Issues Related to RFID Security and Privacy

Jongki Kim [a], Chao Yang [b], Jinhwan Jeon [c]

[a] Division of Business Administration, College of Business, Pusan National University
30, GeumJeong-Gu, Busan, 609-735, Korea
Tel: +82-51-510-2582, E-mail: jkkim1@pusan.ac.kr

[b] Department of Business Administration, Graduate School, Pusan National University
Tel: +82-51-510-1659, E-mail: jeonjinhwan@pusan.ac.kr
Tel:+82-51-510-2582, E-mail:nvhair0818@hanmail.net

[c] Research and Education Institute of Banking, Security and Derivatives, Pusan National University
30, GeumJeong-Gu, Busan, 609-735, Korea
Tel:+82-51-510-2582, E-mail: jeonjinhwan@pusan.ac.kr

Abstract

Radio Frequency Identification (RFID) is a technology for automated identification of objects and people. RFID may be viewed as a means of explicitly labeling objects to facilitate their "perception" by computing devices. RFID systems have been gaining more popularity in areas especially in supply chain management and automated identification systems. However, there are many existing and potential problems in the RFID systems which could threat the technology's future. To successfully adopt RFID technology in various applications, we need to develop the solutions to protect the RFID system's data information. This study investigates important issues related to privacy and security of RFID based on the recent literature and suggests solutions to cope with the problem.

***Keywords*:**

RFID; RFID-tag; Privacy; Security

I. Introduction

Radio Frequency Identification (RFID) is a technology for identification of objects and people automatically, as a supplementary technology or replace traditional barcode technology to identify, track, and trace items automatically. RFID may be viewed as a means of explicitly labeling objects to facilitate their "perception" (Juels, 2006) by computing devices.

RFID dates back to the 1940's. The British Air Force used RFID-like technology in World War II to identify whether planes belonged to them or not. The theory of RFID was first put forwarded in 1948 in a conference paper which entitled "Communication by Means of Reflected Power" by Stockman, and the first patent for RFID was filed by Charles Walton in 1973.

RFID system is composed of two core components, reader which is the central component of an RFID system and RFID-tag in which records the production's information and a unique ID. Moreover, antenna, middleware, and back database also play an important role in RFID system.

RFID-tag is small microchip designed for wireless data transmission. Tags have various forms and functional characteristics, and could be classified into active tags and passive tags. Active tags use the onboard power sources, like batteries, so can support more sophisticated electronics with increased data storage, long read/write range, sensor interfaces, and specialized functions. Passive tags designed without onboard power source, receive the power from the RFID reader devices, so the read/write range is shorter than active tags.

Thanks to the effort of large organizations, such as Wal-Mart, Procter and Gamble, and the U.S. Department of Defense, to deploy RFID as a tool for automated oversight of their supply chains, RFID has been paid more and more attention in the past years. RFID technologies could have been used in so many applications, the combination of dropping tag cost and forceful RFID standardization is an important reason.

However, RFID confronts many challenges, in order to accept this technology in broader fields, we need to develop the solution to secure and protect the human's privacy. Thus, we will review the attacks to the systems, reported privacy threats and some possible solutions.

II. Security and Privacy Issues

In the near future, RFID will become part of more high-profile applications. But at the mean time, more and more people worry that security and privacy problems would interfere the future of this technology, particularly as it is used for more critical purposes. Now, we review the issues related to RFID system first.

2.1 Risks in RFID business process

Many threats to RFID systems can be aroused by human or the environment in management and technical areas. Anybody can damage or destroy a tag mindfully or mindlessly, also can remove the tag from the item to which it was attached, or replace a tag with another one to meet some certain intentions.

The environment's changes also can influence the RFID systems' data. In the extreme heat, cold, moisture, vibration, shock, and radiation circumstance, the tag performance could be menaced because of the impacts, which include degradation of the tags and their performance, and separation of the tags from the associated items.

A mount of factors can influence the business risks in RFID systems, including the importance of the RFID-supported business processes to the mission of the organization, the robustness of business continuity planning or fallback procedures, the existence of adversaries with the motivation and the capability to perform RFID attacks, and the presence and effectiveness of RFID security controls.

NIST (2006) proposed some other factors that influence business intelligence risk, including the type of information stored on the tag, the usefulness or relevance of information available to the adversary, and the location of RFID components.

Externality risk is another important risk worth discussing in RFID system, which results from electromagnetic radiation. The main types of hazards from electromagnetic radiation are the hazards to ordnance which is evaluated by the U.S. military regulations, the hazards to fuel that is the danger of electromagnetic waves causing the sparking or arcing between two metals, the hazards to people which can heat living tissue and the hazards to other materials such as blood products, vaccines, and pharmaceuticals. Although each type has special characteristics, the influence factors are similar. Include RFID operating power and frequency, distance between RFID system components and object, and the complex cavity effects (NIST, 2006).

2.2 Attacks to RFID tag

Since RFID tag computational resource is limited, the RFID environment connects everything, and an RFID tag can't identify authentic readers generally, so RFID system is vulnerable to suffer from variable attacks.

Denial-of-Service (DoS) Attacks

Computer and Information Science Security Research Group at Edith Cowan University indicates that hackers could launch DoS attacks against some types of RFID systems (Sixto, 2006).

Attacking and Modifying Tags

Lukas Grunwald noted that hackers with the proper equipment could record data from a low-cost RFID chip and upload another data to it. He also said that some programs could access the Internet and become available to hackers. Specially, counterfeiting tags is an attack that consisted in modifying the identity of an item (Sixto, 2006).

Traffic analysis

Traffic analysis is another kind of attacks that describes the process of intercepting and examining messages in order to extract information from patterns in communication (Pedris-Lopez et al., 2006).

Spoofing

Spoofing tag can occur if an attacker is able to impersonate a legitimate tag successfully (Pedris-Lopez et al., 2006).

2.3 Privacy Threat

The biggest social issue centers on privacy concerns and threat of legislative oversight. Artifact LLC and BIG research recently found that more than 60% of consumers concerned on the privacy issues about the RFID (Stegeman, 2004).

RFID tags respond to reader interrogation without alerting their owners or bearers. Therefore, if the read range permits, it is possible to do the clandestine scanning of tag. Whoever carrying an RFID tag can broadcast a serial number to the nearby readers effectively, so provides a good vehicle for clandestine physical tracking, even if the tag number is random and carries no intrinsic data (Juels, 2006). The privacy threat will become serious if a tag number combines with personal information.

Location Threat

Users who carry RFID tags can be monitored and then their location revealed. A tagged object's location may be unauthorized disclosure without thinking of who is carrying it (Vajda and Buttyan, 2003).

Constellation Threat

The tags form a unique RFID constellation around the person whether user's identity is associated with a tag set or not and adversaries can use this constellation to track people (Kim et al., 2006).

Transaction Threat

Anyone who takes RFID reader can conjecture the transaction between users associated with the constellation when tagged objects change from one constellation to another. Tow typical threats of this threat are action threat that the individual's behavior is inferred by monitoring the action of a group of tags and the association threat that the individual's identity can be associated with the purchased items containing the RFID tag (Lee and Kim, 2006).

Preference Threat

A tag uniquely identifies the manufacture, the product type, and the object's unique identity. This shows the customer preferences at a low cost. If the adversary can easily determine the item's monetary value, this threat can become a value threat (Garfinkel et al., 2005).

Breadcrumb threat

This is a threat that the discarded breadcrumbs keep tagged items and identities associating with them, so they can be subject to be used to commit malicious act (Kim et al., 2006).

2.4 Other Risks

Besides those risks and threats mentioned above, there are some other issues, such as the risk of embedding virus into the RFID tags and the problem of cloning tags.

Viruses

Researchers of Vrije University's Computer Systems Group said that hackers could create viruses and embed them in RFID tags. The viruses could exploit application vulnerabilities and cause a buffer overflow or some other problem that could infect a back-end system. Once the database is infected, RFID applications that access its information could write the mal-ware into other tags and thereby propagate the infection (Sixto, 2006).

Cloning RFID Tags

Johns Hopkins University's Information Security Institute and RSA Laboratories' researchers have demonstrated that hackers could clone implanted tags in the way that thieves steal RFID-protected vehicles (Garfinkel et al., 2005). Hackers could use cloners to intercept a tag's digital identity, and then crack the encryption and use a software radio simulate the legitimate tag, and then deceive the reader.

III. Solutions

In the following, we will describe several mechanisms have bee proposed to enhance the RFID's security and privacy. Effective mechanisms should provide protection against the risks mentioned. But at the meanwhile, the cost of the approaches should also be taken into account.

"Killing" and "Sleeping" command

EPC tags address users protect the privacy in the way of killing tags. When tagged objects are purchased, the EPC tag receives a "kill" command from a reader and then it deactivated itself permanently. Sleeping tag is an improved approach which is similar to killing tag, but the merit of it is that the deactivated tag can be activated by "wake" (Juels et al. 2003).

Tag Password

Verifying PINs or passwords in basic RFID tags is a simple way to protect the information. The tags do not send out important information unless it receives the right password. Only if the reader knows the tag's identity, otherwise it can not know which password to transmit to a tag (Xiao et al., 2006).

Blocking tag

Juels et al. (2003) proposed the blocker tag, which enhances RFID privacy in a different way. This scheme depends on the incorporation into tags of a modifiable bit called a privacy bit.

However, the blocking tags approach has some limitations. Such as, it may enable the store pickpocket to be possible to hide the stores' security check. Thus, the authors proposed the selective blocking tags in the same paper, and then Juels and Brainard (2004) proposed another improved scheme-soft blocking, which are the schemes can protect against the preference threat.

Schemes based on Hash Functions

Weis et al. (2003) proposed a Hash-Lock scheme to protect information privacy of RFID. In this approach, a tag's ID is saved in memory in two states: locked and unlocked. It is possible that using the ID to lock a tag to prevent revealing information, and use another key to unlock a locked tag. Then he designed another randomized Hash-Lock scheme to improve the temporarily unchanged meta-ID problem which existed in the Hash-Lock scheme. Ohkubo et al. (2003) designed Hash-Chain scheme to satisfy the requirements that tag embeds two different hash functions and can generate one out-going value to response and new secret value quickly.

Regulating Tags

Garfinkel (2002) proposed RFID Bill of Rights that should be upheld when using RFID systems. The RFID Bill of Rights addresses privacy problems through regulation on consumers' knowledge of the RFID tags' existence, removal/deactivation on purchase, consumers' data and service accessibility, the time and location, and the tags accessing reasons.

Classic Cryptography

Kinoshita et al. (2003) proposed an anonymous-ID scheme based on rewritable memory. Concealing a tag's permanent ID, which has a rewritable memory contains a user-chosen private ID or assign a partial ID sequence to a user-assignable tag, so that users could control the uniqueness of IDs from local to global without revealing the relationship between the ID and the object.

Symmetric key encryption is another approach which was proposed by Feldhofer et al. (2004) based on a simple two-way challenge-response algorithm. And an RFID protocol-yoking was proposed by Juels (2004). He pointed the cryptographic proof that two tags have been scanned simultaneously, and evidence that the tags were scanned in physical proximity to one another. This scheme is suitable for basic tags that require no computation virtually.

Public key encryption is also an approach that based on the cryptographic principle of re-encryption.

As the approach to protect information privacy, encryption is an effective method, but it dose have limits. First, the encrypted identifier itself is just another identifier. Second, there is the problem of key management in encryption scheme. Moreover, the problem of cost is the most important and it is difficult to apply them to low-cost tags.

Distance Measurement

Signal-to-noise ratio of the reader signal in an RFID system provides a rough metric of the distance between a reader and a tag (Floerkemeier et al., 2004). With some additional, low-cost circuitry tag might achieve rough measurement of the distance of an interrogating reader, and proposed that this distance can serve as a metric for trust.

Shielding Tag

The faraday cage approach is one kind of shielding. It isolates RFID tags from any kind of electromagnetic waves by using a faraday cage which is a container made of metal mesh or foil that is impenetrably by radio signals. In addition, after products are taken out of the containers, they can still be scanned by unauthorized personal. Another approach of shielding tags is the active jamming approach which isolating from electromagnetic waves by disturbing the radio channel (Xiao et al., 2006).

Proxy Approach

It is possible that users carry their own privacy-enforcing devices for RFID instead of relying on public RFID readers to enforce privacy protection, like the mobile devices. RFID Guardian is a typical approach, which is a platform that offers centralized RFID security and privacy management for individual people which is meant for personal use. The consumers can protect their privacy through carrying a battery-powered mobile device that monitors and regulates their RFID usage. The heart of the RFID Guardian is that it integrates four previously separate security properties that include auditing, key management, access control, and authentication into a single device (Rieback et al., 2005).

Tag Pseudonyms

It is an approach that uses a small pseudonyms collection and rotates these pseudonyms as its identifier in every tag, release a different one on each reader query. The authorized readers share the full pseudonym set with tag in advance, so they can identify the tag. Since attackers are unable to correlate two different pseudonyms of the same tag, it would be more difficult for unauthorized tag to track (Juels, 2006).

Trusted Computing

Molnar et al. (2005) proposed an approach which relies on "privacy bits". They describe how equipped with trusted platform modules can internally enforce tag privacy policies. However, this scheme dose not solve the rogue readers' problem, it can be as a complement for other privacy protection (Juels, 2006).

Authentication

Molar and Wagner (2004) proposed a basic PRF private authentication scheme for mutual authentication between tags and readers. This protocol uses a shared secret and a Pseudo-Random Function (PRF) to protect the messages exchanged between the tag and the reader. In the same paper, the authors proposed a tree-based private authentication and delegation tree scheme to reduce the server's load which exists in the hash schemes.

Non-Cryptographic Primitives

Vajda and Buttyan (2003) proposed a set of extremely lightweight challenge-response authentication protocols which can be used for authenticating tags.

Human protocols

Weis (2005) introduced the concept of human computer authentication protocol due to Hopper and Blum, adaptable to low-cost RFID.

Besides the mechanisms described above, the National Institute of Standards and Technology of U.S. drew up the guidance for securing RFID systems. This security controls divided into 3 groups that are management, operational and technical in which described the considerations and controls in detail. Besides these security controls, it also discusses the privacy considerations including the privacy principles, applicable privacy controls and some other recommendations (NIST, 2006).

In addition, the experts have been paying more attention to legal concerns over RFID data collection. For example, in 1998, the European Parliament enacted guidelines on information privacy called the "European Community Directive on Data Protection". Under the EU Directive, information can be collected and used only if in some certain purpose and conditions. To determine the lawfulness of a data processing operation, the Directive also sets out a number of principles. In the practical implementation of RFID systems, 6 golden rules have to be obeyed (Van Eecke and Skouma, 2005).

Not only European, many countries also have set up regulations to restrict RFID uses from tag production to data collection. Especially, Korea Ministry of Information and Communication set up the privacy protection guardian to regulate every stage of the use of RFID.

The security loophole and the privacy threats are so complex, it is not possible to solve the problem by depending upon one measure alone, therefore it should evaluate each aspect of the question overall. Any single solution is not comprehensive, and it has the possibility to cause the RFID system to appear other security weakness and loophole. In order to guarantee the RFID system secure, the extendibility, administration and system expenses should be evaluated in overall.

IV. Conclusion

RFID technology is universal, useful and convenient, and will be continued to develop quickly in the future. However, it brings many challenges in the implementation, especially on the security and privacy aspects.

This paper provides investigates the security risks and privacy threat in the RFID systems, and gives several approaches in which to solve the issues of RFID based on the recent literature.

With the development of the RFID technology, it will create more and complex problems. Since this technology will be used in more high level applications broadly in the future, the demands in security will also be higher.

References

[1] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J. (2004). "Strong Authentication for RFID Systems Using the AES Algorithm," *Proceedings of Cryptographic Hardware and Embedded Systems-CHES'04*, Vol. 3156 of LNCS, pp. 357-370.

[2] Floerkemeier, C., Schneider, R., and Langheinrich, M. (2004). "Scanning With Purpose-Supporting the Fair Information Principles in RFID Protocols", *Proceedings of the 2nd International Symposium on Ubiquitous Computing Systems (UCS)*, pp. 1-9.

[3] Garfinkel, S. L. (2002). "An RFID Bill of Rights," *Technology Review*, page 35.

[4] Garfinkel, S. L., Juels, A., and Pappu, R. (2005). "RFID Privacy: An Overview of Problems and Proposed Solutions," IEEE Security and Privacy, vol. 3, pp. 34-43.

[5] Juels, A. (2004). "Yoking-proof's for RFID Tags," *Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW04)*, pp.138-143.

[6] Juels, A. (2006). "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, Vol. 24, NO. 2, pp.381-394.

[7] Juels, A., and Brainared, J. (2004). "Soft blocking: Flexible Blocker Tags on the Cheap," *Proceedings of Workshop on Privacy in the Electronic Society(WPES04)*, pp. 1-7.

[8] Juels, A., Rivest, R. L., and Szydlo, M. (2003). "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pp. 103-111.

[9] Kim, I., Lee, B., and Kim, H. (2006). "Privacy Protection Based on User-defined Preferences in RFID System," *International Conference on Advanced Communication Technology-ICACT'06*, pp. 858-862.

[10] Kinoshita, S., Hoshino, F., Komuro, T., Fujimura, A., and Ohkubo., M. (2003). "Low-cost RFID Privacy Protection Scheme," *Journal of the International Planetarium Society*, Vol. 8, pp.2007-2021.

[11] Molnar, D., and Wagner. D. (2004). "Privacy and Security in Library RFID: Issues, Practices, and Architectures," *Proceedings of the 11th ACM Conference on Computer and Communications Security*, pp. 210-219.

[12] Molnar, D., Soppera, A., and Wagner, D. (2005). "Privacy for RFID Through Trusted Computing", *Proceedings of Workshop on Privacy in the Electronic Society*, pp. 31-34.

[13] NIST (2006). "Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft)", Special Publication 800-98.

[14] Ohkubo, M., Suzuki, K., and Kinoshita, S. (2003). "Cryptographic Approach to Privacy-friendly Tags," RFID Privacy Workshop, http://www.rfidprivacy.us/2003/agenda.php.

[15] Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., and Ribagorda, A. (2006). "RFID

Systems: A Survey on Security Threats and Proposed Solutions," *The 11th IFIP International Conference on Personal Wireless Communications-PWC'06,* Vol. 4217, pp. 159-170.

[16] Rieback, M., Cripo, C., and Tanenbaum, A. (2005). "RFID Guardian: A Battery-powered Mobile Device for RFID Privacy Management", *Proceedings of the 10th Australasian Conference on Information Security and Privacy (ACISP2005),* Vol. 3574 of LNCS, pp. 184-194.

[17] Sixto Ortiz Jr. (2006). "How Secure Is RFID?," IEEE COMPUTER SOCIETY, Computer Archive Vol. 39, pp.17-19.

[18] Stegeman, L. (2004). *Who's Afraid of the Big Bad Wolf?* Market Wire.

[19] Vajda, I., and Buttyan, L. (2003). "Lightweight Authentication Protocols for Low-Cost RFID Tags," *Proceedings of the 2nd Workshop on Security in Ubiquitous Computing,* pp. 1-10.

[20] Van Eecke, P., and Skouma, G. (2005). "RFID and Privacy:. A Difficult Marriage?," *Journal of Computer, Media and Telecommunications Law,* Vol. 3, pp. 84-90.

[21] Weis, S. A. (2003). "Security and Privacy in Radio-Frequency Identification Devices," Masters Thesis, Dept. of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

[22] Weis, S. A. (2005). "Security Parallels Between People and Pervasive Devices," *The 3rd IEEE Conference on Pervasive Computing and Communications Workshops-PERSEC'05,* pp. 105-109.

[23] Weis, S. A., Sarma, S. E., Ronald Rivest, L., and Daiel Engels, W. (2003). "Security and Privacy Aspects of Low-cost Radio Frequency Identification System", *Proceedings of the 1st International Conference on Security in Pervasive Computing,* pp. 201-212.

[24] Xiao, Y., Shen, X., Sun, B., and Cai, L. (2006). "Security and Privacy in RFID and Applications in Telemedicine," *IEEE Communications Magazine,* Vol. 44, No. 4, pp.64-72.