Improvements In RFID System Via Secure Mutual Authentication Protocol

Mr. Janak Tank, Prof. H. B. Jethva
G.T.U. M.Tech. in Computer Engineering.
L.D. Engineering College, Ahmedabad

Abstract- Radio Frequency Identification (RFID) systems are increasinglybeing deployed in a variety of applications these days. So, the security and privacy issues of these systems should be handled carefully, the main focus is on authentication of reader and tag. Many of the existing research protocols use the modern cryptographic functions which will not fit into the RFID systems where the RFID tags have very limited memory and computational power. So, some light weight authentication protocols are also proposed. In this work, we present a light weight mutual authentication protocol which is the improvement over extended LMAP+ protocol. The proposed protocol will also provide security over traceability and de-synchronization attacks.

Index Terms**—LAMP+, 250-3K, RFID systems, mutual, protocol. Light weight, versions, rotate, pseudonyms random, skimming attack, replay attack, eavesdropping, spoofing attack**

I. INTRODUCTION

Radio Frequency Identification (RFID) systems are used for automated identification of objects and people. This technology is widely adopted to a variety of applications. This system uses radio frequency to send and receive data. 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 that the tag has been attached to. The reader is a device that can read/modify the stored information of the tags and (if needed) transfer these data to a back-end database, with or without modification. Back end database will store this information and will keep track of the data needed by the reader.

In the recent era many applications including warehouse management, logistics, railroad car tracking, product identification, library books check-in/check-out, asset tracking, passport and credit cards are using RFID technology, but there are issues and problems related to RFID security and privacy. The possible security threats for RFID systems include denial of service (DoS), man in the middle(MIM), counterfeiting, spoofing, eavesdropping, traffic analysis, etc.

The low cost demands for RFID tags forces the lack of resources for performing true cryptographic operations to provide security. Typically, these tags can only store hundreds of bits and have 5K-10K logic gates, but only 250-3K can be devoted to security tasks. In spite of these restrictions, many researchers have proposed solutions which are based on the use of hash functions. Though this is good and secure solution, it is non-trivial task to implement these cryptographic hash functions with only 250-3K gates. Alternatively we have solutions which exclusively use non-cryptographic operations such as AND, OR, X-OR, Concatenate, Rotate, etc for authentication. The authentication protocols using these operations are called Light Weight Authentication Protocols. In this paper our proposed authentication protocol also uses this light weight operations.

The rest of the paper is organized as follows: Related work is described in section 2 and section 3 describes the proposed protocol. Section 4 shows defense against traceability and de-synchronization attacks. Finally, we end with conclusion and future work.

II. RELATED WORK

Though providing light weight security in RFID systems is not a trivial task, efforts are done in this direction. The authors of [2] propose a set of extremely lightweight challenge response authentication algorithms. These can be used for authenticating the tags, but they may be easily broken by a powerful adversary. In [3], Juels proposes a solution based on the use of pseudonyms, without using any hash function. The RFID tag stores a short list of pseudonyms: it rotates them, releasing a different one 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] have already been broken by [7], [8], [9].

In [10] Peris et al. proposed a Lightweight Mutual Authentication Protocol called LMAP. In addition, they proposed an extension of this protocol and called it LMAP+. These protocols are extremely lightweight and use only simple bitwise operations. However, it has been discovered very soon that these protocols do not achieve the claimed security [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 in [11], Authors presented two possible attacks on this protocol which is extension of LAMP.

In this paper we propose a protocol which is improvement over Li's protocol in [12]. Our work follows the design of [12], but with more security and light weight operations.

III. PROPOSED PROTOCOL

As we have discussed 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, it must be written with its identifier (in ROM), its pseudo-ID (in EEPROM) and several secret values (for authentication purpose).

IV. SYSTEM OVERVIEW

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 scheme as follows:

Privacy: a tag's ID is never disclosed means the tag will never transmit its unique ID. Reader will identify the Tag by its pseudo-ID and corresponding tag entry in the database. pseudo-ID is and the keys used will be changed after every successful protocol round.

Security: the scheme defends against a variety of attacks such as: replay attack, eavesdropping, spoofing attack,
skimming attack, active man-in-the-middle attack, traceability attack and desynchronization attack.

Compact: the 3-pass authentication protocol uses only ultra lightweight functions like X-OR and mod addition, whose hardware implementations require only hundreds of gates.

IV.1 PROTOCOL NOTATIONS

The proposed protocol is an ultra-lightweight RFID mutual authentication protocol using only bitwise operations. We use only simple operations such as: bitwise XOR () and addition *mod* (+). Costly operations such as multiplications and hash evaluations are not required at all, and random number generation is only done by the reader. Some of frequently used notations in this paper is listed below:

- $ID_{tag(i)}$: indicates tag's static identifier.
- $PID^{n}_{tag(i)}$: indicates tag's dynamic pseudonym at the n^{th}successful run of protocol.
- $K1^{n}_{tag(i)}$, $K2^{n}_{tag(i)}$ and $K3^{n}_{tag(i)}$: indicate tag's secret keys at the n^{th}successful run of protocol.
- r : indicates a pseudorandom number which is generated by the reader.
- A, B, C : indicates messages transferred between reader and tag.
- $\oplus$: indicates XOR operation.
- $\|$: indicates concatenation operator.
- + : indicates addition mod 2^{n}.
- All parameters in the protocol are of length 96-bit.

The system is initialized as follows:
Tag Initialization: An RFID tag is assigned with two identifiers: one is a pseudo-ID (PID) which will change for every protocol run; the other is a real 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 [4]). 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: The owner of the RFID tags needs to build a central database to store all the information. For each tag, it stored 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.

IV.2 PROTOCOL DESCRIPTION

The protocol has three main stages: tag identification, mutual authentication and updating.

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

Tag Identification: Before starting the protocol for mutual authentication, the reader has to identify the tag. The reader will send a hello message to the tag, which will answer 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*. With *r* and the keys *K*1 and *K*2, the reader generates the messages *A* and *B*, and then sends them to the tag. By this way, 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 separately. If *r*1 equals to *r*2, the tag can obtain *r* correctly and prepare the answer message *C*. On the reader side it calculates the value of C according to the equation in the above table as it has all required terms with it and compares its calculated C value with the 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 reader proceeds with update operations. And if the reader is not authenticated, the authentication protocol is aborted. 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 authenticated each other, they carry out the pseudonym and key updating operations at both sides synchronously with the equations mentioned in the above table.
The mechanism to overcome the de-synchronization attack is same as described by Li in [12]. both reader and tag contains a status bit in the protocol denoted by s. In each run, if the protocol successfully completed, s will be initialized with 0 otherwise it sets to 1. Hence, s = 1 indicates that the protocol was not successfully completed. So it should be reset or restarted.

V. DEFENSE AGAINST TRACEABILITY AND DE-SYNCHRONIZATION ATTACKS

Our protocol is improvements over Li's extended LAMP+ protocol. As the authors of [12], with the fact that considering only the last significant bit(LSB) modular additions mod 2m can be replaced by bitwise XOR has proved that the adversary can trace and find the least significant bit of the unique ID of the tag. 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 in further transactions. Out protocols defenses these attacks as in our protocol 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 in our protocol will not be able to trace the tag or de-synchronize the communication between reader and tag.

VI. CONCLUSION

In this paper we come up with a light weight mutual authentication protocol for low cost RFID systems. The protocol is secure and uses only light weight bitwise operations. The protocol works in three phases and identifies the tag without the transmission of the tag unique ID. So it is secure against traceability and de-synchronization attacks in which adversary uses this unique ID.

REFERENCES

[1] Juels. Minimalist cryptography for low-cost RFID tags. In Proc. of SCN'04, volume 3352 of LNCS, pages 149–164. Springer-Verlag, 2004

[2] M. Safkhani, M. Naderi, and H. Rashvand. Cryptanalysis of AFMAP. International Journal of Computer & Communication Technologys, 2(2):182–186, 2010.

[3] 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

[4] 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

[5] Sadighian and R. Jalili. Afmap: Anonymous forward-secure mutual authentication protocols for rfid systems. In The Third IEEE International Conference on Emerging Security Information, Systems and Technologies(SECURWARE 2009), pages 31–36, 2009.

[6] T. Li. Employing lightweight primitives on low-cost rfid tags for authentication. In VTC Fall, pages 1–5, 2008.

[7] T. Li and G. Wang. Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In IFIP SEC 2007, Sandton, Gauteng, South Africa, May 2007.

[8] M. Safkhani, M. Naderi, and H. Rashvand. Cryptanalysis of AFMAP. International Journal of Computer & Communication Technologys, 2(2):182–186, 2010.

[9] Juels. Minimalist cryptography for low-cost RFID tags. In Proc. of SCN’04, volume 3352 of LNCS, pages 149–164. Springer-Verlag, 2004.

[10] Sadighian and R. Jalili. Afmap: Anonymous forward-secure mutual authentication protocols for rfid systems. In The Third IEEE International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009), pages 31–36, 2009.

[11] Rama N. And Suganya R., “An Enhanced Power-efficient Gossamerbased Protocol for Passive RFID Tags”, unpublished, Submitted for review and publication to International Journal of Computer and Internet Security on February 2010

[12] Rama N. And Suganya R., “An Enhanced Power-efficient Gossamerbased Protocol for Passive RFID Tags”, unpublished, Submitted for review and publication to International Journal of Computer and Internet Security on February 2011.