Passive Secret Disclosure Attack on an Ultralightweight Authentication Protocol for Internet of Things

Masoumeh Safkhani[1], Nasour Bagheri[2]

[1] Computer Engineering Department, Shahid Rajaee Teacher Training University, Iran, Safkhani@srttu.edu
[2] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Iran, NBagheri@srttu.edu

Abstract. Recently, Tewari and Gupta have proposed an ultralightweight RFID authentication protocol [13]. In this paper, we consider the security of the proposed protocol and present a passive secret disclosure attack against it. The success probability of the attack is '1' while the complexity of the attack is only eavesdropping one session of the protocol. The presented attack has negligible complexity. We simulated our attack and verified its correctness.

keywords: RFID, Secret Disclosure, Authentication, Internet of Things

1 Introduction

Internet of Things (IoT) is an architecture to connect several devices to Internet to manage them or provide different services over them, *e.g.* to authenticate devises through a cloud server. In many IoT architectures, RFID tags are an essential part of them, where they are attached to an object to identify them. To identify an object in a secure way, we need a secure authentication protocol. However, most of those tags are passive and standard authentication protocols, based on asymmetric crypto-systems such as RSA [12] or symmetric crypto-systems such as AES [7], may not be applicable. On the other hand, employing a protocol that does not provide enough security will compromise the user's privacy. To address this emergence, several protocols have already been proposed in literature. Among them a type of protocols, that is called *ultralightweight* protocols, are sounds to be more suitable for passive tags. An *ultralightweight* protocol generally uses a few bitwise operations while computes the messages that are transfered over the protocol. Designing such protocols have a long history on RFID literature, *e.g.* Gossamer [10], SASI [6] and RAPP [14]) are just examples. However, despite of these attempts, past studies such as [1–5,8,9,11] show that it may not be possible to design a secure authentication protocol without employing a secure cryptographic primitive. On the other hand, very recently Tewari and Gupta [13] proposed another ultralightweight authentication protocol to be employed in IoT. The designers have compared the security of their protocol with several other ultralightweight authentication protocols such as Gossamer, SASI and RAPP and claimed that their protocol is secure against desynchronization, secret disclosure and traceability attacks [13, Table 1, Page 15].

In this paper, we study the security of this protocol and show that, similar to other ultralightweight protocols, this protocol also does not provide desired security against the mentioned attacks. More precisely, we present a very efficient passive attack that retrieves all secret parameters of the tag by only eavesdropping a session of protocol between the target tag and the legitimate reader. The computational complexity of the attack is negligible and can be executed in a fraction of second (we verified our attack by implementing it on simulation). Our attack ruined any security claim.

1.1 Paper Organization

Tewari and Gupta authentication protocol is described in Section 2. In Section 3, we show how an adversary can disclose all the secrets of the protocol only by one session of protocol eavesdropping. Finally, we conclude the paper in Section 4.

2 Tewari and Gupta Authentication Protocol

Throughout the paper we use the notations represented in Table 1, which are similar to the notations used by Tewari and Gupta [13].

The Tewari and Gupta ultralightwight authentication protocol, as depicted in Fig.1, runs as below:

1. The reader starts the protocol and sends "*hello*" message to the tag.
2. The tag once received the message, sends its old and new pseudonyms to the reader, *i.e.* (IDS_{new}, IDS_{old}).
3. Upon receipt of the message, the reader searches its database based on received IDS_{old} and IDS_{new}. If the reader does not find any match, stops the protocol, otherwise it:
   - Assuming the tag records in the reader side are (IDS_{new}, IDS_{old}) and (K_{new}, K_{old}), if $IDS'_{new} = IDS_{new}$ and $IDS'_{old} = IDS_{old}$ then IDS_{new} and K_{new} are used through calculations;

Table 1. Notations used in this paper

Symbol	Description
R	An RFID reader
T	An RFID tag
K	The secret key of tag which is shared between the tag and the reader
IDS_{old}, IDS_{new}	The last and current pseudonyms of the tag
m, n	96-bit random numbers generated by the reader
$Rot(X,Y)$	The left-rotation of X by the hamming weight of Y ($wt(Y)$)
$\oplus$	The exclusive or operation
$B \rightarrow A$	Assign B value to A
$X \ggg Y$	The right-rotation of X, Y times

- generates two 96-bit random numbers m and n;
- calculates P, Q and R as below:
  - $P = IDS \oplus m \oplus n$;
  - $Q = K \oplus n$;
  - $R = Rot(Rot(K \oplus n, IDS), K \oplus m)$;
- and sends (P, Q, R) to the tag.

4. Once reception of the message, the tag:
   - extracts n as $Q \oplus K$ and m as $P \oplus IDS \oplus n$;
   - calculates $R' = Rot(Rot(K \oplus n, IDS), K \oplus m)$. If $R' = R$, it authenticates the reader otherwise it stops the protocol. If the reader has been authenticated, the tag:
     - calculates $S = Rot(Rot(IDS \oplus m, K), R' \oplus n)$;
     - sends S to the reader and goes to updating phase.
5. The reader once received the message, calculate $S' = Rot(Rot(IDS \oplus m, K), R \oplus n)$ with its local values and if $S' = S$ then the reader successfully authenticates the tag and goes to updating phase.
6. In the updating phase, the tag and the reader both update their IDS_{old}, K_{old}, IDS_{new} and K_{new} as below:
   - $IDS_{old} = IDS_{new}$
   - $K_{old} = K_{new}$
   - $IDS_{new} = Rot(Rot(IDS \oplus n, K \oplus n), IDS \oplus m)$;
   - $K_{new} = Rot(R \oplus n, IDS \oplus m)$;

It should be noted the protocol includes a process to synchronize the tag and the reader records of IDS and K, if the reader has not updated its records of the tag in the last session successfully. However, it has no effect

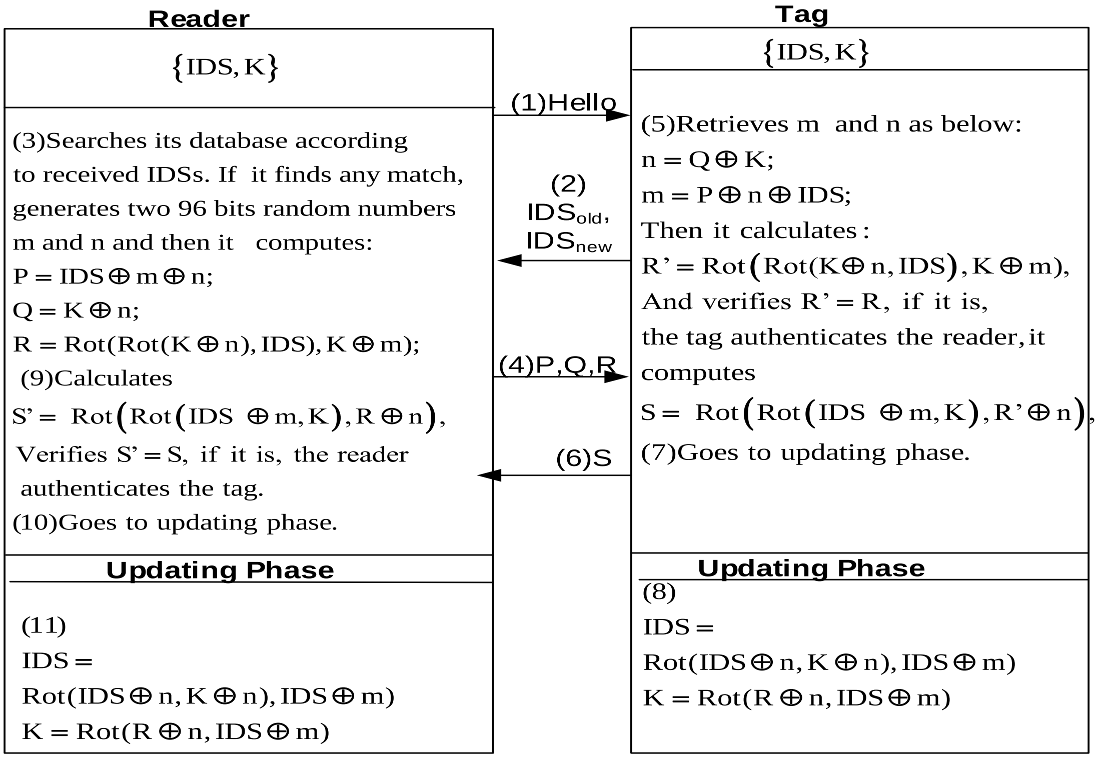
Reader
{IDS, K}
Tag
{IDS, K}
(1)Hello
(2) IDSold, IDSnew
(4)P,Q,R
(6)S
(3)Searches its database according to received IDSs. If it finds any match, generates two 96 bits random numbers m and n and then it computes:
P = IDS ⊕ m ⊕ n;
Q = K ⊕ n;
R = Rot(Rot(K ⊕ n), IDS), K ⊕ m);
(9)Calculates
S' = Rot(Rot(IDS ⊕ m, K), R ⊕ n),
Verifies S' = S, if it is, the reader authenticates the tag.
(10)Goes to updating phase.
(5)Retrieves m and n as below:
n = Q ⊕ K;
m = P ⊕ n ⊕ IDS;
Then it calculates:
R' = Rot(Rot(K ⊕ n, IDS), K ⊕ m),
And verifies R' = R, if it is, the tag authenticates the reader, it computes
S = Rot(Rot(IDS ⊕ m, K), R' ⊕ n),
(7)Goes to updating phase.
Updating Phase
(11)
IDS =
Rot(IDS ⊕ n, K ⊕ n), IDS ⊕ m)
K = Rot(R ⊕ n, IDS ⊕ m)
Updating Phase
(8)
IDS =
Rot(IDS ⊕ n, K ⊕ n), IDS ⊕ m)
K = Rot(R ⊕ n, IDS ⊕ m)

Fig. 1. The Tewari and Gupta ultralightweight authentication protocol [13]

on our attack because we will disclose all secret parameters. Hence, we presented the protocol procedure when the synchronization between the tag and the server remains unbroken.

3 Secret Disclosure Attack against Tewari and Gupta Protocol

Adversary Model : The attacker in this paper is a passive adversary who is able to only eavesdrop the ongoing reader-tag message exchanged without been detected.

Attack Procedure : Tewari and Gupta [13] claim that their protocol is resistant against all known active and passive attacks, including secret disclosure attack. However, we present a rather simple passive attack which can disclose all secrets of the protocol as follows:

1. (**Phase 1**:Learning Phase:) In this phase of the attack, the adversary eavesdrops one session of the protocol and stores the exchanged messages of the protocol including IDS_{old}, IDS_{new}, P, Q, R and S.
2. (**Phase 2**:Passive Secret Disclosure Attack:)
   In this phase of the attack, the adversary by using values which eavesdropped in the previous phase, can disclose all secrets of the protocol as bellow:
   (a) for $i = 0, ..., L$, the adversary does:
      - $S \ggg i \to x$;
      - $IDS \oplus x \to m$;
      - $P \oplus m \oplus IDS \to n$;
      - $Q \oplus n \to K$;
      - If $Rot(Rot(K \oplus n, IDS), K \oplus m) = R$:
         - $IDS \to IDS_{old}$
         - $K \to K_{old}$
         - $Rot(Rot(IDS \oplus n, K \oplus n), IDS \oplus m) \to IDS_{new}$;
         - $Rot(R \oplus n, IDS \oplus m) \to K_{new}$;
         - returns IDS_{old}, IDS_{new}, K_{old}, K_{new}, n and m.

So, the attacker can disclose all secrets of the protocol only by eavesdropping one session of the protocol and doing the above offline operations which its related code can be executed in a fraction of second in any ordinary personal computer. Given this secret disclosure attack, any other attack such as impersonation attack, desynchronization attack or traceability attack would be trivial.

3.1 Implementation Results

We implemented the proposed attack using C++ to verify the correctness of the proposed procedure. For example, for $L = 32$, which means that all parameters are 32-bit variables, consider the following parameters:

```
IDS=0x13579bdf;
K  =0x2468ace0;
n  =0x12345678;
m  =0x9abcdef0 ;
```

Then the transfered messages that are eavesdropped by the adversary are as follows:

```
Q=K⊕n=0x365cfa98;
P=IDS⊕m⊕n=0x9bdf1357;
```

```
R=Rot(Rot(K⊕n, IDS), K⊕m)=0xb2e7d4c1;
S=Rot(Rot(IDS⊕m,K), R⊕n)=0xbe27ad14;
```

Now, when we apply our attack, for $i = 26$ we have:

```
-  S⋙i=0x89eb452f→x;
-  IDS⊕x=0x13579bdf⊕0x89eb452f=0x9abcdef0→m;
-  P⊕m⊕IDS =0x9bdf1357⊕0x9abcdef0⊕0x13579bdf=0x12345678→n;
-  Q⊕n=0x365cfa98⊕0x12345678=0x2468ace0→K;
-  Since:Rot(Rot(K⊕n,IDS),K⊕m)=
Rot(Rot(0x365cfa98,0x13579bdf),0xbed47210)=0xb2e7d4c1=R:
+   IDS=0x13579bdf→IDS_old;
+   K=0x2468ace0→K_old;
+   Rot(Rot(IDS⊕n,K⊕n),IDS⊕m)=0x058f369c→IDS_new;
+   Rot(R⊕n,IDS⊕m)=0x057341a7→K_new;
+   returns 0x13579bdf,0x0b1e6d38,0x2468ace0,
0x058f369c,0x12345678 and 0x057341a7 as
IDS_old,IDS_new,K_old,K_new,n and m.
```

It is clear that all parameters have been extracted correctly which confirms the correctness of our attack.

4 Conclusion

In this paper, we analyzed the security of an ultralightweight authentication protocol, which had been recently proposed by Tewari and Gupta [13]. We present a passive secret disclosure attack, for which the success probability is '1' and the complexity is only eavesdropping a session of the protocol.

Acknowledgment: The authors would like to thank the anonymous reviewers for their suggestions to improve the content and presentation of this paper.

References

1. Z. Ahmadian, M. Salmasizadeh, and M. R. Aref. Desynchronization attack on RAPP ultralightweight authentication protocol. *Inf. Process. Lett.*, 113(7):205–209, 2013.
2. Z. Ahmadian, M. Salmasizadeh, and M. R. Aref. Recursive linear and differential cryptanalysis of ultralightweight authentication protocols. *IEEE Transactions on Information Forensics and Security*, 8(7):1140–1151, 2013.
3. G. Avoine and X. Carpent. Yet another ultralightweight authentication protocol that is broken. In *Workshop on s Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.

4. G. Avoine, X. Carpent, and B. Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *J. Network and Computer Applications*, 35(2):826–843, 2012.
5. N. Bagheri, M. Safkhani, P. Peris-Lopez, and J. E. Tapiador. Weaknesses in a new ultralightweight RFID authentication protocol with permutation - RAPP. *Security and Communication Networks*, 7(6):945–949, 2014.
6. H.-Y. Chien. Sasi: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Trans. Dependable Sec. Comput.*, 4(4):337–340, 2007.
7. J. Daemen and V. Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.
8. P. D'Arco and A. D. Santis. Weaknesses in a recent ultra-lightweight RFID authentication protocol. In S. Vaudenay, editor, *AFRICACRYPT*, volume 5023 of *Lecture Notes in Computer Science*, pages 27–39. Springer, 2008.
9. P. D'Arco and A. D. Santis. On ultralightweight RFID authentication protocols. *IEEE Trans. Dependable Sec. Comput.*, 8(4):548–563, 2011.
10. P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In *WISA*, pages 56–68, 2008.
11. R. C.-W. Phan. Cryptanalysis of a new ultralightweight RFID authentication protocol - sasi. *IEEE Transactions on Dependable and Secure Computing*, 6(4):316–320, 2009.
12. R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978.
13. A. Tewari and B. B. Gupta. Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for iot devices using rfid tags. *The Journal of Supercomputing*, pages 1–18, 2016.
14. Y. Tian, G. Chen, and J. Li. A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, 16(5):702–705, 2012.