Available online at www.sciencedirect.com

SciVerse ScienceDirect

Physics Procedia 24 (2012) 1385 – 1391

Physics Procedia

2012 International Conference on Applied Physics and Industrial Engineering

An Gen2 Based Security Authentication Protocol for RFID System

Xiaoluo YI[1], Liangmin WANG[2], Dongmei MAO[1], Yongzhao ZHAN[1]

School of Computer Science and Communication Engineering
Zhenjiang, P.R.China
The Department of Computer Science
Zhenjiang, P.R.China
+Corresponding Author

Abstract

EPC Class-1 Generation-2 specification(Gen2 in brief) has been accepted as the standard for RFID tags under grant number ISO18000-6C. However, Gen2 does not pay due attention to security. For this reason, a Gen2 based security authentication protocol is developed in this paper. In details, we study the security requirements presented in the current Gen2 based RFID authentication protocols[7-13]. Then we point out the security flaws of Chien's mutual authentication protocol[7], and improve the protocol based on a 11 security requirements. Our improved protocol merely uses CRC and PRNG operations supported by Gen2 and meets the 11 security requirements. In contrast to the similar work [14-15] on Chien's protocol or other Gen2 based schemes, our protocol is more secure and our security analysis is much more comprehensive and qualitative.

Keywords: RFID, EPC Class-1 Generation-2 Specification, Security Protocol

1. Introduction

Radio Frequency Identification (RFID) systems are used to identify remote objects equipped with RFID tags by wireless scanning without manual intervention. To promote the adoption of RFID technology and to support interoperability, EPCglobal proposed one of the most important standards EPCglobal Class-1 Gen2 RFID specification (Gen2 in brief) [1]. Unfortunately, Duc [2] has pointed out that Gen2 is inherently vulnerable to eavesdropping under wireless communication environment. In order to prevent RFID tags from leaking message, three classes of schemes have been proposed: physical schemes, provable security schemes and practical Gen2 based schemes.

Physical schemes, such as tag killing, Faraday cage, active jamming and blocker tag, etc.[3], are too expensive to large-scale use in practice [3]. The provable security schemes [4-5] are not applicable for Gen2 tags, because encryption functions and hash function are not supported by Gen2 although Yksel[6] presented a novel Hash solution with around 1.7K gates, it doesn't pass the strict security analysis until now. Practical Gen2 based schemes[7-13] that just use lightweight algorithms supported by Gen2, such as bitwise operations, CRC operation, or PRNG operation did not well meet the security requirements shown in TABLE I.

The rest of the paper is organized as follows. Section II, we give a short review of Chien's protocol [7] and then point out its drawbacks. In Section III, we improve Chien's protocol to meet the security requirements and compare it with Gen2 based RFID protocols [7-13]. Finally, we conclude the paper in section IV.

2. Chien's Protocol and Security Analysis

In this Section, we analyze Chien's protocol[7] and take the analysis as a preparation for designing protocol.

2.1 Chien's Protocol

In Chien's Protocol, the server randomly selects an initial authentication key K_{x_0} and initial access key P_{x_0}. Tag_x initially shares three values (EPC_x, K_{x_0}, P_{x_0}) with sever S, where EPC_x is the EPC code of the tag. K_{x_0} and P_{x_0} will be updated to K_{x_i} and P_{x_i} after *i*-th successful authentication. S stores (K_{new}, P_{new}, K_{old}, P_{old}, EPC_x, DATA) , where K_{old} and P_{old} are the most recent 'old' values of K_{new} and P_{new}. Initially, K_{old}, K_{new} and P_{new}, P_{old} both are set to K_{x_0}, P_{x_0}, respectively.

Chien's protocol has four passes shown in Figure1. The detailed scenarios are described as follows:

1) R → Tag_x: N_1, where N_1 is a random nonce.

Tag_x: Compute $M_1=CRC(EPC_x \| N_1\| N_2) \oplus K_{x\_i}$, where N_2 is a random nonce.

2) Tag_x → R: M_1 , N_2 R→S: M_1, N_2, N_1

S: Search all (K_{new}, K_{old}, EPC_x) and compute $I_{old} = M_1 \oplus K_{old}$, $I_{new} = M_1 \oplus K_{new}$, then verify the tag by checking whether I_{new} or $I_{old} = CRC(EPC_x \| N_1\| N_2)$ holds.

3) S → R: M_2, DATA

S: Compute $M_2=CRC(EPC_x\|N_2) \oplus P_{new}$ or $M_2= CRC(EPC_x \|N_2) \oplus P_{old}$ depending on which value (K_{new} or K_{old}) satisfies the verification equation in the previous step. Then update : $K_{old} \leftarrow K_{new}$, $P_{old} \leftarrow P_{new}$, $K_{new} \leftarrow PRNG(K_{new})$, $P_{new} \leftarrow PRNG(P_{new})$.

4) R → Tag_x: M_2

Verify S by checking whether $M_2 \oplus P_{x\_i} =CRC(EPC_x \| N_2)$ holds. If satisfies, update $K_{x\_i} \leftarrow PRNG(K_{x\_i})$, $P_{x\_i} \leftarrow PRNG(P_{x\_i})$.

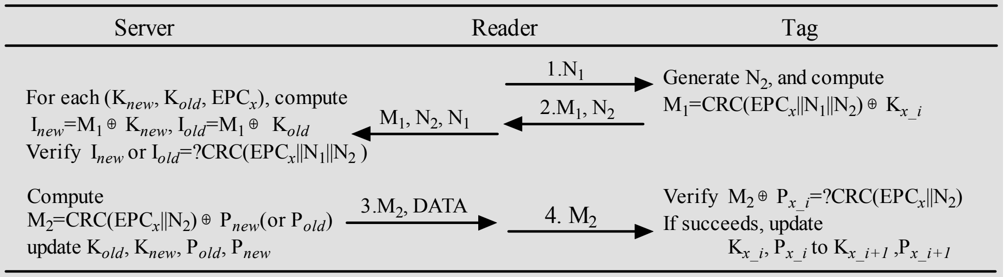
Server
Reader
Tag
1.N1
Generate N2, and compute
M1=CRC(EPCx||N1||N2) ⊕ Kx_i
For each (Knew, Kold, EPCx), compute
Inew=M1 ⊕ Knew, Iold=M1 ⊕ Kold
Verify Inew or Iold=?CRC(EPCx||N1||N2)
M1, N2, N1
2.M1, N2
Compute
M2=CRC(EPCx||N2) ⊕ Pnew(or Pold)
update Kold, Knew, Pold, Pnew
3.M2, DATA
4. M2
Verify M2 ⊕ Px_i=?CRC(EPCx||N2)
If succeeds, update
Kx_i, Px_i to Kx_i+1 ,Px_i+1

Figure 1. Chien's protocol

2.2 Security Analysis

To clearly express our contribution to security analysis, the following part is arranged as follows: the attacks that have been analyzed in [14-15] are briefly shown first in Proposition 1~3, and then the details of the new four attacks we find is shown in Proposition 4 and Proposition 5.

Proposition 1. Tag Forgery Resistance is not guaranteed due to the linearity of CRC and the plaintext N_2.

Proof: The exchanged plaintext M_1 can be obtained by an attacker. By using the lemma of CRC[14]:

$$CRC(A||B)=CRC(A_{x<<n} \oplus B)=CRC(A_{x<<n}) \oplus CRC(B) \quad (1)$$

and M_1, the attacker gets Eq.(2):

$$CRC(EPC_{x<<2l}) \oplus K_{x\_i}= M_1 \oplus CRC(N_{x<<l}) \oplus CRC(N_2) \quad (2)$$

Since he knows value of $CRC(EPC_{x<<2l}) \oplus K_{x\_i}$ using N_1, N_2, $CRC(N_{1<<l})$ and $CRC(N_2)$. Therefore, the attacker can pre-compute the value M_1^* before the next successful authentication as follows: $M_1^*=CRC(EPC_x \,||\, N_1 || N_2^*) \oplus K_{x\_i}$.

Then S will be spoofed successfully when verifying. Hence the protocol does not guarantee Tag Forgery Resistance.

Proposition 2. The linearity of CRC makes Tag Anonymity of Chien's protocol not guaranteed.

Proof: Form Proposition 1, we know an attacker can obtain the value of $CRC(EPC_{x<<2l}) \oplus K_{x\_i}$. Note that, before the next updating, the value of $CRC(EPC_{x<<2l}) \oplus K_{x\_i}$ is a constant for the attacker, that is, the message M_1 can be transformed into a constant and could be tracked by the attacker. As a result, user location is revealed. Therefore, Anonymity is not guaranteed.

Proposition 3. Chien's protocol doesn't achieve Forward Security and Resist to DoS attack.

Proof: From two consecutive sessions eavesdropped, the attacker can obtain the following four values like that in [14]:

$$M_{1i} =CRC(EPC_x \,||\, N_{1i} \,||\, N_{2i}) \oplus K_{x\_i} \quad (3)$$

$$M_{2i} =CRC(EPC_x \,||\, N_{2i}) \oplus P_{x\_i} \quad (4)$$

$$M_{1(i+1)} =CRC(EPC_x \,||\, N_{1(i+1)} \,||\, N_{2(i+1)}) \oplus K_{x\_i+1} \quad (5)$$

$$M_{2(i+1)} =CRC(EPC_x \,||\, N_{2(i+1)}) \oplus P_{x\_i+1} \quad (6)$$

By using Eq.(1), the attacker obtains Eq.(7) by (3) ⊕ (5):

$$K_{x\_i} \oplus K_{x\_i+1} = M_{1i} \oplus M_{1(i+1)} \oplus CRC(N_{1i} \,||\, N_{2i}) \oplus CRC(N_{1(i+1)} || N_{2(i+1)}) \quad (7)$$

Since the M_{1i}, $M_{1(i+1)}$, N_{1i}, N_{2i}, $N_{1(i+1)}$ and $N_{2(i+1)}$ are plaintext, the value of $K_{x\_i} \oplus K_{x\_i+1}$ would be revealed by Eq.(7). Then the length l of K_{x_i} is revealed.

The value of K_s can be obtained by $PRNG(K)=K \oplus C$ where C is a constant. The attacker could check which K_s is right by trying an authentication in the (i+3)-th session. In this case，at least, K_{x_i} satisfies. Thus, we may regard that K_{x_i} is revealed. Now, From the knowledge of K_{x_i}, Eq.(3) and Eq.(5), the attacker could obtain $CRC(EPC_{x<<2l})$. Likewise, he obtains P_{x_i} and $CRC(EPC_{x<<l})$ from Eq.(4) and Eq.(6).

Due to the random two consecutive sessions and the knowledge of K_{x_i} and P_{x_i}, the attacker could know the following sessions that have been transmitted. Thus Forward Security is not guaranteed.

Tag Forgery Resistance is not guaranteed as follows: By using $K_{x\_i+1}=PRNG(K_{x\_i})$, the attacker calculates K_{x_j} ($j \geq i+1$). And then he can pre-compute the value M_{1k}^* when receiving a new N_1' in the (k+1)-th ($k \geq i+3$) session as follows:

$$M_{1k}^{*}=CRC(EPC_x \,||\, N_1' \,||\, N_{2k}^{*}) \oplus K_{x\_k}$$

and tag-to-reader authentication can be performed successfully.

DoS attack happens as follows: If the above attack happens twice or more, the secrets between server and tag will be out of synchronization. They will never authenticate each other.

Proposition 4. Chien's protocol has no Privacy, Data Confidentiality, and Server Forgery Resistance.

Proof: From two consecutive sessions shown in Proposition 3, an attacker gets the values of K_{x_i} and P_{x_i}, and then could get EPC_x from $CRC(EPC_{x<<l})= C'$ (where C' is a constant). Then the attacker checks which EPC_x is genuine by trying an authentication in the (i+3)-th session. So we regard EPC_x is revealed. Thus, Privacy is not achieved.

By using P_{x_i+1} =PRNG(P_{x_i}), the attacker calculates P_{x_k} ($k \geq i+3$). Then he can pre-compute the value M_{2k}^{*} in (k+1)-th session as follows:

$$M_{2k}^{*}=CRC(EPC_x \,||\, N_{2k}) \oplus P_{x\_k}.$$

Then reader-to-tag authentication will be performed successfully. Hence, Server Forgery Resistance is not met.

Furthermore, this attack will make authentication key and access key update illegally. A portion of the tag's memory is rewritten, as a result, Data Confidentiality is not guaranteed.

Proposition 5. Backward Security is not guaranteed in Chien's protocol.

Proof: If an attacker obtains EPC_x, K_{x_i} and P_{x_i}, he will obtain K_{x_j} and P_{x_j} ($j \geq i$) by using K_{x_i+1}=PRNG(K_{x_i}) and P_{x_i+1}=PRNG(P_{x_i}). Thus, the messages transmitted in the (j+1)-th session can be decrypted. Therefore, the protocol does not achieve Backward Security.

3. Improved Protocol and SECURITY Analysis

To solve the problem in Section II, in this section we present an improved version, and then a comprehensive security analysis is given.

3.1 The Improved Protocol

The plaintext N_2 in message 2 is transmitted which causes M_1 to be tracked and other security problems. Thus, in the improved protocol it is encrypted. Meanwhile, M_1 is re-encrypted by K_i. To enhance the Backward Security, the nonce N_2 is used in the update stage. The details of the improved protocol is as follows.

1) R $\rightarrow$ Tag_x: N_1, where N_1 is a random nonce.

Tag_x: Compute $M_1= N_2 \oplus K_{x\_i}$, $M_2=CRC(K_{x\_i} \,||EPC_x \,||\, N_1|| \,N_2) \oplus K_{x\_i}$, where N_2 is a random nonce.

2) Tag_x $\rightarrow$ R: M_1, M_2 R→S: M_1, M_2, N_1

S: Search all (K_{new}, K_{old}, EPC_x) and compute $M_2' = CRC(K_{new}||EPC_x||N_1||(M_1 \oplus K_{new})) \oplus K_{new}$ or $M_2''=CRC\ (K_{old}\ ||EPC_x||N_1||(M_1 \oplus K_{old})) \oplus K_{old}$. Verify the tag by checking whether M_2' or $M_2''= M_2$.

3) S $\rightarrow$ R: M_3, DATA

S: Depending on which value (K_{new} or K_{old}) satisfies the verification equation in the previous step, compute $M_3= CRC(EPC_x||N_2) \oplus P_{new}$(or P_{old}) send M_3, DATA to R. Update $K_{old} \leftarrow K_{new}$, $P_{old} \leftarrow P_{new}$, $K_{new} \leftarrow PRNG(K_{new} \oplus N_2)$, $P_{new} \leftarrow PRNG(P_{new} \oplus N_2)$.

4) R $\rightarrow$ Tag_x: M_3

Verify S by checking whether $M_3 \oplus P_{x\_i} = CRC(EPC_x||\ N_2)$ holds. If succeeds, update $K_{x\_i+1} \leftarrow PRNG(K_{x\_i} \oplus N_2)$, $P_{x\_i+1} \leftarrow PRNG(P_{x\_i} \oplus N_2)$.

3.2 Security Analysis of the Improved Protocol

We analyze Chien's protocol and show that the protocol does not meet 8 security requirements. The following part shows the improved protocol basically meets the 8 properties.

1) Tag Forgery Resistance: If a weak attacker intends to forge the tag, it must be able to pre-compute a valid response (M_1, M_2) to a reader query. However, it is infeasible to compute such a valid pair without knowledge of N_2 and the case in Proposition 1 or Proposition 3 will not happen.

2) Tag Anonymity: The location privacy of tag holders can be revealed when the tag's answers are constant. Specifically, location privacy can be more significant when a certain tag is exposed to long-term tracking. It is therefore crucial to make all the information sent by the tag anonymous. As we have seen, in the mutual-authentication stage, the tag generates a nonce, by which all the transmitted messages are encrypted. In addition, the attack like that in Proposition 2 can not succeed without the nonce. Thus, Tag Anonymity is guaranteed and privacy location of the tag owner is not compromised.

3) Forward Security: Forward security is the property that guarantees the security of messages sent in this session will be valid in the next session. Since key updating is fulfilled after the mutual authentication, and the attacker can not obtain K_{x_i} or P_{x_i} by using the method in Proposition 4, a security breach of an RFID tag will not reveal data previously transmitted.

4) Resist to DOS attack: If the fourth flow doesn't reach the tag, the shared secrets of the server and tag might be out of synchronization, because the server will update the shared secrets while the tag will not. However, in the improved protocol, the server maintains both the old and new values of K_{x_i} and P_{x_i} for Tag_x in its database, so the server can resynchronize with the tag in such situation. Additionally, although Server Forgery attack can also desynchronize the shared keys, the improved protocol can resist this attack

5) Privacy: EPC code must be kept secure to guarantee user privacy. The messages M_2 and M_3 which can be eavesdropped by an attacker. However, EPC code is encrypted by a nonce N_2 or K_{x_i} or P_{x_i}, and an attacker will not obtain these three values which were discussed in Tag Forgery Resistance. Therefore, only authorized server and reader are able to access the information associated with the tag.

6) Server Forgery Resist: Server Forgery Resist is usually used to protect the secrets synchronization between tag and server in the protocol. A legitimate server responds with a message M_3 to a tag in order to enable the tag to authenticate the server. An attacker cannot create a valid M_3 without knowing P_{x_i}. Actually, P_{x_i} is shared between Tag_x and S and not yet exchanged in this (i+1)-th session. Additionally, it's not revealed in the prior i times which has been discussed when analyzing Tag Forgery Resistance. Hence, our protocol resists such an attack.

7) Data Confidentiality: A portion of the tag's memory is rewritable, so modifications are possible. In this part of the memory, the tag stores the EPC code, authentication keyand access key. If an attacker does succeed in modifying this part of the memory, the reader will never authenticate the tag. Except physical attacks, Server Forgery attack will result in such modification by illegally updating K_{x_i} and P_{x_i}. However, the improved protocol can resist this attack shown in 6).

8) Backward Security: The improved scheme provides Backward Security if an attacker misses N_2 just once in a single successful authentication session after compromising the tag's secret. That is, if the attacker does not have access to the value of N_2 once which is needed to update K_{x_i} and P_{x_i}, he cannot compute the new keys and know future transactions.

From analysis above, we find the improved protocol basically meets the 8 properties. Next, we show that the improved protocol also satisfies the other 3 requirements.

9) Resist to Reply attack: An eavesdropper could store all the messages exchanged between reader and tag. Then a reader may be impersonated which may cause loss of synchronization between sever and tag or spoof the system, However, this is not the case due to the challenge-response technology and the freshness of N_1 and N_2 per session.

10) Data Recovery: The interception or blocking of messages is a DoS attack which prevents tag identification. When dismissing messages, S can still recover the message thanks to the storage of K_{old} and P_{old} in its database.

11) Mutual Authentication: In the improved protocol, server identifies tag by verifying K_{x_i} in M_1 and M_2 , and tag authenticates server by verifying P_{x_i} in M_3.

From the analysis above, we can see that the improved protocol basically meets all the 11 requirements in TABLE I where the security properties are summed up from [7-9]. The detailed necessity of these 11 security properties has already been analyzed above.

To solve the security problem, many schemes have been proposed[7-13]. However, they did not well fulfill the 11 security requirements shown in TABLE I. From the comparison with other recent Gen2 based schemes in TABLE I, we can see the improved protocol has the most security properties and basically meets all the 11 security requirements.

Table I. Security Properties of Existing Protocols

Properties	Chien[7]	Pedro[8]	Kart[9]	Chen[10]	Cai[11]	Choi[12]	Sun[13]	Ours
(1)Privacy	×	O	O	O	O	O	O	O
(2)Anonymity	×	O	O	O	O	×	O	O
(3)Resist to reply attack	O	O	×	×	O	O	×	O
(4)Resist to DOS attack	▽	×	×	O	O	O	O	▽
(5)Forward Security	×	O	O	×	×	×	O	O
(6)Backward Security	×	×	×	×	×	×	×	▽
(7)Data Confidentiality	×	O	×	O	O	O	O	O
(8)Mutual Authentication	O	O	O	O	O	O	O	O
(9)Tag Forgery Resist	×	O	O	O	×	O	O	O
(10)Server Forgery Resist	×	O	O	O	O	×	×	O
(11)Data Recovery	O	×	×	O	O	O	O	O

Notation: ×: not provided; O: provided; ▽:partially provided

4. Concluding Remarks

In this paper, we analyze Chien's protocol and find four new attacks that not discussed in prior literatures, and then present an improved version which still uses CRC and PRNG. The improved protocol basically meets all the 11 security requirements and may be the first protocol that basically meets these security requirements in Gen2 based schemes. However, the back-end server still needs exhausted search to authenticate a tag. It would be one of research topics to design secure Gen2 based protocol with little computation load.

Acknowledgment

The work of this paper is supported by National Natural Science Foundation of China(60703115), and National Social Science Foundation of China (09CTJ006).The author Liang-min WANG is supported by Science Foundation of China Post-doc under No.200801357, 20070420955, and 0702003B of Jiangsu Post-doc, and "Qing Lan Project" for Excellent Youth Scholars of Jiangsu Province and Talents Foundation of Jiangsu University under No.07JDG080.

References

[1]EPCglobal, http://www.EPCglobalinc.org/.

[2]D N Duc, J Park, H Lee, K Kim. Enhancing Security of EPCglobal EPC Class 1 Generation 2 RFID Tag against Traceability and Cloning, The 2006 Symposium on Cryptography and Information Security. Berlin: Springer, 2006.

[3]A Juels. RFID Security and Privacy: A Research Survey [J]. IEEE Journal on Selected Areas in Communications. 2006.24(2):381–394.

[4]B Song, C Mitchell. RFID Authentication Protocol for Low-cost Tags [C]. In Proceedings of the First ACM Conference on Wireless Network Security .2008:140-147

[5]S Weis, S Sarma, R Rivest, D W Engels. Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems[C], In Proceedings of the First Security in Pervasive Computing. Berlin: Springer, 2003: 454-469.

[6]K Yksel, J P Kaps, B Sunar. Universal Hash Functions for Emerging Ultra-low-power Networks[C]. In Proceedings of The Communications Networks and Distributed Systems Modeling and Simulation Conference (CNDS). San Diego, CA. 2004.

[7]H Chien, C Chen. Mutual authentication Protocol for RFID Conforming to EPC Class 1 Generation-2 Standard ,Computer Standards & Interfaces, 2007.29(2):254-259

[8]P Pedro, C Julio , M Juan , A Ribagorda . An Ultra Light Authentication Protocol Resistant to Passive Attacks under the Gen2 Specification [J]. J. Inf. Sci. Eng.2009. 25(1): 33-57

[9]S Karthikeyan, M Nesterenko. RFID Security without Extensive Cryptography[C], In Proceedings of the 3rd ACM Workshop on Security of AdHoc and Sensor Networks, 2005:63–67.

[10]C Chen, Y Deng. Conformation of EPC Class 1 Generation 2 Standards RFID system with Mutual Authentication and Privacy Protection [J]. Engineering Applications of Artificial Intelligence ,In Press, doi:10.1016/j.engappai.2008.10.022

[11]Q Cai, Y Zhan, Y Wang. A Minimalist Mutual Authentication Protocol for RFID system and BAN logic Analysis[C]. In Proceedings of the 2008 ISECS International Colloquium on Computing, Communication, Control, and Management.2008.2: 449–453

[12]E Choi, D Lee, J Lim. Anti-cloning Protocol Suitable to EPCglobal Class-1 Generation-2 RFID Systems [J]. Computer Standards & Interfaces. 2009.31(6):1124-1130

[13]H Sun, W Ting. A Gen2-based RFID Authentication Protocol for Security and Privacy[C]. IEEE Transactions on Mobile Computing.2009.8(8):1052-1062

[14]D Han, D Kwon. “Vulnerability of an RFID authentication protocol conforming to EPC Class 1 Generation 2 Standards” Computer Standards & Interfaces[J]. 2009.31(4):648-652.

[15]P Peris-Lopez, J C Hernandez-Castro, J M. Estevez-Tapiador, and A Ribagorda. Cryptanalysis of a Novel Authentication Protocol Conforming to EPC-C1G2 Standard. In Workshop on RFID Security– RFIDSec’07, Malaga, Spain, July 2007.