Amirkabir University of Technology
(Tehran Polytechnic)

Amirkabir International Jounrnal of Science & Research
Electrical & Electronics Engineering
(AIJ-EEE)
Vol. 48, No. 2, Fall 2016, pp. 71-79

HMAC-Based Authentication Protocol: Attacks and Improvements

B. Abdolmaleki[1], K. Baghery[1], M. J. Emadi[2,*]

1- M.Sc. Student, Information Systems and Security Laboratory (ISSL), Sharif University of Technology
2- Assistant Professor, Department of Electrical Engineering, Amirkabir University of Technology

(Received 11 October 2015, Accepted 3 February 2016)

ABSTRACT

As a response to a growing interest in RFID systems, such as the Internet of Things technology along with satisfying the security of these networks, proposing secure authentication protocols is an indispensable part of the system design. Hence, authentication protocols to increase security and privacy in RFID applications have gained much attention in the literature. In this study, security and privacy of the recent well-known HMAC-based RFID mutual authentication protocol is analyzed. We prove that this protocol is not secure against various attacks and also does not provide untraceability. Also, in order to improve the performance of the mentioned protocol and enhance the security of RFID users, a more effective and secure authentication HMAC-based protocol is presented. Furthermore, security of our protocol is explored against different attacks, such as the replay attack, the tag's ID exposure, the spoofing attack, DoS attack and traceability attack. It is shown that our proposed protocol is safe against the attacks. Finally, the security of the presented protocol is compared with some well-known related protocols.

KEYWORDS:

RFID Systems, Authentication Protocols, HMAC, Security Analysis

Please cite this article using:
Abdolmaleki, B., Baghery, K., and Emadi, M. J., 2016. "HMAC-Based Authentication Protocol: Attacks and Improvements". *Amirkabir International Journal of Electrical and Electronics Engineering*, 48(2), pp. 71–79.
DOI: 10.22060/eej.2016.817
URL: http://eej.aut.ac.ir/article_817.html
*Corresponding Author, Email: mj.emadi@aut.ac.ir

1- Introduction

Nowadays, as the demand for highly secure Radio Frequency Identification (RFID) systems is increasing, enhancing security and privacy in RFID applications become more important [1-5]. Fig. 1 depicts a typical RFID system which includes a tag, reader and back-end server. Note that each RFID tag has the unique Identification (ID) code and there is not any limitation on the number of tags in an implemented RFID system. Basically, an RFID tag has a memory which contains specialized secret keys and various cryptography functions and operators such as one-way Hash, Cyclic Redundancy Check (CRC), and pseudo Random Number Generator (PRNG) which PRNG is unique for each tag. For instance, $PRNG_i^j$ shows the j-th invocation of the PRNG of the tag i. Note that, for the two given values $PRNG_i^j$ and $PRNG_i^k$, deciding whether $i=j$ is computationally difficult for any input of PRNG [6]. During the authentication process, the reader first sends data to the tag and requests to access the tag's information. After successful identification processes, the tag responses to the reader. Next, the reader forwards the received data to the back-end server to identify the tag. Then, the back-end server authenticates both the tag and the reader. Finally, after some authentication process between the tag, the reader, and the back-end server, the reader could retrieve corresponding data from a database of the back-end server [7].

Since the RFID systems are generally low cost, they may suffer from privacy and security threats. In order to overcome these problems, there are two main schemes. The first is a physical method and the other one is encryption method. Cryptology methods havegained much attention due to their low cost. These days, most of the RFID systems are using cryptology methods that include dynamic ID and static ID mechanisms. In static ID mechanism, the tag maintains itself as an identifier in all sessions of the authentication process, but in the dynamic ID mechanism, the tag identifier will change. Some of the protocols using static ID mechanism are considered by Jung et al.'s [5], Cho et al.'s [8], Cho et al.'s [9] and Wang et al. [1]. In this study, we also use the static ID mechanism.

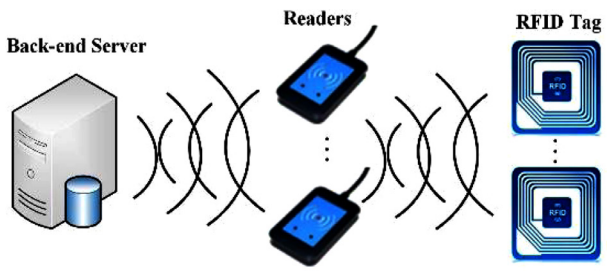

Fig. 1. A conventional RFID system model

In this paper, we first analyze the security and the privacy of keyed-Hash Message Authentication Code (HMAC)-based RFID mutual authentication protocol which is introduced by Jung et al. in [5]. This protocol is based on HMAC, and it is assumed that the communications channel between the reader and the back-end server is secure, but the communications channel between the reader and the tag is not a secure one. In Jung et al.'s protocol, the authors claimed that their protocol is secure against most of the famous attacks. In this paper, it is argued that the protocol has some weaknesses and is not safe against most of the attacks at all. Furthermore, in order to improve the performance of this protocol and increase the security of the user, we propose a more effective and secure authentication protocol. The presented scheme is also based on HMAC. Similarly, in the proposed protocol, we assume a secure communications channel between the reader and the back-end server, but the communications channel between the reader and the tag is not secure. In the presented protocol, a Hash function of the tag ID is eXclusive-OR (XOR)-ed by a random number that is concatenated with another random number, thus the security of the recommended protocol is very high and the attacker could not compute the secret values. In addition, it is proved that the new protocol is secure against various attacks and also provides user privacy. Ultimately, the security of our protocol is compared with some known protocols.

The remainder of the paper is organized as follows: section II reviews several threats for RFID systems. The HMAC-based authentication protocol which is studied by Jung et al. is introduced in section III. The weaknesses of Jung et al.'s protocol are analyzed in section IV. Section V presents our proposals. In section VI, the security and privacy of the improved protocol are investigated, and also the performance of the protocol is compared with other related protocols. Finally, we conclude the paper in section VII.

2- Overview of RFID attacks and threats

In RFID systems and their applications, the security problem is one of the most important challenges. In this section, some of the well-known

Table 1. Summarizes the notations used throughout the paper

Notation	Description
$HMAC$	Hash-based Message Authentication Code
$\mathcal{A}$	Malicious adversary
C_A	A random number of entity
C_{new}	A random number of current step
C_{old}	A random number of the previous step
ID_A	Identity of an entity
T_A	Timestamp from an entity
$(.)'$	For the second run of protocol
$(.)''$	For the third run of protocol
$H(.)$	Hash function
K_i	The authentication key stored in the tag for database to authenticate the tag at the th authentication phase
R	The legitimate reader
T	The legitimate Tag
T_t	Timestamp
$\oplus$	Bitwise XOR
$\|\|$	Concatenation operation
$A \oplus B$	Message is XORed with message
$A \rightarrow B$	forwards a message to

attacks and threats that RFID systems are vulnerable to them are introduced briefly.

2- 1- Information leakage

In RFID systems, when the tag and the reader want to send messages to each other, if the communications channel between the tag and the reader is not safe, this signaling could be eavesdropped by an adversary. Therefore, it is necessary to guarantee that the user authentication protocol must be secure against eavesdropper. That is, the sent data between the tag and the reader should not leak any secret information to illegitimate parties [10].

2- 2- Tag tracing and tracking

Tag tracing and tracking are two major issues in RFID systems. In the tag tracking, in order to recognize the tag's behavior, an attacker can track the tag by the use of tag identifier. Also, in the tag tracing, an attacker can trace the location of the user using the tag identifier. Therefore, in the authentication protocol design, untraceability is too important. In other words, it is important when the tag and the reader send signals to each other, the adversary could not eavesdrop the transmitted message [11] and [12].

2- 3- Denial-of-Service attack

Message blocking attack or Denial-of-Service (DoS) attack is another attack on RFID systems. In this case, the attacker tries to block the sent messages between the tag and the reader. DoS attack causes de-synchronization between the tag, the reader, and the back-end server. De-synchronization causes the back-end server and the tag could not recognize each other in the next steps [13] and [14].

2- 4- Replay attack

The replay attack occurs when an attacker tries to obtain transmitted messages between the tag and the reader using eavesdropping. Consequently, after obtaining the message by the attacker, the attacker replays it to the tag or the reader. It means that the attacker uses the obtained message to impersonate a legitimate reader or a legitimate tag [15].

2- 5- Tag impersonation attack

Tag impersonation attack occurs when an attacker is between a reader and the tag, and the attacker tries to impersonate a reader to receive a response from the tag. The attacker plays this role by sending an impersonated query to the tag. Then, an attacker sends the obtained response to the reader to impersonate the tag [13].

3- Review of Jung et al.'s protocol

Recently, Jung et al. proposed an HMAC-based RFID authentication protocol with minimal retrieval at the server [5]. Jung et al.'s protocol is based on the HMAC technique; see Fig. 2 for the whole procedure of the protocol involves five steps as follows.

Step 0: Enrollment phase

a) The following values are shared by the tag and the back-end server;

- C_0: A random number
- HMAC function
- k: a secret key
- ID_t: tag identifiers

b) Then, a pair of $<ID_t, ID_t \oplus C_0>$ is saved in the database of the tag and the back-end server as well.

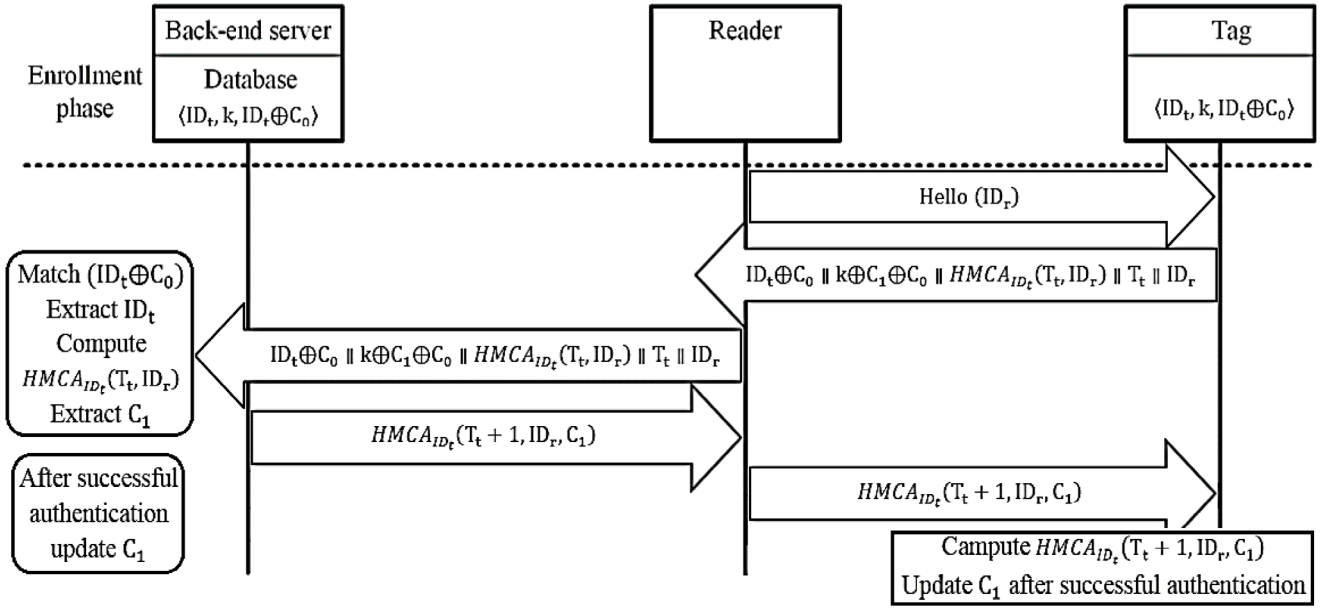

Fig. 2. The Junget al.'s protocol [5]

Step 1: Hello

The reader transmits a hello message for the tag with his/her ID (ID_r).

Step 2: Response of the tag

a) The tag T generates random number C_1 independent of the other one.

b) Then, the tag computes the following parameters and transmits them to the reader;

- $ID_t \oplus C_0$
- $k \oplus C_0 \oplus C_1$
- $a=HMCA_{ID_t}(T_t, ID_r)$
- ID_r and T_t.

Step 3: The tag authentication

a) First, the reader sends $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, ID_r and T_t to the back-end server.

b) Secondly, the back-end server matches $ID_t \oplus C_0$ with the first part of the received message and obtains $<ID_t, ID_t \oplus C_0>$ with $ID_t \oplus C_0$ and use them to extract ID_t.

c) After that, the back-end server calculates $a'=HMCA_{ID_t}(T_t, ID_r)$ and $C_1=k \oplus C_0 \oplus C_1 k \oplus C_0$.

d) Then, the back-end server checks whether $a'=a$ or not.

e) Next, $\beta=HMAC_{ID_t}(T_t+1, ID_r, C_1)$ is calculated by the back-end server and is sent back to the reader.

f) Finally, β it is transmitted to the tag by the reader.

Step 4: The back-end server authentication

a) Firstly, $\beta'=HMAC_{ID_t}(T_t+1, ID_r, C_1)$ is calculated by the tag using his/her T_t, C_1 and the received ID_r.

b) The tag checks whether $\beta'=\beta$ or not. If $\beta'=\beta$, then the authentication of the back-end server is confirmed by the tag.

Step 5: Update C_1

After the successful authentication process at the tag and the back-end server, the tag and the back-end server substitute $<ID_t, k, ID_t \oplus C_0>$ with $<ID_t, k, ID_t \oplus C_1>$ and in the next session $ID_t \oplus C_1$ will be used.

4- Vulnerabilities of Jung's protocol

In this section, we analyze the Jung et al.'s protocol and present some weaknesses of the protocol. In [5], the authors claimed that their protocol is secure against replay, eavesdropping, DoS and impersonation attacks. In the following, we prove that not only their protocol suffers from several threats such as replay, eavesdropping, DoS and impersonation attacks but also it does not provide privacy, and the adversary could track the tag. These attacks are analyzed as follows:

4- 1- Eavesdropping and impersonation attack

In this subsection, an impersonate attack against the Jung et al.'s protocol is studied. This attack consists of two phases; a learning phase and the attack phase.

- **Learning phase:** In this phase, the attacker is an eavesdropper. After one successful run, the attacker saves the transmitted messages between the reader and the tag including $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, $HMCA_{ID_t}(T_t, ID_r)$, ID_r and T_t. Note that, for the variable T_t, in the next run of protocol, T'_t it is used.

• Attack phase

In this phase, an attacker plays the reader role and performs the following steps;

- The attacker transmits ID_r to the tag
- The tag responses as;

a) The tag selects a random number C_2

b) The tag computes $ID_t \oplus C_1$, $k \oplus C_1 \oplus C_2$, ID_r, T'_t and $a=HMCA_{ID_t}(T'_t,ID_r)$ and transmits them to the spoofed reader or the attacker.

- Using $ID_t \oplus C_0, k \oplus C_0 \oplus C_1$ which are obtained from the first step, and $ID_t \oplus C_1$ received from the tag, the attacker computes the secret key as: $k=ID_t \oplus C_1 \oplus ID_t \oplus C_0 \oplus k \oplus C_0 \oplus C_1$.

- Using $ID_t \oplus C_1$, $k \oplus C_1 \oplus C_2$ that are received in the second step, and computed in the previous phase, the attacker computes $ID_t \oplus C_2=ID_t \oplus C_1 \oplus k \oplus C_1 \oplus C_2 \oplus k$.

- In this phase, the attacker changes the received messages from the tag, $ID_t \oplus C_1$, $k \oplus C_1 \oplus C_2$, ID_r, T'_t, $HMCA_{ID_t}(T'_t,ID_r)$ to $ID_t \oplus C_1$, k, ID_r, T'_t, $HMCA_{ID_t}(T'_t,ID_r)$. Now the attacker plays the role of the tag and transmits these messages to the reader and the reader forwards them to the back-end server.

- The tag authentication

a) The back-end server matches $ID_t \oplus C_1$ with the first part of the received message and obtains $<ID_t, ID_t \oplus C_1>$ and $ID_t \oplus C_1$ and utilize them to extracts ID_t.

b) The back-end server calculates $a'=HMAC_{ID_t}(T'_t,ID_r)$ and $C_2=k \oplus k \oplus C_1$.

c) Then, the back-end server checks whether $a'=a$ or $a' \neq a$.

d) Next, $\beta=HMAC_{ID_t}(T'_t+1,ID_r,C_2)$ is calculated by the back-end server and is sent back to the reader. At the end, the back-end server updates $<ID_t,k,ID_t \oplus C_1>$ with $<ID_t,k,ID_t \oplus C_2>$ for the next session. Note that from now, the value of C_2 is equal to C_1 in the back-end server.

- When the reader wants to send the received message from the back-end server to the tag, the attacker blocks the transmitted message from the reader and stops the rest of protocol run. Then, the attacker impersonates the tag and transmits $ID_t \oplus C_1$, k, ID_r, T'_t, $HMCA_{ID_t}(T'_t,ID_r)$ to the back-end server, and the back-end server authenticates the attacker and updates $<ID_t,k,ID_t \oplus C_1>$ with $<ID_t,k,ID_t \oplus C_1>$ for the next session.

Note that, after this session the attacker can impersonate the tag by transmitting $ID_t \oplus C_1$, k, ID_r, T'_t, $HMCA_{ID_t})(T'_t,ID_r)$ to the back-end server.

4- 2- DoS attack

In this subsection, a DoS attack against the Jung's protocol is presented. In this attack, after running three steps of the protocol, when the reader wants to transmit a message to the tag, the attacker intercepts the transmitted message to the tag. Therefore, the back-end server is updated $<ID_t,k,ID_t \oplus C_0>$ with $<ID_t,k,ID_t \oplus C_1>$ but the tag does not update its information. Hence, in the next session of protocol, the back-end server cannot authenticate the tag.

4- 3- Replay attack and privacy problem

In [5], the authors claimed that their protocol is secure against the replay attack and the privacy of this protocol is provided. In this subsection, we prove that their protocol is not secure against the replay attack and the tag could be tracked by the attacker. In the following, two traceability attacks are provided.

4- 3- 1- First traceability attack

In this attack, the attacker performs two following phases:

• **Learning phase:** After two successful runs, the attacker achieves $ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, $ID_t \oplus C_1$, $k \oplus C_1 \oplus C_2$ by eavesdropping. Afterwards, using these messages, the attacker computes $k=ID_t \oplus C_1 \oplus ID_t \oplus C_0 \oplus k \oplus C_0 \oplus C_1$. With the use of k, the attacker obtains $\gamma=ID_t \oplus C_1 \oplus k \oplus C_1 \oplus C_2 \oplus k$.

• **Attack phase:** The attacker plays the role of the reader and performs the following operations;

- The tag responses $ID_t \oplus C_2$, $k \oplus C_2 \oplus C_3$, ID_r, T''_t and $HMAC_{ID_t}(T''_t,ID_r)$ to the attacker.
- After two successful runs of protocol, the tag updates with $<ID_t,k,ID_t \oplus C_2>$ and the attacker observes $\gamma=ID_t \oplus C_2$. Therefore, the attacker tracks the tag.

4- 3- 2- Second traceability attack

This attack consists of the two following phases.

• **Learning phase:** After running three steps of the protocol, the attacker obtains $\gamma_1=ID_t \oplus C_0$, $k \oplus C_0 \oplus C_1$, ID_r, T_t and $a=HMCA_{ID_t}(T_t,ID_r)$. When the reader transmits the message to the tag, the attacker blocks the transmitted message to the tag. Therefore, the tag does not update its data.

• **Attack phase:** The attacker performs the

following operations:

- The attacker sends a *hello* message, ID_r to the tag

- The tag responses $\gamma_2=ID_t\oplus C_0$, $k\oplus C_0\oplus C_1$, ID_r, T_t and $HMAC_{ID_t}(T_t,ID_r)$ to the attacker. Note that because of the interception done by the attacker in the learning phase, the tag does not update its database, thus the values of γ_1 and γ_2 are the same. Therefore the attacker could track the tag easily.

In summary, we proved that the protocol suggested in [5] is not secure at all. In the following section, we improve the protocol to overcome all the mentioned vulnerabilities.

5- Proposed protocol

In this section, an improved version of the Jung's protocol is presented which eliminates all the above weaknesses. The summary of the proposed protocol is presented in Fig. 3. We show that our protocol is secure against all of the attacks and provide forward secrecy and untraceability attacks. The suggested protocol consists of five steps as follows:

Step 0: Initialization phase

a) The following values are shared by the tag and the back-end server;

- C_{old}: A random number
- HMAC function
- k: a secret key
- ID_t: tag identifiers.

b) Then, a triple of $<ID_t,k,ID_t\oplus C_{old},ID_t\oplus C_{new}>$ is saved in the database of the back-end server, and,

c) A triple of $<ID_t,k,ID_t\oplus C_{old}>$ is saved in the database of the tag.

Note that in this phase C_{new} and C_{old} are the same.

Step 1: Hello

This phase is the same as Jung's protocol.

Step 2: Response of tag

a) A random number C_1 is selected by the tag

b) The tag computes $H(ID_t\oplus C_0\|C_1)$, $k\oplus C_0\oplus C_1$, ID_r, T_t and $a=HMAC_{ID_t}(T_t,ID_r,C_1)$, then sends them to the reader.

Step 3: The tag authentication

a) The reader sends $H(ID_t\oplus C_0\|C_1)$, $k\oplus C_0\oplus C_1$, a, ID_r, and T_t to the back-end server.

b) With the use of $k\oplus C_{new}$ and $k\oplus C_{old}$, the back-end server computes

$I_{new}=k\oplus C_0\oplus C_1\oplus k\oplus C_{new}$

$I_{old}=k\oplus C_0\oplus C_1\oplus k\oplus C_{old}$

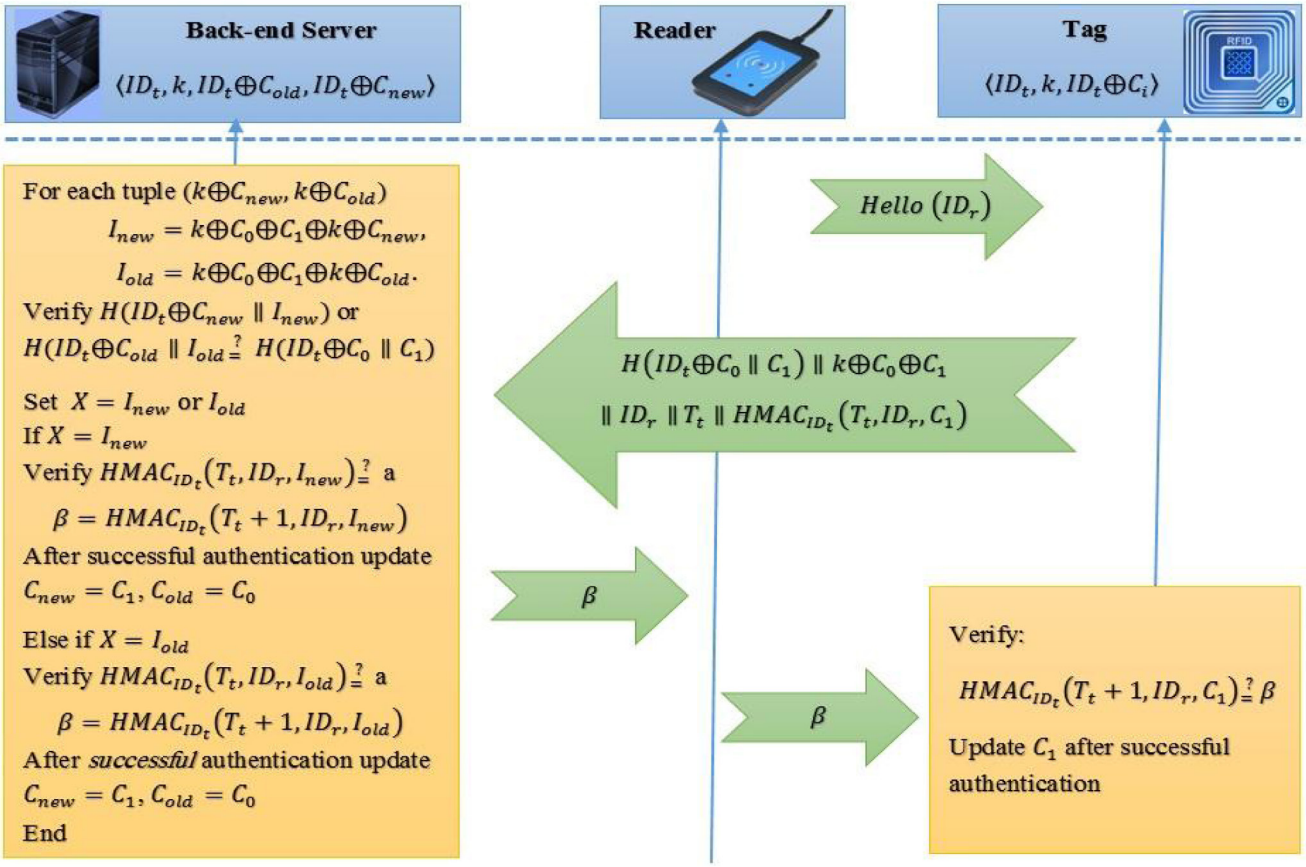

Fig. 3. The proposed protocol

c) Then, the back-end server computes $H(ID_t \oplus C_{new}||I_{new})$ and $H(ID_t \oplus C_{old}||I_{old})$ using I_{new} and I_{old}.

d) The back-end server checks whether $H(ID_t \oplus C_{new}||I_{new})$ or $H(ID_t \oplus C_{old}||I_{old})$ matches with $H(ID_t \oplus C_0||C_1)$ received in the first phase of this step. In order to find a match, this process is done for both $H(ID_t \oplus C_{new}||I_{new})$ and $H(ID_t \oplus C_{old}||I_{old})$. The matched one will set value as I_{new} or I_{old}. Note that the value of (I_{new} or I_{old}) X is saved as a random number in the tag.

1) If $X=I_{new}$, the back-end server computes $HMAC_{ID_t}(T_t,ID_r,I_{new})$ and compares it with the received a and authenticate the tag. Then, computes $\beta=HMAC_{ID_t}(T_t+1,ID_r,I_{new})$ and sends it β to the reader. Finally, the reader sends it to the tag.

2) If $X=I_{old}$, the back-end server computes $HMAC_{ID_t}(T_t,ID_r,I_{old})$ and compares it with the received a and authenticate the tag. Then, computes $\beta=HMAC_{ID_t}(T_t+1,ID_r,I_{old})$ and sends it to the reader. Finally, the reader sends it β to the tag.

Step 4: The back-end server authentication

This phase is the same as Jung et al.'s protocol.

Step 5: Update C_i

a) After the successful authentication at the tag and the back-end server, if $X=I_{new}$ is used, the back-end server and the tag update, and replace $<ID_t,k,ID_t \oplus C_0>$ with $<ID_t,k,ID_t \oplus C_1>$.

b) Otherwise, the back-end server and the tag use the previous values.

6- Security analysis

In this section, the security of the proposed protocol against various attacks described in section IV is analyzed. Similar to [5], we assume that communications channel between the reader and the back-end server is secure but the communications channel between the reader and the tag is not secure.

6- 1- Eavesdropping

Although, the attacker can eavesdrop $H(ID_t \oplus C_0||C_1)$, $k \oplus C_0 \oplus C_1$, ID_r, T_t and $HMAC_{ID_t}(T_t,ID_r,C_1)$,but, because of using the Hash function and the XOR operator, the security of the proposed protocol is very high and the attacker could not compute the secret values. Therefore, the proposed protocol is secure against the eavesdropping.

6- 2- DoS attack

In this case, the attacker tries to block the sent message between the tag and the back-end server. But due to the use of $ID_t \oplus C_{old}$ and $ID_t \oplus C_{new}$ at the back-end server, if an attacker blocks the protocol, he/she could not perform DoS attack. As a result, the proposed protocol is secure against DoS attack and the attacker is not able to cause de-synchronization between the tag and the back-end server.

6- 3- Replay attack

In the replay attack, the attacker tries to impersonate the tag and the reader to access the transmitted messages, modify, and even delete them [16]. In the proposed protocol, because of generating a new random number in each session and utilizing a Hash of it, our suggested protocol provides a strong resistant against the replay attack.

6- 4- Tag impersonation

In order to impersonate a legitimate tag, the attacker tries to use the secret keys ID_t and k/or two consecutive tag's response. In the proposed protocols, the secret key ID_t is protected by a hash function and the attacker does not have access to it directly. In addition, due to the use of a random number C_i in each run of the protocol, the dependency between different parts of two consecutive tag's responses is omitted. By applying these changes, the attacker cannot use the responses of the two consecutive run of the protocol to impersonate the legitimate tag.

6- 5- Privacy

In the proposed protocol, the tag ID is XOR-ed with an old random number and the result is concatenated with another new random number. Then, the Hash function is applied which results in $H(ID_t \oplus C_{old}||C_{new})$. Therefore, the privacy of our proposed protocol is high and the attacker could not trace the tag. Note that the values of C_{old} and C_{new} are updated after each successful session and only the back-end server and the tag know the values of ID_t, C_{old} and C_{new}.

We have compared the security and the privacy of the recommended protocol with some similar protocols such as Lim et al. [17], Lee et al. [18], Wang et al. [19], Cho et al. [8] and Jung et al. [5] that are introduced in recent years. The results are summarized in Table 2. It can be seen that all of the mentioned protocols have some weaknesses. But the proposed protocol is secure against various attacks and also provides the user privacy.

Table 2. Security analysis comparison

Protocols / Threats	[17]	[18]	[19]	[8]	[5]	Proposed Protocol
Eavesdropping	×	×	§	×	×	§
Spoofing Attack	§	§	§	×	×	§
DoS Attack	§	×	×	×	×	§
Replay Attack	×	×	§	×	×	§
Untraceability	§	§	×	§	×	§

§: Secure ×: Insecure

7- Conclusion

In the paper, the security and the privacy of HMAC-based RFID mutual authentication protocol studied by Jung et al. is analyzed. Although the authors claimed that this protocol is secure against various attacks, we proved that their protocol is not secure against most of the well-known attacks and also does not provide untraceability. To improve the performance of the mentioned protocol and increase the security of the users, we proposed a more effective and secure authentication protocol. In additions, the security, and privacy of our protocol are investigated against various attacks. The analyses showed that the protocol is safe against the well-known attacks and provide users' privacy. Finally, the security and the privacy comparisons with other protocols claims that our protocol outperforms the other recent protocols.

8- References

[1] Wang, S. P.; Ma, Q. M.; Zhang, Y. L. and Li, Y. S.; "A HMAC-Based RFID Authentication Protocol," *in 2nd International Symposium on Information Engineering and Electronic Commerce (IEEC)*, pp. 1–4, 2010.

[2] Baghery, K.; Abdolmaleki, B. and Emadi, M. J.; "Game-Based Cryptanalysis of a Ligthwigth CRC-Based Authentication Protocol for EPC Tags," *Amirkabir International Journal of Electrical and Electronics Engineering (AIJ-EEE)*, Vol. 46, No. 1, pp. 27–36, 2014.

[3] Ren, X.; Xu, X. and Li, Y.; "An One-Way Hash Function Based Lightweight Mutual Authentication RFID Protocol," *Journal of Computers*, Vol. 8, No. 9, pp. 2405–2412, 2013.

[4] Asadpour, M. and Dashti, M. T.; "A Privacy-Friendly RFID Protocol Using Reusable Anonymous Tickets," *in 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Changsha, pp. 206–213, 2011.

[5] Jung, S. W. and Jung, S.; "HMAC-Based RFID Authentication Protocol with Minimal Retrieval at Server," *in The 5th International Conference on Evolving Internet*, pp. 52–55, 2013.

[6] Tsudik, G.; YA-TRAP: Yet Another Trivial RFID Authentication Protocol," *in 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, 2006.

[7] Zhang, X.; Cheng, L. and Zhu, Q.; "Improvement of Filtering Algorithm for RFID Middleware Using KDB-tree Query Index," *Journal of Software*, Vol. 6, No. 12, pp. 2521–2527, 2011.

[8] Cho, J. S.; Yeo, S. S. and Kim, S. K.; "Securing Against Brute-Force Attack: A Hash-Based RFID Mutual Authentication Protocol Using a Secret Value," *Computer Communication*, Vol. 34, No. 3, pp. 391–397, 2011.

[9] Cho, J.; Kim, S. C. and Kim, S. K.; "Hash-Based RFID Tag Mutual Authentication Scheme with Retrieval Efficiency," *in 9th IEEE Internation Symposium on Parallel and Distributed Processing with Applications*, pp. 324–328, 2011.

[10] Van-Deursen, T. and Radomirovic, S.; "Attacks on RFID Protocol," *Cryptology ePrint Archive*, 2008.

[11] Phan, R.; "Cryptanalysis of a New Ultralightweight RFID Authentication Protocol-SASI," *IEEE Transactionson Dependable and Secure Computing*, Vol. 6, No. 4, pp. 316–320, 2009.

[12] Lim, C. H. and Kwon, T.; "Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer," *in Proceedings of ICICS'06*, LNCS 4307, pp. 1–20, 2006.

[13] Piramuthu, S.; "Lightweight Cryptographic Authentication in Passive RFID-Tagged Systems," *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 38, No. 3, pp. 360–376, 2008.

[14] Peris-Lopez, P.; Hernandez-Castro, J. C.; Estevez-Tapiador, J. M. and Ribagorda, A.; "Vulnerability Analysis of RFID Protocols for Tag Ownership Transfer," *Computer Networks*, Vol. 54, pp. 1502–1508, 2010.

[15] Kulseng, L.; Yu, Z.; Wei, Y. and Guan, Y.;

"Lightweight Mutual Authentication and Ownership Transfer for RFID Systems," *IEEE INFOCOM*, pp. 251–255, 2010.

[16] Liu, H. and Ning, H.; "Zero-Knowledge Authentication Protocol Based on Alternative Mode in RFID Systems," *IEEE Sensors Journal*, Vol. 11, No. 12, pp. 3235–3245, 2011.

[17] Lim, J.; Oh, H. and Kim, S.; "A New Hash-Based RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection," *in Information Security Practice and Experience*, Springer Berlin Heidelberg, pp. 278–289, 2008.

[18] Lee, Y. C.; Hsieh, Y. C.; You, P. S. and Chen, T. C.; "An Improvement on RFID Authentication Protocol with Privacy Protection," *in 3rd International Conference on Convergence and Hybrid Information Technology*, South Korea, Busan, 2008.

[19] Wang, S.; Ma, Q. M.; Zhang, Y. L. and Li, Y. S.; "A HMAC-Based RFID Authentication Protocol," *in 2nd International Symposium on Infromation Engineering and Electronic Commerce (IEEC)*, 2010.