International Journal of Informatics and Communication Technology (IJ-ICT)
Vol.2, No.2, July 2013, pp. 99~105
ISSN: 2252-8776

Cryptanalysis and Improvement of the Zhu *et al.*'s Authentication Protocol

Mahdi Azizi*, Abdolrasoul Mirgadri* and Nasour Bagheri**
* Faculty of Communication and Information Technology, IHU University, Tehran, Iran,
** Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran

Article Info

Article history:

Received Jan 12th, 2013
Revised Mar 20th, 2013
Accepted Jun 18th, 2013

Keyword:

RFID
Authentication protocol
Traceability attack
Formal proof
BAN logic

ABSTRACT

Zhu *et al.* recently have proposed an authentication prpotocol for RFID systems. In this paper, we analyze its security and explain its security drawbacks. More precisely, we present traceability attack against this protocol. In addition, we propose an improvement on the Zhu *et al.*'s to resists these security drawbacks. Finally, we investigate the formal security of the improved protocol based on the BAN logic method.

Corresponding Author:

Mahdi Azizi,
Faculty of Communication and Information Technology,
IHU University, Tehran, Iran,
mmazizi2006@gmail.com

1. INTRODUCTION

The main application of an RFID system could be to identify tags to the reader over a wireless communication channel. This technology has diverse usages in wide range of areas such as logistics; retail, manufacturing, garment industry, medical, identification, traffic, aviation and so on. Nowadays, many applications use low-cost passive tags as the best alternative to barcodes, which are cheapest identifier [2], [3]. However, this type of tags are restricted by memory and power of calculation, thus designers are forced to utilize lightweight authentication protocols. Generally, RFID systems make up of three main components. The transponder or RFID tag, which is used to label each object, the transceiver or RFID reader, which is utilized for querying tags and the backend database or server, where the information of whole tags are verified.

Since the channel between the tag and the reader is not secure, the adversary may easily eavesdrop the transferred information in RFID system. Tags are divided into three classes: passive, semi-passive and active. A passive tag is cheaper, compared to the other types of tags, and has extremely limited computation and storage capability. Hence, it is not possible to use the conventional symmetric encryption algorithms to provide the desired security for these tags. Therefore, designing a lightweight authentication protocol which resists the known attacks in the context is a challenging task.

Recently, Zhu *et al.* [1] have proposed a forward-secure anonymous RFID authentication Protocol. This paper focuses on analyzing and finding a security drawback on it. In addition, we propose the improved version of the protocol which resists the attack suggested in this paper and other attacks in the context.

The rest of this paper is organized as follows. Section 2 introduces related works, and section 3 reviews the Zhu *et al.*'s protocol. In section 4, we analyze and improve the Zhu *et al.*'s protocol. In Section 5, we give a formal proof based on BAN logic for the improved protocol. Finally, we conclude the paper in section 6.

2. RELATED WORK

Security and privacy are important concerns for RFID systems. Some researcher have attempted to resolve this problem, we refer interested reader to [2],[3],[4],[5],[6], [7], [8]. On the other hand, untraceability is an important property of RFID protocols which provide anonymity of the tag's holder which is crucial to provide the user privacy. The protocol suffers from traceability property if adversary (*A*) is able to distinguish the tag *(T)* better than random guessing. The advantage of adversary is defined as follows:

$$Adv_A = \left| pr\left[Acorrect\right] - \frac{1}{2} \right|,$$

Where $pr\left[Acorrect\right] = pr\left[A = yes \middle| T = \bar{T}\right] + pr\left[A = no \middle| T \neq \bar{T}\right]$. If the probable advantage of the adversary is negligible, then protocol will be untraceable.

In 2006, Gene Tsudik [9] proposed a lightweight authentication, named YA-TRAP**.** This protocol is vulnerable to DoS attack to resist this attack ,Chatmon *et al.* [10] improvement YA-TRAP protocol . However, in WiCOM'09, He *et al.*[11] analyzed and found the security drawback to Chatmon's protocol and then improvement it. Latter, Zhu *et al.*[1] analyzed the He *et al.*'s protocol and found the security drawbacks of this protocol and improved it. The improvement of the He *et al.*'s protocol is more efficient than the original one. In this paper, we analyze the security of Zhu *et al.*'s protocol.

3. ZHU *ET AL.*'S PROTOCOL

Zhu *et al.* have analyzed the He *et al.*'s protocol and found its security drawbacks [1]. They have also proposed the improved version of this protocol. They have claimed that the improved protocol is more efficient than the He *et al.*'s protocol. The Zhu *et al.*'s Protocol works as follows (also see Figure 1.), where the notations are introduced in Table 1.:

1) Reader broadcasts $\left(t_{sys}, r_{sys}\right) \rightarrow Tag$

2) Tag calculate : $\begin{cases} if\ t_{sys} > t_{tag}\ ,\ h_1 = H_K\left(0, t_{sys}, r_{sys}\right),\ r_{tag} \\ Else\ ,\ h_1 = H_K\left(1, r_{tag}, r_{sys}\right),\ r_{tag} \end{cases}$,then $Tag \longrightarrow Reader: h_1, r_{tag}$

3) $Reader \longrightarrow Server: h_1, r_{tag}, r_{sys}$

4) The server authenticates the tag in two ways:

$If\ \exists\left(K, K_p\right) \in \mathcal{K}; \left(h_1 = H_K\left(0, t_{sys}, r_{sys}\right) \vee h_1 = H_K\left(1, r_{tag}, r_{sys}\right)\right)$

Then, it computes $h_2 = H_K\left(2, r_{tag}, t_{sys}\right)$ and updates $\left(K, K_p\right)$ as $K = H(K)$ and $K_p = K$.

Or $If\ \exists\left(K, K_p\right) \in \mathcal{K}; \left(h_1 = H_{Kp}\left(0, t_{sys}, r_{sys}\right) \vee h_1 = H_{Kp}\left(1, r_{tag}, r_{sys}\right)\right)$

the server computes $h_2 = H_{Kp}\left(2, r_{tag}, t_{sys}\right)$

5) $Server \longrightarrow Reader \longrightarrow Tag: h_2$

6) The tag checks: if received h_2 is the same as the calculated $h_2 = H_{Kp}\left(2, r_{tag}, t_{sys}\right)$,then sets $t_{sys} = t_{tag}\ if\ t_{sys} \geq t_{tag}$ and updates $K = H(K)$.

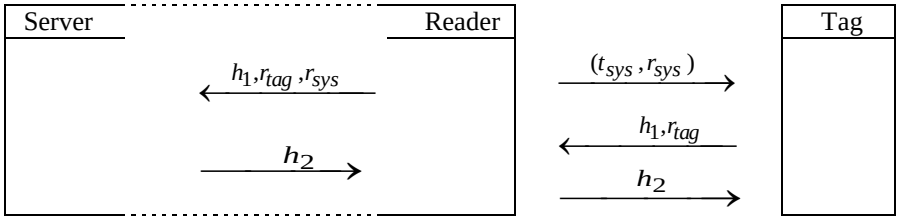

Figure 1. Zhu *et al.*'s protocol[1]

Table 1. Notations

t_{sys}	System's timesatamp generated by reader(system)
r_{sys}	Random number generated by reader(system)
t_{tag}	Timesatamp of tag
r_{tag}	Random number of tag

r_{Adv}	Random number chosen by adversary
t_{Adv}	Timesatamp of adversary
N_T, N_D	Two counters respectively in the tag and backend database
T_t	Variable tag called timestamp
T_r	Variable reader called timestamp
$H_r, H_K(.)$	Pseudo-random string and hash function respectively
K, K_p	K is the currently stored key and K_p is the key used in the last authentication

4. SECURITY ANALYSIS AND IMPROVEMENT OF ZHU *ET AL.*'S PROTOCOL

In this section, we analyze the Zhu *et al.*'s protocol and show its security drawbacks. The untraceability property is one of the most important specifications of privacy for authentication protocol. In the Zhu *et al.*'s protocol, we can trace RFID tag, i.e. we can find a traceability attack for this protocol. Then, we improve the Zhu *et al.*'s Protocol to overcome this security drawback.

4.1 TRACEABILITY ATTACK

The communication between the tag and reader occurs over an insecure channel. Thus, adversaries can eavesdrop on this channel and save it. In traceability attack, the adversary can recognize either readers or tags which he or she has already seen. In other words, if the adversary can find the goal between two tags or readers with the probability of greater than half, he or she is successful traceability attack. We analyze the Zhu *et al.*'s protocol through traceability attack. This attack consists of the following phases:

Phase1 (Learning):
Adversary eavesdrop one successful run of the protocol and stores transferred the messages between the reader and the tag include (t_{sys}, r_{sys}).

Phase 2 (Traceability):
To trace the legitimate tag, the adversary waits after phase 1 upon recived the reader requests from the tag, the tag upon receives the request, it replies to the reader with r_{tag} and h_1. Now, we suppose that the adversary chooses a new (t_{sys}, r_{sys}) and sends to the tag. According to step one of the protocol, the tag responds with a new h_1 as h_1' and a new r_{tag} as r_{tag}'. In this phase the details are as follows:

1) The adversary chooses $(t_{Adv} > t_{sys}, r_{Adv} = r_{sys})$ and sends to the tag.
2) The tag receives the message and does as follows:
   a) Generates new r_{tag} as r_{tag}',
   b) Computes new h_1 as h_1' ,
   c) Sends r_{tag}' and h_1' to the adversary as the reader.
3) The adversary resends the same pair $(t_{Adv}, r_{Adv} = r_{sys})$ to the tag.
4) The tag responses to the adversary according to the step 2 of the protocol.
5) The adversary again receives a new h_1 as h_1'', and there are two cases :
   a) $If\ t_{Adv} > t_{sys} > t_{tag},\ then\ h_1'' = H_K(0, t_{sys}, r_{sys}) = h_1 = h_1'$
   b) $If\ t_{sys} < t_{Adv} \leq t_{tag},\ then\ h_1 = h_1' = H_K(1, r_{tag}, r_{sys}) \neq H_K(1, r_{tag}', r_{sys}) = h_1''$.
      i) The adversary returns to the step (5-a)as follows:
      ii) Chooses $r_{Adv} = r_{sys}$ and increases $t_{Adv} > t_{sys}$,
      iii) Sends twice $(t_{Adv}, r_{Adv} = r_{sys})$ to the tag and the tag responds with new h_1 and r_{tag}.
6) If $h_1' = h_1''$, the adversary is succeed to trace the tag. Otherwise, go to step 1 and chooses a new $t_{Adv}' > t_{Adv}$.

As above mentioned, the adversary can trace the tag with only two runs of the protocol.

4.2 IMPROVEMENT OF ZHU *ET AL.*'S PROTOCOL

As we mentioned in the above, in the Zhu *et al.*'s protocol if the adversary sends several values of $(t_{Adv}, r_{Adv} = r_{sys})$ to the tag, she can trace the tag. We can overcome this weakness with a few modifications in the Zhu *et al.*'s protocol. To provide untraceability, we improve the Zhu *et al.*'s protocol slightly in step 2. We suggest that through the calculating h_1, the tag should use a random term in. Our improvement is as follows:

1) Reader broadcasts: $(t_{sys}, r_{sys}) \rightarrow Tag$

2) $Tag \rightarrow Reader$: $\begin{cases} if\ t_{sys} > t_{tag}\ ,\ h_1 = H_K(0, t_{sys}, r_{tag})\ ,\ r_{tag} \\ if\ t_{sys} \leq t_{tag}\ ,\ h_1 = H_K(1, r_{tag}, r_{sys})\ ,\ r_{tag} \end{cases}$

The rest of the protocol is the same as the Zhu *et al.*'s protocol [1].

Since , in step 2of th improved protocol the response of the tag depends on a random variable, the adversary cannot trace the tag.

As just mentioned, for the proposed improvement on the Zhu *et al.*'s Protocol the modification is minor. Thus the performance and efficiency of the improved protocol is the same as the Zhu *et al.*'s protocol.

4.3 SECURITY ANALYSIS OF THE IMPROVED PROTOCOL

1. Mutual authentication: it is trivial that the proposed protocol satisfies this property.
2. Untraceability/Anonymous: our protocol uses an increasing timestamps and updates keyed hash to provide tracking-resistance. Even if the adversary can sends the same value several times to the tag, then it is unable to obtain any information from key and cannot distinguish between two tags. Therefore, the adversary cannot trace the tag, since the value of h_1 is dependent on the random r_{tag} in any run of the protocol.
3. Replay attack: all variables used in the protocol are different, thus the adversary cannot mount replay attack.
4. Forward security: In every round of the protocol the secret key is updated by a one-way hash function $K = H(K)$. Thus, the adversary cannot reveal any information about the tag.
5. De-synchronization attack: an adversary can intercept the message in step 5 of the protocol such that h_2 is not received by the tag, and then the tag's secret key is not updated, whereas the key in the server is updated. Therefor the legitimate tag next time would not pass the authentication and de-synchronization is happened. This problem is resolved in step 4 of the protocol.

Table 2 shows the efficiency and securitycomparison of the improved protocol and other related protocols.

Table 2: Compare efficiency and Security of several protocols

Protocols / Properties	Ts udik[4]	Chatm on *et al.*[6]	He *et al.*[5]	Zhu *et al.*[1]	Our protocol
Anonymity	√	×	×	×	√
Mutual Authentication	×	√	√	√	√
DoS Resistance	×	√	√	√	√
Replay Resistance	×	√	√	√	√
Forward security	×	×	√	√	√
De-syn. Resistance	-	-	√	√	√
Server complexity	$O(n)$	$O(n)$	$(N_T - N_D + 1)O(n)$	$O(n)$	$O(n)$
Tag complexity	1	2	3	3	3
Tag storge	t_{tag}, K	t_{tag}, r_{tag}, K	t_{tag}, r_{tag}, K, N_T	t_{tag}, r_{tag}, K	t_{tag}, r_{tag}, K

5. BAN LOGIC

Any authentication the protocol is based on the exchanging of message between participants A and B. If a protocol ‘s security passes a formal security analysis based on a logic method, it gives an extra about the protocol functionality. A logical calculation based on an agreed set of deduction rules about authentication protocols is called logical authentication. Logical methods provide at least three advantages which are correctness, efficiency and applicability respectively. An important logical method to verify the security of a protocol was introduced by Burrows, Abadi and Needham [10], called BAN logic method. The basis of BAN logic is the belief. Formalization of every protocol using the BAN logic method includes three phases: assuming goals as formulas with symbolic notation, transforming the protocol into symbolic notation and applying a set of deduction rules.

Some of concepts that are used in BAN logic are as follows:

- Belief, when an agent or principal is persuaded of the truth of a formula, means that the principal believes it. For example, if the principal be P and formula be X, we write "P believes X" and show with symbols "P |≡ X ".
- Sees, the principal P receives a message X which is encrypted. Since P can decrypt this message, thus P can to extract X from the message. The term "sees" means that observe only formula. If the principal be P and formula be X, we write "P sees X" and show with symbols "P ◅ X".
- Said, when principal P have sent a message containing X, we write "P said X" and show with symbols "P |~ X ".
- Controls, when the principal P has jurisdiction over X, we write "P controls X" and show with symbols "P |⇒ X ".
- Fresh, if message X has not been sent in previous message before the current run of the protocol. This is concept of nonce, that is, the X generated for the purpose of being fresh. It writes "Fresh(x)" and shows with symbol "#(X)".
- Shared key, if two principals P and Q use the shared secret key K to communicate and show with symbols "P←K→Q ".
- Encrypted X, the formula X is encrypted under the key k. and show with symbols "{X}K ".

In order to analysis the protocol using BAN logic method, at the first the protocol should be written in the language of BAN logic, this step called idealized. Next one should write assumptions about the initial state. The third step is postulate and deductions rules and lastly interprets the statements.

5.1 CORRECTNESS PROOF BY BAN LOGIC METHOD

Without loss of generality, the reader and the server of the protocol can be assumed unique. So, the proposed protocol is idealized as Figure 2:

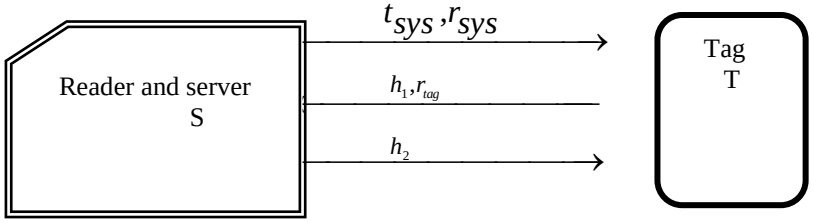

Figure 2: the simplified protocol

a)General type of protocol

Message 1: S $\xrightarrow{t_{sys}, r_{sys}}$ T

Message 2: T $\xrightarrow{h_1, r_{tag}}$ S , Message 3: S $\xrightarrow{h_2}$ T

b)Idealized protocol

Message 2: T $\longrightarrow$ S: r_{tag} , $H(T \xleftrightarrow{K} S, t_{sys}, r_{tag}, r_{sys})$

Message 3: S $\longrightarrow$ T: $H(T \xleftrightarrow{K} S, t_{sys}, r_{tag})$

c) Initial Assumptions:

In this protocol, the tag and the server have shared a secret key in each round. In any round of the protocol the key is updated, thus the key is fresh. The initial assumptions are as follows:

$A_1.\ H_K(X) \in T$ $A_2.\ H_K(X) \in S$

$A_3.\ T \mid\equiv \#(r_{tag})$ $A_4.\ S \mid\equiv \#(t_{sys}, r_{sys})$

$A_5.\ T \mid\equiv \#(K)$ $A_6.\ S \mid\equiv \#(K)$

$A_7.\ T \mid\equiv T \xleftrightarrow{K} S$ $A_8.\ S \mid\equiv T \xleftrightarrow{K} S$

The goals of the protocol:

$S \mid\equiv T \mid\sim \#(T \xleftrightarrow{K} B)$ *and* $T \mid\equiv S \mid\sim \#(T \xleftrightarrow{K} B)$

Verification:

From the message 2: $S \triangleleft H(T \xleftrightarrow{K} S, r_{tag})$, therefore, we have: $S \mid\equiv T \xleftrightarrow{K} S$

According to the message interpretation rule:

$P \mid\equiv Q \xleftrightarrow{K} P,\ P \triangleleft \langle X \rangle_K \Rightarrow P \mid\equiv Q \mid\sim X$

We can deduce: $S \mid\equiv T \xleftrightarrow{K} S, S \triangleleft H(T \xleftrightarrow{K} S, r_{tag}) \Rightarrow S \mid\equiv T \mid\sim r_{tag}$

Using the hash rule:

$P \mid\equiv Q \mid\sim H(X_1, X_2, ..., X_n)\ P \triangleleft X_1, ..., P \triangleleft X_n \Rightarrow P \mid\equiv Q \sim (X_1, X_2, ..., X_n)$

Server can see: $S \triangleleft t_{sys}, S \triangleleft r_{sys}, S \triangleleft r_{tag}, S \triangleleft (T \xleftrightarrow{K} S)$

$S \mid\equiv T \mid\square H(T \xleftrightarrow{K} S, t_{sys}, r_{tag}, r_{sys}),\ S \triangleleft t_{sys}, S \triangleleft r_{sys}, S \triangleleft r_{tag}, S \triangleleft (T \xleftrightarrow{K} S)$

$\Rightarrow S \mid\equiv T \mid\square (T \xleftrightarrow{K} S, t_{sys}, r_{tag}, r_{sys}) \Rightarrow S \mid\equiv T \mid\sim (T \xleftrightarrow{K} S)$ (1)

We can deduce from the assumption that:

$S \mid\equiv \left(S \xleftrightarrow{K} T\right)$ **(2)**

From (1) and (2), we can deduce the first goal of the protocol:

$S \mid\equiv T \mid\sim \#(T \xleftrightarrow{K} S)$

For the second goal of the protocol:

$T \triangleleft H(T \xleftrightarrow{K} S)$ *and* $T \mid\equiv (T \xleftrightarrow{K} S)$

According to the interpretation rule:

$S \mid\equiv T \xleftrightarrow{K} S, S \triangleleft H(T \xleftrightarrow{K} S, r_{tag}) \Rightarrow S \mid\equiv T \mid\sim (r_{tag})$

We can deduce that:

$T \mid\equiv S \mid\sim H(T \xleftrightarrow{K} S)\ , T \triangleleft (t_{sys}, r_{sys}, r_{tag}, T \xleftrightarrow{K} S) \Rightarrow T \mid\equiv S \mid\sim (T \xleftrightarrow{K} S)$ (3)

From the assumption:

$T \mid\equiv \#(k)$

Given the freshness rules, we can deduce:

$T \mid\equiv S \mid\sim \#(T \xleftrightarrow{K} S)$

Therefore, the second goal has been proved.

6. CONCLUSION

In this paper, we analyzed the security of an RFID authentication protocol proposed by Zhu et al [1]. Our analysis is a passive attack which can trace a legitimate tag. The cost of this attack is only eavesdropping one session of the protocol. In addition, we proposed a suitable solution to overcome this threat. In this solution, we improved Zhu *et al.*'s protocol by a little modification on the original protocol. The improved protocol provides the desired security against the attacks on the context. More precisely, the security analysis was

shown that the improved protocol provides mutual authentication, untraceability/anonymity. Finally, we verified the security of the protocol formally based on BAN logic method.

ACKNOWLEDGEMENTS
We would like to thank anonymous reviewers for useful comments that helped in improving the paper.

REFERENCES

[1] Zhu, H., Zhao, Y., Ding, S., & Jin, B " An Improved Forward-Secure Anonymous RFID Authentication Protocol." In *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on* (pp. 1-5). IEEE
[2] Jules.A." Rfid security and privacy: a research survey" *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381–394, 2006
[3] Ouafi, K. "Security and Privacy in RFID Systems." PhD diss., ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, 2012.
[4] Mukherjee, S., Hasan, M., Chowdhury, B., & Chowdhury, M." Security of RFID systems-a hybrid approach" *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2011 12th ACIS International Conference on*. IEEE, 2011.
[5] Sarma, S., Weis, S., & Engels,D. . "RFID systems and security and privacy implications." *Cryptographic Hardware and Embedded Systems-CHES 2002* (2003): 1-19.
[6] Avoine, G. "Privacy challenges in RFID." *Data Privacy Management and Autonomous Spontaneus Security* (2012): 1-8.
[7] Shao-hui, W., Sujuan, L., & Danwei, C. "Efficient Passive Full-disclosure Attack on RFID Light-weight Authentication Protocols LMAP++ and SUAP. " TELKOMNIKA Indonesian Journal of Electrical Engineering, 10(6), 1458-1464, 2012.
[8] Deng, M., & Zhu, W. "Desynchronization Attacks on RFID Security Protocols. " TELKOMNIKA Indonesian Journal of Electrical Engineering, 11(2), 2013.
[9] *Tsudik, G. "Ya-trap: Yet another trivial rfid authentication protocol," in PerCom Workshops, 2006, pp. 640–643.*
[10] C. Chatmon, T. van Le, and M. Burmester, "Secure anonymous rfid authentication protocols," Computer & Information Sciences, Florida *A*& M University, Tech. Rep., 2006
[11] L. He, S. Jin, T. Zhang, and N. Li, "An enhanced 2-pass optimistic anonymous rfid authentication protocol with forward security," in *WiCOM2009,pp.1-4,*
[12] Burrows, M.; Abadi, M. and Needham,R., "A logic of authentication," ACM Transactions on Computer Systems, 1990.

Mahdi Azizi received his M.S. degree in Communications, Cryptology &Information Security in 2005. Currently, he is a Ph.D. candidate at the Department of Information and Communication Technology I.H University, Tehran, Iran. His research interests include RFID security, authentication protocols and Cryptanalysis.

Abdolrasoul Mirghadri received the B.Sc., M.Sc. and Ph.D degrees in Mathematical Statistics, from the faculty of Science, Shiraz Universityin 1986, 1989 and 2001, respectively. He is an associate professor at the faculty and research center of communication and information technology, IHU, Tehran, Iran since 1989. His researchinterest includes: Cryptography, Statistics and Stochastic Processes.He is a member of ISC, ISS and IMS

Nasour Bagheri is an assistant professor at Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran. He is the author of about 15 articles in information security and cryptology. Homepage of the author is available at: http://n-bagheri.srttu.ir/