Title	Design and Analysis for RFID Authentication Protocol
Author(s)	Zheng, Z; Zhou, S; Luo, Z
Citation	IEEE International Conference on e-Business Engineering, Xi'an, China, 22-24 October 2008, p. 574 - 577
Issued Date	2008
URL	http://hdl.handle.net/10722/223750
Rights	2008 IEEE International Conference on e-Business Engineering. Copyright © IEEE.; ©20xx IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.; This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Design and Analysis for RFID Authentication Protocol

Zhen Zhang[1], Shijie Zhou[1],
[1]*SCSE, the University of Electronic Science and Technology of China,*
zhangzhenjua@163.com,sjzhou@uestc.edu.cn

Zongwei Luo[2]
[2]*ETI, the University of Hong Kong,*
zwluo@eti.hku.hk

Abstract

Radio frequency identification (RFID) technology has been widely used in ubiquitous infrastructures. On the other hand, the low-cost RFID system has potential risks such as privacy and security problems, which would be a big barrier for the application. First of all, we analyze the current security protocols for the RFID system. To protect user privacy and remove security vulnerabilities, we propose a robust and privacy preserving mutual authentication protocol that is suitable for the low-cost RFID environment. Finally, the correctness of the proposed authentication protocol is proved by the BAN logic.

1. Introduction

As an important technology, the secure problems of the RFID system attract a lot of attention. The low cost demanded for RFID tags forces them to be very resource limited. Thus the current Cryptographic algorithm can't be directly used on them. A robust authentication protocol plays a key role in the RFID system. Unfortunately, most of the existing proposed protocols have some problems. Therefore, we put forward a robust RFID protocol and give a comprehensive analysis of it.

The paper is organized as following: in section 2, the related protocols are introduced. Our approach is proposed in section 3. In section 4, we analyze our protocol in several aspects. Finally, we make the conclusion in section 5.

2. Related Work

In the HBVI protocol [6], the TID is increased in each successful authentication session which can resist replay attack. The protocol also resolves the location problem by making a tag's ID randomized in each interrogation. Unfortunately, this protocol can not resist man-in-the-middle attack. The attacker can query any tag before it is interrogated by the legitimate reader and he can be authenticated with the obtained data.

HB^{++}[3] relies on the computational hardness of Leaning Parity with Noise problem. It is also prone to the similar attack as Selwyn Piramuthu analyzed in[2]. This is a great problem that the protocol may possibly reveal the secrets to the adversary. On the other hand, the protocol is a unilateral authentication protocol.

LMAP [4] only uses the most basic operations such as bitwise XOR($\oplus$),bitwise OR($\vee$),bitwise AND($\wedge$) and addition of $mod2^m$(+). The random number is generated by the reader. Thus the cost is very low. But it also has some problems. As Li and Wang showed in

978-0-7695-3395-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ICEBE.2008.92

[1], this protocol is prone to be under two kinds of active attacks: De-synchronization Attack and Full Disclosure Attack.

3. Robust Protocol Design

3.1. Main Idea

Our protocol is based on the challenge - response mechanism. The contents of tags can be searched out by the server through index-pseudonym (IDS). The mutual authentication between tags and the server is fulfilled by sharing a secret key. In each round, the back-end server and the tag update the secret key, which ensures that the tag's response is random. In our protocol, all important messages are encrypted with the hash algorithm.

3.2. System Assumptions and Initialization

We assume that each tag shares a random secret key with the back-end server in the initiation. The secret keys are stored in the back-end database and can be indexed by the IDS. Tags only need to have a one-way hash function and the XOR ability. The reader and the server share a secret key ,*K*, and can carry out the keyed hash operation with the *K*. The records including the IDS, the key and the application-related information are managed by the back-end server. Besides, the reader is not regarded as the trusted third party (TTP). So it must be authenticated by the server.

3.3. Detailed Description

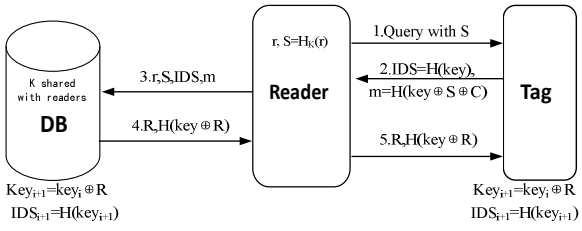

Figure 1**. Our protocol**

The process of our proposed protocol is shown as figure 1.

(1)Challenge: Firstly the reader generates a random number *r* and calculates $S = H_K(r)$.

(2)Respond: While receiving the challenge, the tag responds IDS, m=H(key ⊕ S ⊕ C) to the reader. The Chip unique serial number, C, is embedded in each tag.

(3)The reader forwards the certification information to the back-end server, including r, S, IDS and m.

(4)While receiving the authentication information from the reader, the back-end server firstly certifies the reader through judging whether the received S is equal to $H_K(r)$. If so, the server considers the reader is valid and retrieves the corresponding information of the tag, such as the secret key, IDS, C and so on, through the received IDS. Then the server calculates H(*key* ⊕ *S* ⊕ *C*) and compares it to the received m. If they are equal, a random number ,*R*, is generated by the back-end server, which is used for XORing with the old key to generate the new secret key $key' = key \oplus R$ and the new index IDS'=H(*key'*).

Here we have two problems must be solved, the uniqueness of the IDS and the anti-synchronization between the back-end server and the tags. A reasonable mechanism is designed to solve the first problem. We make the server testing the uniqueness of the H (*key'*). If the new index is not unique, the server renews R until H(*key'*) becomes unique. For the second problem, an anti-synchronous resistant mechanism is needed since the attacker may probably disturb the synchronization of the update between the server and the tag. If the attacker is successful, the valid tag can never be legally certified. We use the existing anti-synchronous resistant mechanism such as the mechanism described in [5] to solve this problem.

(5) While receiving the information from the reader, the tag retrieves the stored key and calculates H(*key* ⊕ *R*). If the output is equal to the received H(*key* ⊕ *R*), the tag considers that the reader is valid and carries out the update accordingly.

4. Analysis of Our Protocol

4.1. Logic Analysis

In this section, we will validate the correctness of the proposed protocol based on the BAN logic[7]. BAN logic is the most important tool to formalize the authentication protocols. The basis for the logic is the belief of a party in the truth of a formula. Although there are other validation logics, we have chosen BAN because its formal process is simple and robust.

Since the main entities of this authentication process are the back-end server and the tag, we idealize the entities in the protocol as B and T.

(1)Generic type of protocol

Message 1: B—>T： S

Message 2: T—>B: H（key）,H(key ⊕ S ⊕ C)

Message 3: B—>T： R, H（key ⊕ R）

(2)Idealized protocol

Message2: T—>B： $H(\ B \overset{key}{\leftrightarrow} T\ ), H((\ B \overset{key}{\leftrightarrow} T\ ),S,C)$

Message 3: B—>T：$H((B \overset{key}{\leftrightarrow} T),R)$

(3)Initial assumptions：Firstly, we can see the tag and the back-end server both believe their shared secret key and it's rational because this is the basic purpose of the protocol's design. Because the tag updates the secret key in each round, the key can be regarded as fresh.

The assumption for the effectiveness of the key:

(A1) $B|\equiv B \overset{key}{\leftrightarrow} T$, (A2) $T|\equiv B \overset{key}{\leftrightarrow} T$

The assumption for the fresh of the random number:

(A3) $B|\equiv \#(R)$ (A4) $B|\equiv \#(S)$ (A5) $T|\equiv \#(key)$

(4)The goal of the protocol ：

$B|\equiv T|\sim\#(\ B \overset{key}{\leftrightarrow} T)$, $T|\equiv B|\sim\#(B \overset{key}{\leftrightarrow} T)$

(5)Verification:

From the message 2, we can educe that:

$$B \lhd H((B \overset{key}{\leftrightarrow} T),S,C)$$

From the assumption A1,we can see： $B|\equiv B \overset{key}{\leftrightarrow} T$

According to the Interpretation Rule: $\frac{P|\equiv Q \overset{K}{\leftrightarrow} P, P \lhd <X>_Y}{P|\equiv Q|\sim X}$

We can deduce: $B|\equiv T|\sim H((B \overset{key}{\leftrightarrow} T),S,C)$

Because B can search out the key and the chip serial number C of the tag, we can educe that:

$$B \lhd C,\ B \lhd S,\ B \lhd (B \overset{key}{\leftrightarrow} T)$$

Applying the hash rule:

$$\frac{P|\equiv Q|\sim H(X1,X2.....Xn), P \lhd X1, P \lhd X2, ...P \lhd Xn}{P|\equiv Q|\sim(X1,X2,.....Xn)}$$

We can deduce that: $B|\equiv T|\sim(\ (B \overset{key}{\leftrightarrow} T),S,C)$

Applying the recognizability rule: $\frac{P|\equiv Q|\sim(X,Y)}{P|\equiv Q|\sim X}$

We can deduce that: $B|\equiv T|\sim(B \overset{key}{\leftrightarrow} T)$①

And from the assumption A4: $B|\equiv \#(S)$,

Applying freshness rule: $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$

We can deduce that: $B|\equiv \#(\ (B \overset{key}{\leftrightarrow} T),S,C)$②,

Applying ①and②: $B|\equiv T|\sim\#(\ B \overset{key}{\leftrightarrow} T)$

The first goal has been proved, now we will prove the second goal:

From the message 3, we can see: $T \lhd H(key, R)$

From the assumption A2: $T|\equiv B \overset{key}{\leftrightarrow} T$

According to the interpretation Rule: $\frac{P|\equiv Q \overset{K}{\leftrightarrow} P, P \lhd <X>_Y}{P|\equiv Q|\sim X}$,

We can deduce that: $T|\equiv B|\sim H((B \overset{key}{\leftrightarrow} T),R)$

Because the tag can see R: $T \lhd R$, $T \lhd\ B \overset{key}{\leftrightarrow} T$

Applying hash rule, we can deduce that:

$$T|\equiv B|\sim(B \overset{key}{\leftrightarrow} T,R)③$$

From the assumption A5: $T|\equiv \#(key)$

Applying the freshness rule: $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$

We can deduce that: $T|\equiv \#(\ B \overset{key}{\leftrightarrow} T,R)$④

According to ③and④:$T|\equiv B|\sim\#(\ B \overset{key}{\leftrightarrow} T,R)$

Applying the recognizability rule: $\frac{P|\equiv Q|\sim(X,Y)}{P|\equiv Q|\sim X}$

We can finally deduce that: $T|\equiv B|\sim\#(\ B \overset{key}{\leftrightarrow} T)$

So the second goal has been proved.

4.2. Theoretical evaluation

We evaluate the protocol by judging whether the protocol satisfies the security requirement:

(1)Data Confidentiality and Integrity: The important information is hidden by the hash function. In addition, we link C to the authentication information, so as to ensure the data integrity.

(2) Scalability: We use the IDS as an index to help the server to search out a tag's information, so the searching is efficient.

(3)Availability

Man-in-the-middle Attack Prevention：Our protocol is based on a mutual authentication, in which two random numbers R and r, refresh in each round of the protocol, are used. Moreover, we make the server validate the reader through the $S=H_K(r)$. Thus the adversary who wants to impersonate the valid reader can be detected.

Forgery Resistance：The chip serial number C is embedded into the tag and refers to the authentication information. Thereby the simple forgery of tag can't make any sense. In addition, the secrete information stored in each tag is pertinent to itself.

Replay Attack Prevention: Since the reader challenges the tag with the random information, the replay attack in step 2 can be prevented. Since the key and the m refresh in each round, the replay attack in step 3 and step 5 can be detected.

De-synchronization Resistance: we use the existing anti-synchronous resistant mechanism such as the mechanism in [5] to meet this requirement.

(4)Location Privacy: If the responses from the tag are constant, the location of the tag can be tracked. In our protocol, the response of the tag will be random in each protocol run. Hence the location privacy is guaranteed.

(5)Forward Security：Since the key updating is fulfilled whenever the authentication is successful, a future security compromise on an RFID tag will not reveal the data previously transmitted.

5. Conclusion

As we discuss, the proposed protocol is correct and suits for the low-cost environment. It can also ensure the privacy of the tag, meet most of the security requirements and resist the typical attacks. Several mechanisms are used to make the protocol more robust, such as the dynamic refresh mechanism, the anti-collision mechanism and challenge-response mechanism. The further work is to design a more robust anti-synchronous resistant mechanism to enhance our protocol.

References

[1] T. Li, G. Wang: Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. IFIP SEC 2007, 14-16 May, Sandton, Gauteng, South Africa, 2007

[2] Selwyn Piramuthu. HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication. Decision and Information Sciences University of Florida, Gainesville, Florida 32611-7169.,2007

[3] J. Bringer, H. Chabanne, and E. Dottax. \HB++: a Lightweight Authentication Protocol Secure Against Some Attacks," IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU, 2006.

[4] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda: LMAP: A Real Lightwight Mutual Authentication Protocol for Low-cost RFID tags. Proceedings of RFIDSec06 Workshop on RFID Security, 12-14 July, Graz,Austria, 2006

[5] Lee S. M., Hwang Y.J. , Lee D.H. , Lim J, I. . Efficient authentication for low-cost RFID systems. Proceeding of the International Conference on computational Science and Its Applications(ICCSA 2005). Lectures Notes in Computer Science 3408, BerkubLSpringer-Verlag,2005

[6] Henrici D, Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers. In : Proceedings of the 2 nd IEEE Annual Conference on Pervasive Computing and Communication Workshops, Washington, DC, USA,2004

[7] Michael Burrows, Martin Abadi, Roger Needham. A Logic of Authentication, DEC SRC Research Report 39. 1989