Cryptanalysis of Chen *et al.*'s RFID Access Control Protocol

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

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

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

Abstract. Recently Chen *et al.* have proposed a RFID access control protocol based on the strategy of indefinite-index and challenge-response. They have claimed that their protocol provides optimal location privacy and resists against man in the middle, spoofed tag and spoofed reader attacks. However, in this paper we show that Chen *et al.* protocol does not provide the claimed security. More precisely, we present the following attacks on the protocol:

1. Tag impersonation attack.
2. Reader impersonation attack.
3. Location traceability attack.

All attacks presented in this paper have the success probability of '1' on the cost of only one or two runs of protocol.

keyword RFID, Access Control, Spoofed Reader Attack, Authentication, Desynchronization Attack.

1 Introduction

Radio Frequency Identification (RFID) technology is a new technology that uses radio frequency in identifying objects, animals and humans includes three entities: the tag, the reader and the back-end data base. The tag is a constrained microchip that connects to objects that we want to authenticate or track them and contact with the reader by antenna. The reader can read or modify tag's information. The back-end data base keeps information related to different tags/readers.

RFID systems have many applications in libraries, e-passports, manufacturing, inventory control, supply chain management, e-health and so on. However, the main problem that impacts RFID system application is data security. For example, an RFID system may put the privacy of the object which the tag is connected to on risk. Hence, for the security concerns, only the authorized readers should be able to read or modify the information on the tags. In addition, only valid tags should be authenticated by reader and it should be infeasible for a fake tag to impersonate a legitimate tag. To address this requirement, several

RFID mutual authentication protocols [1–16] and access control protocols [17, 18] have already been proposed in the literatures.

Most of the available access control protocols are based on hash-functions. Nevertheless, two main drawbacks dissuade for the practical use of hash based-protocols in an RFID system. Firstly, the resource requirement of hash functions (circuit size, memory and power consumption) may not be available on a tag which is supposed to be very chip [19]. Secondly, when we send all data hashed the search process in the readers would be required, to find a matching between the values received from the tag and the records stored in the reader, which often implies a heavy computation load for the back-end data base.

Chen *et al.* [12] recently proposed a hash based access control protocol. To improve the search time for the reader, they proposed a novel approach. They proposed to represent the tag index as (x_i, y_i) an select two non-parallel random lines that crosses (x_i, y_i). Then, they select two random points on each line and include this information on a matrix. The generated matrix will be multiplied by a secret matrix and passed to the reader. Since the reader knows the secret matrix it can extract the tag index. However, we show that their protocol compromises privacy location. In addition, we show that a fake tag can impersonate a legitimate one and an adversary can impersonate a legitimate reader. It will get worse if we know that the success probabilities of our attacks are almost '1' while the complexities are at most two runs of protocol.

Paper Organization : In § 2 we review notations and preliminaries that are used through the paper. A brief description of Chen *et al.* protocol is given in § 3. Our reader impersonation and the tag impersonation attacks on the protocol are given in § 4 and § 5 respectively. We present our traceability attack on protocol in section § 6. Finally concluding remarks are presented in § 7.

2 Preliminaries

Throughout this paper, we will use the following notations:

- $index_i$: Tag's serial number.
- Key_i: Tag's secret value.
- $h(.)$: A one way hash function.
- Q: A random number generated by the reader side.
- R: A random number generated by the Tag.
- ω: A square matrix which is stored in all tags.
- ω^{-1}: The inverse matrix of ω which is stored in the reader.
- π: A square matrix generated by tag which includes some information related to $index_i$.

- f_{CRC}: A cyclic redundancy check function.
- $E_{Key_i}(.)$: An encryption function with the key of Key_i.
- $D_{Key_i}(.)$: The decryption function with the key of Key_i.
- ϵ: The critical response time.
- $\oplus$: Exclusive-or operation.

3 Chen *et al.* RFID Access Control Protocol

Recently, Chen *et al.* [12] proposed an access control protocol for RFID systems. The proposed protocol includes an authentication mechanism and an access right authorization mechanism to be used in low-cost RFID systems. The protocol, see also Figure 1, works as follows:

1. The reader generates a random number Q and sends it to the tag.
2. As the tag receives Q, it generates a random number R and computes $\gamma = h(Key_i \oplus Q \oplus R)$. To keep the tag's location private the serial number is pre-processed to be different in each access. The tag index is included in a matrix π as follows:
   (a) Use the tag index as a tuple denoted by (x_i, y_i).
   (b) Generated two non parallel lines crossed on tag index denotes by L_1 and L_2 respectively.
   (c) Select two random points on L_1 and denote them by (x_1, y_1) and (x_2, y_2).
   (d) Select two random points on L_2 and denote them by (x_3, y_3) and (x_4, y_4).
   (e) Generate π matrix as follows:
$$\pi = \begin{bmatrix} \mathbf{x_1} & \mathbf{y_1} & \mathbf{x_2} \\ \mathbf{y_2} & \mathbf{x_3} & \mathbf{y_3} \\ \mathbf{x_4} & \mathbf{y_4} & \mathbf{R \oplus Q} \end{bmatrix}$$
3. The tag computes matrix product $\pi.\omega$ and passes it along with γ to the reader.
4. As the reader receives $(\pi.\omega, \gamma)$, it pass $(\pi.\omega, \gamma, Q)$ to the back-end data base.
5. The back-end data base obtains π matrix by multiplying ω^{-1} to $\pi.\omega$ and obtains tag index (x_i, y_i) and R from π.
6. Given tag index, the back-end data base retrieves the tag's secret value Key_i from data base and verifies whether $\gamma \stackrel{?}{=} h(Key_i \oplus Q \oplus R)$. In the case of equality, it authenticates the tag, computes $\alpha = h(Key_i \oplus R)$ and sends Key_i, R and α to the reader.
7. Reader passes α to the tag.
8. Once the tag receives α, at first it checks that the response time is shorter than ϵ. Then, it verifies whether $\alpha \stackrel{?}{=} h(Key_i \oplus R)$ to authenticate the reader. If tag authenticated the reader the reader would be authorized to access the ciphertext C in the tag, where the tag sends C and related check value $V = h(f_{CRC}(C) \oplus Key_i \oplus R)$ to the reader.
9. As the reader receives C and V, the reader checks the integrity of C by comparing the received V with $h(f_{CRC}(C) \oplus Key_i \oplus R)$. In the case of equality, the reader decrypts C with the Key_i as $M = Dec_{Key_i}(C)$.

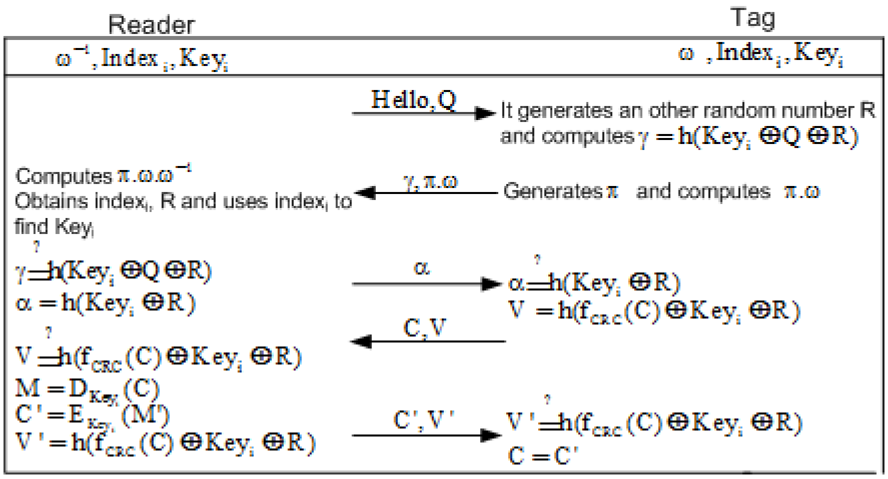

Fig. 1. Chen *et al.*'s RFID access control protocol.

10. Whenever the reader desires to modify data M' to the tag, it encrypts new information M' with the Key_i as $C' = E_{Key_i}(M')$ and sends C' with its check value $V' = h(f_{CRC}(C') \oplus Key_i \oplus R)$ to the tag.
11. Once the tag receives the message it verifies whether $V' \stackrel{?}{=} h(f_{CRC}(C') \oplus Key_i \oplus R)$ to update C to C'.

The authors claimed that the above protocol satisfies the following goals for an RFID system:

– guarantees the mutual authentication.
– provides the location privacy.
– resists the man-in-the-middle attack.
– resists to the spoofed reader attack.
– resists to the spoofed tag attack.

4 Reader Impersonation attack

Chen *et al.* [12] claim that their protocol is resistant against the spoofed reader attacks. More precisely, the authors state that to impersonate the reader, given $\gamma = h(Key_i \oplus Q \oplus R)$, the adversary at least requires to find a preimage for $h(.)$ to obtain $Key_i \oplus Q \oplus R$ and generate a valid $\alpha = h(Key_i \oplus R)$. However, we present a rather simple attack which can impersonate a legitimate reader as follows:

1. The adversary supplants a legal reader in a mutual authentication session and sends $Q = 0$ to the tag.

2. As the tag receives Q, it generates a random number R and computes $\gamma = h(Key_i \oplus R \oplus Q)$ and generate the matrix π following the given approach on the protocol description. Then, it replies with the tuple $(\gamma, \pi.\omega)$.
3. Recall that the adversary had selected $Q = 0$ so we have:

$$\gamma = h(Key_i \oplus R \oplus Q) = h(Key_i \oplus R \oplus 0) = h(Key_i \oplus R)$$

   Hence, when the adversary is expected to send some value as α, it just replies with the received γ as α and passes it to the tag.
4. As the tag receives α, which is equal to $h(Key_i \oplus R)$, it will authenticate the adversary as a legitimate reader.

The success probability of the given attack is '1' while the complexity is only a single run of protocol. Hence, despite of the authors claim, the protocol is vulnerable to the reader impersonation attack.

5 Tag Impersonation attack

The authors [12] claim that their protocol is resistant against the spoofed tag attacks. More precisely, similar to their argument for the spoofed reader, the authors state that to impersonate the tag, a fake tag needs $\bar{X} = Key_i \oplus R$ to generate a valid $\gamma = h(Key_i \oplus Q \oplus R) = h(\bar{X} \oplus Q)$. Therefore, they have claimed that the tag impersonation costs $2^n/2$ in average. However, we show that their assumption is not correct and, to impersonate a legitimate tag, an adversary does not necessarily require $\bar{X} = Key_i \oplus R$. At the follows, we present an attack which can impersonate a legitimate tag in a rather easy way:

1. The adversary eavesdrops a run of protocol and stores the tag replay to the reader query Q which is the $(\gamma, \pi.\omega)$ tuple.
2. In the future, to impersonate the tag, on receiving Q' the adversary replies with the stored tuple $(\gamma, \pi.\omega)$ as the expected $(\gamma', \pi'.\omega)$, where $\gamma = h(Key_i \oplus R \oplus Q)$ and:

$$\pi = \begin{bmatrix} \mathbf{x_1} & \mathbf{y_1} & \mathbf{x_2} \\ \mathbf{y_2} & \mathbf{x_3} & \mathbf{y_3} \\ \mathbf{x_4} & \mathbf{y_4} & \mathbf{R \oplus Q} \end{bmatrix}$$

3. As the back-end data base receives the tuple $(Q', \gamma', \pi'.\omega)$, it retrieves the matrix π' as follows:

$$\pi' = \pi'.\omega.\omega^{\mathbf{-1}} = \pi.\omega.\omega^{\mathbf{-1}} = \pi = \begin{bmatrix} \mathbf{x_1} & \mathbf{y_1} & \mathbf{x_2} \\ \mathbf{y_2} & \mathbf{x_3} & \mathbf{y_3} \\ \mathbf{x_4} & \mathbf{y_4} & \mathbf{R \oplus Q} \end{bmatrix}$$

4. Given the matrix π' and Q', the back-end data base assigns $R \oplus Q \oplus Q'$ to R' which is used on the verification of received γ'. In addition, given $\pi' = \pi$, the back-end data base extracts the tag index (x_i, y_i) correctly and retrieves the related Key_i from data base.

5. To authenticates the tag the back-end database verifies whether $\gamma' \stackrel{?}{=} h(Key_i \oplus Q' \oplus R')$, where, given that $R' = R \oplus Q \oplus Q'$, we have:

   $$h(Key_i \oplus Q' \oplus R') = h(Key_i \oplus Q' \oplus R \oplus Q \oplus Q') = h(Key_i \oplus Q \oplus R) = \gamma = \gamma'$$

6. The reader will authenticate the adversary as a legitimate tag.

The success probability of the given attack is '1' while the complexity is only two runs of protocol. Hence, despite of the authors claim, the protocol is also vulnerable to tag impersonation attack.

6 Traceability Attack on the Mutual Authentication Protocol

In this section we show how Chen *et al.* protocol puts at stake the location privacy of tags' holders because it is possible to track tags with the probability of '1'. Our traceability attack follows the used approach to mount the reader impersonation attack on the protocol, presented in § 4. However, in this attack, the adversary continues the protocol to receive the stored C value in the tag. More precisely, to trace a tag T_i, an adversary $\mathcal{A}$ can follow the steps described below:

1. $\mathcal{A}$ supplants a legal reader in a mutual authentication session and sends $Q = 0$ to the tag.
2. As the tag receives Q, it generates a random number R and computes $\gamma = h(Key_i \oplus R \oplus Q)$ and generates the matrix π following the given approach on the protocol description. Then, it replies with the tuple $(\gamma, \pi.\omega)$.
3. Recall that the adversary had selected $Q = 0$, so we have:

   $$\gamma = h(Key_i \oplus R \oplus Q) = h(Key_i \oplus R \oplus 0) = h(Key_i \oplus R)$$

   Hence, $\mathcal{A}$ just replies with the received γ as the expected α to be sent to T_i.
4. As the tag receives α, which is equal to $h(Key_i \oplus R)$, it will authenticate $\mathcal{A}$ as a legitimate reader.
5. When tag authenticates $\mathcal{A}$ as a legitimate reader, it would be authorized to access the ciphertext C in the tag where the tag replies with C and the related check value $V = h(f_{CRC}(C) \oplus Key_i \oplus R)$.
6. $\mathcal{A}$ stores C.
7. In the future, given T_j, $\mathcal{A}$ runes the above steps again to receive the stored C' of T_j.
8. If $C' = C$ then the adversary conclude that T_j is the target T_i.

As long as a legitimate reader does not update the stored decrypted value in T_j an adversary which follows the above attack would be able to trace T_i. In addition, if the adversary presents during the protocol run that change the encrypted value to C', it can store C and trace T_i based on this value. The success probability of the above attack is $1 - 2^{-n}$, where n is the length of ciphertext C , and the complexity is two runs of protocol.

7 Conclusion

In this paper we analyzed the security of Chen *et al.*'s RFID access control protocol and demonstrated several successful attacks against the protocol. We showed that this protocol does not resist against spoofed reader and spoofed tag. In addition, we demonstrated a traceability attack on protocol which can be applied to protocol between two data updating. The success probabilities of attacks are almost '1' and the complexities are at most two runs of protocol.

References

1. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361, Montpellier, France, November 2006. Springer-Verlag.
2. Chien Hung-Yu. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, December 2007.
3. Pedro Peris-Lopez, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. LMAP:A Real Lightweight Mutual Authentication Protocol for Low cost RFID tags. In *RFIDSec*, 2006.
4. Pedro Peris-Lopez, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *WISA*, volume 5379 of *Lecture Notes in Computer Science*, pages 56–68. Springer, 2008.
5. Alireza Sadighian and Rasoul Jalili. AFMAP: Anonymous Forward-Secure Mutual Authentication Protocols for RFID systems. In Rainer Falk, Wilson Goudalo, Eric Y. Chen, Reijo Savola, and Manuela Popescu, editors, *The Third IEEE International Conference on Emerging Security Information, Systems and Technologies(SECURWARE 2009)*, pages 31–36, Athens, Greece, 2009. IEEE Computer Society.
6. Alireza Sadighian and Rasool Jalili. FLMAP: A fast lightweight mutual authentication protocol for RFID systems. In *ICON*, pages 1–6. IEEE, 2008.
7. Lars Kulseng, Zhen Yu, Yawen Wei, and Yong Guan. Lightweight Mutual Authentication and Ownership Transfer for RFID systems. In *The proceedings of IEEE INFOCOM 2010*, pages 1–5, March 2010.
8. S. Weis. *Security and Privacy in Radio Frequency Identification Devices*. Masters Thesis, Massachusetts Institute of Technology (MIT), 2003.
9. Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *International Conference on Security in Pervasive Computing-SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212, 2004.
10. Kinoshita S. Ohkubo M., Suzuki K. Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In *Proc. of the 2004 Symposium on Cryptography and Information Security (SCI 2004)*, pages 719–724, 2004.

11. Yiyuan Luo, Qi Chai, Guang Gong, and Xuejia Lai. A lightweight stream cipher WG-7 for RFID encryption and authentication. In *GLOBECOM*, pages 1–6. IEEE, 2010.
12. Meng-Lin Tsai Yu-Yi Chen and Jinn-Ke Jan. The design of rfid access control protocol using the strategy of indefinite-index and challenge -response. *computer communication*, 34(3):250–256, 2011.
13. Jung-Sik Cho, Sang-Soo Yeo, and Sung Kwon Kim. Securing against brute-force attack: A hash-based rfid mutual authentication protocol using a secret value. *Computer Communications*, 34(3):391–397, 2011.
14. Tzu-Chang Yeh, Chien-Hung Wu, and Yuh-Min Tseng. Improvement of the rfid authentication scheme based on quadratic residues. *Computer Communications*, 34(3):337–341, 2011.
15. Dang Nguyen Duc and Kwangjo Kim. Defending rfid authentication protocols against dos attacks. *Computer Communications*, 34(3):384–390, 2011.
16. Chiu Chiang Tan, Bo Sheng, and Qun Li. Secure and serverless RFID authentication and search protocols. *IEEE Transactions on Wireless Communications*, 7(4):1400–1407, 2008.
17. R.Rivest D. Engels S.Weis, S.Sarma. Security and privacy aspects of low-cost radio frequency identification systems. In *1st International Conference on Wierless Communications, Networking and mobile computing 2007(WiCom 2007)*, pages 2078–2080, 2007.
18. H.Y.Chien. Secure access control schemes for rfid systems with anonymity.
19. M. Feldhofer and C. Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In *On the Move to Meaningful Internet Systems 2006 – OTM 2006*, volume 4277 of *Lecture Notes in Computer Science*, pages 372–381. Springer, November 2006.