SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

A Secure RFID Reader Protocol based on SLRRP

Hyunrok Lee * Kwangjo Kim *

Abstract— The research on the security of RFID (Radio Frequency Identification) has occupied the attention. Most of previous research results focus on the security and privacy between a RFID tag and a reader. However, the research on the security between a reader and a back-end server leaves much to be desired. And moreover The standard parties of RFID reader protocol, that are EPCglobal Reader Protocol Specification v1.1 (EPCRP) and IETF Simple Lightweight RFID Reader Protocol (SLRRP), simply mentioned that using HTTPS and TLS can be recommended for the security solution of reader protocol. However, they do not consider the properties of various environments like communication channel, computing power of the reader, limitation of hardware, etc. Or even if they give proper consideration of various environments, the security mechanism is supported over specific communication protocol. So, we keenly establish the standard of secure reader protocol which contains authentication protocol, key agreement, message format, etc. In this paper, we introduce the reader protocol standards and raise several problems, and then propose a secure RFID reader protocol which can be satisfied with the security requirements for the reader protocol based on SLRRP. The comparison shows that our protocol adopt the advantages of SLRRP with solving raised security problems.

Keywords: Reader Protocol, RFID, SLRRP

1 Introduction

Radio Frequency Identification(RFID), which can be used to identify objects, is going to be an important technology to be not just an alternative to bar code system, but rather, offer alternatives for much of information technology. The micro-chip equipped on a RFID tag has a unique identification and can be applied for various fields such as not only inventory and supply chain management but also payment, entrance system, anti-counterfeit bank note, home network,etc.

The price of the RFID tag was a barrier to wide deployment so far. Because of the tendency to decrease the price dramatically, RFID technology will be expanded into whole industry within 2 or 3 years. Also, RFID will become core and base technology to build ubiquitous computing environment due to low cost tag and many applications. However, the privacy of user information such as buying details, preference, ownership, location information, and so forth can be unconsciously leaked out on RFID. To make preparation against privacy issues, overall development of security technology including lightweight cryptography technology, authentication protocol, etc. should be considered. For forming a part of the development, many previous research results have been presented. Most of them focus on the security and privacy between a RFID tag.

But the research on the security between a reader and a back-end server leaves much to be desired. The standard parties of RFID reader protocol, that are EPCglobal Reader Protocol Specification v1.1 (EPCRP)[12] and IETF Simple Lightweight RFID Reader Protocol (SLRRP)[13], simply mentioned that using HTTPS[14] and TLS[15] can be recommended for the security solution of reader protocol. However, they do not consider the properties of various environments like communication channel, computing power of the reader, limitation of hardware, etc. Or even if they give proper consideration of various environments, the security mechanism is supported over specific communication protocol. So, we keenly establish the standard of secure reader protocol which contains authentication protocol, key agreement, message format, etc.

In this paper, we introduce typical reader protocol standards; EPCRP and SLRRP; and raise several problems, then derive security requirements from vulnerabilities. And then we propose a secure RFID reader protocol which can be satisfied with the security requirements for the reader protocol based on SLRRP.

The remainder of the paper is organized as follows: In Section 2, we briefly introduce previous security scheme on RFID and the concept of RFID reader protocol with drawbacks. Section 3 describes the security requirement of the reader protocol and proposes secure RFID reader protocol. We compare the reader protocols in Section 4 and finally concluding remarks and future work will be made in Section 5.

2 Related work

2.1 Security scheme on RFID

Many researchers focus on the security and privacy between a RFID tag and a reader which are not only kill, sleeping and blocker tag,[1][2][3] but also hash, pseudonym, zero knowledge and tree based protocol using pseudonym generator that attempts to address the

* Information and Communications University, International Research center for Information Security (IRIS), Information and Communications University (ICU), 103-6 Munji-Dong, Yusong-Gu, Daejeon, 305-714, Korea. {tank, kkj}@icu.ac.kr

security concerns raised as using RFID tags. Hash Lock and Randomized Hash Lock scheme[4] is based on one-way hash function and Universal re-encryption[10] and PUF(Physically Unclonable Function)[11] is adopted for the RFID security. Henrici et al.[6], Lee et al.[7], Ohkubo et al.[5], Wong et al.[8] and Yang et al.[9] protocol are also famous protocol. But it is believed that there is no perfect protocol that avoids all of the threats with reasonably low cost until now.

2.2 RFID Reader Protocol

RFID reader protocol is a rule or standard that controls the communication, connection and data format between a reader device and a back-end server. In this section, we introduce two typical reader protocol; EPCRP and SLRRP, then derive problems correspond to the protocols, and describe rough solutions.

2.2.1 EPCRP

EPCRP is a reader protocol standard compatible with EPC framework ,which is the mainstream for building RFID system in the area of inventory and supply chain management, established by EPCglobal. This standard specification mainly supports EPC Gen 2 Class 0/1 RF protocol and reader. EPCRP can be categorized into largely reader, messaging, transport layer as follows:

- *Reader Layer* : This layer specifies the content and abstract syntax of messages exchanged between the reader and back-end server with defining the operations and meaning.
- *Messaging Layer* : This layer specifies the definition of messages in the reader layer that are formatted, framed, transformed, and carried on a specific network transport.
- *Transport Layer* : This layer provides the networking facilities supported by the operating system or equivalent.

Also EPCRP specification provides Messaging / Transport Binding(MTB) for consequently multiple alternative implementations, ranging from TCP, Bluetooth to serial communication, of each layer can be. The specification indicates how to make API provided by pseudo code, and defines XML schema for data representation. EPCRP is a detailed specification, nevertheless security concern is just using HTTPS, applying certificate profile from EPCglobal.[16] Therefore, the advantage caused by various binding will be faded out and become limitations. So EPCRP should hold own security mechanism for solving these problems.

2.2.2 SLRRP

IETF reviews a reader protocol draft called SLRRP based on wireless IP network to say WLAN. The draft describes that it can manage large-scale RFID platform efficiently through WLAN enterprise network, be compatible with all RF protocol, and especially be implemented easily due to simple protocol stack. The draft follows RFID structure like as Figure 1, and defines reader protocol between RNC(RFID Network Controller) and reader Figure 2. SLRRP specifies reader setup, access, inventory, status and data command with detail message format.

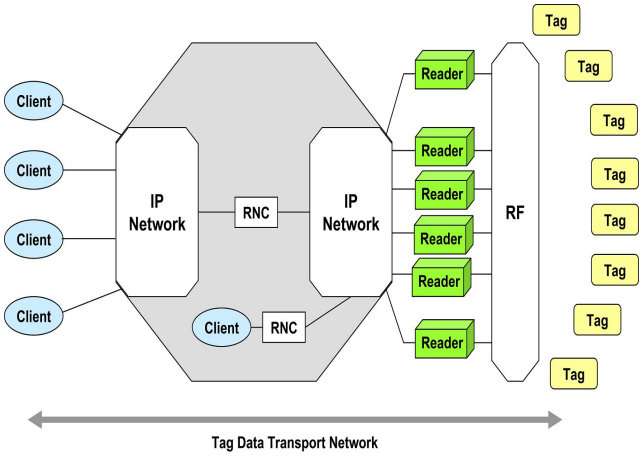

Figure 1: RFID System structure in SLRRP

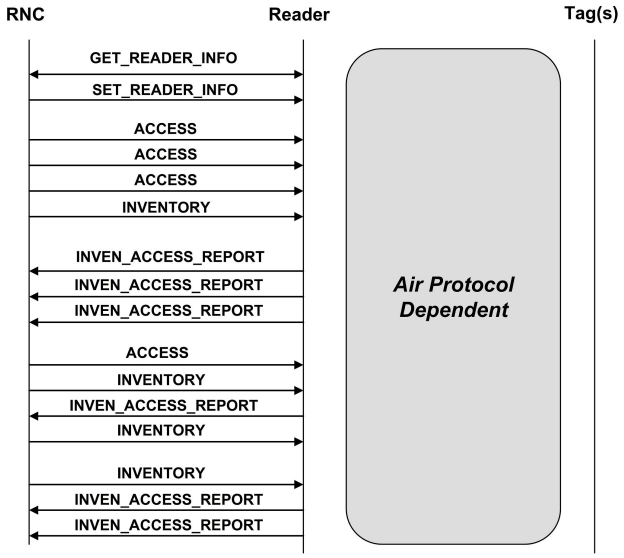

Figure 2: SLRRP Protocol

This protocol recommend that the secure channel will be established by TLS mechanism based on IP network, however we should consider another network environment where the reader can be installed in industrial field. The industrial field still uses a legacy interface which was already installed before like serial, parallel, or proprietary interface to communicate with each device. For overcoming the limitation due to IP network based TLS, therefore, we must include the standard of secure reader protocol which contains authentication protocol, key agreement, message format, etc. into the reader protocol standard.

3 Secure RFID Reader Protocol

The requirements of reader protocol satisfied from confidentiality to replay attack prevention, proposed secure RFID reader authentication protocol, key agreement and message format will be described in this section.

3.1 Security Requirements of RFID Reader Protocol

Security vulnerabilities on RFID reader protocol summarize as follows:

- *Malicious reader* : Malicious reader can join the communication between legitimate reader and back-end server for spoofing attack and collecting information.
- *Compromised reader* : Attacker can capture legitimate reader, then collect data and eavesdrop.
- *Communication eavesdropping* : Active and passive eavesdropping is possible via wire and wireless communication channel
- *Replay attack* : Attacker can replay a message and get the information of reader, tag data, etc.

In order to prevent above vulnerabilities, the security requirements of reader protocol in RFID systems can be listed as follows:

- *Authentication* : Periodic device authentication and cryptographic authentication protocol is needed because of preventing malicious reader join the communication, compromised reader.
- *Integrity* : For preventing spoofing attack, active eavesdropping, etc., integrity should be provided.
- *Confidentiality* : Due to securing against passive eavesdropping, the message should be encrypted.
- *Preventing replay attack* : To prevent replay attack, adopt encryption with updating session key.

3.2 Secure RFID Reader Protocol based on SLRRP

For supporting secure communication in basic SLRRP, firstly the establishment phase of secure communication channel should be provided like Figure 3, where message type is defined in Figure 4.

Figure 5 shows examples of message format expansion, GET_READER_SEC_INFO and GET_READER_SEC_INFO_RESPONSE for exchanging the information to establish secure channel.

In the setup phase, the authentication will be performed by Proxy certificate[17] based authentication protocol. This authentication mechanism can reduce efficiently cost of issuing official certificate.

Notation. We use the notations as summarized in Table 1 to simplify description of our protocol.

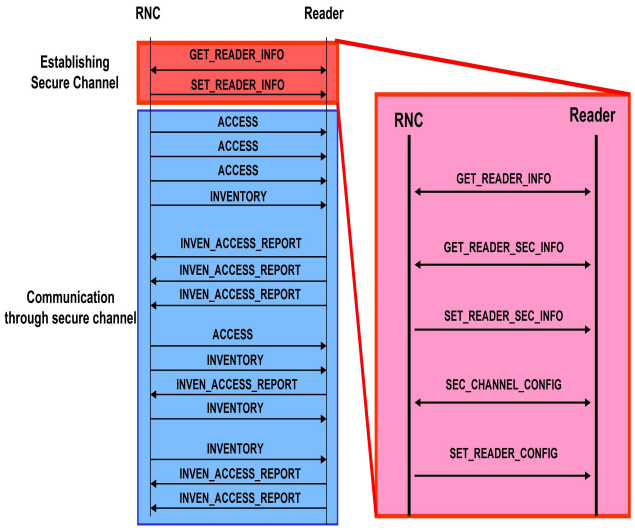

Figure 3: Message for establishing secure channel in SLRRP

Table 1: Notations

$\mathcal{BS}$	Back-end server within specific domain.
$\mathcal{R}$	RF tag reader within specific domain.
$Cert_x$	Certificate of $\mathcal{BS}$ x, issued by official CA.
$PCert_y$	Proxy certificate of $\mathcal{R}$ y, issued by $\mathcal{BS}$.
EN_k	Symmetric encryption using key k
E_x	Asymmetric encryption using public key of x,(x =$\mathcal{R}$ or $\mathcal{BS}$)
S_x	Digital signature using private key of x, (x =$\mathcal{R}$ or $\mathcal{BS}$)
t_x	Time stamp of x, (x =$\mathcal{R}$ or $\mathcal{BS}$)
$h(m)$	Hash value of m.
$MAC_k(m)$	Message Authentication Code of m with key k.
MK	Master key generated by Diffie-Hellman, ($MK = g^{ab}$).
SK	Session key between $\mathcal{BS}$ and $\mathcal{R}$, ($SK = MAC_{MK}(t_{\mathcal{BS}}, t_{\mathcal{R}})$).

Authentication Protocol.

1. $\mathcal{BS} \rightarrow \mathcal{R} : t_{\mathcal{BS}}$
2. $\mathcal{BS} \leftarrow \mathcal{R} : PCert_{\mathcal{R}}, t_{\mathcal{R}}, \mathcal{BS}, S_{\mathcal{R}}(t_{\mathcal{R}}, t_{\mathcal{BS}}, \mathcal{BS})$
3. $\mathcal{BS} \rightarrow \mathcal{R} : Cert_{\mathcal{BS}}, \mathcal{R}, S_{\mathcal{BS}}(t_{\mathcal{BS}}, t_{\mathcal{R}}, \mathcal{R})$

Key Agreement Protocol.

1. $\mathcal{BS} \rightarrow \mathcal{R} : t_{\mathcal{BS}}$
2. $\mathcal{BS} \leftarrow \mathcal{R} : t_{\mathcal{R}}$
3. $\mathcal{BS} \rightarrow \mathcal{R} :$ $S_{\mathcal{BS}}(h(t_{\mathcal{BS}}, t_{\mathcal{R}})), EN_{SK}(h(t_{\mathcal{BS}}, t_{\mathcal{R}}, S_{\mathcal{BS}}(h(t_{\mathcal{BS}}, t_{\mathcal{R}}))))$
4. $\mathcal{BS} \leftarrow \mathcal{R} : EN_{SK}(h(t_{\mathcal{BS}}, t_{\mathcal{R}}, S_{\mathcal{BS}}(h(t_{\mathcal{BS}}, t_{\mathcal{R}}))))$

Type	Message Name
0x00	(reserved by IETF)
0x01	GET_READER_INFO
0x02	GET_READER_INFO_RESPONSE
0x03	SET_READER_CONFIG
0x04	SET_READER_RESPONSE
0x10	INVENTORY
0x11	INVENTORY_RESPONSE
0x12	STOP_INVENTORY
0x13	STOP_INVENTORY_RESPONSE
0x18	ACCESS
0x19	ACCESS_RESPONSE
0x1A	STOP_ACCESS
0x1B	STOP_ACCESS_RESPONSE
0x20	INVENTORY_ACCESS_REPORT
0x30	GET_READER_SEC_INFO
0x31	GET_READER_SEC_INFO_RESPONSE
0x32	SET_READER_SEC_INFO
0x33	SET_READER_SEC_INFO_RESPONSE
0x34	SEC_CHANNEL_CONFIG
0x35	SEC_CHANNEL_CONFIG_RESPONSE

Figure 4: Message format expansion

GET_READER_SEC_INFO

x	x	x	x	x	Ver	Type = 0x30	Message Length = 0xB
Message Seq Num							x x x x x x x x x x x x x x x x
Requested Data							

GET_READER_SEC_INFO_RESPONSE

x	x	x	x	x	Ver	Type = 0x31	Message Length = Variable
Message Seq Num							x x x x x x x x x x x x x x x x
Requested Parameters or Operation Error Parameters							

Figure 5: Example of Message format expansion

After finishing the authentication and key agreement protocol as state above, the negotiation step of cipher suite is followed for selecting designated symmetric cipher. In the sequel, SEC_CHANNEL_CONFIG phase is passed to establish secure channel between the reader and back-end server. Due to including own security mechanism into the reader protocol, we can achieve secure RFID reader protocol which not only provides various communication channel, but also satisfies security requirements of reader protocol.

4 Comparison

The result of comparison between reader protocols is summarized in Table 2. The table shows that our protocol, which receives the advantage of SLRRP, can manage large-scale RFID platform efficiently through enterprise network, be easily implemented due to simple protocol stack. And also the protocol can solve the problems of existing protocol that they do not consider the properties of various environments and the security mechanism is supported over specific communication protocol.

Table 2: The comparison between reader protocols

Category	EPCRP	SLRRP	Our Protocol
Support various RF protocol & compatibility	GEN 2 class 0/1 oriented	Support all RF protocol	Support all RF protocol
Tag inventory control	Read stage	All stage	All stage
Support TID	No	Yes	Yes
Support various communication channel	Yes	WLAN	Yes
Efficiency of managing certificate	Inefficient	Inefficient	Efficient
Satisfy security requirement	Partial	Partial	All

5 Concluding Remarks

Most of the previous research results of secure RFID system focus on the security and privacy between a RFID tag and a reader. However, the research on the security between a reader and a back-end server leaves much to be desired.

In this paper, we introduce typical reader protocol standards; EPCRP and SLRRP; and raise several problems, and then propose a secure RFID reader protocol which can be satisfied with the security requirements for the reader protocol based on SLRRP. The comparison shows that our protocol adopt the advantages of SLRRP with solving raised security problems.

To make our protocol concrete, the implementation and verification of the protocol after detail design will be needed. Furthermore, we will make strenuous efforts in order to positively adopt international standard such as EPCglobal, IETF, etc.

References

[1] EPCglobal, "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz Version 1.1.0 Draft 1".

[2] Ari Juels, Ronald Rivest, and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", *ACM CCS 2003*, October 2003.

[3] Ari Juels, "RFID Security and Privacy: A research Survey", *IEEE Journal on selected areas in communication Vol. 24, No. 2*, February 2006.

[4] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, "Security and privacy aspects of low-

cost radio frequency identification systems", *International Conference on Security in Pervasive Computing 2003*, March 2003.

[5] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "Cryptographic Approach to 'Privacy-Friendly' Tags", *RFID Privacy Workshop 2003*, November 2003.

[6] Dirk Henrici and Paul Müller, "Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers", *PerSec 2004*, March 2004.

[7] Su-Mi Lee, Young Ju Hwang, Dong Hoon Lee and Jong In Lim, "Efficient Authentication for Low-Cost RFID Systems", *International Conference on Computational Science and its Applications - ICCSA 2005, LNCS 3480, pp.619-627*, May 2005, Springer-Verlag, Singapore.

[8] Kirk Wong, Patrick Hui and Allan Chan, "Cryptography and Authentication on RFID Passive Tags for Apparel Products", *Computers in Industry, Elsevier Science, Article In press*, November 2006.

[9] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim, "Mutual authentication protocol for low-cost RFID", *Workshop on RFID and Lightweight Crypto, pp.17-24*, July 14 15, 2005, Graz, Austria.

[10] Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson, "Universal Re-Encryption for Mixnets", *CT-RSA 2004*, February 2004.

[11] Pim Tuyls and Lejla Batina, "RFID-Tags for Anti-Counterfeiting", *CT-RSA 2006*, February 2006.

[12] EPCglobal, "Reader Protocol(RP) Standard, Version 1.1", *http://www.epcglobalinc.org/standards*.

[13] IETF, "Simple Lightweight RFID Reader Protocol", *http://www.ietf.org/ietf/05mar/slrrp.txt*.

[14] IETF, "HTTP over TLS standard", *http://www.ietf.org/rfc/rfc2818.txt*.

[15] IETF, "Transport Layer Security standard", *http://www.ietf.org/rfc/rfc2246.txt*.

[16] EPCglobal, "EPCglobal Certificate Profile Standard, Ratified Specification 1.0", March 8 , 2006 , *http://www.epcglobalinc.org/standards*.

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