© 2017 IJSRSET | Volume 3 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey of Authentication of RFID Devices Using Hash Function

Suthar Monali, Prof Alka J Patel
IT Department, LDCE, Ahmedabad, Gujarat, India

ABSTRACT

RFID is a wireless technology for automatic identification and data capture . RFID is the core technology to implement the internet of things. So the security issue of RFID is becoming more and more important, in the past decade, a large number of research papers dealing with security issues of RFID technology have appeared [1]. The problem of authentication and privacy are fundamental to RFID devices. In this paper we discuss security attack possible on RFID and three different authentication algorithm of RFID.

Keywords: RFID, Reader, Tag, Backend Sever , Authentication , Security , HASH, HMAC.

I. INTRODUCTION

RFID system is composed of tags, readers, backend sever, and antennas. RFID tags are inexpensive wireless devices which can communicate with RFID readers [1].RFID architecture shown in figure 1 which consist tag , reader and back end server . Tag consist EPC(electronic product code) which store details about tag. Reader is responsible for reading and writing tag information . Back end sever will save all data about tag which are in one group .communication in RFID network will start on reader broadcast message or query.

Communication between tag-reader and reader-server is in insecure channel.

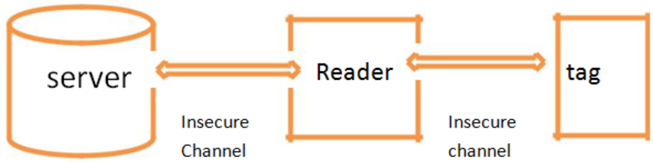


Figure 1

In this paper we first analyze security attack possible on RFID in section 2 , then we discuss RFID device performance measurement in section 3, three authentication method or protocol discussed in section 4 .

SECURITY ATTCK ON RFID

Denial of Service (DOS) :

In both of wireless and wired communication, there are Denial of Service (DOS) . Once attackers control a large number of fake readers and tags, they can make the data connection to abuse computational resources, and even use up the resources and network bandwidth.[1]

Eavesdropping :

The communication channel between the tag and the reader can be eavesdropped, because the radio frequency channel is not secure communication channel .[2]

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.[2]

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.[2]

Spoofing attack :

The attacker impersonates a reader, sends a query to a tag, and then obtains 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.[2]

Cloning attack :

An attacker can build a cloned tag which will be interpreted by the reader as the legitimate tag, due to the fact that most tags are not tamper-proof.[2]

3. PERFORMANCE

RFID schemes cannot use computationally intensive cryptographic algorithms for privacy and security because tight tag cost requirements make tag-side resources (such as processing power and storage) scarce .[3]

- Capacity minimisation: The volume of data stored in a tag should be minimised because of the limited size of tag memory
- Computation minimization: Tag-side computations should be minimized because of the very limited power available to a tag.
- Communication compression: The volume of data that each tag can transmit per second is limited by the bandwidth available for RFID tags [3]
- Scalability: The server should be able to handle growing amounts of work in a large tag population. It should be able to identify multiple tags using the same radio channel [3] Performing an exhaustive search to identify individual tags could be difficult when the tag population is large [3].

II. AUTHENTICATION METHOD

a) Simple Hash based authentication protocol

This scheme is based on one-way hash function. As shown in **figure 2**, when the RFID reader sends the request to the tag, the tag will return the H(k), the k is shared key between the tag and the reader, then the reader gets the (k,ID) from the database according the H(k) and sends k to the tag, the tag calculates H'(k) using the k received from the reader, if H(k) and H'(k) is equal, the tag will return ID to the reader. In this way, using H(k) to replace real tag ID prevents the tag being tracked.[1]

To improve simple hash based algorithm we can use random number with hash.[1]

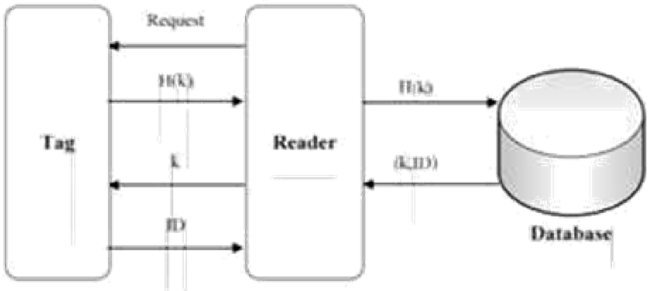


Figure 2. Hash-Lock authentication

b) HMAC based authentication algorithm

This algorithm used PUF (physically Unclonable function) which is innovative circuit primitive to derive a secret from complex physical characteristics of ICs rather than storing the secret in memory. It has a drawback that the back-end server stores a large number of Challenge-Response Paris (CRPs) of PUF. Also always a fresh challenge must be used to prevent from replay attack so that CRPs will be consumed very fast. Therefore, the huge CRPs are required. [2]

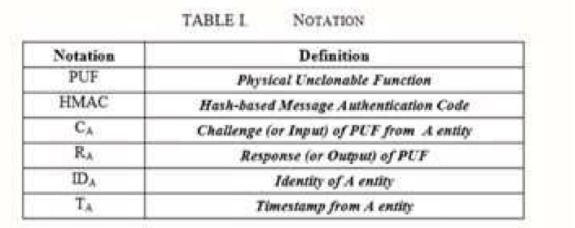
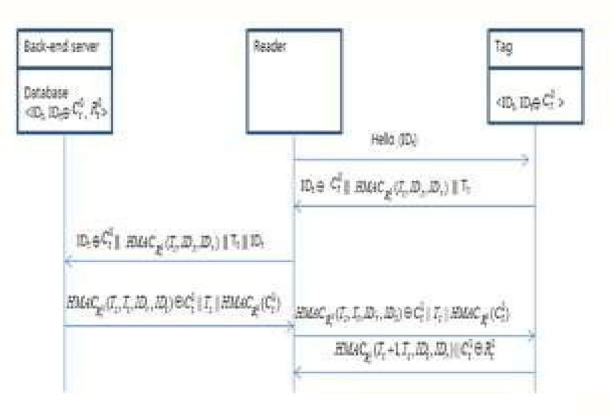


TABLE I. NOTATION

Notation	Definition
PUF	*Physical Unclonable Function*
HMAC	*Hash-based Message Authentication Code*
C_A	*Challenge (or Input) of PUF from A entity*
R_A	*Response (or Output) of PUF*
ID_A	*Identity of A entity*
T_A	*Timestamp from A entity*

HRP:A HMAC-based RFID mutual authentication protocol using PUF in this paper a HMAC-based mutual authentication protocol using PUF in RFID system. The proposed protocol uses a response as a secret key of HMAC rather than sending the response against a corresponding challenge. The response is known to only the tag and the back-end server. The proposed protocol needs to maintain only one CRP rather than a huge number of CRPs.

The proposed protocol is based on PUF. Therefore, cloning attack is infeasible. Moreover, the proposed protocol can support privacy protection in a way that the identifier of the tag is XORed by the challenge which is a random number and is changed at every session.

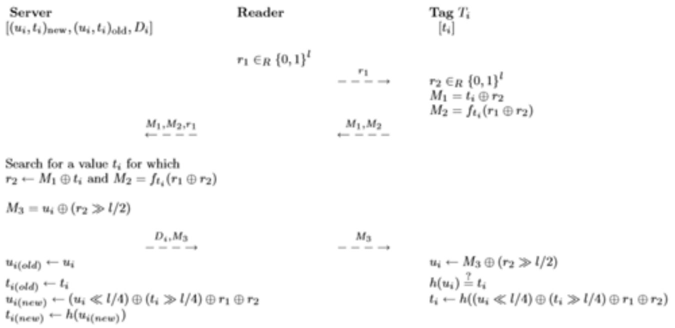


HMAC based algorithm is secure against cloning ,eavesdropping, user privacy, reply attack. But with the use of this protocol has to computes HMAC function four times at the tag and the back-end server. Which means two more computation required than simple hash protocols .[2]

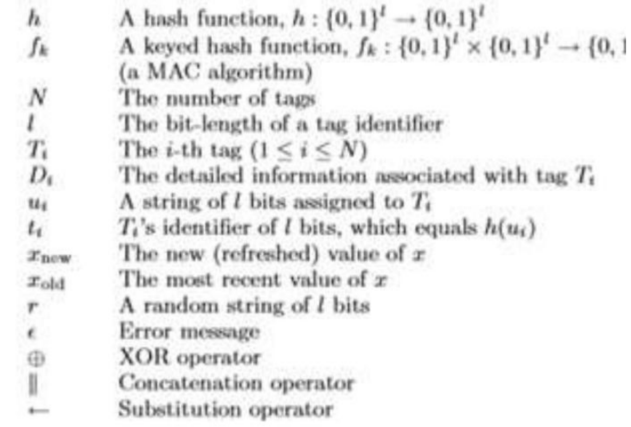
- **A novel approach by Boyeon Song and Cheris**

As we seen above two method are simple with hash, random number and MAC . Seung's algo[2] with HMAC is not efficient in based on HMAC computation . Xiao's algorithm*1+ which is simple hash based algorithm . These both are use same tag ID for each communication . boyen's novel approach shown in **figure 4** will use a challenge-response approach. It uses random numbers to give anonymity for each tag response, The server database stores both the most recent and the current data for each tag to protect against desynchronization between the server and tags. One of the main features of the protocol is that a random number generated by a tag serves as a temporary secret for the tag. Another feature is that a tag only needs to store an identifier, where this identifier is the cryptographic hash of a bit-string assigned to the tag. A server database stores tag bit-strings as well as tag identifiers. The bit-string is used for server validation. The scheme is designed to minimize the use of complex cryptographic functions, and instead wherever possible uses combinations of simple functions such as right and left shifts and bit-wise exclusive-or operations to combine data strings.[3]

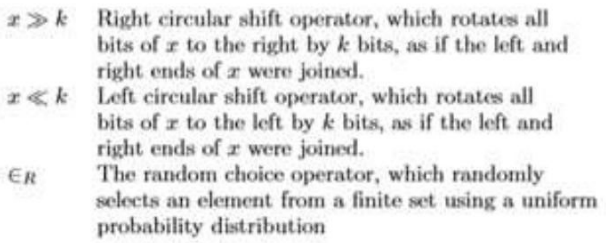
Figure 4


Server
$[(u_i,t_i)_{new},(u_i,t_i)_{old},D_i]$
Reader
Tag T_i
$[t_i]$
$r_1 \in_R \{0,1\}^l$
r_1
$r_2 \in_R \{0,1\}^l$
$M_1 = t_i \oplus r_2$
$M_2 = f_{t_i}(r_1 \oplus r_2)$
M_1,M_2,r_1
M_1,M_2
Search for a value t_i for which
$r_2 \leftarrow M_1 \oplus t_i$ and $M_2 = f_{t_i}(r_1 \oplus r_2)$
$M_3 = u_i \oplus (r_2 \gg l/2)$
D_i,M_3
M_3
$u_{i(old)} \leftarrow u_i$
$t_{i(old)} \leftarrow t_i$
$u_{i(new)} \leftarrow (u_i \ll l/4) \oplus (t_i \gg l/4) \oplus r_1 \oplus r_2$
$t_{i(new)} \leftarrow h(u_{i(new)})$
$u_i \leftarrow M_3 \oplus (r_2 \gg l/2)$
$h(u_i) \overset{?}{=} t_i$
$t_i \leftarrow h((u_i \ll l/4) \oplus (t_i \gg l/4) \oplus r_1 \oplus r_2)$

Notation



h	A hash function, $h : \{0,1\}^l \rightarrow \{0,1\}^l$
f_k	A keyed hash function, $f_k : \{0,1\}^l \times \{0,1\}^l \rightarrow \{0,$ (a MAC algorithm)
N	The number of tags
l	The bit-length of a tag identifier
T_i	The i-th tag $(1 \le i \le N)$
D_i	The detailed information associated with tag T_i
u_i	A string of l bits assigned to T_i
t_i	T_i's identifier of l bits, which equals $h(u_i)$
x_{new}	The new (refreshed) value of x
x_{old}	The most recent value of x
r	A random string of l bits
ϵ	Error message
$\oplus$	XOR operator
$\|$	Concatenation operator
$\leftarrow$	Substitution operator



$x \gg k$	Right circular shift operator, which rotates all bits of x to the right by k bits, as if the left and right ends of x were joined.
$x \ll k$	Left circular shift operator, which rotates all bits of x to the left by k bits, as if the left and right ends of x were joined.
$\in_R$	The random choice operator, which randomly selects an element from a finite set using a uniform probability distribution

SECURITY ANALYSIS

Security attack	Paper1	Paper2	Paper3
Mutual authentication	YES	-	YES
Replay	YES	YES	YES
Cloning	-	YES	-
Spoofing/server impression	-	YES	-
Forward security	-	YES	YES
DOS	-	-	YES

III. CONCLUSION AND FUTURE WORK

Here we discussed three authentication approach based on HASH function . As we seen each approach is focus on different security attack and performance measurement . in these three approach boyen’s approach is good with respect to other two approaches. But PKI infrastructure is good for RFID then HASH. In public key – private key reference elliptic curve, RSA , with certificate authority , digital signature , biometric feature is possible.

IV. REFERENCES

[1]. Xiao Nie, Xiong Zhong “Security In the Internet of Things Based on RFID: Issues and Current Countermeasures” Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013), Published by Atlantis Press, Paris, France.

[2]. Seung Wook Jung , Souhwan Jung ” HRP : A HMAC-based RFID mutual authentication protocol using PUF” , ICOIN 2013, IEEE publication , pp 578-582.

[3]. Boyeon Song , Chris J Mitchell ” RFID AuthenticationProtocolfor Low-cost Tags” WiSec’08, March 31–April 2,2008,Alexandria, Virginia, USA.