SULMA: A SECURE ULTRA LIGHT-WEIGHT MUTUAL AUTHENTICATION PROTOCOL FOR LOW-COST RFID TAGS

Mehrdad Kianersi[1], Mahmoud Gardeshi[2] and Mohammad Arjmand[3]

[1]Department of Information Technology and Communication, IHU University, Tehran, Iran
mehrdad.kianersi@gmail.com
[2]Department of Information Technology and Communication, IHU University, Tehran, Iran
mgardeshi2000@yahoo.com
Islamic Azad University, Shoushtar Branch, Shoushtar, Iran
Arjmand88@yahoo.com

ABSTRACT

In 2006, Peris et al. proposed the first member of UMAP family for low-cost RFID tags. This family does not provide significant security due to limitations that exist in using strong cryptographic primitives, and show much vulnerability against attacks. In this paper, we introduce a new ultra light-weight mutual authentication protocol with inspiring Gossamer protocol that proposed by Peris et al. We show that our protocol provides more security for RFID technology.

KEYWORDS

RFID, Ultra light-weight, Mutual authentication, Low-cost Tag

1. INTRODUCTION

Radio frequency identification (RFID) is an emerging technology. It is the next generation of an optical barcode with several major advantages over an optical barcode since a line of sight between the reader and the barcode is not needed, and several tags can be read simultaneously.
RFID technology is rapidly finding more diversified applications in today's marketplace. For example, RFID technology is now being used for automatic tariff payment in public transport, animal identification and tracking, automated manufacturing, and logistical control for automatic object identification since every object can be identified by a unique identification tag number. A RFID system consists of three parts: the radio frequency (RF) tags, the RF readers, and the back-end database server. The back-end server associates records with the tag data collected by the readers. Tags are typically composed of a microchip for storage and performing logical operations and a coupling element such as an antenna coil for wireless communications. Memory chips on the tags can be read-only, write-once/read-many, or fully writable. Each memory chip holds a unique ID and other pertinent information transmitted to the tag reader using a RF. The readers interrogate the tags using a RF antenna and interact with the back-end database for more functionality.

The notable parameter in Low-Cost RFID tags is their sever limits in power consumption and computation that allow them to execute the simple bitwise operations. So we introduce a secure

DOI:10.5121/iju.2011.2202

ultra lightweight mutual authentication (SULMA) protocol that present considerable amount of security and efficiency.

2. RELATED WORKS

Huang chien [1] classified RFID tags according to their computation capability. In that classification, RFID tags are divided into two main categories, high-cost and low-cost. High-cost tags are divided into full-fledged and simple tags. Full-fledged tags support conventional cryptographies like symmetric key encryption, one-way hash functions and public key cryptography. Simple tags can support random number generator and one-way hash functions. But, in another one, low-cost tags are divided into light-weight and ultra light-weight tags. Light-weight tags can support random number generators and simple functions such as CRC. But ultra light-weight tags can only compute simple bitwise operations like AND, OR, XOR and rotation, etc. In 2006, Peris et al. proposed the first ultra light-weight protocol called M2AP[2] and followed by EMAP[3] and LMAP[4]. These protocols are based on simple bitwise operations and despite of their compatibility with ultra light-weight RFID tags limits, they did not provide sufficient security and were attacked by researchers, frequently [5, 6, 7, 8, 9]. After these protocols, in 2007, Chien [1] proposed a relatively strong protocol titled SASI. The SASI protocol is highly reminiscent of the UMAP family, and more concretely, of the LMAP protocol. The main difference between these two protocols is the inclusion of rotation in the set of operations supported by each tag. Indeed, the messages transmitted over the insecure channel in the UMAP family are computed by the composition of triangular-functions (e.g. addition modulo 2, bitwise OR, AND, etc.) – easily implemented in hardware – which finally results in another triangular-function [15]. A triangular-function has the property that output bits only depend of the leftmost input bits, instead of all input bits. This undesirable characteristic (lack of diffusion) greatly facilitated the analysis of the messages transmitted by the UMAP protocols, and thus the work of the cryptanalyst. But some attacks such as de-synchronization [20] and full disclosure [10] introduced on SASI due to carelessness in computing public messages and bitwise operations [10].

In 2008, Peris et al. [11] proposed another strong ultra light-weight mutual authentication called Gossamer. This protocol was appeared more secure because of using two consecutive rotation functions and also defining a MixBits function that generates new random numbers by using two random numbers. But Gossamer was attacked and broken also, due to some structural and MixBits function weaknesses [12, 13]. Before executing any attack on Gossamer, Rama et al. [14] proposed an improved version of Gossamer that called SSL-MAP and claimed that their protocol is stronger than Gossamer, because they used Sign/Logarithm system for increasing the complexity of Gossamer. But their protocol attacked by Kianersi et al. [15]. We showed SSL-MAP vulnerable against full-disclosure and de-synchronization attacks. Subsequently, David-Prasad [16] and Lee et al. [17] proposed two ultra light-weight protocols that Peris et al. [18, 19] introduced successful attacks such as traceability, full disclosure, cloning and de-synchronization on their protocols.

3. SULMA PROTOCOL MODEL

In our protocol, each tag has unique *ID*, the old and new values of index pseudonym (IDS^{old}, IDS^{new}) and the values of old and new keys (k_1^{old}, k_2^{old}, k_1^{new}, k_2^{new}). In reader side these values are stored, too. We use two consecutive rotation functions for computing public messages and internal state variables, in which the first *Rot(x, y)* function, rotates value of *x*, (*y* mod 96) positions to left and the second *Rot(x, y)*, rotates value of *x*, *wh(y)* positions to left, too. In which

wh(y) denotes Hamming weight of variable y. For security enhancement we introduce a MixBits function that has high Non-linearity properties. For this work, we used a structure similar to Feistel structure. The proposed MixBits function is illustrated in Fig. 1. This function is used for generating a random number from two another random numbers. In this figure, F_1 and F_2 are defined as follows:

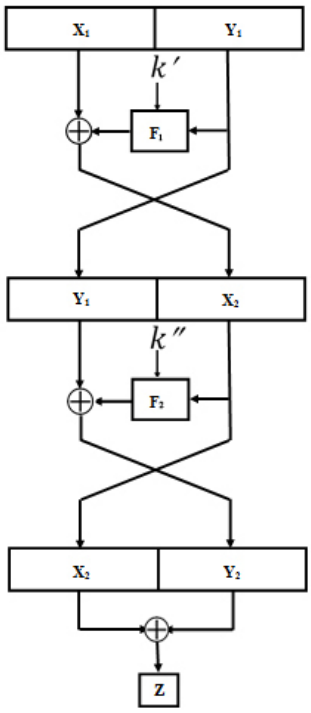


Figure 1. MixBits function

$$F_1 = Rot(Y_1 + k' + c, k' + Y_1)$$
$$F_2 = Rot(X_1 + k'' + c, k'' + X_1)$$

In which, *Rot(x, y)* in F_1, performs a circular shift on the value *x*, *wh(y)* positions to left and *Rot(x, y)* in F_2, performs a circular shift on value *x*, (*y* mod 96) positions to left. For a mathematical description of rotation functions, we have:

$$Rot(x, y \bmod N) = x \times 2^{N-(y \bmod N)} \bmod 2^N - 1$$

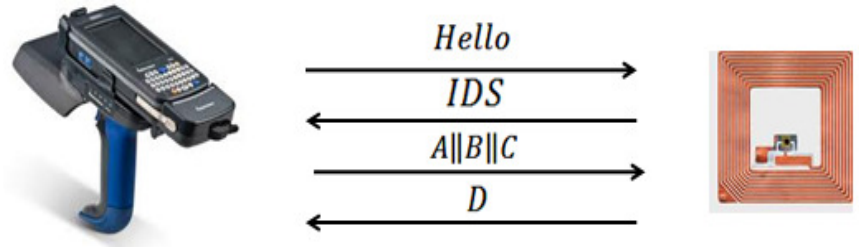
In which *N* equals 96 in our protocol. It is obvious that this equation is one-way. And about *Rot(x, wh(y))*, by considering the fact that in $\binom{96}{k}$ states *wh(y)* equals *k*, we can assert that *Rot(x, wh(y))* is one-way. So those are suitable for using in the structure similar Feistel structure.

4. SULMA PROTOCOL

This protocol consists of three phases: tag identification, mutual authentication and update phase.

Tag Identification: the reader first sends a "HELLO" message toward tag and the tag answers with its IDS^{next}. The reader after receiving this message tries finding an identical entry in data base. If it succeeds, the tag is identified and mutual authentication phase starts. Otherwise, the reader requests IDS^{old} and after tag's answer, it verified then they enter mutual authentication phase.

Mutual authentication: in this step, the reader generates two random numbers n_1, n_2. If n_1 or n_2 or both of them equal zero (a sequence of 96 zeros), the reader generate two another random numbers. Then, computes public messages A, B, C using n_1, n_2 and shared keys between itself and the tag. Now it sends to the tag. The tag extracts n_1, n_2 from A and B respectively and computes C', if C' equals C the reader is authenticated. Now, the tag computes message D



$A = Rot\ (Rot\ (IDS + K_1 + c + n_1, K_2) + K_1, K_1)$
$B = Rot\ (Rot\ (IDS + K_2 + c + n_2, K_1) + K_2, K_2)$
$n_3 = MixBits\ (n_1, n_2, K_1, K_2)$
$K_1^* = Rot\ (Rot\ (n_2 + K_1 + c + n_3, n_2) + K_2 \oplus n_3, K_1)$
$K_2^* = Rot\ (Rot\ (n_1 + K_2 + c + n_3, K_2) + K_1 + n_3, n_1)$
$n_1' = MixBits(n_3, n_2, K_1^*, K_2^*)$
$C = Rot\ (Rot\ (n_3 + K_1^* + c + n_1', n_3) + K_2^* \oplus n_1', K_2) \oplus n_1'$
$D = Rot\ (Rot\ (n_2 + K_2^* + ID + n_1', K_1) + K_1^* + n_1', n_3) + n_1'$

Updating Phase (in both Tag and Reader side):

$n_2' = MixBits\ (n_1', K_1^*, n_3, K_2^*)$
$IDS^{old} = IDS$
$IDS^{next} = Rot\ (Rot\ (n_1' + K_1^* + IDS + n_2', n_1') + K_2^* \oplus n_2', K_1) \oplus n_2'$
$K_1^{old} = K_1$
$K_1^{next} = Rot\ (Rot\ (n_3 + K_2^* + c + n_2', n_3) + K_1^* + n_2', K_2) + n_2'$
$K_2^{old} = K_2$
$K_2^{next} = Rot\ (Rot\ (IDS^{next} + K_1^* + c + K_1^{next}, IDS^{next}) + K_2^* + K_1^{next}, n_2')$

Figure 2. SULMA Protocol

and starts update phase after sending D for reader. The reader verifies received message D and enters to update phase, too.

Update Phase: in this phase, the tag and the reader update their secret values such as IDS, k_1 and k_2 according to Figure 2.

5. Security Analysis

In this section, we analyze SULMA protocol for various aspects of security.

5.1. Data Confidentiality

All public messages in this protocol consist of at least three secret common values between tag and reader. So, only the authorized tags and readers can produce public message, and this causes that the integrity of received data be confident.

5.2. Tag anonymity and resistance against traceability attacks

After successful mutual authentication, each tag updates its *IDS*. Update procedure contains various random numbers. So, *IDS* of all tags have random nature and the attacker cannot identify or trace the tag by using it. Of course, if the attacker request *IDS* from the tag, between two successful mutual authentications, the tag answers with same *IDS* (old and new) but this scenario don't worth in real world. Because, if the malicious reader is following the tag, not need to ask it in order to track it. There is another condition that supposes the tag be authenticated with authorized reader then after updating *IDS* value successfully the malicious reader cannot trace it.

5.3. Passive attacks

Considering the fact that, we used two consecutive circular shift and two MixBits functions with non-linear characteristics in computing public messages, therefore the non-linear specification of these messages increase significantly. So, discovering any relationship between these messages in consecutive sessions would be very difficult.

5.4. De-synchronization attack

In this protocol, we stored the old and new values of *IDS* and keys in both side tag and reader. This cause, even in launching an active attack, the de-synchronization would not happen. Also, because of using the different random numbers in various sessions and verifying the received messages in both sides (verifying the message *C* in tag and verifying the message *D* in reader), an active attacker cannot alter the messages and interrupt the protocol's procedure. By this way the de-synchronization attack that lunched on Gossamer would not be able to de-synchronize the SULMA protocol. The similar solution is proposed in [15] for improving the SSL-MAP against de-synchronization.

5.5. Mutual authentication

The notable point in this protocol is that the tag first authenticates the reader (by verifying received message C) and then sends it's ID. This protocol provides mutual authentication for tags and readers. Only an authorized reader that has (k_1, k_2) can produce a valid $A\|B\|C$ message and similarly only an authorized tag can extract n_1, n_2 from $A\|B\|C$ and compute a valid message *D*. The protocol procedure prevents any message forging because of freshness and randomness in public messages and verifying the messages in any stage of protocol.

5.6. Forward Security

Forward security is a property that guarantees the security of past communications, even when a tag is compromised at a later stage. Suppose a tag is exposed and its secret values (*IDS*, k_1, k_2) are revealed, the attacker still cannot infer any information from previous sessions. As two unknown nonce's (n_1, n_2) and five internal secret values (n_3, n'_1, n'_2, k_1^*, k_2^*) are involved in the message

creation (mutual authentication phase). Additionally, these internal values are employed in the updating phase. Consequently, past communications cannot be easily jeopardized.

5.7. Performance analysis

We compare SULMA protocol with other Ultra light-weight mutual authentication protocols are proposed yet, in Table 1.

Table 1. Performance Comparison of Ultra-lightweight Authentication Protocols

	UMAP Family	*SASI*	*Gossamer*	*UMA*	*David Prasad*	*SULMA*
Resistance to De-synchronization Attacks	*NO*	*NO*	*NO*	*NO*	*NO*	*YES*
Resistance to Disclosure Attacks	*NO*	*NO*	*NO*	*NO*	*NO*	*YES*
Privacy and Anonymity	*YES*	*YES*	*YES*	*YES*	*YES*	*YES*
Mutual Authentication and Forward Security	*YES*	*YES*	*YES*	*YES*	*YES*	*YES*
Total Messages for Mutual Authentication	*4-5L*[1]	*4L*	*4L*	*3L*	*5L*	*4L*
Memory Size on Tag	*6L*	*7L*	*7L*	*5L*	*4L*	*7L*
Memory Size for each Tag on Database	*6L*	*4L*	*4L*	*3L*	*3L*	*7L*
Operation Types on Tag	,∨ ,⊕ + ∧	∧ ,∨ ,⊕ *Rot* [2] ,+	+ ,⊕ ,*Rot*[3] *MixBits*	∨ ,^ ,⊕ *Rot*[2]	⊕ , ∧	+ ,⊕ *Rot*[2,3], *MixBits*

1. L denotes the bit length of variables
2. Rot(x, y) = x << wh(y), being wh(y) the Hamming weight of vector y
3. Rot(x, y) = x << (y mod L) for a given value of L in our case L = 96

6. CONCLUSIONS

In this paper we introduced a new ultra light-weight mutual authentication protocol inspiring SASI and Gossamer. In which, we used a structure similar to Feistel structure for producing a random number from two another random numbers for increasing randomness of messages and security enhancement. Also, we stored the old and new values of shared data in both reader and tag for preventing de-synchronization attack. This scheme provides strong authentication and strong integrity of the transmissions and of the updated data, and can withstand all the possible attacks that break the security of the previous schemes. The tag in SULMA requires only simple operations such as AND, OR, XOR and rotations for computing the public messages and update parameters. These excellent features make it very attractive to low-cost RFID tags.

Acknowledgement

This work is supported by the education & Research Institute for ICT, Tehran, Iran.

REFERENCES

[1] Huang, Chien, (2007) "SASI: A New Ultra lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE *Transactions on Dependable and Secure Computing* 4(4), pp 337–340.

[2] Pedro, P. Lopez & Julio, C. Hernandez & Juan, M. Estevez-Tapiador & Arturo, Ribagorda, (2006) "M2AP: A minimalist mutual authentication protocol for low-cost RFID tags", *Proc. of UIC'06,* vol 4159 of LNCS, pp 912–923.

[3] Pedro, P. Lopez & Julio, C. Hernandez & Juan, M. Estevez-Tapiador & Arturo, Ribagorda (2006) "LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags", *Hand. of Workshop on RFID and Lightweight Cryptography.*

[4] Pedro, P. Lopez & Julio, C. Hernandez & Juan, M. Estevez-Tapiador & Arturo, Ribagorda (2006), "EMAP: An efficient mutual authentication protocol for low-cost RFID tags", *In Proc. of IS'06, Springer-Verlag*, vol 4277 of LNCS, pp 352–361.

[5] Tieyan, Li & Robert, Deng (2007) "analysis of EMAP - an efficient RFID mutual authentication protocol", *In Proc. of AReS'07.*

[6] Tieyan, Li & G, Wang (2007) "Security analysis of two ultra-lightweight RFID authentication protocols", *Proc. of IFIP-SEC'07.*

[7] C, Hung-Yu & H. Chen-Wei. (2007) "Security of ultra-lightweight RFID authentication protocols and its improvement", *SIGOPS Oper. Syst. Rev.,* 41(4), pp 83–86.

[8] M. B´ar´asz, & B. Boros & P. Ligeti & K. L´oja & D. Nagy (2007)" Breaking LMAP", *Proc. Of RFIDSec'07.*

[9] M. B´ar´asz & B. Boros & P. Ligeti & K. L´oja & D. Nagy(2007) "Passive Attack Against the M2AP Mutual Authentication Protocol for RFID Tags", *Proc. of First International EURASIP Workshop on RFID Technology.*

[10] Julio, C. Hernandez-Castro & Juan, M. E. Tapiador & Pedro, Peris-Lopez & Juan.-J. Quisquater(2008) "Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol". IEEE *Transactions on Dependable and Secure Computing.*

[11] Pedro, P. Lopez & Julio, C. Hernandez & Juan, M. Estevez-Tapiador & Arturo, Ribagorda (2009) "Advances in Ultra ightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol", *Journal of Information Science and Engineering*, Vol. 25 No. 1, pp. 33-57.

[12] Zeeshan, Bilal & Ashraf Masood & Firdos Kausar (2009) "Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol," *International Conference on Network Based Information System.*

[13] Eslam, Gamal & Eman, shaaban, Mohamed, Hashem (2010) "Lightweight Mutual Authentication Protocol for Low Cost RFID Tags" , *International Journal of Network Security & Its Applications (IJNSA)*, Vol 2, Num 2. Pp 27-37.

[14] Rama, N & Suganya, R (2010) "SSL-MAP: A More Secure Gossamer Based Mutual Authentication Protocol for Passive RFID Tags" , *International Journal on Computer Science and Engineering*, Vol. 02, pp 363-367.

[15] Mehrdad, Kianersi & Mahmoud, Gardeshi & Hamed, Yousefi (2011) "Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFID Tags:SSL-MAP", *proc. of CoNeCo 11, Ankara.*

[16] Matiue, David & Nile, Prasad (2010) "Providing Strong Security and High Privacy in Low-Cost RFID Networks", *SpringerLink.*

[17] Y,-C. Lee & Y, -C. Hsieh & P, -S. You & T,-C. Chen(2010) "A New Ultra lightweight RFID Protocol with Mutual Authentication", *In Proc. of WASE'09*, Vol 2 of ICIE, pp 58-61.

[18] Pedro, P. Lopez & Julio, C. Hernandez & Juan, M. Estevez-Tapiador & Arturo, Ribagorda (2010) "Security Flaws in a Recent Ultra lightweight RFID Protocol", *rfid sec asia' 10.*

[19] Julio, C. Hernandez & Pedro, P. Lopez & R, C. W. Phan & Juan M. E. Tapiador (2010) " Cryptanalysis of the David-Prasad RFID Ultra lightweight Authentication Protocol", *RFIDSec'10, Istanbul.*

[20] T, Cao & E, Bertino & H, Lei (2009) "Security Analysis of the SASI Protocol". *IEEE Transactions on Dependable and Secure Computing 6(1)*, pp 73–77.

Authors

Mehrdad Kianersi received the Bachelor's degree in Telecommunication Engineering from Islamic Azad University of Najaf abad, Iran, in 2008 and Master's degree in Telecommunication in the field of Cryptography from IHU, Tehran, Iran (2011). Currently, he is research assistant (RA) at the research centre of cryptography, IHU, Tehran, Iran. His research interests includes: Lightweight cryptography, RFID security and authentication protocols.

Mahmoud Gardeshi received his Erudition Degree in applied mathematics from Amir Kabir University, Islamic Republic of Iran in 2000. Currently, he is a researcher at the I. H. University. His research interest includes: cryptography and information security.

Mohammad Arjmand* received the Bachelor's degree in Telecommunication Engineering from IH University, Tehran, Iran, in 2008 and Master's degree in Telecommunication in the field of Cryptography from IHU, Tehran, Iran (2011). Currently, he is teacher assistant in Islamic Azad University, Shoushtar branch, Shoushtar, Iran. His research interest includes: Cryptography, Applications of RFID.