofer, etcs, "Strong authentication for RFID systems using the AES algorithm," Cryptographic hardware and embedded systems", CHES 2004, v.31, n.56, pp.357-370, 2004

[6] 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

[7] P. Peris-Lopez, etcs, "LMAP: A Real Lightweight Low-cost RFID Tags", Proc. Second Workshop RFID Security, July, 2006

[8] P. Peris-Lopez, etcs, "EMAP: An Efficient Mutal Authentication Protocol for Low-Cost RFIDs", Proc. OTM Federated Conf and Workshop: IS Workshop, Nov. 2006

[9] 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

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

[11] Selwyn Piramuthu, "Lightweight Cryptographic Authentication in Passive RFID Tagged Systems," IEEE Tran. On Systems, Man, and Cybernetics—Part C: Applications and review, v.38, n.3, pp.360-376, May 2008

[12] P. Peris-Lopez, J. C. Hernandez-Castro, J. Estevez-Tapiador, and A. Rib-agorda, "RFID systems: A survey on security threats and proposed solutions," in 11th IFIP International Conference on Personal Wireless Communications – PWC06, ser. Lecture Notes in Computer Science, vol.4217. Springer-Verlag, September 2006, pp. 159–170.

[13] Ari Juels, "RFID Security and Privacy: A Research Survey", IEEE Journal of selected areas in communications, V.24, N.2, pp.381-394, February, 2006

[14] P. Ekdahl, and T. Johansson, "Another attack on A5/1", IEEE Transactions on Information Theory, V.49, N.1, pp.284-289, 2003A

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

[16] Faouzi Kamoun, "RFID System Management: State-of-the Art and Open Research Issues", IEEE Trans. on Network and Service Management, V. 6, N. 3, pp.190-205, Sep. 2009.

[17] J.D.H, etcs, "Strong Authentication and improving privacy with ultra-weight RFID authentication Protocol", KIISC, v.19, n.19, pp.81-91, 2009

[18] P. Peris-Lopez, etcs, "M2AP: A Minimalist mutual authentication Protocol for Low-cost RFID Tags", Proc. Int' Conf Ubiquitous Intelligence and Computing, pp.912-923, 2006.

[19] H.Y. Chien. "SASI: A New Ultra-weight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing., vol.4, n.4, pp.337-340, Oct. 2007

[20] Karygiannis, "Karygianni's Taxonomy Model in RFID Threats", 2008 11th IEEE International Conference on Communication Technology Proceedings, pp.765-768

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 security technology that includes network security system design, RFID&USN and wireless security protocol.