Lightweight RFID Mutual Authentication Protocol against Feasible Problems

Yongming Jin[1,2], Huiping Sun[3], Wei Xin[1,2], Song Luo[1,2], and Zhong Chen[1,2]

[1] School of Electronics Engineering and Computer Science
Peking University, Beijing, China
[2] Key Laboratory of High Confidence Software Technologies
Ministry of Education, Beijing, China
[3] School of Software and Microelectronics
Peking University, Beijing, China
{jinym,xinwei,luosong,chen}@infosec.pku.edu.cn,
sunhp@ss.pku.edu.cn

Abstract. The wide deployment of RFID systems has raised many concerns about the security and privacy. Many RFID authentication protocols are proposed for these low-cost RFID tags. However, most of existing RFID authentication protocols suffer from some feasible problems. In this paper, we first discuss the feasible problems that exist in some RFID authentication protocols. Then we propose a lightweight RFID mutual authentication protocol against these feasible problems. To the best of our knowledge, it is the first scalable RFID authentication protocol that based on the SQUASH scheme. The new protocol is lightweight and can provide the forward security. In every authentication session, the tag produces the random number and the response is fresh. It also prevents the asynchronization between the reader and the tag. Additionally, the new protocol is secure against such attacks as replay attack, denial of service attack, man-in-the-middle attack and so on. We also show that it requires less cost of computation and storage than other similar protocols.

Keywords: Security, RFID, Protocol, Authentication, SQUASH.

1 Introduction

Radio Frequency Identification (RFID) is a wireless automatic identification and data capture technology that uses radio signals to identify a product, animal or person without the need for physical access or line of sight. The architecture of an RFID system basically consists of the tag, the reader and the database. The tag is an identification device attached to items. The reader can read and access the tag's data by broadcasting an RF signal. The database connects to the reader via a secure network. The main benefits of RFID systems are that they can provide automated and multiple identification capture and system analysis, can read several tags in the field at the same time automatically, and can help to track valuable objects. However, the wide deployment of RFID systems has raised many concerns about the security and privacy[1].

S. Qing et al. (Eds.): ICICS 2011, LNCS 7043, pp. 69–77, 2011.

A counterfeit reader can be used for communication with a real tag. It implements the same protocol and sends the messages the tag expects to receive. The attacker can capture the transmitted signals using suitable radio frequency equipment. In some scenes, it is possible to relay messages from a legitimate tag to a legitimate reader using a man-in-the-middle device. For this purpose, tags must be authenticated. The low cost demanded for RFID tags forces them to be very resource limited. Typically, the tags only have hundreds of store bits and 5-10K logic gates that only between 250 to 3000 gates can be devoted to security functions[2]. Much research has focused on providing RFID tags with lightweight cryptographic protocols. A lot of efforts have already been put in developing efficient RFID identification or authentication protocols[3,4]. However, there are several common feasible problems that exist in the RFID authentication protocols.

In this paper, we discuss these feasible problems and present a lightweight RFID mutual authentication protocol against feasible problems. We determine the feasible requirements of RFID authentication protocols. It is shown that if a protocol satisfies these requirements, the protocol will be feasible and practical.

The remainder of the paper is organized as follows. In Section 2, related work is reviewed. We propose the feasible problems and lightweight RFID mutual authentication protocol in Section 3 and Section 4 respectively. In Section 5, the security and performance is analyzed. Finally, we conclude our paper in Section 6.

2 Related Work

Ohkubo et al. propose an RFID privacy protection scheme providing indistinguishability and forward security [5]. This protocol uses a low-cost hash chain mechanism to update tag secret information to provide these two security properties. However, it is subject to replay attacks, and it permits an adversary to impersonate a tag without knowing the tag secrets.

Molnar and Wagner propose a private authentication protocol for library RFID which uses a shared secret and a pseudorandom number function to protect the messages communicated between tag and reader[6]. This scheme cannot provide forward security. Once a tag is compromised, the attacker can trace past communications from this tag, because a tag's identifier and secret key are static.

Dimitriou proposes an RFID authentication protocol that enforces user privacy and protects against tag cloning[7]. The protocol is based on the use of a secret shared between tag and database that is refreshed to avoid tag tracing. However, the scheme is prone to the asynchronization attack.

Lopez et al. propose a lightweight mutual authentication protocol for low-cost RFID tags, called LMAP[8]. It offers an adequate security level and can be implemented in the most RFID systems that only need around 300 gates. In order to implement the new protocol, tags should be fitted with a small portion of rewritable memory and another read-only memory. Lopez et al. also proposed a M^2AP protocol that has the similar properties[2]. However, the attacker can

break the synchronization between the RFID reader and the tag in a single protocol run so that they cannot authenticate each other in any following protocol runs[9].

Chien and Chen introduce a mutual authentication protocol for RFID conforming to the EPC C1G2 standards[10]. The server database maintains copies of both old and new tag keys to resist the asynchronization attack. In order to give forward security, the authentication key and the access key are updated after a successful session. However, a strong attacker that compromises a tag can identify a tag's past interactions from the previous communications.

Berbain et al. proposed a novel forward private authentication scheme build upon less computationally expensive cryptographic ingredients instead of one way hash functions[11]. The new protocol is based on less complex cryptographic building blocks. This yields efficient hardware implementations compared to previous RFID protocols.

Ma et al. refine the definition of unp-privacy and proven that ind-privacy is weaker than unp-privacy. In this sense, a pseudorandom function family is the minimal requirement on an RFID tag's computational power for enforcing strong RFID system privacy. They also propose a new RFID protocol that satisfy the minimal requirement[12].

3 Feasible Problems

In this section, we discuss some feasible problems existing in the known RFID authentication protocols. We only discuss the most important requirement that RFID authentication protocols should be satisfied. If a protocol has these problems, it may be a theoretical protocol, not a feasible protocol. For example, the low cost demanded for RFID tags forces them to be very resource limited. Therefore the protocol should be lightweight and constructed on the base of the minimalist cryptography[13]. If a protocol is vulnerable to the asynchronization attack, the tag will be disfunctional and the reliability of the RFID system will be reduced. The tracking and forward security are also important issues along with the large-scale deployment of the RFID tags. We don't discuss the replay attack, man-in-the-middle attack, etc. in this section, because they are very common problems and many literature have discussed these requirements.

3.1 Lightweight

RFID tags are highly resource constrained and cannot support strong cryptography. Even a standard cryptographic hash function, such as MD5 or SHA-1, is beyond the capabilities of the most tags. Therefore, there is a strong need for new, lightweight cryptographic primitives that can be supported by low-cost RFID tags. In this paper, we introduce the SQUASH scheme (which is a squashed form of SQUare-hASH), which is ideally suited to RFID-based challenge-response authentication [14]. The basic idea of SQUASH is to mimic the operation of the Rabin encryption scheme, in which a message m is encrypted under key n. n is

the product of at least two unknown prime factors. The cipher text $c = m^2 \pmod{n}$. The scheme describes how to simplify and speed up the Rabin encryption scheme without affecting its well studied one-wayness. The details can be found in the literature [14].

3.2 Asynchronization

An adversary disturbs the interactions between reader and tag by intercepting or blocking messages transmitted. Such an attack could cause a reader and a tag to lose synchronization. This can be viewed as a kind of denial of service (DoS) attack. For example, in the DPLK protocol[15], the server might update the shared data, while the tag does not. In such a case they would no longer be able to authenticate each other.

3.3 Tracking

In some cases, outsiders to the RFID system may also be interested in monitoring and profiling the users of the RFID system. If a person does not want others to know what items he carries, then the RFID tags attached to these items must not reveal this information to unauthorized RFID readers[16]. The tracking problem means an attacker can link two different authentication actions to the same RFID tag. That is to say, the tag is tracked. In order to prevent the tracking, the protocol should be designed to respond with a fresh randomly messages in every interactive session.

3.4 Forward Security

If given all the internal state of a target tag at time t, the attacker is able to identify target tag interactions that occurred at a time $t' < t$. That is, knowledge of a tag's current internal state could help identify the tag's past interactions, and the past transcripts of a tag may allow tracking of the tag owner's past behavior. This issue is related to the leakage of tag's secret key. When the tag's current secret key is exposed, the tag's past interaction should be protected. Therefore, the protocol that satisfies this requirement should update the tag's secret key with the one-way cryptographical function. There are many RFID authentication protocols don't satisfy the forward security[11].

4 Lightweight RFID Authentication Protocol against Feasible Problems

Based on the above feasible problems, we propose a lightweight RFID mutual authentication protocol that satisfies these requirements. The new protocol can be viewed as a research case of the RFID feasible protocol. It is lightweight and the SQUASH is simple enough to be implemented on low-cost RFID tags[17,18]. Meanwhile, the SQUASH is provably as secure as the Rabin cryptosystem.

The new protocol save the previous secret key and can prevent the asynchronization between the reader and the tag. In every authentication session, the tag produces a random number and refreshs the response. If the authentication succeeds, the tag's secret key will be updated by Rabin algorithm. Nobody can identify the tag's past interactions even if he has the current secret key of the tag.

4.1 Definitions

We use the following definitions.

T_i: A tag
R_i: An RFID Reader
D_i: The Database of the T_i
k: A security parameter, $1200<k<1300$
n: The product of unknown prime factors, $n=2^k$-1
t: The length of the exchange ciphertext
s_i: A string of l bits assigned to T_i
t_i: T_i's identifier of l bits, which equals s_i^2 mod n
u_i: The previous string of l bits assigned to T_i
v_i: T_i's previous identifier of l bits, which equals u_i^2 mod n
U_i: The detailed information associated with tag T_i
s_i' : A new string of l bits assigned to T_i
t_i' : T_i's new identifier of l bits, which equals $s_i'^2$ mod n
$\oplus$: XOR operator
$[x]_t$: The value x's t bits.
$\leftarrow$: Substitution operator
x>>a: Right circular shift operator, which rotates all bits of x to the right by the bits, as if the right and left ends of x were joined.

4.2 Protocol Description

1. $R_i \rightarrow T_i$: Query request.
2. $T_i \rightarrow R_i \rightarrow D_i$: M, N.

The tag selects a random number r_T, computes $M=t_i \oplus r_T$, $N'=r_T^2 \bmod n$, $N=[N']_t$, and sends (Query, M, N) to the reader, where the reader will forward (M, N) to the backend database. If an adversary forges a new message f_M by M and f_N by N, he needs to compute r_T and solve *SQUASH* scheme. It is provably at least as secure as Rabin's public key encryption scheme.

3. $D_i \rightarrow R_i$: s_i, r_T ,U_i

For each tuple (s_i,t_i) in the backend database, D_i computes $N'=(M \oplus t_i)^2$ mod n and verifies whether the equations $N=[N']_t$. If it can find a match, then the tag T_i is successfully identified and authenticated, and the D_i will forward the tag's token (s_i,r_T) and information U_i to the R_i via the secure channel. If it can't find a match, it has two chooses which depends on the tradeoff between security and efficiency. In order to obtain the better security, D_i stops the process with failure. Otherwise, the D_i computes $N' = (M \oplus v_i)^2$ mod n and verifies

whether the equations $N = [N']_t$ hold for each tuple (u_i,v_i) in its database. If there is a match, D_i sends (u_i, r_T) which replaces (s_i, r_T), and U_i to R_i. If not, it stops the process with failure. Finally, D_i computes $s'_i = t_i$, and $t'_i = s'^2_i \bmod n$, updates the old secret value(u_i,v_i) by (s_i,t_i), and saves the new secret(s'_i,t'_i).

4. $R_i \rightarrow T_i : P$

To authentication itself to the tag and update the identification T_i on the tag, R_i computes $P = s_i \oplus (r_T >> l/2)$, and sends P to T_i.

5. The Tag T_i

T_i computes $s_i = P \oplus (r_T >> l/2)$. If $t_i = s_i^2 \bmod n$, then update t_i by $t'_i = t_i^2 \bmod n$.

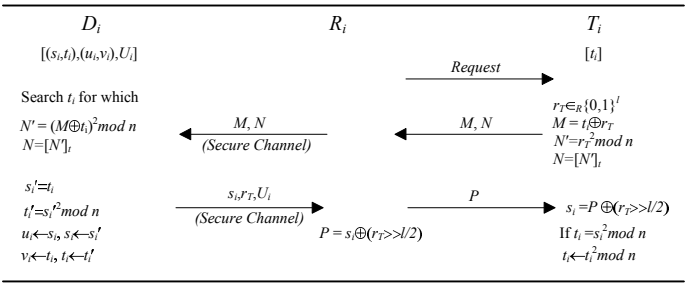

Fig. 1. Lightweight RFID Authentication Protocol Against Feasible Problems

5 Analysis

5.1 Security and Privacy

In this section, we give a security and privacy analysis of our proposed scheme.

Forward Security (FS): The new protocol can protect the privacy of the tag T_i. A strong attacker cannot identify the tag's past interactions, even if he knows the present internal state of T_i. Nobody is able to discover the previous identifiers of T_i because the reader and the tag produce new secrets (s'_i, t'_i) by Rabin algorithm. As a result, the attacker cannot find t_i to match $t'_i = t_i^2 \bmod n$.

Backward Security (BS): If the current tag secrets have been revealed, the only way of maintaining the backward security is to replace the exposed key to protect future transactions. This issue is related to tag ownership transfer. The new protocol can prevent the previous owners to read communications between the new owner and the tag. When the new owner updates secrets (s_i,t_i) for T_i using the Rabin Encryption Scheme in authentication process, the old owner cannot pry into the new owner's secrets using the knowledge of the exposed secrets.

Replay Attack (RA): The new protocol can protect against the replay attack. If an attacker uses the old message, for example, (M, N), the attacker cannot find a t_i to match $N' = (M \oplus t_i)^2 \bmod n$, $N = [N']_t$ because the tag's secret is changed and the old secret is no longer valid.

Denial of Service (DoS): To resist the DoS attack, we require the database to save the old values to recover synchronization with T_i. If an adversary prevents message P from reaching T_i, T_i will not update its identifier, but D_i will. In the following authentication process, T_i will use old secret value to compute M, N and D_i can recover the old secret value from (u_i,v_i).

Man-in-the-middle Attack (MITM): Any attacker can obtain the message (M,N) and P. He can prevent the correct message and send a different message. If he change the old message, he should find a t_i that exists in the database to satisfy the equation $N = (M \oplus t_i)^2 \bmod n$, $N = [N']_t$. Its security is based on the Rabin's public key encryption scheme. If an attacker changes the values P and try to let the tag update an error t_i, he needs know the r_T to find out t_i' , then computes the s_i' . However, the r_T is a random number produced by the tag T_i. It is very hard to find out.

The following table shows the comparison in the sense of security and privacy discussed in this Section.

Table 1. Security and Privacy Comparison

Schemes	FS	BS	RA	DoS	MITM
Ohkubo et al.[5]	√	√	×	√	√
Molnar et al.[6]	×	×	√	√	√
Dimitriou[7]	√	√	√	×	√
Lopez et al.[8]	√	√	√	×	√
Chien et al.[10]	∗	√	√	√	√
Berbain et al.[11]	√	√	×	×	√
Ma et al.[12]	×	√	√	√	√
The new scheme	√	√	√	√	√

√: resist such an attack.
∗: resist attack under some assumptions
×: can't protect against such an attack.

5.2 Efficiency Considerations

In the new protocol, the tag needs l bits of non-volatile memory to store its secret t_i. It is common condition that we can find out through the following table. Compare to other schemes, the new protocol has lower tag computation and tag communication cost.

Obviously, the new protocol needs the DB more storage cost to storage the old secret value (u_i,v_i) to prevent the asynchronization between the DB and the tag when the tag fails to receive the last message authentication code. In the practical application, it is a trade-in measure. Let l is the length of the random number and the secret value of T_i, k is the length of the tag's ID, q is the length of hash value. Let the number of total tags is n, p is the cost of PRNG

operation, h is the cost of Hash function, r is the cost of Rabin encryption. In general, r is less than h. The cost of XOR, bit shift, etc. operation is negligible.

The table 2 shows the performance comparison between the existing scheme and the new scheme.

Table 2. Performance Comparison

Schemes	TC	TS	RC	RS	CC
Ohkubo et al.[5]	$2h$	l	$2h$	$l+k$	l
Molnar et al.[6]	$h+p$	$l+k$	$O(n)h+p$	$l+k$	$2l+2k$
Dimitriou[7]	$2h+p$	k	$2h+p$	k	$2l+3q$
Lopez et al.[8]	$O(1)$	$l+k$	$2p$	$l+k$	$5l$
Chien et al.[10]	p	$l+k$	p	$l+k$	$2l+2q$
Berbain et al.[11]	$3h$	l	$O(n)h+p$	$l+k$	$l+q$
Ma et al.[12]	$2h$	$l+q$	$2h+p$	$2q+l+k$	$l+2q$
The new scheme	$3r+p$	$l+q$	$O(n)h+h$	$2q+l+k$	$2l+t$

6 Conclusions

In this paper, we discuss the feasible problems that exist in the known RFID authentication protocols. Then a lightweight RFID mutual authentication protocol against these problems is proposed. It is based on the SQUASH, which is a new MAC scheme for highly constrained devices such as RFID Tags. It is exceptionally simple that can be efficiently implemented on processors and is provably at least as secure as Rabin's public key encryption scheme. The new protocol is lightweight and can provide the forward security. We also analyze the new scheme's security and efficiency and give the comparison with other schemes.

As a part of future work, a model of feasible RFID authentication protocol will be deeply researched. And by the formalized analyze, we try to prove that the new model has better architecture and arts.

Acknowledgments. Research works in this paper are partial supported by Natural Science Foundation of China (No.61170263).

References

1. Juels, A.: RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006)
2. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: M^{2}AP: A Minimalist Mutual-authentication Protocol for Low-cost RFID Tags. In: Ma, J., Jin, H., Yang, L.T., Tsai, J.J.-P. (eds.) UIC 2006. LNCS, vol. 4159, pp. 912–923. Springer, Heidelberg (2006)

3. Lehtonen, M., Staake, T., Michahelles, F.: From identification to authentication-a review of RFID product authentication techniques. In: Networked RFID Systems and Lightweight Cryptography, pp. 169–187 (2008)
4. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic Approaches for Improving Security and Privacy Issues of RFID Systems. Wiley Online Library (2010)
5. Ohkubo, M., Suzuki, K., Kinoshita, S.: Cryptographic approach to "privacy-friendly" tags. In: RFID Privacy Workshop. MIT, MA (2003)
6. Molnar, D., Wagner, D.: Privacy and security in library RFID: Issues, practices, and architectures. In: Pfitzmann, B., Liu, P. (eds.) Conference on Computer and Communications Security – ACM CCS, pp. 210–219. ACM Press, Washington, DC (2004)
7. Dimitriou, T.: A lightweight RFID protocol to protect against traceability and cloning attacks. In: First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 59–66 (2005)
8. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags. In: Proceedings of 2nd Workshop on RFID Security (2006)
9. Li, T., Wang, G.: Security analysis of two ultra-lightweight RFID authentication protocols. In: New Approaches for Security, Privacy and Trust in Complex Environments, pp. 109–120 (2007)
10. Chien, H.-Y., Chen, C.-H.: Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards. Computer Standards & Interfaces 29(2), 254–259 (2007)
11. Berbain, C., Billet, O., Etrog, J., Gilbert, H.: An efficient forward private RFID protocol. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 43–53. ACM Press (2009)
12. Ma, C., Li, Y., Deng, R.H., Li, T.: RFID privacy: relation between two notions, minimal condition, and efficient construction. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM Press, New York (2009)
13. Juels, A.: Minimalist Cryptography for Low-Cost RFID Tags. In: Blundo, C., Cimato, S. (eds.) SCN 2004. LNCS, vol. 3352, pp. 149–164. Springer, Heidelberg (2005)
14. Shamir, A.: SQUASH – A New MAC with Provable Security Properties for Highly Constrained Devices such as RFID Tags. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 144–157. Springer, Heidelberg (2008)
15. Duc, D.N., Park, J., Lee, H., Kim, K.: Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning. In: Symposium on Cryptography and Information Security, Hiroshima, Japan (2006)
16. Langheinrich, M.: A survey of RFID privacy approaches. Personal and Ubiquitous Computing 13(6), 413–421 (2009)
17. Koshy, P., Valentin, J., Zhang, X.: Implementation and performance testing of the SQUASH RFID authentication protocol. In: Applications and Technology Conference (LISAT), 2010 Long Island Systems. IEEE Press, New York (2010)
18. Gosset, F., Standaert, F.X., Quisquater, J.J.: FPGA implementation of SQUASH. In: Proceedings of the 29th Symposium on Information Theory in the Benelux (2008)