Cryptanalysis of AZUMI: an EPC Class-1 Generation-2 Standard Compliant RFID Authentication Protocol

Masoumeh Safkhani[1], Nasour Bagheri[2], and Majid Naderi[1]

[1] Electrical Engineering Department, Iran University of Science and Technology, Tehran, Iran{M_Safkhani, M_Naderi}@iust.ac.ir

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

Abstract. In this paper, we analyze the security of AZUMI protocol which is compliant with the EPC-Class-1 Generation-2 standard and recently has been proposed by Peris *et al.* This protocol is an improvement to a protocol proposed by Chen and Deng which has been cryptanalysed by Peris *et al.* and Kapoor and Piramuthu. However, our security analysis clearly shows that the designers were not successful in their attempt to improve the Chen and Deng protocol. More precisely, we present an efficient attack to disclose the tag and the reader secret parameters. In addition, we present a simple tag impersonation attack against this protocol. The success probability of all attacks are almost "1" and the cost of given attacks are at most eavesdropping two sessions of protocol. However, the given secrets disclosure attack also requires $O(2^{16})$ off-line evaluation of a *PRNG* function.

keywords: RFID, EPC-C1 G2, Mutual Authentication, Secret Disclosure, Tag Impersonation.

1 Introduction

Radio Frequency Identification (RFID) is a promising technology that can revolutionize the way we lead our life. A typical RFID system includes a reader and a number of tags, which may range from the battery-powered ones with Wi-Fi capabilities to the low-cost ones that are constrained in resources with even no internal power. The later tags also known as passive tags which is the subject of this study. A passive RFID tag is a small electronic component which is used to identify and track an object and it can be read/modified by a reader which is normally supported by a back-end database. This device keeps unique identification information related to the tagged object and performs simple computations. These features provide significant advantages for tags to be employed in various applications such as inventory tracking, supply-chain management, theft-prevention, e-passport, etc. Notably, low-cost RFID can be a good replacement for the conventional bar-codes that are currently the most extended identification systems. The main advantages of RFID over bar-codes are as follows:

1. A tag can provide identification and authentication of tagged objects and allows data storage and data processing on the tag.
2. Data which can be stored on RFID tags is larger than what a Bar-coding can provide.
3. The distance of the RFID reader from the tags can vary from few centimeters to more than 20 meters.
4. Further, the RFID reader need not be in the line of sight of the tag.

However, security and privacy are the main concerns in the rapid and wide spread application of this distinguished technology. In 2004 [3, 4], the Electronic Product Code Class-1 Generation-2 specification (EPC-C1 G2 in short) was announced by EPC Global. However, the later security analysis that carried out on the light of EPC-C1 G2 specification have demonstrated important security flaws in this standard [1, 6].

Due to the flaws in the standard protocol, researchers have proposed several EPC-compliant mutual authentication protocols in the literature. Among the current researches in this field, one of the most recent proposals was an EPC-C1 G2-compliant protocol proposed by Chen and Deng [2]. However, the later security analysis that carried out on this protocol have demonstrated important security flaws in this protocol [5,7]. To improve the security of this protocol, Peris *et al.* [7] proposed an improved version called AZUMI, which is the main concern of this paper. The designers have claimed optimal security for AZUMI. However, in this paper we show they were not successful in their attempt to improve the security of the Chen and Deng's protocol significantly and the proposed protocol is really weak. In this study we show an approach to retrieve the secret values of the tag and the reader efficiently. The interesting point of this attack is its passiveness. The main cost of this attack is $O(2^{16})$ evaluation of a *PRNG*- function in off-line mode which is completely acceptable cost and can be provided by a conventional adversary.

Paper Organization : In § 2 some preliminaries and notations are introduced. We describe AZUMI protocol in § 3. *ID* disclosure attacks and tag impersonation attack against AZUMI are presented in § 4. Finally, in § 5 we present the paper conclusion.

2 Preliminaries

Throughout the paper, we use the following notations:

- R_i: i^{th} RFID reader.
- T_i: i^{th} RFID Tag.
- N_{T_i}: 32-bit access password of T_i.
- $N16_{T_i}$: The access password of T_i is divided into two 16-bit blocks and XORred to provide $N16_{T_i}$.
- K_{T_i}: The 32-bit kill password of T_i.
- $K16_{T_i}$: The kill password of T_i is divided into two 16-bit blocks and XORred to provide $K16_{T_i}$.
- EPC_{T_i}: 96-bit *EPC* identification number of tag T_i.
- $EPC16_{T_i}$: The *EPC* identification number of tag T_i is divided into six 16 bit blocks and XORred to provide $EPC16_{T_i}$.
- $ID16_{R_i}$: 16-bit identification number of the i^{th} reader.
- $PRNG()$: Pseudo random number generator with 16-bit output length.

- RND_x: 16-bit random number generated by x.
- $\oplus$: XOR operation.
- M_{req}: Reader's request.
- $B \longleftarrow A$: Assign the value of A to B.

3 Protocol Description

We now give a brief description of AZUMI protocol [7]. The authors of AZUMI have supposed that each tag T_i of this protocol keeps a data set includes $EPC16_{T_i}, N16_{T_i}$ and $K16_{T_i}$ and the reader also keeps a record of data for each tag T_i includes $EPC16_{T_i}, N16^{old}_{T_i}, K16^{old}_{T_i}, N16^{new}_{T_i}$, and $K16^{new}_{T_i}$. The reader keeps the *old* version of information to provide resistance against desynchronization attacks.

The AZUMI protocol consists of two phases: registration phase and mutual authentication phase. In the registration phase of protocol, in a secure environment, the tags and the readers are registered in the database separately where each tag sends its unique $EPC16_{T_i}$ to the database. The database then responds with $N16_{T_i}$ and $K16_{T_i}$ to each tag T_i which requests for the registration. In addition, in database, the old and the new version of variables are set to the same value, $N16^{old}_{T_i} = N16^{new}_{T_i}, K16^{old}_{T_i} = K16^{new}_{T_i}$. However, the details of this phase of protocol has no affect on our attacks (the interested reader can find more details on [7]). After registration, tags and readers can mutually communicate. The mutual authentication steps of AZUMI protocol [7] are as follows:

1. The reader starts the protocol by sending RND_{R_i} and M_{req} (includes $ID16_{R_i}$).
2. Once the tag receipts the message, it generates two fresh random numbers (RND_{T_i}, RND'_{T_i}), computes A, B and C as below and sends RND_{T_i}, A, B, C to the reader:

$$\begin{aligned} A &\leftarrow PRNG(N_{T_i} \oplus RND_{T_i} \oplus RND_{R_i} \oplus ID16_{R_i}) \\ B &\leftarrow PRNG(EPC16_{T_i} \oplus RND'_{T_i}) \\ C &\leftarrow RND'_{T_i} \oplus K16_{T_i} \end{aligned} \tag{1}$$

3. The reader receives RND_{T_i}, A, B and C and upon receipt of these values, it proceeds as follows:
   (a) **Tag Identification:** For any entry in database the reader picks $EPC16_{T_i}$ and $K16_{Ti} \in (K16^{old}_{Ti}, K16^{new}_{Ti})$, extracts RND'_{T_i} from $C \oplus K16_{Ti}$, computes $PRNG(EPC16_{T_i} \oplus RND'_{T_i})$ and compares it with the received value of B to identify the tag. The protocol aborts if the reader reaches the end of records without any match.
   (b) **Tag Authentication:** After successful tag identification, the reader computes $PRNG(N_{T_i} \oplus RND_{T_i} \oplus RND_{R_i} \oplus ID16_{R_i})$ and compares it with the received value of A to authenticate the tag. If tag is successfully authenticated, the reader calculates $D = PRNG(N_{T_i} \oplus RND_{R_i} \oplus RND_{T_i} \oplus EPC16_{T_i} \oplus RND'_{T_i})$ and sends it to the tag.
   (c) **Updating Phase:** After successful authentication of the tag T_i, the reader updates the record of T_i in database as bellows, where $p = 0$ and $p = 1$ determine usage of old and new values of record of T_i in the identification and authentication phases:

$$\text{If } p = 0 \begin{cases} N16^{new}_{T_i} \leftarrow PRNG(N16^{old}_{T_i} \oplus RND'_{T_i}) \\ K16^{new}_{T_i} \leftarrow PRNG(K16^{old}_{T_i} \oplus RND'_{T_i}) \end{cases} \tag{2}$$

$$\text{If } p = 1 \begin{cases} N16^{old}_{T_i} \leftarrow N16^{new}_{T_i} \\ N16^{new}_{T_i} \leftarrow PRNG(N16^{old}_{T_i} \oplus RND'_{T_i}) \\ K16^{old}_{T_i} \leftarrow K16^{new}_{T_i} \\ K16^{new}_{T_i} \leftarrow PRNG(N16^{old}_{T_i} \oplus RND'_{T_i}) \end{cases} \tag{3}$$

4. The tag receives D and after receiving this value, it compares the received value by $PRNG(N_{T_i} \oplus RND_{R_i} \oplus RND_{T_i} \oplus EPC16_{T_i} \oplus RND'_{T_i})$ to whether authenticate the reader. After the reader successful authentication, the tag updates its records as follows:

$$\begin{aligned} N16_{T_i} &\leftarrow PRNG(N16_{T_i} \oplus RND'_{T_i}) \\ K16_{T_i} &\leftarrow PRNG(K16_{T_i} \oplus RND'_{T_i}) \end{aligned} \tag{4}$$

4 Secret Disclosure Attack

In this section we show that how a passive adversary can disclose all secret parameters related to the tag T_i that are $EPC16_{T_i}, N16_{T_i}, K16_{T_i}, N16^{old}_{T_i}, K16^{old}_{T_i}, N16^{new}_{T_i}$ and $K16^{new}_{T_i}$. The main observations, that are the milestones of our attack, are as follows:

1. In step 2 of the protocol the value of $C = N16^{old}_{T_i} \oplus RND'_{T_i}$ is sent by T_i to R_i in public while in step 3c of the protocol, the reader updates the secret key $K16^{new}_{T_i}$ as $K16^{new}_{T_i} = PRNG(N16^{old}_{T_i} \oplus RND'_{T_i})$ (also T_i updates its secret key in the same manner). Hence, given the eavesdropped value of C which is transmitted in public and assuming that the $PRNG$- function is a public function then it is possible for a passive adversary to determine the value of $K16^{new}_{T_i}$ stored in the reader record of T_i(which equals to $K16_{T_i}$ in the tag T_i).
2. Given the $Y = PRNG(X)$ and assumptions that the $PRNG$-function is a public function and the length of Y and X are 16-bit, then it is possible to do an exhaustive search and find X as a pre-image of Y in the cost of at most 2^{16} evaluation of $PRNG$-function.

Following the above observations and given the tag T_i which communicants with the reader R_i, an adversary ($\mathcal{A}$) can disclose the secret parameters of T_i as follows:

1. $\mathcal{A}$ eavesdrops two sequential successful runs of the protocol between T_i and R_i and stores the transferred value of C in the first run, $C^{1^{th}}$, and the messages $RND^{2^{nd}}_{T_i}, RND^{2^{nd}}_{R_i}, A^{2^{nd}}, B^{2^{nd}}, C^{2^{nd}}, D^{2^{nd}}$ and $M^{2^{nd}}_{req}$ (includes $ID16_{R_i}$) from the second run of protocol.
2. Then $\mathcal{A}$ does the following computations:
   (a) $K16^{2^{nd}}_{Ti} \leftarrow PRNG(C^{1^{th}})$,
   (b) $RND'^{2^{nd}}_{T_i} \leftarrow C^{2^{nd}} \oplus K16^{2^{nd}}_{Ti}$.
   (c) $\forall\ i = 0 \ldots N_d$:
      i. $EPC16_{T_i} \longleftarrow i$,
      ii. If $B^{2^{nd}} = PRNG(EPC16_{T_i} \oplus RND'^{2^{nd}}_{T_i})$ then returns $EPC16_{T_i}$.
   (d) $\forall\ i = 0 \ldots N_d$:
      i. $N^{2^{nd}}_{T_i} \longleftarrow i$,
      ii. If $A = PRNG(N_{T_i} \oplus RND_{T_i} \oplus RND_{R_i} \oplus ID16_{R_i})$ then returns $N^{2^{nd}}_{T_i}$.

(e) To confirm the correctness of the retrieved parameters, the returned $EPC16_{T_i}$ from Step 2c and the returned $N_{T_i}^{2^{nd}}$ from Step 2d, $\mathcal{A}$ verifies whether $D^{2nd} \stackrel{?}{=} PRNG(N_{T_i} \oplus RND_{R_i} \oplus RND_{T_i} \oplus EPC16_{T_i} \oplus RND'_{T_i})$.

3. Returns the following values:
   (a) $EPC16_{T_i}$,
   (b) $N16_{T_i}^{old} = N_{T_i}^{2^{nd}}$,
   (c) $N16_{T_i}^{new} = PRNG(N16_{T_i}^{old} \oplus RND'^{2^{nd}}_{T_i})$,
   (d) $K16_{T_i}^{old} = PRNG(C^{1^{nd}})$,
   (e) $K16_{T_i}^{new} = PRNG(C^{2^{nd}})$.

The complexity of the given attack is eavesdropping two sessions of protocol between the T_i and R_i and 2×2^{16} evaluation of the *PRNG*-function. However, the adversary may comes up with more than one pre-image in Step 2c or Step 2d of the given attack(it must be noted that the existence of at least one pre-image in each step is guaranteed). Then, the adversary can use step 2e to roll out the wrong guesses.

Remark 1. Given all secret parameters of the tag, it would be easy to apply the following attacks on the protocol with the success probability of "1" and the cost of one run of protocol:

1. Traceability attack,
2. Tag impersonation attack,
3. Reader impersonation attack,
4. Desynchronization attack.

Remark 2. One may suggest to improve the security of protocol by pre-store the ID_{R_i} in T_i. However, then it is possible to retrieve it if $\mathcal{A}$ modifies steps 2d and 2e as follows:

(2d) For the returned value of $EPC16_{T_i}$ from Step 2c and $\forall\ i = 0 \ \ldots \ N_d$:
   1. $N_{T_i}^{2^{nd}} \longleftarrow i$,
   2. If $D^{2nd} = PRNG(N_{T_i}^{2^{nd}} \oplus RND_{R_i}^{2nd} \oplus RND_{T_i}^{2nd} \oplus EPC16_{T_i} \oplus RND'^{2nd}_{T_i})$ then returns $N_{T_i}^{2^{nd}}$.

(2e) For the returned value of $EPC16_{T_i}$ from Step 2c, the returned value $N_{T_i}^{2^{nd}}$ from Step 2d and $\forall\ i = 0 \ \ldots \ N_d$:
   1. $ID16_{R_i} \longleftarrow i$,
   2. If $A^{2nd} = PRNG(N_{T_i}^{2nd} \oplus RND_{T_i}^{2nd} \oplus RND_{R_i}^{2nd} \oplus ID16_{R_i})$ then returns $ID16_{R_i}$.

However, in this case the adversary would be successful in its attack if it comes up with only one pre-image in each of steps 2c and the modified 2d and 2e of the given attack. Otherwise, it should repeat the attack several times to come up with a unique solution. Given that the values of $ID16_{R_i}$ and $EPC16_{T_i}$ are static, eavesdropping three runs of protocol should be fairly enough to extract all given parameters.

4.1 Tag Impersonation Attack

To show another undesired property of AZUMI, in this section, we present an efficient tag impersonation attack against this protocol. Tag impersonation attack is a forgery attack that leads to identifying spoofed tags by a legitimate reader as a legitimate tag. In this section we show how an attacker can deceive the reader to authenticate it as a legitimate tag. To impersonate the tag T_i which communicants with the reader R_i, an adversary ($\mathcal{A}$) can follow the bellows steps:

Phase 1(Learning) : $\mathcal{A}$ eavesdrops one successful run of protocol and stores transferred messages between the reader and the legitimate tag include M_{req}, RND_{R_i}, RND_{T_i}, A, B, C, D where:

- $A = PRNG(N_{T_i} \oplus RND_{T_i} \oplus RND_{R_i} \oplus ID16_{R_i})$
- $B = PRNG(EPC16_{T_i} \oplus RND'_{T_i})$
- $C = RND'_{T_i} \oplus K16_{T_i}$
- $D = PRNG(N_{T_i} \oplus RND_{R_i} \oplus RND_{T_i} \oplus EPC16_{T_i} \oplus RND'_{T_i})$

Phase 2 (Impersonation) : To impersonate the legitimate tag, $\mathcal{A}$ waits until the reader initiates a new session of protocol, where:

1. The R_i generates a random number RND'_{R_i} and sends it with M_{req} to the T_i.
2. Once $\mathcal{A}$ receipts the message, it replies by sending RND''_{T_i}, A', B', C' where:
   - $RND''_{T_i} = RND'_{R_i} \oplus RND_{R_i} \oplus RND_{T_i}$,
   - $A' = A$,
   - $B' = B$,
   - $C' = C$
3. The reader receives RND''_{T_i}, A', B' and C' and upon receipt of these values, it proceeds as follows:
   - Starts the search process by picking $EPC16_{T_i}$ and $K16_{Ti} \in (K16^{old}_{Ti}, K16^{new}_{Ti})$ from each record.
   - Extracts RND'_{T_i} from $C' \oplus K16_{Ti}$.
   - Computes $PRNG(EPC16_{T_i} \oplus RND'_{T_i})$ and compares it with the received value of B', which is equal, so $\mathcal{A}$ is successfully identified as a legitimate tag.
   - Computes $PRNG(N_{T_i} \oplus RND''_{T_i} \oplus RND_{R_i} \oplus ID16_{R_i})$ and compares it with the received value of A' and authenticates $\mathcal{A}$ as a legitimate tag.

Following the given attack, the adversary would be authenticated by the reader as a legitimate tag with the probability of “1” while the complexity of attack is only two runs of protocol.

5 Conclusions

In this paper we considered the security of AZUMI which is an RFID mutual authentication protocol and presented several efficient attacks against the protocol. We presented a secret parameters disclosure attack that can retrieve all secret parameters related to a given tag T_i stored in tag or reader. The presented attack is a passive attack which needs two runs of protocol to determine all secret parameters. In addition, we presented an efficient tag impersonation attack against this protocol with the success probability of “1” and the cost of two runs of protocol.

Recall that the AZUMI protocol was proposed to fix the vulnerabilities of Chen and Deng’s protocol, our study shows that the designers have not reached their target at all. Hence, we encourage the other researchers to try to design a secure EPC-C1 G2-friendly protocol which is vital.

References

1. D. V. Bailey and A. Juels. Shoehorning security into the EPC tag standard. In R. D. Prisco and M. Yung, editors, *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 303–320. Springer, 2006.
2. C.-L. Chen and Y.-Y. Deng. Conformation of EPC class 1 generation 2 standards RFID system with mutual authentication and privacy protection. *Eng. Appl. of AI*, 22(8):1284–1291, 2009.
3. Class-1 generation 2 UHF air interface protocol standard version 1.2.0, Gen2, 2008. http://www.epcglobalinc.org/standards/.
4. EPC Tag data standar dversion 1.4.2008. http://www.epcglobalinc.org/standards/. Yearly report on algorithms and keysizes, Technical Report D.SPA.13Rev.1.0,ICT-2007-216676,. In *Gen2*. ECRYPT, 2010.
5. G. Kapoor and S. Piramuthu. Vulnerabilities in chen and dengs rfid mutual authentication and privacy protection protocol. *Eng. Appl. of AI*, doi:10.1016/j.engappai.2011.06.011, 2011.
6. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. RFID specification revisited. In *The internet of things:From RFID to The Next-Generation Pervasive Networked Systems*, pages 311–346. Taylor & Francis Group, 2008.
7. P. Peris-Lopez, J. C. Hernandez-Castro, J. E. Tapiador, and J. C. A. van der Lubbe. Cryptanalysis of an EPC class-1 generation-2 standard compliant authentication protocol. *Eng. Appl. of AI*, 24(6):1061–1069, 2011.