On the Security of the Revised SRP^{+} RFID Authentication Protocol

Masoumeh Safkhani[1], Amir Abbasian[2]
1- Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran.
Email:Safkhani@srttu.edu
2- Computer Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran.
Email: A.abbasian@srttu.edu

ABSTRACT: These days, many researchers work on RFID EPC-C1 G2 authentication protocols designing with the use of 16-bit PRNGs. However, thanks to short input/output length of such *PRNG* functions that makes it feasible to convert it, most of such protocols are vulnerable against full secret disclosure attacks. Recently, Moradi *et al.* in [1] analyzed an EPC-C1 G2 authentication protocol named SRP^{+} and presented a revised version of the SRP^{+} protocol. In this paper, we show that unfortunately the revised version of SRP^{+}protocol, same as its predecessor i.e. SRP^{+} protocol, is still vulnerable against full secret disclosure attack. In the presented attack, adversary discloses all secrets of the protocol only by eavesdropping one run of the protocol, impersonating the reader in one run of the protocol and doing only 3×2^{16} off -line *PRNG* function evaluations.

KEYWORDS: RFID, EPC-C1 G2, 16-bit *PRNG* Function, Authentication, Secret Disclosure Attack.

1. INTRODUCTION

Same as all wireless technologies, RFID needs security protocols to provide CIA triangle of security which are confidentiality, integrity and availability. An RFID security protocol is a protocol between three components including tags, readers and back-end database. Passive tags, active tags and semi-active tags are three different types of tags that may be employed in an RFID protocol, and each of them have its related standards.

EPC-C1 G2 [2] is an important standard related to passive tags which recommends using 96-bit EPCs, 16-bit *CRC*s and 16-bit *PRNG*s. Up to now, a lot of EPC-C1 G2 RFID security protocols have been proposed in the related literature, e.g. [3], [4], [5], [6], [7], [8], [9], [10], [11]. However, unfortunately these proposals were not successful in providing their security goals [12], [13], [14], [15], [17]. The lack of such a secure EPC-C1 G2 complaint RFID protocol leads to more attempts to design a secure protocol in the framework of EPC-C1 G2 standard.

Recently, Moradi *et al.* in [1], presented a desynchronization attack and a secret disclosure attack against an EPC-C1 G2 compliant protocol, SRP^{+} [10] protocol. Their proposed desynchronization attack uses toggling only one bit of the transferred random number and their proposed secret disclosure attack costs at most 2^4 CRC evaluations and eavesdropping two consecutive sessions of the protocol. To strengthen SRP^{+} protocol against their attacks, Moradi *et al.* also proposed a revised version of the protocol in the framework of EPC-C1 G2. Designers security claims for the revised version of SRP^{+} is the security against traceability attack, tag impersonation attack, reader impersonation attack, replay attack, secret disclosure attack and other known active and passive attacks. However, in this paper, we show that the revised SRP^{+} protocol, same as its predecessor, i.e. SRP^{+} protocol, is still vulnerable against full secret disclosure attack. It worth to note that the adversary model which is used in this paper is identical to the model used by Moradi *et al.* for security analysis of the SRP^{+} protocol.

The rest of this paper is organized as follows: In Section 2, we give a review of the revised $\boldsymbol{SRP^{+}}$ protocol. Our secret disclosure attack against the revised $\boldsymbol{SRP^{+}}$ protocol is described in Section 3. In Section 4, we present some recommendations to improve the revised $\boldsymbol{SRP^{+}}$ protocol and finally we conclude the paper in Section 5.

Table1: NOTATIONS

Symbol	Description
T_i	The i^{th} RFID tag
R	The RFID reader
EPC_s	The 96-bit electronic product code *EPC* has divided to six parts and XORed with each other to provide 16-bit EPC_s
K_{iold}	The last successful authentication keys
K_{inew}	The new authentication keys
C_{iold} and C_{inew}	The last and current data base indexes
N_1	The reader generated random number
N_2	The tag generated random number
$\oplus$	The exclusive or operation
$PRNG$	A pseudo random number generator
$A \leftarrow B$	Assigning B value to A

تاریخ دریافت : ۱۳۹۵/۰۶/۰۱ تاریخ پذیرش : ۱۳۹۵/۱۰/۲۵

2. REVISED SRP^+ PROTOCOL

In this section, following the notation represented in Table 1, we describe the revised version of SRP^+ protocol [1]. The revised SRP^+ protocol as depicted in Fig. 1 runs as below:

1. The reader generates a random number N_1 and sends it to the tag.
2. When the tag receives N_1, it:
   - generates another random number N_2; computes M_1 and CN_2 as follows:
   - $M_1 = PRNG(C_i \oplus N_1) \oplus PRNG(K_i \oplus N_2)$ $CN_2 = N_2 \oplus C_i \oplus EPC_s$
   - and sends M_1 and CN_2 to the reader.
3. Upon reception, the reader sends M_1, CN_2 and N_1 to the back-end data base.
4. The back-end databases, once receives the message, searches it database to find C_{ix}, K_{ix}, EPC_s where $X \in (old, new)$, and then it:
   a) retrieves N_2 as $N_2 = CN_2 \oplus C_{ix} \oplus EPC_s$
   b) verifies whether $M_1 \stackrel{?}{=} PRNG(C_{ix} \oplus N_1) \oplus PRNG(K_{ix} \oplus N_2)$. In the case of equality, the reader authenticates the tag; otherwise when it reaches the end of the list in its database it sends an error message and stops the protocol.
   c) after successful tag's authentication, the reader computes $M_2 = PRNG(EPC_s \oplus N_2 \oplus K_{ix})$ and updates its records related to the current tag as follows:
   $C_{iold} \leftarrow C_i$
   $C_{inew} \leftarrow PRNG(C_i)$
   $K_{iold} \leftarrow K_i$
   $K_{inew} \leftarrow PRNG(K_i)$
   d) and sends M_2 and D_i to the reader.
5. Upon reception the message, the reader sends M_2 to the back-end data base.
6. Once the tag receives the message, it verifies whether $PRNG(EPC_s \oplus N_2 \oplus K_i) \stackrel{?}{=} M_2$. In the case of equality, the tag authenticates the back-end server and updates its values as below:
   $C_i \leftarrow PRNG(C_i)$
   $K_i \leftarrow PRNG(K_i)$

3. SECRET DISCLOSURE ATTACK AGAINST REVISED SRP^+ PROTOCOL

In this section, we present a secret disclosure attack which can disclose all secrets of the revised $\boldsymbol{SRP^+}$ protocol efficiently. The main observation that we are using in our attack, which has been also used by Moradi *et. al.* [1] to provide secret disclosure attack against SRP^+, is that given $PRNG(X) = Y$, where X and Y are 16-bit values, one can determine the input of *PRNG* function, i.e. X, only by using 2^{16} off-line evaluations of *PRNG* function and comparing the result of *PRNG* function with the given Y. Alternatively, the adversary can create a dictionary of all possible values of X and the related $PRNG(X)$. In this case with the cost of 2^{16} words of memory, for any given Y, finding X such that $PRNG(X) = Y$ costs only a memory access, if there is a value for X such that $PRNG(X) = Y$. Hence, in attack that is presented in this paper, to find X such that $PRNG(X) = Y$, the adversary can either do 2^{16} off-line evaluations of *PRNG* function or already create a dictionary of $PRNG(X) = Y$ and just find the related pre-image of Y in the dictionary.

Our secret disclosure attack, runs as below in two phases:

Phase 1: Learning phase

In this phase of the attack, the adversary:

1) waits until the legal reader starts the protocol and sends N_1 to the tag;
2) eavesdrops the transferred messages including
   $N_1, M_1 = PRNG(C_i \oplus N_1) \oplus PRNG(K_i \oplus N_2)$,
   $CN_2 = N_2 \oplus C_i \oplus EPC_s$ and
   $M_2 = PRNG(EPC_s \oplus N_2 \oplus K_i)$
3) stops the last message of the protocol, where the legal reader sent to the tag the message M_2. So, the tag does not update its secret values including C_i and K_i.
4) impersonates the reader and sends the eavesdropped N_1 to the tag;
5) receives the tag's response including
   $M_1' = PRNG(C_i \oplus N_1) \oplus PRNG(K_i \oplus N_2')$
   and $CN_2' = N_2' \oplus C_i \oplus EPC_s$;
6) and stops the protocol without sending the last message to the tag. So, the tag does not update its secret values including C_i and K_i.

Phase 2: Disclosing the tags secrets

In this phase of the attack, the attacker does offline operations as below:

1) computes following values:

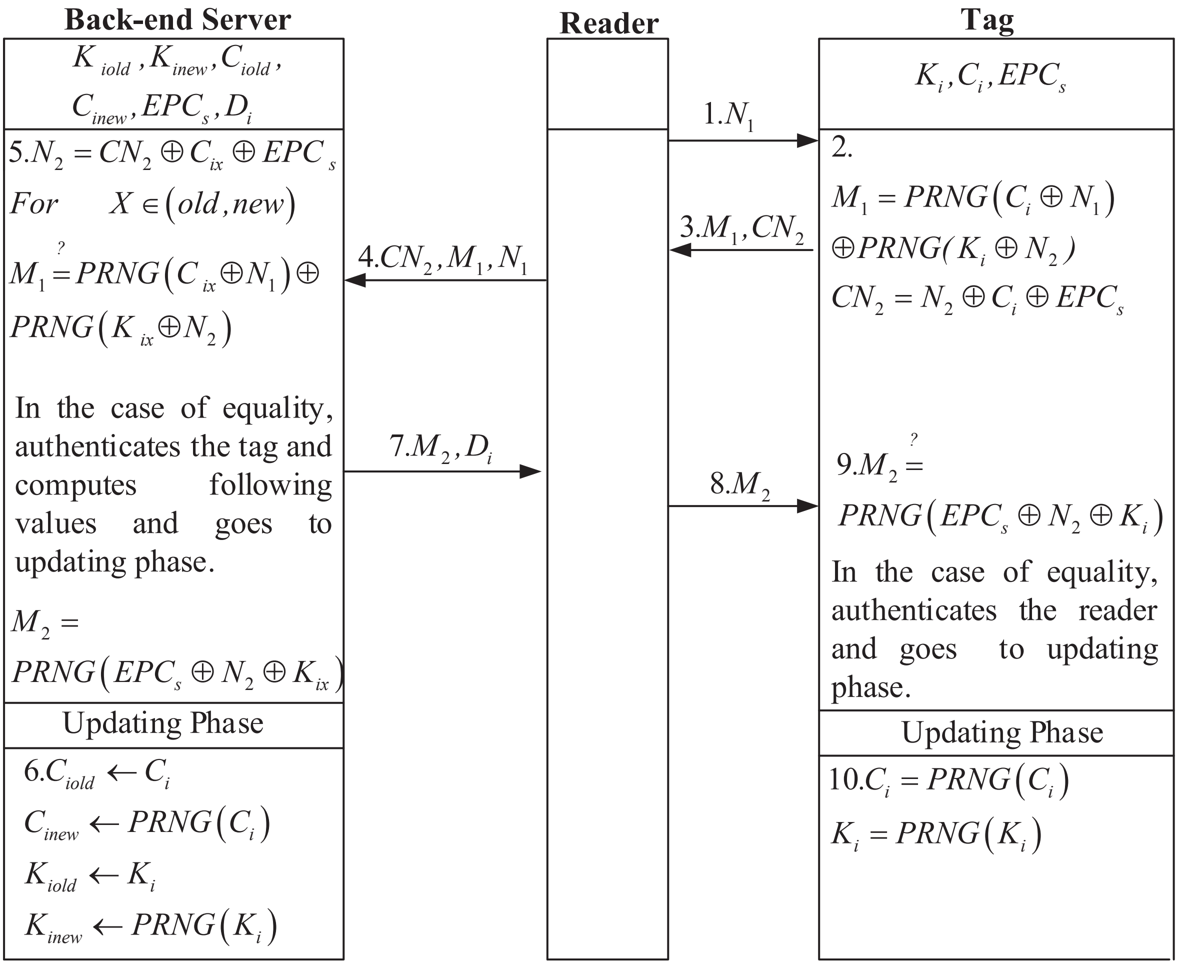

Figure 1. The Revised SRP^+ Protocol [1].

$M_1 \oplus M_1' = PRNG(C_i \oplus N_1) \oplus PRNG(K_i \oplus N_2) \oplus PRNG(C_i \oplus N_1) \oplus PRNG(K_i \oplus N_2') = PRNG(K_i \oplus N_2) \oplus PRNG(K_i \oplus N_2')\ \Delta$
$\Delta = CN_2 \oplus CN_2' = N_2 \oplus C_i \oplus EPC_s \oplus N_2' \oplus C_i \oplus EPC_s = N_2 \oplus N_2'$

2) for $i=0, \dots, 2^{16}-1$ does:
   a) $K_i \oplus N_2 \leftarrow i$;
   b) If $M_1 \oplus M_1' = PRNG(i) \oplus PRNG(i \oplus \Delta)$, returns i as $K_i \oplus N_2$.
3) using retrieved $K_i \oplus N_2$ value from step 2b and for $j=0, \dots, 2^{16}-1$ does as below:
   a) $EPC_s \oplus N_2 \oplus K_i \leftarrow j$;
   b) If $M_2 = PRNG(j)$, returns j as $EPC_s \oplus N_2 \oplus K_i$.
4) using retrieved $K_i \oplus N_2$ value from step 2b and retrieved $EPC_s \oplus N_2 \oplus K_i$ value from step 3b, computes $EPC_s = i \oplus j = K_i \oplus N_2 \oplus EPC_s \oplus N_2 \oplus K_i$.
5) using retrieved $K_i \oplus N_2$ value from step 2b and for $t=0, \dots, 2^{16}-1$ does as follows:
   a) if $PRNG(t \oplus N_1) = M_1 \oplus PRNG(K_i \oplus N_2)$, returns t as C_i.
6) using EPC_s from step 4 and C_i from step 5a retrieves N_2 as $CN_2 \oplus C_i \oplus EPC_s$.
7) using $K_i \oplus N_2$ from 2b and N_2 from 6 retrieves K_i as $(K_i \oplus N_2) \oplus N_2$.

The complexity of our proposed secret disclosure attack is only eavesdropping one run of the protocol between the legitimate reader and the target tag and consequently followed impersonating the reader to the target tag and finally doing only 3×2^{16} off-line *PRNG* function evaluations.

4. RECOMMENDATIONS TO IMPROVE THE REVISED *SRP*+ PROTOCOL

Our analysis in this paper shows that improving 16-bit *PRNG* functions based security protocols is not such an easy work and achieving beyond 2^{16} security level by using only a few calls to 16-bit

PRNG functions may not be possible, also see [21]. The main drawback of such protocols is their fundamental building block, *i.e.* 16-bit *PRNG* function, can be easily inverted by doing only 2^{16} offline evaluations of the underlying 16-bit *PRNG*. Given that the minimum acceptable security-level for many applications these days is 2^{80}, so if we want to use *PRNG*s in designing a security protocol that provides such security-level, its input/output length should be at least 80 bits. As already have shown in [21] and [20], to provide security beyond 2^{16}, there could be two ways to solve the weakness of RFID EPC-C1 G2 compliant security protocols against full secret disclosure attack presented in this paper and similar papers such as [1], which are:

- replacing 16-bit *PRNG* functions with longer input-output *PRNG* functions that are also lightweight, e.g. AKARI *PRNG*s [18];
- replacing 16-bit *PRNG* functions with lightweight block ciphers such as SIMON [19].

In either case, the input of *PRNG/*block cipher cannot be easily retrieved. Hence, such an improved version of the revised SRP^{+} protocol could be secure against the attacks that are using the weakness of short length of *PRNGs* input/output.

5. CONCLUSION

In this paper, we have shown once again that use of 16-bit *PRNG* functions with 16-bit inputs/output in RFID security protocols, as the main source of security, does not lead to resistance of protocols against secret disclosure attacks beyond the complexity of $O(2^{16})$. Hence, to enhance the security of these protocols employing longer output-input *PRNG* functions may be necessary. In the current work, we considered security of the revised SRP^{+}protocol which recently proposed by Moradi *et al.* in [1]. More precisely, we presented an efficient full secret disclosure attack against it. We also presented several advices that can be considered to design a secure protocol for RFID applications.

6. ACKNOWLEDGMENT

This work was supported by Shahid Rajaee Teacher Training University under contract number 7502.

7. REFERENCES

[1] F. Moradi and H. Mala and B. Tork Ladani, “Cryptanalysis and Strengthening of SRP^{+} Protocol”, Information Security and Cryptology (ISCISC), 2015 12th International Iranian Society of Cryptology Conference on, pp. 91-97, 2015 .

[2] EPCglobal Inc., [Online]: Available: http://www.epcglobalinc.org. [Accessed 04 06 2016].

[3] F. Xiao and Y. Zhou and J. Zhou and H. Zhu and X. Niu, “Security Protocol for RFID System Conforming to EPC-C1G2 Standard”, Journal of Computers, vol. 8, no. 3, pp. 605-612, 2013.

[4] M. Burmester and B. de Medeiros and J. Munilla and A. Peinado, “Secure EPC Gen2 Compliant Radio Frequency Identification”, In: Ruiz PM, Garcia-Luna-Aceves JJ (eds). ADHOC-NOW, vol. 5,793 of Lecture Notes in Computer Science, Springer, Berlin, pp. 227-240, 2009.

[5] C-L .Chen, Y-Y. Deng, “Conformation of EPC Class 1 Generation 2 Standards RFID System with Mutual Authentication and Privacy Protection”, Eng. Appl. AI, vol. 22, no. 8, pp. 1284-1291, 2009.

[6] E-Y. Choi and D-H. Lee and J-I. Lim, “Anti-cloning Protocol Suitable to EPCglobal Class-1 Generation-2 RFID Systems”, Comput. Stand. Interfaces, vol. 31, no. 6, pp. 1124-1130, 2009.

[7] T.-C. Yeh and Y.-J. Wang and T.-C. Kuo and S.-S. Wang, “Securing RFID Systems Conforming to EPC Class 1 Generation 2 Standard”, Expert Systems with Applications, vol. 37, pp. 7678-7683, 2010.

[8] E.-J. Yoon, “Improvement of the Securing RFID Systems Conforming to EPC Class 1 Generation 2 Standard”, Expert Systems with Applications, vol. 39, pp. 1589-1594, 2012.

[9] A. Mohammadali and Z. Ahmadian and M. R. Aref, “Analysis and Improvement of the Securing RFID Systems Conforming to EPC Class 1 Generation 2 Standard”, IACR Cryptology ePrint Archive, 2013:66,2013.

[10] L. Pang and L. He and Q. Pei and Y. Wang, “Secure and Efficient Mutual Authentication Protocol for RFID Conforming to the EPC C-1G-2 Standard”, in Wireless Communications and Networking Conference (WCNC), 2013 IEEE, 2013, pp. 1870-1875.

[11] S. Wang and S. Liu and D. Chen, “Security Analysis and Improvement on Two RFID Authentication Protocols, Wireless Personal Communications”, vol. 82, pp. 21-33, 2014.

[12] P. Peris-Lopez and J.C. Hernandez-Castro and J. M. Tapiador and J.C. Van der Lubbe, “Cryptanalysis of an EPC Class-1 Generation-2 Standard Compliant Authentication Protocol”, Engineering Applications of Artificial Intelligence, vol. 24, pp. 1061-1069, 2011.

[13] M. H. Habibi and M. Gardeshi and M.R. Alaghband, “Practical Attacks on a RFID Authentication Protocol Conforming to EPC C-1 G-2 Standard”, arXiv preprint arXiv:1102.0763, 2011.

[14] P. Peris-Lopez and T. Li and T.-L. Lim and J.C. Hernandez-Castro and J.M. Estevez-Tapiador, “Vulnerability Analysis of a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard”, in Workshop on RFID Security, p. 11, 2008.

[15] M. H. Habibi and M.R. Alaghband and M.R. Aref , “Attacks on a Lightweight Mutual Authentication Protocol under EPC C-1 G-2 Standard”, In: Ardagna CA, Zhou J (eds) WISTP, vol. 6,633 of Lecture Notes in Computer Science, Springer, Berlin, pp 254-263, 2011.

[16] P. Peris-Lopez and T. Li and J.C. Hernandez-Castro, “Lightweight Props on the Weak Security of EPC Class-1 Generation-2 Standard”, IEICE Trans., vol. 93-D, no. 3, pp. 518-527, 2010.

[17] P. Peris-Lopez and T. Li and J.C. Hernandez-Castro and J.E. Tapiador, “Practical Attacks on a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard”, Comput. Commun., vol. 32, no. (7-10), pp. 1185-1193, 2009.

[18] H. Martin and E.S. Milln and L. Entrena and J. C. H. Castro and P. Peris-Lopez, “Akari-x: A Pseudorandom Number Generator for Secure Lightweight Systems”, in IOLTS, pp. 228-233, IEEE, 2011. 17th IEEE International On-Line Testing Symposium IOLTS 2011, 13-15 July, 2011, Athens, Greece.

[19] R. Beaulieu and D. Shors and J. Smith and S. Treatman-Clark and B. Weeks, and L. Wingers, “The SIMON and SPECK Families of Lightweight Block Ciphers”, IACR Cryptology ePrint Archive,2013:404, 2013.

[20] M. Safkhani and N. Bagheri and M. Naderi, “A Note on the Security of IS-RFID, an Inpatient Medication Safety”, Int. J. Med. Inform., 2014 Jan., vol. 83, no. 1, pp. 82-5. doi: 10.1016/j.ijmedinf.2013.04.003. Epub 2013 May7.

[21] M. Safkhani and N. Bagheri and M. Hosseinzadeh and M.E. Namin and S. Rostampour, “On the (im) possibility of Receiving Security Beyond 2^l Using an l-bit PRNG: the case of Wang *et al.* Protocol”, IACR Cryptology ePrint Archive, 2015:365, 2015.