IEICE Electronics Express, Vol.8, No.2, 50–56

RFID tag search protocol preserving privacy of mobile reader holders

Ji Young Chun[1a)], **Jung Yeon Hwang**[2b)], **and Dong Hoon Lee**[1c)]

[1] *Graduate School of Information Management & Security, CIST, Korea University, 1, 5-Ka, Anam-dong Sungbuk-ku, Seoul, 136-701, Korea*

[2] *Electronics and Telecommunications Research Institute (ETRI), 161 Gajeong-dong, Yuseong-Gu, Daejeon, 305-700, Korea*

a) *jychun@korea.ac.kr*

b) *videmot@etri.re.kr*

c) *donghlee@korea.ac.kr*

Abstract: RFID tag search system which is used to find specific tags has many applications such as inventory management, supply chain, and search for books in the library. Recently, secure serverless search protocols using mobile readers are proposed in the environment where a persistent connection between mobile readers and a backend server cannot be guaranteed. However, the protocols are insecure against replay attacks and breach the privacy of mobile reader holders. In this paper, we point out the vulnerabilities of the previous protocols and propose an RFID tag search protocol which protects the privacy of mobile reader holders. Our protocol is secure against all known major attacks in RFID systems.

Keywords: RFID, privacy, security, serverless search, passive tag

Classification: Science and engineering for electronics

References

[1] C. Tan, B. Sheng, and Q. Li, "Secure and Serverless RFID Authentication and Search Protocols," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1400–1407, April 2008.

[2] S. I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, and T. Nakajima, "S3PR : Secure Serverless Search Protocols for RFID," *Proc. 2nd International Conference on Information Security and Assurance (ISA)*, Busan, Korea, pp. 187–192, April 2008.

[3] S. I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, and T. Nakajima, "Secure and Efficient Tag Searching in RFID Systems using Serverless Search Protocol," *Int. J. Security and Its Applications*, vol. 2, no. 4, pp. 57–66, Oct. 2008.

[4] T. Y. Won, J. Y. Chun, and D. H. Lee, "Strong Authentication Protocol for Secure RFID Tag Search Without Help of Central Database," *Proc. 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*, Shanghai, China, vol. 2, pp. 153–158, Dec. 2008.

[5] Md. E. Hoque, F. Rahman, S. I. Ahamed, and J. H. Park, "Enhancing Privacy and Security of RFID System with Serverless Authentication and

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011

Search Protocols in Pervasive Environments," *Wireless Personal Communications*, vol. 55, no. 1, pp. 65–79, July 2009.
[6] *Radio Frequency Identification (RFID): A Focus on Information Security and Privacy*, OECD Working Party on Information Security and Privacy, DSTI/ICCP/REG(2007)9/FINAL, p. 70, Jan. 2008.
[7] S. Vaudenay, "On Privacy Models for RFID," *Advances in Cryptology - ASIACRYPT*, Sarawak, Malaysia, LNCS 4833, pp. 68–87, March 2007.
[8] M. Feldhofer and J. Wolkerstorfer, "Strong crypto for RFID tags-A comparison of low-power hardware implementations," *Proc. 2007 IEEE International Symposium on Circuits and Systems (ISCAS)*, New Orleans, USA, pp. 1839–1842, May 2007.

1 Introduction

Radio frequency identification (RFID) technology which is used to identify RFID tags automatically has been applied to many real-life applications. One of the practical applications of RFID technology is RFID tag search system which can be used to find a particular tag among numerous tags. However, there are lots of security and privacy concerns about RFID technology, such as leakage of sensitive information and illegal tracking.

To treat the security and privacy concerns in RFID tag search system, secure serverless search protocols were proposed in [5]. These protocols enable users with mobile readers to search specific tags even though the mobile readers cannot connect to a backend server. The protocols also provide the robustness against the losses of mobile readers. Since mobile readers can be easily lost or stolen, the losses of mobile readers lead to leakage of sensitive information such as identifiers or secret keys of tags. After the protocols, various search protocols [2, 3, 4, 5] have been proposed to meet its own security and privacy requirements.

However, most security and privacy requirements are considered only for static readers. In RFID tag search system, since mobile readers are commonly used to find a specific tag, there need additional requirements for mobile readers such as the privacy of mobile reader holders. In fact, these privacy requirements for mobile readers have been overlooked so far.

In this paper, we propose an RFID tag search protocol which preserves the privacy of mobile reader holders. In Section 2, we analyze the requirements for mobile readers in RFID tag search system, and point out the vulnerabilities of the previous protocols based on the analyzed requirements in Section 3. In Section 4, we propose and analyze our protocol. Finally, we conclude the paper in Section 5.

2 Security & privacy requirements for mobile readers

There are five attacks to be considered in serverless search protocols, such as tracking, cloning, eavesdropping, physical, and DoS attacks (for the details, please refer to [1]). Besides security and privacy requirements in serverless

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011

search protocols, we should consider the privacy of mobile reader holders. Since users commonly handle mobile readers while RFID-tagged objects are attached to goods or products in RFID tag search system. Moreover, the signal strength of a reader is much stronger than that of a tag. The signal strength of a reader is $100\,m$, while the signal strength of a tag is $3\,m$ [6]. Therefore, a message from a reader can be more easily eavesdropped than a message from a tag.

The other privacy requirement to be considered is the search result of a mobile reader. It is undesirable to reveal the search result of a mobile reader. In some circumstances to an adversary, it might be useful information whether a mobile reader holder found a particular tag or not. An adversary could gather information about tags as in the authentication protocols [7].

3 Analysis of serverless search protocols

One of serverless search protocols [1] is described in Table I. ($\mathcal{H}(\cdot)$ and $\mathcal{F}(\cdot,\cdot)$ are cryptographic hash functions such as SHA-1. And RD_j and ID_i are identifiers of a reader R_j and a tag T_i, respectively.) To find a tag T_i, a mobile reader R_j uses a secret value $\mathcal{F}(\mathsf{RD}_j, t_i)$ which is received from a backend server. Mobile reader sends a message $\mathcal{H}(\mathcal{F}(\mathsf{RD}_j, t_i)\|n_r) \oplus \mathsf{ID}_i \| n_r \| \mathsf{RD}_j$. If T_i exists near R_j, then T_i sends a message $\mathcal{H}(\mathcal{F}(\mathsf{RD}_j, t_i)||n_t) \oplus \mathsf{ID}_i \| n_t$ where t_i is a secret key of T_i. The other tags send random numbers with the predefined probability.

Table I. The Serverless Search Protocol in [5]

Reader R_j		Tag T^*
$\alpha = \mathcal{H}(\mathcal{F}(\mathsf{RD}_j, t_i)\|n_r) \oplus \mathsf{ID}_i$		
$\beta = \alpha \| n_r \| \mathsf{RD}_j$	$\xrightarrow{\beta}$	If $\mathsf{ID}_i^* = \mathcal{H}(\mathcal{F}(\mathsf{RD}_j, t_i^*)\|\|n_r) \oplus \alpha$
		$\gamma = \mathcal{H}(\mathcal{F}(\mathsf{RD}_j, t_i^*)\|\|n_t^*) \oplus \mathsf{ID}_i^*$
	$\xleftarrow{\delta}$	then sends $\delta = \gamma \| n_t^*$
		else chooses random number $rand$
	$\xleftarrow{\delta}$	then sends $\delta = rand \| n_t^*$
Verify γ		with the predefined probability

However, this protocol seriously breaches the privacy of mobile reader holders. In the protocol, since a mobile reader R_j always sends its own identifier RD_j, an adversary can trace the movements of a mobile reader holder. Similarly the search protocols [2, 3, 5] are vulnerable to tracking attacks.

Additionally, the protocol is insecure against replay attacks. In the response message of tag T_i, $\mathcal{H}(\mathcal{F}(\mathsf{RD}_j, t_i)||n_t) \oplus \mathsf{ID}_i$, the random value n_r from R_j is not used. Therefore, an adversary can replay this eavesdropped message after this session. Later, when R_j wants to find T_i, if an adversary replays this eavesdropped message she can pass the authentication.

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011

4 Proposed RFID tag search protocol

In this section, we propose RFID tag search protocol which preserves the privacy of mobile reader holders. Our protocol satisfies the requirements for mobile readers in Section 2 and for serverless search protocols.

4.1 Our protocol

Our protocol uses a symmetric encryption algorithm $\mathsf{SE} = (\mathcal{E}, \mathcal{D})$, where λ denotes the bit length of a plaintext and a ciphertext, and ℓ denotes that of a key. A symmetric encryption algorithm SE consists of two algorithms, an encryption algorithm $\mathcal{E}$ and a decryption algorithm $\mathcal{D}$ associated to a key space $\mathcal{K}_D = \{0,1\}^\ell$ for a positive integer. We can use an efficient symmetric encryption algorithm AES-128 [8] which is designed for RFID passive tags:

- $\chi \leftarrow \mathcal{E}_t(m)$. A deterministic polynomial-time algorithm that takes as input a symmetric key $t \in \mathcal{K}_D$ and a message $m \in \{0,1\}^\lambda$, outputs a ciphertext $\chi \in \{0,1\}^\lambda$.

- $m \leftarrow \mathcal{D}_t(\chi)$. A deterministic polynomial-time algorithm that takes as input a private key t and a ciphertext χ, outputs a plaintext m.

The overall protocol is divided into two phases, an initial setup and a tag search. In the initial setup phase, from a backend server, each reader receives an access list of which each entry is encrypted with the identifiers of the reader and a tag. Then, in the tag search phase, the reader searches a specific tag using this list.

We denote by RD_j and ID_i the identifier of a mobile reader R_j and an RFID tag T_i, respectively. Also t_i denotes a secret encryption key of the RFID tag T_i. Assume that the bit-length of the identifiers is λ.

Table II. Access List L_j for a Mobile Reader R_j

ID	PW
ID_1	$\mathcal{E}_{t_1}(\mathsf{RD}_j \oplus \mathsf{ID}_1)$
$\cdots$	$\cdots$
ID_n	$\mathcal{E}_{t_n}(\mathsf{RD}_j \oplus \mathsf{ID}_n)$

Initial Setup Phase. The phase consists of two parts. The first part is performed to generate information for an RFID tag and the second for a mobile reader.

- For each RFID tag T_i, the backend server generates a tag identifier ID_i and a secret encryption key t_i and then stores the pair (ID_i, t_i) with the additional tag information into its own central database. Each tag T_i stores the pair (ID_i, t_i).

- For a mobile reader R_j, the backend server generates an access list L_j as follows: If the mobile reader R_j is assumed to access to the tags T_i $(1 \leq$

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011

$i \leq n$), the backend server computes each ciphertext $\mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i)$ for $i = 1, ..., n$ by encrypting $\mathsf{RD}_j \oplus \mathsf{ID}_i$ with the secret key t_i under the given encryption algorithm $\mathcal{E}$. Then the backend server adds the pairs $(\mathsf{ID}_i, \mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i))$ $(1 \leq i \leq n)$ in the access list L_j. (See Table II.) The backend server transmits this access list L_j to the mobile reader R_j over a secure channel.

Note that the mobile reader R_j cannot know the secret key t_i of a tag T_i from $\mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i)$ if the given encryption algorithm such as AES-128 is secure against the chosen plaintext attack.

Tag Search Phase. The whole protocol is illustrated in Table III. The protocol is performed as follows:

Table III. Our Protocol

Reader R_j		Tag T^*
$\alpha = \mathcal{E}_{\mathsf{ID}_i}(\mathsf{RD}_j \oplus n_r)$	$\xrightarrow{\alpha \| n_r}$	$\beta = \mathcal{D}_{\mathsf{ID}_i^*}(\alpha)$
		$= \mathcal{D}_{\mathsf{ID}_i^*}(\mathcal{E}_{\mathsf{ID}_i}(\mathsf{RD}_j \oplus n_r))$
		$\mathsf{RD}'_j = \beta \oplus n_r$
		$K_i^* = \mathcal{E}_{t_i^*}(\mathsf{RD}'_j \oplus \mathsf{ID}_i^*) \oplus n_r$
$K_i = \mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i) \oplus n_r$	$\xleftarrow{\gamma \| n_t^*}$	$\gamma = \mathcal{E}_{K_i^*}(\mathsf{ID}_i^* \oplus n_t^*)$
$\delta = \mathcal{D}_{K_i}(\gamma)$		
$= \mathcal{D}_{K_i}(\mathcal{E}_{K_i^*}(\mathsf{ID}_i^* \oplus n_t^*))$		
$\mathsf{ID}'_i = \delta \oplus n_t^*$		
Check if $\mathsf{ID}_i = \mathsf{ID}'_i$		

1. $R_j \rightarrow T^* : \mathcal{E}_{\mathsf{ID}_i}(\mathsf{RD}_j \oplus n_r) \| n_r$
When R_j wants to search T_i, R_j first chooses a λ-bit random number n_r and computes $\alpha = \mathcal{E}_{\mathsf{ID}_i}(\mathsf{RD}_j \oplus n_r)$, then broadcasts $\alpha \| n_r$.

2. $T^* : \beta = \mathcal{D}_{\mathsf{ID}_i^*}(\alpha) = \mathcal{D}_{\mathsf{ID}_i^*}(\mathcal{E}_{\mathsf{ID}_i}(\mathsf{RD}_j \oplus n_r))$
Each tag who receives a message α decrypts the message using its own identifier ID_i^*, and then obtains $\mathcal{D}_{\mathsf{ID}_i^*}(\alpha) = \mathcal{D}_{\mathsf{ID}_i^*}(\mathcal{E}_{\mathsf{ID}_i}(\mathsf{RD}_j \oplus n_r))$. Let $\beta = \mathcal{D}_{\mathsf{ID}_i^*}(\alpha)$ and $\mathsf{RD}'_j = \beta \oplus n_r$.

3. $T^* : K_i^* = \mathcal{E}_{t_i^*}(\mathsf{RD}'_j \oplus \mathsf{ID}_i^*) \oplus n_r$
Each tag computes $K_i^* = \mathcal{E}_{t_i^*}(\mathsf{RD}'_j \oplus \mathsf{ID}_i^*) \oplus n_r = \mathcal{E}_{t_i^*}(\beta \oplus n_r \oplus \mathsf{ID}_i^*) \oplus n_r$ with its own secret key t_i^*.

4. $R_j \leftarrow T^* : \mathcal{E}_{K_i^*}(\mathsf{ID}_i^* \oplus n_t^*) \| n_t^*$
Each tag chooses a λ-bit random number n_t^* and computes $\gamma = \mathcal{E}_{K_i^*}(\mathsf{ID}_i^* \oplus n_t^*)$, then sends $\gamma \| n_t^*$ to R_j. Note that all tags nearby R_j respond to the request of R_j, but the only tag T_i which R_j wants to find can send the correct response.

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011

5. R_j : $K_i = \mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i) \oplus n_r$
R_j computes $K_i = \mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i) \oplus n_r$ using the random number n_r chosen before and the stored value $\mathcal{E}_{t_i}(\mathsf{RD}_j \oplus \mathsf{ID}_i)$ in the access list L_j.

6. R_j : $\delta = \mathcal{D}_{K_i}(\gamma) = \mathcal{D}_{K_i}(\mathcal{E}_{K_i^*}(\mathsf{ID}_i^* \oplus n_t^*))$
R_j decrypts each of the previous values using K_i and then obtains $\mathcal{D}_{K_i}(\gamma) = \mathcal{D}_{K_i}(\mathcal{E}_{K_i^*}(\mathsf{ID}_i^* \oplus n_t^*))$. Let $\delta = \mathcal{D}_{K_i}(\gamma)$ and $\mathsf{ID}_i' = \delta \oplus n_t^*$.

7. R_j : Check if $\mathsf{ID}_i = \mathsf{ID}_i'$
R_j finally checks whether $\mathsf{ID}_i = \mathsf{ID}_i'$ or not. If $\mathsf{ID}_i = \mathsf{ID}_i'$ then R_j knows that T_i exists nearby R_j.

4.2 Analysis

Our protocol preserves the privacy of mobile reader holders.

- Each message from a mobile reader is changed in every session, since a mobile reader uses a fresh random value n_r in each session. Hence, an adversary cannot trace the movements of a mobile reader holder. Our protocol protects the search result of a mobile reader. In our protocol, since all tags T^* nearby a mobile reader R_j respond to the request of R_j, an adversary cannot learn whether R_j found a specific tag or not. Note that in our protocol even a particular tag T_i itself cannot know whether R_j wants to find him or not. Since T_i does not know the identifier RD_j of R_j, T_i cannot decide whether the identifier RD_j' which is extracted from the broadcasted message α is correct or not. In RFID tag search protocol, if only a specific tag which a mobile reader wants to find responds to the request of a reader as the protocols in [2, 3, 4, 5], the search result of a mobile reader cannot be protected.

Our protocol is also secure against tracking, cloning, eavesdropping, physical, and DoS attacks.

- A message for a tag is changed in every session because of a random value n_t, hence a tag holder cannot be traced. Cloning attacks in [1] is that an adversary can create a fake tag using an obtained response of a legitimate tag. However, our protocol uses a fresh random value in every session, using this fake tag, an adversary cannot pass the authentication. Since our protocol uses a symmetric encryption algorithm SE, an adversary cannot extract any meaningful information from an eavesdropped message. If an adversary can mount physical attacks on a mobile reader, an adversary can get all the stored information in a compromised reader. However, since an access list L_j stored in R_j has encrypted data like $\mathcal{E}_{t_1}(\mathsf{RD}_j \oplus \mathsf{ID}_1)$, an adversary cannot know secret keys of tags. Therefore, our protocol is secure against physical attacks. Even if a backend server is disabled due to DoS attacks, a mobile reader can search a specific tag without the help of a backend server. This can be possible because of the access list stored in each mobile reader.

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011

5 Conclusion

In this paper we analyzed the security and privacy requirements for mobile readers, and then pointed out the vulnerabilities of previous serverless search protocols. Based on the analyzed requirements, we propose RFID tag search protocol which satisfies the requirements for mobile readers and for serverless search protocols. Our future work is to design RFID tag search protocol which satisfies a forward secrecy.

Acknowledgments

This work was partly supported by the IT R&D program of MKE/KEIT [KI002113, Development of Security Technology for Car-Healthcare] and the IT R&D program of MKE/KEIT [KI001917, Development of Anonymity-based u-knowledge Security Technology].

DOI: 10.1587/elex.8.50
Received October 19, 2010
Accepted December 21, 2010
Published January 25, 2011