HMAC-based RFID Authentication Protocol with Minimal Retrieval at Server

Seung Wook Jung, Souhwan Jung
School of Electronic Engineering
Soongsil University
Seoul, Korea
seungwookj@ssu.ac.kr, souhwanj@ssu.ac.kr

Abstract—**This paper proposes a HMAC-based RFID mutual authentication protocol to improve performance at the back-end server. In existing hash-based protocols, the tag ID is a secret value for privacy, so the back-end server computes a lot of hash operations or modular operations to retrieve the tag ID. In our protocol, the Tag ID is used as a secret key of HMAC and sends the tag ID XOR-ed by a random number, where XOR-ed tag ID is stored at the back-end server and the tag. The XOR-ed tag ID is changed every session like OTP. The tag sends XORed ID to the back-end server for authentication. Thus, simple matching operation is required to retrieve the tag ID. Therefore, our protocol is much more practical than existing protocols.**

Keyword- RFID; HMAC; mutual authentication

I. INTRODUCTION

Radio Frequency Identification (RFID) is an automatically identifying mobile object called RFID tags through wireless radio. RFID system has three components: low-cost RFID tag, RFID reader, and back-end server. The RFID tag contains a unique identifier, and the RFID reader can obtain the unique identifier from the RFID tag through short-range wireless radio channel. The RFID reader sends the unique identifier to the back-end server in order to recognize information of the object attaching RFID tag [2] [3][7][9].

RFID has various advantages over traditional bar code [1][2]. However, it has various security risks including privacy violation [7], impersonate attack, and message blocking attack [4].

Recently, lightweight mutual authentication protocols [4][14][15] are studied. These protocols are suitable for passive tags. However, such lightweight mutual authentication protocols seem to be vulnerable to various attacks [15], because of not using cryptographic functions of which security are proven.

Another direction of researches for securing RFID is using cryptographically secure hash functions such as SHA-1[16]. S. Wang et al.[8], S-S. Yeo et al. [9], and J. Cho et al. [17] proposed Hash or a keyed-Hash Message Authentication Code (HMAC) based mutual authentication protocols in RFID system. However, these protocols have a disadvantage that the back-end server retrieves IDentifier(ID) with 2*n* hash operations in the worst case, where *n* is the number of tags that are registered to the back-end server. Recently, Cho et al. [17] reduces the cost of retrieving the ID, but still 2*n* modular arithmetic operations in the worst case are required at the back-end server.

This paper proposes a HMAC-based mutual authentication protocol with minimal retrieval cost at the back-end server for RFID system. The proposed protocol uses a tag ID as a secret key of HMAC and sends the tag ID eXclusive OR(XOR)-ed by a random number rather than sending a tag ID in plaintext, where XOR-ed tag ID is stored at the back-end server and the tag. Also, XOR-ed tag ID is changed every session like One-Time Pad (OTP) to provide privacy. The back-end server can retrieve the tag ID with simply comparing the XOR-ed tag ID in DB with received XOR-ed tag ID rather than computing 2*n* hash operations or modular arithmetic operations like [8][9][17] do. Moreover, the proposed protocol is strong against the message blocking attack, called also denial of service or desynchronization problem.

The remainder of this paper is organized as follows: In Section 2, various attacks are described. Section 3 describes the proposed protocol. Section 4 analyzes the security and performance of the proposed protocol. Finally, Section 5 concludes this paper.

II. SECURITY THREAT AND ATTACKS

Because the wireless communication channel between the tag and the reader is an insecure channel, RFID system is vulnerable to various attacks as following

A. Eavesdroppin

The communication channel between the tag and the reader can be eavesdropped, because the radio frequency channel is not secure communication channel [5][6]

B. User privacy

The attacker can monitor the tag using the tag identifier in order to know the user's behavior, when the user identity is linked to a certain tag. Also, the attacker can trace the user location with the tag identifier, when the output of the tag such as the tag identifier is unchangeable [7].

C. Blocking message attack

When an attacker blocks a message between the tag and the reader, the attack causes de-synchronization problem between the tag and the reader/the back-end server [4][8].

ISBN: 978-1-61208-285-1

D. *Replay attack*

The attacker obtains messages between the tag and the reader by eavesdropping and reuses the message in order to impersonate a legitimate tag or a legitimate reader.

E. *Spoofing attack*

The attacker can impersonate a reader, send a query to a tag and obtain the response of the tag. When the legitimate reader queries the tag, the attacker will send the obtained response to reader in order to impersonate the tag [8].

III. PROPOSED PROTOCOL

This paper proposes a HMAC-based mutual authentication protocol for RFID which is secure against various types of attacks that are described in the previous section. The proposed protocol is based on HMAC [1].

A. *Prior condition and Notation*

In the proposed protocol, a secure communication channel between the reader and the back-end server is established at the enrollment phase, while the communication channel between the tag and the reader is insecure at the authentication phase. The notations are depicted at Table 1.

TABLE I. NOTATION

Notation	Definition
HMAC	***Hash-based Message Authentication Code***
C_A	***A random number of a entity A***
ID_A	***Identity of an entity A***
T_A	***Timestamp from an entity A***

B. *Description of the proposed protocol*

The proposed mutual authentication protocol is based on HMAC having a tag ID (ID_t) as a secret key. The ID is shorter than the cryptographic key length which is required for ensuring required security level. Therefore, actually the tag ID is used as a seed of a random number generator of which an output is a cryptographic key. For convenience, in this paper, 'tag ID' means 'a secret key generated from a random number generator. The processes of proposed protocol are following and Fig. 1 shows authentication procedures.

Step 0: Enrollment phase

- The back-end server and the tag share HMAC function, the identifier of tag (ID_t), a secret key k, and a random number (C_0).
- The back-end server and the tag stores a tuple <ID_t, $ID_t \oplus C_0$> in his/her own database.

Step 1: Reader sends hello message with his/her ID (ID_r)

Step 2: Tag response

- A tag selects a random number (C_1).
- A tag sends $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, $\alpha = HMAC_{ID_t}$ (T_t, ID_r), ID_r and T_t, where T_t is a timestamp of the tag.

Step 3: Tag authentication

- Reader forwards $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, α, ID_r, and T_t to the back-end server
- The back-end server retrieves a tuple <ID_t, k, $ID_t \oplus C_0$> with $ID_t \oplus C_0$ and extracts ID_t.
- The back-end server computes C_1 ($=k \oplus C_0 \oplus C_1 \oplus k \oplus C_0$) and $\alpha' = HMAC_{ID_t}$ (T_t, ID_r).
- The back-end server checks whether α' = α.
- The back-end server computes $\beta = HMAC_{ID_t}$ (T_t +1, ID_r, C_1) and sends β to the reader.

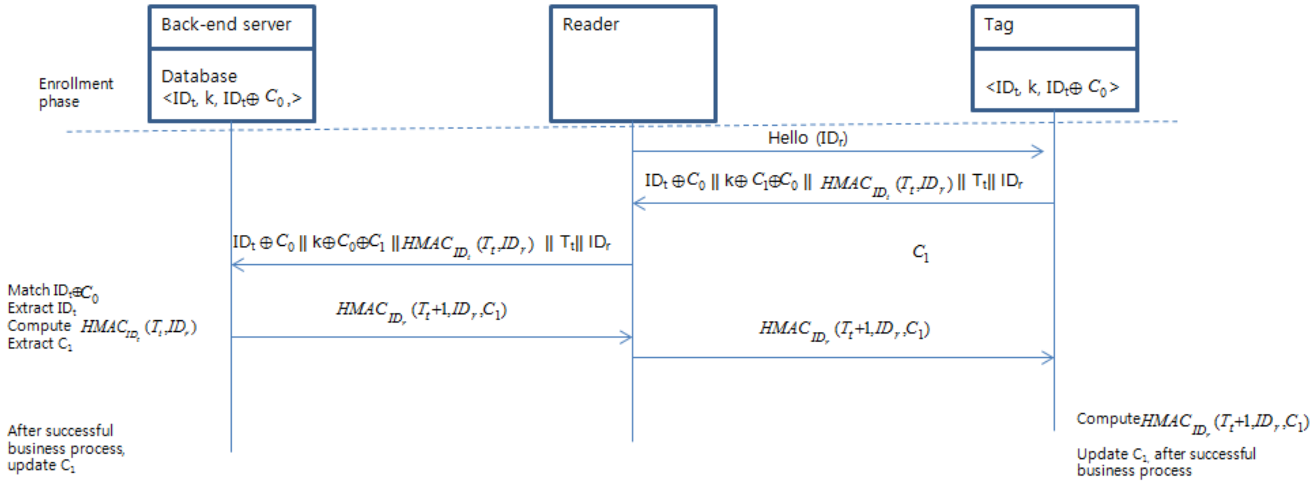
Back-end server
Database
<ID_t, k, $ID_t \oplus C_0$,>
Reader
Tag
<ID_t, k, $ID_t \oplus C_0$>
Enrollment phase
Hello (ID_r)
$ID_t \oplus C_0$ || $k \oplus C_1 \oplus C_0$ || $HMAC_{ID_t}(T_t, ID_r)$ || T_t|| ID_r
$ID_t \oplus C_0$ || $k \oplus C_0 \oplus C_1$ ||$HMAC_{ID_t}(T_t, ID_r)$ || T_t|| ID_r
C_1
Match $ID_t \oplus C_0$
Extract ID_t
Compute $HMAC_{ID_t}(T_t, ID_r)$
Extract C_1
$HMAC_{ID_t}(T_t+1, ID_r, C_1)$
$HMAC_{ID_t}(T_t+1, ID_r, C_1)$
After successful business process, update C_1
Compute $HMAC_{ID_t}(T_t+1, ID_r, C_1)$
Update C_1 after successful business process

Figure 1. The Proposed Protocol

ISBN: 978-1-61208-285-1

- The reader forwards β to the tag.

Step 3: back-end server authentication

- The tag computes β’ = $HMAC_{ID_t}$ (T_t +1, ID_r, C_1,) using his/her T_t, C_1, and received ID_r.

The tag checks β’ = β. If β’ = β, the back-end server is authenticated and actual business communication such sending the tag information will be started.

Step 3: update C_1

- After successful business communication such as sending Tag Information, the back-end server and the tag replace <ID_t, k, $ID_t \oplus C_0$> as <ID_t, k, $ID_t \oplus C_1$>, where $ID_t \oplus C_1$ will be used for next session. With successful the business communication, the back-end server and the tag know C_1 is properly transmitted.

IV. Security Analysis and Preformance Analysis

The attacks mentioned in Section 2 such as replay attack, privacy violation, and blocking message attack are common security threat that a RFID faces. This section analyzes the security of the proposed protocol.

A. Eavesdropping

Throughout the proposed protocol, ID_r, T_t, $ID_t \oplus C_0$, $C_0 \oplus C_1$, $HMAC_{ID_t}$ (T_t, ID_r), $HMAC_{ID_t}$ (ID_r, C_1, T_t +1) can be eavesdropping by an attacker. The attacker can try to use this information to obtain ID_t, C_0, and C_1. All these values are XORed and ID is also used as a secret key so the attacker cannot compute any of these values. Therefore, the proposed protocol is secure against eavesdropping.

B. User privacy

The tag identity ID_t is XORed by C_0 which is a random value and is known to only the tag, and the back-end server. Moreover, every session uses different C_i to encrypt ID_t and each C_i has no relationship with other C_{i+n} values, so the attacker cannot link $ID_t \oplus C_i$ of each session. Therefore, the attacker cannot track the tag.

C. Blocking message attack

The proposed protocol updates C_{i+1} at the session i for next session during the mutual authentication. After mutual authentication, the tag and the back-end server communicates business protocol such as sending the tag information. Therefore, the tag and the back-end server know that both are authenticated and updated C_{i+1}. Therefore, the blocking message attack is prevented.

D. Replay attack

Every session uses a fresh C_i and C_{i+1}, and uses a new timestamp. Therefore, the replay attack is impossible.

E. Spoofing attack

When the attacker who impersonates a legitimate reader queries the tag, the attacker can only get the public values ID_r, T_t, $ID_t \oplus C_0$, $C_0 \oplus C_1$, $HMAC_{ID_t}$ (T_t, ID_r). Therefore, the spoofing attack with reusing the values cannot be successful because of a timestamp and a fresh C_i, and C_{i+1}.

TABLE 2
Performance Evaluation (Worst Case)

Performance		Cho[9]	Wang[8]	Cho[17]	Our Protocol
Computation Cost	Tag	2*H*+2 *MOD*	2*H*	2*H*+4× *MOD*	2*H*
	BS	(2*n*+2) ×*H*	(*n*+1)×*H*	3*H*+ (6*n*+2)× *MOD*	2*H*
Communication Cost	T→BS	$1l+1l_H$	$1l+1l_H$	$1l+1l_H$	$3l+1l_H$
	BS→T	$1l+1l_H$	$1l_H$	$2l+2l_H$	$1l_H$

BS: Back-end Server,*n:*number of tags,
*H:*hash or Keyed Hash operation
l: the length of timestamp, challenge or random number,
l_H: the length of hash value
MOD: modular operation

F. Performance Analysis

The proposed protocol can effectively retrieve a tuple <ID_t, $ID_t \oplus C_i$ > with received $ID_t \oplus C_i$. The previous hash-based protocol computes 2*n* hash operations [8][9] or 2*n* modular arithmetic operations [17] in the worst case. Comparing with Wang’s protocol [8], Cho’s protocol l[9], and Cho’s protocol [17], the proposed protocol is very efficient to retrieve the tuple in DB.

The proposed protocol has to compute HMAC function two times at the tag and the back-end server. Which means the proposed protocol is more efficient than previous protocols [8][9][17].

Also, the proposed protocol requires $3l+2\ l_H$ during mutual authentication. When comparing the most efficient protocol [8] for communication cost, the proposed protocol requires 2*l* more communication cost. However, the proposed protocol solves retrieval problems at the back-end server and message blocking problem of [8].

V. Conclusion and Further Work

Existing lightweight mutual authentication protocols for RFID are vulnerable to various attacks because of not using cryptographic functions of which security are proven.

Existing hash-based mutual authentication protocols for RFID have a problem that should compute 2*n* hash operations in the worst case, where n is the number of tags enrolled at the back-end server. Most recent protocols also have to compute 2*n* modular operations in the worst case. It is not efficient.

This paper introduced a HMAC-based mutual authentication protocol with minimal retrieval cost at the back-end server for RFID system to solve all above problems: (1) the propose protocol is secure because of standard cryptographic function; (2) simple comparison for retrieving ID is required. Also, the proposed protocol is secure against eavesdropping, replay attack, and spoofing attack using HMAC and XOR. Moreover, the proposed protocol solves desynchronization problem with only two communication paths, while the previous protocols are suffered from the message blocking attack. The proposed protocol can be used for the active tags, which are more powerful than the passive tags.

The proposed protocol will be implemented for the active tag in hardware and we will experiment the feasibility for the real-world usages.

ACKNOWLEDGMENT

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2012-H301-12-4008) supervised by the NIPA(National IT Industry Promotion Agency)

REFERENCES

[1] H. Krawczyk, M. Bellare, and R. Canetti, “HMAC: Keyed-hashing for Message Authentication,” RFC 2104 IETF, Feb. 1997.

[2] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz–960 MHz Version 1.2.0, EPCglobal.

[3] S. Devadas, G. E. Suh, S. Praal, R. Sowell, T. Ziola, and V. Khandelwal, “Design and implementation of PUF-based unclonable RFID ICs for anti-counterfeiting and security applications”, Proceedings of the IEEE International Conference on RFID, Apr. 2008, pp. 58–64.

[4] R. Bassil, W. El-Beaino, W. Itanti, A. Kayssi, and A. Chehab, “PUMAP : PUF-based Ultra-Lightweight Mutual-Authentication RFID Protocol,” Internation Journal of RFID Security an Cryptography, vol. 1, Mar. 2012, pp. 58-66.

[5] X. Leng, K. Mayes, and K. Markantonakis, “HB-MP + protocol: an improvement on the HB-MP protocol,” IEEE International Conference on RFID, Apr. 2008, pp. 118–124.

[6] Y.-C. Lee, Y.-C. Hsieh, P.-S. You, and T.-C. Chen, “An improvement on RFID authentication protocol with privacy protection,” Third International Conference on Convergence and Hybrid Information Technology – ICCIT 2008, vol. 2, Nov. 2008, pp. 569–573.

[7] A. Juels, “RFID security and privacy: a research survey,” IEEE Journal on Selected Areas in Communications, vol. 24, No. 2, Feb. 2006, pp. 381-394.

[8] S. Wang, Q-m, Ma, Y-l. Zhang, and Y-s, Li, “A HMAC-Based RFID Authentication Protocol,” 2nd International Symposium on Infromation Engineering and Electronic Commerce (IEEC), July 2010, pp. 1-4.

[9] S-S. Yeo, J-S. Cho, and S. K. Kim. “Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value,” Computer Communication, vol. 34, 2011, pp. 391-397.

[10] P. Tuyls and L. Batina, “RFID-tags for Anti-Counterfeiting, Topics in Cryptology CT-RSA,” Lecture Notes in Computer Science, Vol.3860 , 2006, pp.115-131.

[11] G.E. Suh and S. Devadas, “Physical Unclonable Functions for Device Authentication and Secret Key Generation,” Proc. 44th ACM Annual Design Automation Conference 2007, June 2007, pp. 9-14.

[12] P. Cortese, F. Gemmiti, B. Palazzi, M. Pizzonia, and M. Rimondini,. “Efficient and Practical Authentication of PUF-Based RFID Tags in Supply Chains,” IEEE International Conference on RFID-Technology and Applications (RFIDTA), June 2010, pp.182-188.

[13] H. Ghaith, O. Erdinc, and S. Berk, “A Tamper-Proof and Lightweight Authentication Scheme,”, Pervasive Mobile Computing, Vol.4(6), 2008, pp. 807-818.

[14] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan, “Lightweight Mutual Authentication and Ownership Transfer for RFID systems,” Proc. Of IEEE INFOCOM 2010, March 2010, pp. 1-5.

[15] M. Akgün, M.S. Kiraz, and H. Demirci, “Cryptanalysis of Lightweight Mutual Authentication and Ownership Transfer for RFID System,” IEEE Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), March 2011, pp. 20-25.

[16] National Institute of Standards and Technology (NIST), SHA-1 Standard, Secure Hash Standard," FIPS PUB 180-1, www.itl.nist.gov/fipspubs/fip180-1.htm, 1995, [retrieved: Apr. 2013].

[17] J. Cho, S-C. Kim, and S. K. Kim, “Hash-based RFID tag Mutual Authentication Scheme with Retrieval Efficiency” 9th IEEE Internation Symposium on Parallel and Distributed Processing with Applications, May 2011, pp. 324-328.

[18] M. Safkhani, P. Peris-Lopez, J. C. Hernandez-Castro, N. Bagheri, and M. Naderi, “Cryptanalysis of Cho et al.’s protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems,” http://eprint.iacr.org/2011/331.pdf, 2011. [retrieved: Apr. 2013].

ISBN: 978-1-61208-285-1