


Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things

Masoumeh Safkhani¹ · Nasour Bagheri² 

Published online: 17 January 2017

© Springer Science+Business Media New York 2017

Abstract Internet of Things (IoT) is a technology in which for any object the ability to send data via communications networks is provided. Ensuring the security of Internet services and applications is an important factor in attracting users to use this platform. In the other words, if people are unable to trust that the equipment and information will be reasonably safe against damage, abuse and the other security threats, this lack of trust leads to a reduction in the use of IoT-based applications. Recently, Tewari and Gupta (J Supercomput 1–18, 2016) have proposed an ultralightweight RFID authentication protocol to provide desired security for objects in IoT. 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 verify the correctness of the presented attack by simulation.

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 devices

✉ Nasour Bagheri
NBagheri@srutu.edu
Masoumeh Safkhani
Safkhani@srutu.edu

¹ Computer Engineering Department, Shahid Rajaei Teacher Training University, Tehran 16788-15811, Iran

² Electrical Engineering Department, Shahid Rajaei Teacher Training University, Tehran 16788-15811, Iran

through a cloud server. All computers and also all objects of various elements tend to enter cyberspace and exchange information with each other and this could threaten their security and privacy. Hence, one of the important conditions to the things entrance to the world of the Internet is providing security. Some of the modern cryptographic solutions for providing cyberspace security have been expressed in [13]. In many IoT architectures, RFID tags are an essential part of them, where they are attached to an object to identify it. 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 cryptosystems such as RSA [17] or symmetric cryptosystems such as AES [9], 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 the literature [3, 12, 16]. Among them a type of protocols, that is called *ultralightweight* protocols, are sound to be more suitable for passive tags. An *ultralightweight* protocol generally uses a few bitwise operations while computes the messages that are transferred over the protocol. Designing such protocols have a long history on RFID literature, e.g., Gossamer [14], SASI [8] and RAPP [21]) are just examples. Despite these attempts, past studies such as [1, 2, 4, 5, 7, 10, 11, 15] 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 [20] 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 [20, 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

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

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 verify our attack by simulation). Our attack ruined any security claim.

1.1 Paper organization

Tewari and Gupta authentication protocol is described in Sect. 2. In Sect. 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 Sect. 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 [20].

The Tewari and Gupta ultralightweight authentication protocol, as depicted in Fig. 1, works as given 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}) .

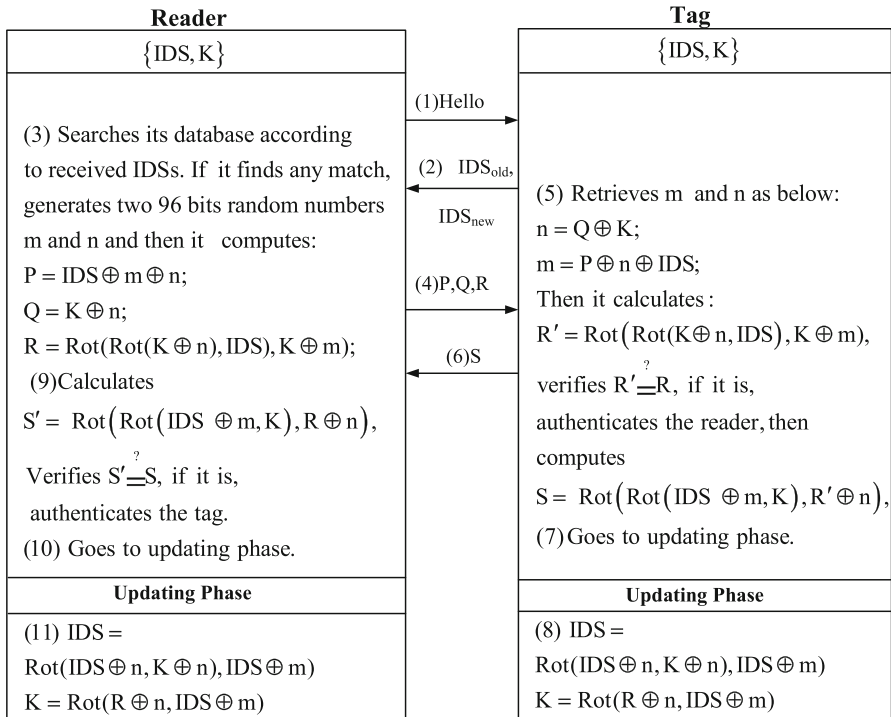


Fig. 1 Tewari and Gupta ultralightweight authentication protocol [20]

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;
 - 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 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 [20] 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 has been eavesdropped in the previous phase, can disclose all secrets of the protocol as bellow:

- (a) for $i = 0, \dots, L$, the adversary does:
- $S \ggg i \rightarrow x$;
 - $IDS \oplus x \rightarrow m$;
 - $P \oplus m \oplus IDS \rightarrow n$;
 - $Q \oplus n \rightarrow K$;
 - If $Rot(Rot(K \oplus n, IDS), K \oplus m) = R$:
 - $IDS \rightarrow IDS_{old}$
 - $K \rightarrow K_{old}$
 - $Rot(Rot(IDS \oplus n, K \oplus n), IDS \oplus m) \rightarrow IDS_{new}$;
 - $Rot(R \oplus n, IDS \oplus m) \rightarrow K_{new}$;
 - 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 [6]. 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 transferred 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:

- $S \ggg i = 0x89eb452f \rightarrow x$;
- $IDS \oplus x = 0x13579bdf \oplus 0x89eb452f = 0x9abcdef0 \rightarrow m$;
- $P \oplus m \oplus IDS = 0x9bdf1357 \oplus 0x9abcdef0 \oplus 0x13579$

```

      bdf=0x12345678→n;
-   Q⊕n=0x365cfa98⊕0x12345678=0x2468ace0→K;
-   Since:Rot(Rot(K⊕n,IDS),K⊕m)=
      Rot(Rot(0x365cfa98,0x13579bdf),0xbcd4
      7210)=0xb2e7d4c1=R:
+   IDS=0x13579bdf→IDSold;
+   K=0x2468ace0→Kold;
+   Rot(Rot(IDS⊕n,K⊕n),IDS⊕m)=0x058f369
      c→IDSnew;
+   Rot(R⊕n,IDS⊕m)=0x057341a7→Knew;
+   returns 0x13579bdf, 0x0b1e6d38,
      0x2468ace0,
      0x058f369c, 0x12345678 and 0x9a
      bcdef0 as
      IDSold, IDSnew, Kold, Knew, n and m,
      respectively.

```

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 [20]. 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.

The results of this paper, along with other recent papers on the security of IoT devices such as [18, 19], clarify this fact that we have not met all security desired for protocols related to these devices and it needs more efforts to address them. Hence, we would like to quote the last sentence of the conclusion of [18] as the last sentence of this paper's conclusion:

We should work together to use the knowledge we gained to protect IoT devices or we might face in the near future large scale attacks that will affect every part of our lives.

Acknowledgements The authors would like to thank the anonymous reviewers for their suggestions to improve the content and presentation of this paper. This work was supported by Shahid Rajaei Teacher Training University under contract number 27770.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Desynchronization attack on RAPP ultralightweight authentication protocol. *Inf Process Lett* 113(7):205–209

2. Ahmadian Z, Salmasizadeh M, Aref MR (2013) Recursive linear and differential cryptanalysis of ultralightweight authentication protocols. *IEEE Trans Inf Forensics Secur* 8(7):1140–1151
3. An R, Feng H, Liu Q, Li L (2017) Three elliptic curve cryptography-based RFID authentication protocols for Internet of Things. Springer, Berlin, pp 857–878
4. Avoine G, Carpent X (2012) Yet another ultralightweight authentication protocol that is broken. In: *Workshop on s Security—RFIDSec'12*, Nijmegen
5. Avoine G, Carpent X, Martin B (2012) Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *J Netw Comput Appl* 35(2):826–843
6. Bagheri N, Safkhani M (2017) Attack on Tewari and Gupta protocol code repository. <https://github.com/nbagheri/Attack-on-Tewari-and-Gupta-protocol>
7. Bagheri N, Safkhani M, Peris-Lopez P, Tapiador JE (2014) Weaknesses in a new ultralightweight RFID authentication protocol with permutation—RAPP. *Secur Commun Netw* 7(6):945–949
8. Chien H-Y (2007) Sasi: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Trans Dependable Secur Comput* 4(4):337–340
9. Daemen J, Rijmen V (2002) The design of Rijndael: AES—the advanced encryption standard. *Information Security and Cryptography*. Springer, Berlin
10. D'Arco P, Santis AD (2008) Weaknesses in a recent ultra-lightweight RFID authentication protocol. In: Vaudenay S (ed) *AFRICACRYPT Lecture Notes in Computer Science*, vol 5023. Springer, Berlin, pp 27–39
11. D'Arco P, Santis AD (2011) On ultralightweight RFID authentication protocols. *IEEE Trans Dependable Secur Comput* 8(4):548–563
12. Guo P, Wang J, Geng XH, Kim CS, Kim J-U (2014) A variable threshold-value authentication architecture for wireless mesh networks. *J Internet Technol* 15(6):929–935
13. Gupta B, Agrawal DP, Yamaguchi S (eds) (2016) *Handbook of research on modern cryptographic solutions for computer and cyber security*. IGI Global, Hershey
14. Peris-Lopez P, Castro JCH, Estévez-Tapiador JM, Ribagorda A (2008) Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In: *WISA*, pp 56–68
15. Phan RC-W (2009) Cryptanalysis of a new ultralightweight RFID authentication protocol—SASI. *IEEE Trans Dependable Secur Comput* 6(4):316–320
16. Quan Q, Jia Y-L, Zhang R (2016) A lightweight RFID security protocol based on elliptic curve cryptography. *Int J Netw Secur* 18(2):354–361
17. Rivest RL, Shamir A, Adleman LM (1978) A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM* 21(2):120–126
18. Ronen E, O'Flynn C, Shamir A, Weingarten A (2016) IoT goes nuclear: creating a zigbee chain reaction. *IACR Cryptology ePrint Archive* 2016:1047
19. Ronen E, Shamir A (2016) Extended functionality attacks on IoT devices: the case of smart lights. In: *IEEE European Symposium on Security and Privacy, EuroS&P 2016*, Saarbrücken, Germany, 21–24 March 2016, pp 3–12
20. Tewari A, Gupta BB (2016) Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *J Supercomput* 1–18. doi:[10.1007/s11227-016-1849-x](https://doi.org/10.1007/s11227-016-1849-x)
21. Tian Y, Chen G, Li J (2012) A new ultralightweight RFID authentication protocol with permutation. *IEEE Commun Lett* 16(5):702–705