Improvements over Extended LMAP+: RFID Authentication Protocol

Jitendra B. Gurubani, Harsh Thakkar, Dhiren R.Patel

Department of Computer Engineering, Sardar Vallabhbhai National Institute of Technology,
Surat-395007, India
{jitendra.gurubani,harsh9t,dhiren29p}@gmail.com

Abstract. Radio Frequency Identification (RFID) systems are increasingly being deployed in a variety of applications. In this paper, we propose a light weight mutual authentication protocol which is an improvement over extended LMAP+ protocol. In mutual authentication, the tag and the reader of the RFID systems will authenticate each other before transmitting unique ID of tag. The proposed protocol provides protection over traceability and de-synchronization attacks.

Keywords: RFID, Pseudonym, LMAP, Mutual Authentication Protocol

1 Introduction

Radio Frequency Identification (RFID) systems are used for automated identification of objects and people. Applications that include warehouse management, logistics, railroad car tracking, product identification, library books check-in/check-out, asset tracking, passport and credit cards, etc. use RFID technology. Most of the RFID systems comprise of three entities [1]: the tag, the reader and the back-end database. The tag is a highly constrained microchip (with antenna) that stores the unique tag identifier and other related information about an object. The reader is a device that can read/modify the stored information of the tags and transfer these data to a back-end database, with or without modification. Back end database stores this information and will keep track of the data exchanged by the reader.

The possible security threats to RFID systems include denial of service (DoS), man in the middle (MIM), counterfeiting, spoofing, eavesdropping, traffic analysis, etc.

The low cost deployment demand for RFID tags forces the lack of resources for performing true cryptographic operations to provide security. Typically, tags can only store few hundreds of bits and have very limited number of logic gates, out of which very few can be devoted to security tasks. Considering these resource constraints, we aimed for authentication protocol that uses light weight primitives.

The rest of the paper is organized as follows: Background and related work is discussed in section 2. Section 3 describes system design considerations and the proposed protocol. Section 4 shows defense against traceability and de-synchronization attacks with conclusions and references at the end.

2 Related Work

Providing light weight security in RFID systems is not a trivial task, yet efforts have been made towards this direction. Vajda and L. Buttyan[2] have proposed a set of extremely lightweight challenge response authentication algorithms. These can be used for authenticating the tags, but they may be easily attacked by a powerful adversary. Juels[3], proposed a solution based on the use of pseudonyms, without using any hash function. The RFID tag stores a short list of pseudonyms which indexes a table (row) where all the information about a tag is stored: it is rotated releasing a different index on each reader query. After a set of authentication sessions, the list of pseudonyms will need to be reused or updated through an out-of-band channel, which limits the practicality of this scheme. In addition to this there are other lightweight mutual authentication protocols proposed in the literature [4], [5], [6]. Attacks have been successfully mounted on all of these as demonstrated in literature [7], [8], [9].

Peris et al[10] proposed a Lightweight Mutual Authentication Protocol called LMAP. In addition, they proposed an extension of this protocol LMAP+. These protocols are extremely lightweight and use only simple bitwise operations. However, it has been discovered that these protocols do not achieve the security they claim [11]. Later, following the LMAP designing strategy, Li [12] proposed a new lightweight protocol which is extension of LMAP proposed by Peris et al. in [10]. After that, Safkhani et al [14] presented two possible attacks on protocol which is extension of LMAP+.

We propose an improvement over Li's protocol [12] LMAP+ - incorporating better security and without compromising performance. Security in terms of overcoming traceability and protection against de-synchronization attacks.

3 Proposed Protocol

3.1 Design Considerations

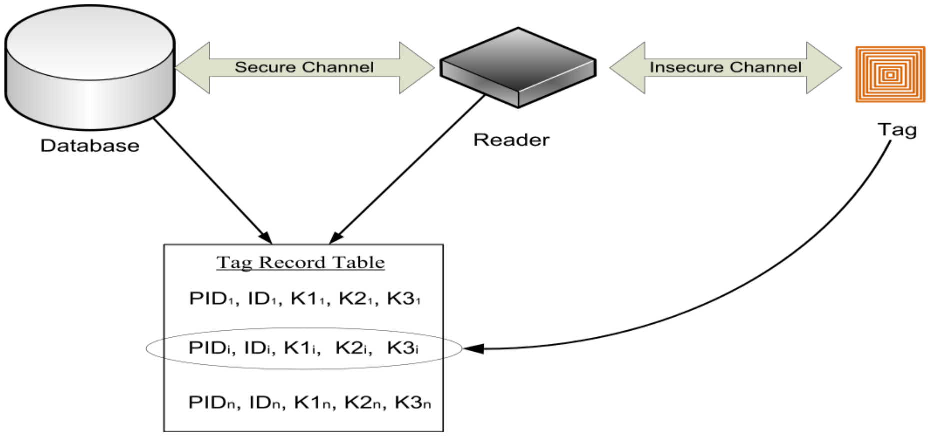
Database
Secure Channel
Reader
Insecure Channel
Tag
Tag Record Table
PID_1, ID_1, $K1_1$, $K2_1$, $K3_1$
PID_i, ID_i, $K1_i$, $K2_i$, $K3_i$
PID_n, ID_n, $K1_n$, $K2_n$, $K3_n$

Fig. 1. Typical RFID System

Fig.1 shows three main entities of the RFID systems which are involved in the mutual authentication scenarios. However, we assume only two roles in our simplified model, namely the reader (maintaining the database, where all tags' records are indexed and stored in a table); and the tag (to be authenticated). Before a tag is dispatched, its Unique ID and Pseudo-ID are written in its ROM and EEPROM respectively together with several secret values (for authentication purpose).

A successful authentication between a reader and a tag will trigger the update operations on the Pseudo-ID and secret values at both the tag and the database. We summarize the promising properties of our proposed scheme as follows:

- Privacy: a tag's Unique ID is never disclosed to unauthorized reader. Only the authorized reader will identify the Tag by its Pseudo-ID along with its corresponding tag entry in the database. Pseudo-ID and the keys used will be changed after every successful protocol round.
- Security: the scheme defends against various attacks like: replay attack, eavesdropping, spoofing attack, active man-in-the-middle attack, traceability attack and de-synchronization attack.
- Compactness: the 3-pass authentication protocol uses only ultra-lightweight functions like X-OR and mod 2^m addition, whose hardware implementations require only few number of gates.

3.2 Protocol Notations

In the proposed protocol, costly operations such as multiplications and hash evaluations are not used at all, and random number generation is only done at the reader end. Frequently used notations in this paper are listed below:

- $ID_{tag(i)}$: Tag's static identifier.
- $PID_{tag(i)}^{n}$: Tag's dynamic pseudonym at the n^{th}successful run of protocol.
- $K1_{tag(i)}^{n}$, $K2_{tag(i)}^{n}$ and $K3_{tag(i)}^{n}$: Tag's secret keys at the n^{th}successful run of protocol.
- r : A pseudorandom number which is generated by the reader.
- A, B, C : Messages transferred between reader and tag.
- $\oplus$: XOR operation.
- || : concatenation operator.
- + : addition $\text{mod}2^{m}$.

All parameters in the protocol are of length 96-bit.

3.3 System Initialization

It is composed of two initializations viz; for tag and for the database.

Tag Initialization: The RFID tag is assigned with two identifiers: a Pseudo-ID (PID) which will change for every protocol run; and a unique identifier (ID) which is a permanent identifier of the tag. Each tag is associated with three keys (K1, K2 and K3). Without loss of generality, we assume all five items have the same bit length L (e.g., L=96 bits for an EPC Gen2 RFID tag). As the PID and the keys must be updated for every successful protocol run, a tag needs 384 bits of nonvolatile memory (EEPROM) to store this data. Additionally, an L-bit ROM memory is required to store the permanent ID.

Database Initialization: A central database must be built in order to store all the information relevant to the RFID Tags. For each tag, it stores a tuple [PID, ID, K1, K2, K3]. All tuples are listed in a single database table, which has N records and the total database size is 5NL bits.

3.4 Protocol Description

The protocol has three main stages: tag identification, mutual authentication and updating as shown in table 1.

Tag Identification
Reader → Tag: Hello
Tag → Reader: $PID^{n}_{tag(i)}$

Mutual Authentication
Reader → Tag: A || B
Tag → Reader: C
Where,
A = $PID^{n}_{tag(i)} \oplus K1^{n}_{tag(i)} + r$
B = $PID^{n}_{tag(i)} + K2^{n}_{tag(i)} + r$
C = $PID^{n}_{tag(i)} \oplus (K3^{n}_{tag(i)} + r)$

Updating
By both Reader and Tag

$$PID^{n+1}_{tag(i)} = PID^{n}_{tag(i)} \oplus r + (K1^{n}_{tag(i)} + K2^{n}_{tag(i)} + K3^{n}_{tag(i)})$$

$$K1^{n+1}_{tag(i)} = K1^{n}_{tag(i)} \oplus r + (PID^{n+1}_{tag(i)} + K2^{n}_{tag(i)})$$

$$K2^{n+1}_{tag(i)} = K2^{n}_{tag(i)} \oplus r + (PID^{n+1}_{tag(i)} + K3^{n}_{tag(i)})$$

$$K3^{n+1}_{tag(i)} = K3^{n}_{tag(i)} \oplus r + (PID^{n+1}_{tag(i)} + K1^{n}_{tag(i)})$$

Table 1. n^{th} Protocol Run

- **Tag Identification**: Before initializing the protocol for mutual authentication, the reader has to identify the tag. The reader will send a hello message to the tag, which will be responded by sending its current pseudonym (PID). By means of this PID, only an authorized reader is able to search the database and access the tag's corresponding secret key (K = K1|K2|K3), which is necessary to carry out the next authentication stage.

- **Mutual Authentication**: The reader first generates a random number *r*. Using *r* and the keys *K*1 and *K*2, the reader generates the messages *A* and *B*, and then sends them to the tag. Thus, the reader actually conveys a random challenge to the tag. At the tag side, upon receiving the messages *A* and *B*, the tag can calculate two random numbers (*r*1 from *A* and *r*2 from *B*) using secret keys *K*1 and *K*2 respectively. If *r*1 equals to *r*2, the tag can obtain *r* correctly and prepare the response message *C*. On the reader side it calculates the value of C according to the equation in the table above as it has all required parameters and compares the calculated C value with the one received from the tag. If both are equal the tag is authenticated. Then using the PID value the reader retrieves the unique tag ID from the database table and considers the tag with this ID. Hereafter that reader proceeds with update operations. If the reader is not authenticated, the authentication protocol is aborted. Thus in this way the tag is identified by the reader without actually transmitting the unique ID of the tag.

- **Updating**: After the reader and the tag have authenticated each other, they carry out the pseudonym and key updating operations at both sides synchronously with the equations mentioned in table 1.

The mechanism for synchronization is same as described by Li [19]. Both reader and tag contain a status bit in the protocol denoted by s. In each run, if the protocol is successfully completed, s will be initialized with 0 otherwise it is set to 1. Hence, s = 1 indicates that the protocol was aborted. So it should be reset or restarted.

4 Security against traceability and de-synchronization attacks

Our protocol reflects improvements over Li's extended LMAP+. Safkhani et al.[14], showed that considering only the last significant bit(LSB), the modular additions mod 2^mcan be replaced by bitwise XOR, the adversary can trace the least significant bit of the unique ID of the tag in the LMAP+ protocol. Also he is able to de-synchronize the reader and tag to update their values to different numbers so that they will not authenticate each other for further communication. Our protocol provides defense from these attacks as the actual unique ID of the tag is not transmitted. Instead, the reader identifies the tag uniquely with the help of PID and corresponding tag entry in the back end database. So, the adversary will not be able to trace the tag or de-synchronize the communication between reader and tag.

5 Conclusion

Mutual authentication protocol for low cost RFID systems is proposed. The protocol is secure (more trustworthy than LMAP+) and uses ultra light weight bitwise operations.

As our proposal is an extension over LMAP+ protocol, it is secure against cloning, spoofing and man in the middle attack as LMAP+ protocol is. In addition it is also secure against traceability and de-synchronization attacks for which LMAP+ was not secure as shown by Safkhani et al.[14].

References.

1. *V.* D. Hunt, A. Puglia, and M. Puglia, *RFID: A Guide to Radio Frequency Identification*: Wiley-Inter science, 2007.
2. Vajda and L. Buttyan. "Lightweight authentication protocols for low-cost RFID tags", *Proc. of UBICOMP'03*, 2003.
3. Juels. "Minimalist cryptography for low-cost RFID tags", *Proc. of SCN'04*, volume 3352 of LNCS, pages 149–164. Springer-Verlag, 2004.
4. Sadighian and R. Jalili. Afmap, " Anonymous forward-secure mutual authentication protocols for rfid systems", *Third IEEE International Conference on Emerging*

Security Information, Systems and Technologies(SECURWARE 2009), pages 31–36, 2009.

5. Sadighian and R. Jalili. Flmap, "A fast lightweight mutual authentication protocol for rfid systems", *16th IEEE International Conference On Networks* (ICON 2008), pages 1–6, New Delhi, India, 2008.
6. H.-Y. Chien. 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.
7. M. Safkhani, M. Naderi, and N. Bagheri, " Cryptanalysis of AFMAP", *IEICE Electronics Express*, 7(17):1240–1245, 2010.
8. M. Safkhani, M. Naderi, and H. Rashvand., "Cryptanalysis of AFMAP", *International Journal of Computer & Communication Technologys*, 2(2):182–186, 2010
9. M. B´ar´asz, B. Boros, P. Ligeti, K. L´oja, and D. Nagy, "Passive Attack Against the M2AP Mutual Authentication Protocol for RFID Tags", *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
10. P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. "Lmap: A real lightwight mutual authentication protocol for low-cost rfid tags", *Proceedings of RFIDSec06 Workshop on RFID Security*, Graz,Austria, 12-14 July 2006.
11. T. Li and G. Wang., "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols", *IFIP SEC 2007,* Sandton, Gauteng, South Africa, May 2007.
12. T. Li., "Employing lightweight primitives on low-cost rfid tags for authentication.", *VTC Fall*, pages 1–5, 2008.
13. Ben Niu; Hui Li; Xiaoyan Zhu; Chao Lv; , "Security Analysis of Some Recent Authentication Protocols for RFID," *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on* , vol., no., pp.665-669, 3-4 Dec. 2011 doi: 10.1109/CIS.2011.152
14. Safkhani, Masoumeh; Bagheri, Nasour; Naderi, Majid; Sanadhya, Somitra Kumar; , "Security analysis of LMAP^{++}, an RFID authentication protocol," *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for* , vol., no., pp.689-694, 11-14 Dec. 2011