Cryptanalysis of an RFID Tag Search Protocol Preserving Privacy of Mobile Reader

Eun-Jun Yoon

Cryptanalysis of an RFID Tag Search Protocol Preserving Privacy of Mobile Reader

Eun-Jun Yoon*

Department of Cyber Security, Kyungil University,
33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea
ejyoon@kiu.ac.kr

Abstract. RFID tag search system can be used to find a particular tag among numerous tags. In 2011, Chun et al. proposed an RFID tag search protocol preserving privacy of mobile reader holders. Chun et al. claimed that their proposed protocol can withstand five attacks to be considered in serverless search protocols, such as tracking, cloning, eavesdropping, physical, and Denial of Service (DoS) attacks. However, this paper points out that the Chun et al.'s protocol still can be vulnerable to the DoS attack.

Keywords: RFID, Privacy, DoS attack, Serverless search, Passive tag.

1 Introduction

Recently, Radio frequency identification (RFID) technology has been applied to many real-life applications [1]. Basically, RFID technology is used to identify RFID tags automatically. RFID tag search system can be used to find a particular tag among numerous tags [2,3]. RFID tag search system has many applications such as inventory management, supply chain, and search for books in the library. In 2009, Tan et al. [4] proposed secure serverless search protocols to treat the security and privacy concerns in RFID tag search system. Tan et al.'s protocols enable users with mobile readers to search specific tags even though the mobile readers cannot connect to a backend server. Tan et al.'s 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. Various RFID tag search protocols [5–9] have been proposed to meet security and privacy requirements based on Tan et al.'s protocols.

In 2011, Chun et al.[9] proposed a new RFID tag search protocol which can preserve privacy of mobile reader holders unlike related protocols. In the security analysis, Chun et al. claimed that their proposed protocol can withstand five attacks to be considered in serverless search protocols, such as tracking, cloning, eavesdropping,

* Corresponding author: Eun-Jun Yoon(ejyoon@kiu.ac.kr) Tel.: +82-53-850-7291; Fax: +82-53-850-7609

physical, and Denial of Service (DoS) attacks. However, this paper points out that the Chun et al.'s protocol still can be vulnerable to the DoS attack.

The paper is organized as follows. Section 2 reviews the Chun et al.'s RFID tag search protocol and then shows its weakness in Section 3. Finally, Section 4 concludes the paper.

2 Review of Chun et al.'s RFID Tag Search Protocol

The Chun et al.'s RFID tag search protocol is composed of two phases, which are 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. Some of the notations used in the Chun et al.'s protocol are defined as follows:

- R_j, T_i : Mobile RFID reader and tag, respectively.
- RD_j, ID_i : Identity of R_j and T_i, respectively.
- $SE = (E, D)$: Efficient symmetric encryption algorithm, e.g. AES-128.
- t_i : Secret encryption key of the RFID tag T_i
- λ : Bit length of a plaintext and a ciphertext.
- $x \leftarrow E_t(m)$: A deterministic polynomial-time algorithm that takes as input a symmetric key $t \in \kappa_D$ and a message $m \in \{0,1\}^{\lambda}$, outputs a ciphertext $x \in \{0,1\}^{\lambda}$.
- $m \leftarrow D_t(x)$: A deterministic polynomial-time algorithm that takes as input a private key t and a ciphertext x, outputs a plaintext m.
- $\oplus$: Bit-wise exclusive-OR (XOR) operation.

2.1 Initial Setup Phase

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

S.1 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).

S.2 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 $T_i (1 \le i \le n)$, the backend server computes each ciphertext $E_{t_i}(RD_j \oplus ID_i)$ for $i = 1,...,n$ by encrypting $RD_j \oplus ID_i$ with the secret key t_i under the given encryption algorithm $E()$. Then, the backend server adds the pairs $(ID_i, E_{t_i}(RD_j \oplus ID_i))$ $(1 \le i \le n)$ in the access list L_j. The backend server also transmits the access list L_j to the mobile reader R_j over a secure channel.

Table 1. Access list L_j for a mobile reader R_j.

ID	PW
ID_1	$E_{t_i}(RD_j \oplus ID_1)$
ID_2	$E_{t_i}(RD_j \oplus ID_2)$
…	…
ID_n	$E_{t_i}(RD_j \oplus ID_n)$

2.2 Tag Search Phase

The Chun et al.'s tag search protocol is illustrated in Fig. 1 and is performed as follows:

T.1 $R_j \to T_i: \ \alpha \| n_r$

When R_j wants to search T_i, R_j first chooses a λ-bit random number n_r and computes $\alpha = E_{ID_i}(RD_j \oplus n_r)$, then broadcasts $\alpha \| n_r$ to T_i.

T.2 $T_i \to R_j: \ \beta \| n_t$

Each tag T_i who receives a message $\alpha \| n_r$ obtains RD_j by computing $D_{ID_i}(\alpha) \oplus n_r = D_{ID_i}(E_{ID_i}(RD_j \oplus n_r)) \oplus n_r$ using its own identifier ID_i and n_r. Then, each tag T_i computes $K_i = E_{t_i}(RD_j \oplus ID_i) \oplus n_r$ with its own secret key t_i. Finally, each tag T_i chooses a λ-bit random number n_t and computes $\beta = E_{K_i}(ID_i \oplus n_t)$, then sends $\beta \| n_t$ to R_j.

T.3 R_j computes $K_i = E_{t_i}(RD_j \oplus ID_i) \oplus n_r$ using the random number n_r chosen before and the stored value $E_{t_i}(RD_j \oplus ID_i)$ in the access list L_j. Then, R_j obtains ID_i' by computing $D_{K_i}(\beta) \oplus n_t = D_{K_i}(E_{K_i}(ID_i \oplus n_t)) \oplus n_t$ using K_i

and n_t. Finally, R_j checks whether $ID_i' \,?= ID_i$ or not. If $ID_i' == ID_i$ then R_j knows that T_i exists nearby R_j.

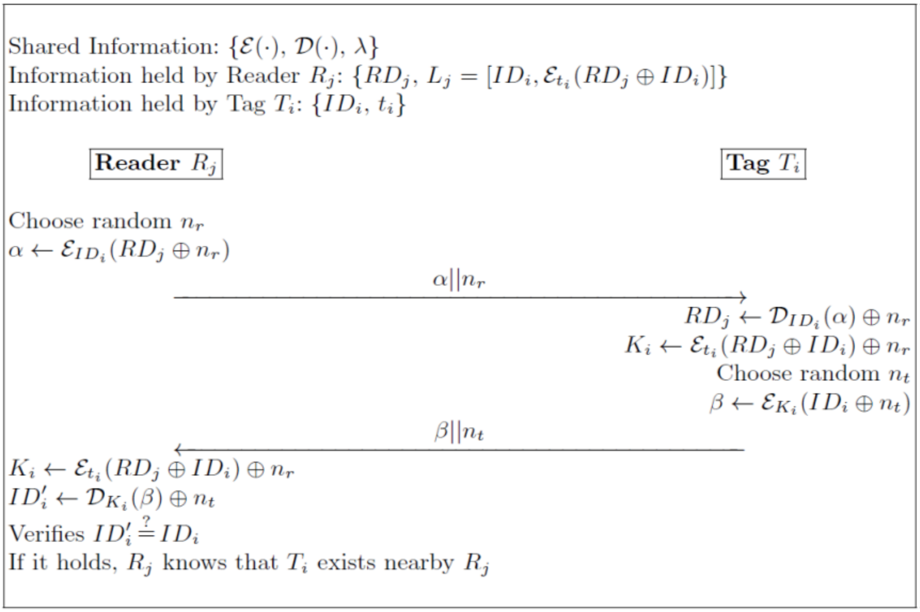

Fig. 1. Chun et al.'s RFID tag search protocol

3 Denial of Service Attack against Chun et al.'s Protocol

The Chun et al.'s RFID tag search protocol is vulnerable to Denial of Service (DoS) attack. DoS attack is one category of attacks on RFID systems. An adversary tries to find ways to fail target tag from receiving services. Almost all resources in an RFID system can become target of the DoS attack, including tag, reader, or backend server. Attacks on the air interface include shielding tags, flooding the reader field with a multitude of tags or selectively jamming the reader field. The goal is usually to sabotage specific resources of an RFID system, such a digital supply chain, effectively making the system unavailable to its intended users.

In the tag search phase, all tags T_i nearby a mobile reader R_j must respond to the request of R_j. Especially, in Step T.2 of the Chun et al.'s RFID tag search phase, all tags T_i always must compute 3 times symmetric encryption operations to respond the request of R_j. These computations can be vulnerable to the following an adversary Adv's DoS attack which is illustrated in Fig. 2.

A.1 $Adv \rightarrow T_i : \alpha \| n_r$

Suppose that an adversary Adv intercepts $\alpha \| n_r$ from Step T.1. Adv broadcasts $\alpha \| n_r$ to T_i.

A.2 $T_i \rightarrow Adv : \beta \| n_t$

All tags T_i nearby Adv will respond to the request of Adv as follows:
Each tag T_i who receives a message $\alpha \| n_r$ will obtain RD_j by computing $D_{ID_i}(\alpha) \oplus n_r = D_{ID_i}(E_{ID_i}(RD_j \oplus n_r)) \oplus n_r$ using its own identifier ID_i and n_r. Then, each tag T_i will compute $K_i = E_{t_i}(RD_j \oplus ID_i) \oplus n_r$ with its own secret key t_i. Finally, each tag T_i will choose a λ-bit random number n_t and compute $\beta = E_{K_i}(ID_i \oplus n_t)$, then send $\beta \| n_t$ to Adv.

A.3 Adv drops $\beta \| n_t$ and then broadcasts $\alpha \| n_r$ to T_i continuously until success DoS attack.

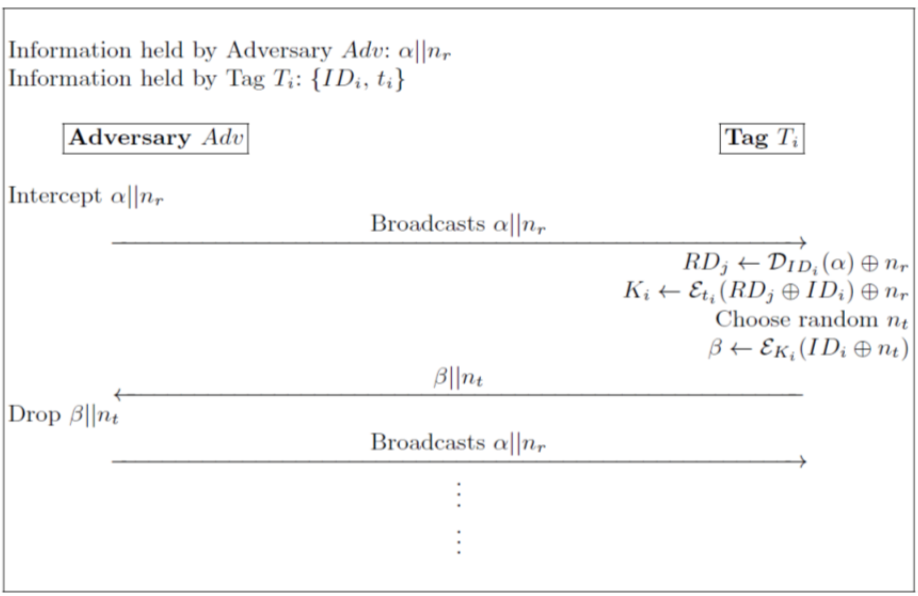

Fig. 2. DoS Attack against Chun et al.'s Protocol

From the computation results of above Step A.2, we can see that all tags T_i automatically must compute 3 times symmetric encryption operations to respond the request of Adv. These 3 times symmetric encryption operations of the RFID passive tag T_i can be quite expensive operations because T_i uses a low-power microcontroller for sensing and communication with the RFID reader R_j.

Therefore, if Adv broadcasts the intercepted $\alpha \| n_r$ continuously, all tags T_i cannot respond to the request of the legitimate leaders. Moreover, Adv can simply perform the above described DoS attack by choosing a random $\alpha^* \| n_r^*$ without intercepting the R_j's sending message $\alpha \| n_r$.

As a result, the Chun et al.'s RFID tag search protocol is vulnerable to the above described DoS attacks.

4 Conclusions

This paper analyzed the security of Chun et al.'s RFID tag search protocol preserving privacy of mobile reader holders. We presented a denial of service (DoS) attack against this protocol. Further works will be focused on improving the protocol which can not only withstand the DoS attack but also provide more computational efficiency.

Acknowledgments. We would like to thank the anonymous reviewers for their helpful comments in improving our manuscript. 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(No. 2010-0010106). This study was also supported by the Intramural Research Support Program funded by the Kyungil University in 2012.

References

1. Radio Frequency Identification(RFID).: A focus on information security and privacy. OECDWorking Party on Information Security and Privacy, DSTI/ICCP/REG(2007)9/FINAL, 2008, 70.
2. S. Vaudenay. On privacy models for RFID.: Advances in Cryptology-ASIACRYPT, LNCS 4833, 2007, 68–87.
3. 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), 2007, 1839–1842.
4. C. Tan, B. Sheng, Q. Li.: Secure and serverless RFID authentication and search protocols. IEEE Trans. Wireless Commun., 2008, 7(4), 1400–1407.
5. S.I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, T. Nakajima.: 3PR : secure server-less search protocols for RFID. Proc. 2nd International Conference on Information Security and Assurance (ISA). 2008, 187–192.
6. S.I. Ahamed, F. Rahman, E. Hoque, F. Kawsar, T. Nakajima.: Secure and efficient tag searching in RFID systems using serverless search protocol. Int. J. Security and Its Applications, 2008, 2(4), 57–66.

7. T.Y. Won, J.Y. Chun, 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), 2008, 153–158.
8. Md.E. Hoque, F. Rahman, S.I. Ahamed, J.H. Park.: Enhancing privacy and security of RFID system with serverless authentication and search protocols in pervasive environments. Wireless Personal Communications. 2009, 55(1), 65–79.
9. L.J. Chun, J.Y. Hwang, D.H. Lee.: RFID tag search protocol preserving privacy of mobile reader holders. IEICE Electronics Express, 2011, 8(2), 50–56.