A Secure and Lightweight Authentication Protocol for RFID

Liu Cheng, Lin Shenwen and Li Yingbo*
National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
lyb@cert.org.cn

Li Na and Wang Xuren
College of Information Engineering, Capital Normal University, Beijing10048, China
wangxr@ihep.ac.cn

***Abstract*—With the increasing popularity of RFID applications, RFID protocols are widely discussed. Most RFID protocols use a central database to store the RFID tag data, while severless RFID protocols are proposed to provide users with security and privacy protection without the connection and security problem between readers and sever. The shortcoming of severless RFID protocols is that the reader is authorized to access limited tags. A new tag cannot be authenticated by a reader if the tag is not appearing in list L_i of the reader. That is not practical especially in product anti-fake considering the quantity of product increasing and so tags. We have developed Tan's work to deal with the problems by introducing two new parameters, brand secret b and series secret s. Product brands and series are limited while the quantity of product is most likely large. And it can resist loss of basic privacy, tracking, cloning, eavesdropping, physical attacks and denial of service attacks. Our protocol can meet the needs of the security, portability and low cost RFID system.**

Keywords-Radio frequency identification; server-less; lightweight authentication protocol for RFID

I. INTRODUCTION

Most of the existing RFID authentication protocol comprises tags, readers and central database. During the certification stage, reader needs to connect back-end database to verify tag information for authentication. So in RFID authentication system with the back-end server, the reader must maintain the security and integrity of communication with the server to ensure real-time communication. It is difficult to achieve this goal. Frequent accessing the server will significantly increase the cost of RFID systems, reducing the portability and flexibility of RFID system [1].

Chiu C. Tan first proposed the concept of severless RFID authentication protocols [2]. In the authentication phase, the reader only reads the tag data and compares it with the value stored in the reader without connecting to the database for data authentication. Tan's work attracted a number of researchers to study severless RFID security authentication protocols [3-8].

These studies made some improvements of Tan's work, but they don't change the basic theory. A reader will need to save a list L including information of tags which CA center has authorized the reader to access [9]. In these studies, the authentication protocol is mainly used for searching the RFID tags, that is, to determine whether or not a specific tag exists in a set of tags. And the number of tags is limited and the reader has mastered all the tags' information. New tags can't be added in this process unless they get the CA certificating. If the new tags come frequently, CA will be required to updates readers frequently too for authentication.

978-1-4799-7284-5 /15/$31.00 ©2015 IEEE

This work was supported by National Key Technology R&D Program (No.2012BAH37B02).

Corresponding author: Li Yingbo, lyb@cert.org.cn

As product quantity is usually large and tags for product increase correspondently, it is inefficient to add new tags to readers frequently though CA and back-end database. But the product bands and series are less. In our work, with two parameters, brand secret b and series secret s, tags can be verified by readers automatically without visiting back-end database and CA center.

In the paper, we analyze the security of serverless authentication protocols, especially the one proposed by Tan et al, and find its weakness in section 2.Thenwe proposed a revised serverless authentication protocol and analyze its security in section 3and efficiency in section 4. We give concluding remarks in Section 5.

II. RELATED WORK

There are many schemes on sever supporting and severless RFID protocols. Protocols [2-7] really do not use back-end severs but as discussed above there are shortcoming with them. All these can't add new tags into list automatically. Protocols based on hash functions, which are lightweight and suitable for low-cost tags, include Hash-Lock protocol[10], Randomized Hash-Lock protocol[11], Hash-Chain protocol[12], Hash-based ID variation[13], Distributed RFID Challenge-Response protocol[14], LCAP protocol[15] etc. These protocols usually are insecure or unpractical. Juels's protocols [16] for RFID authentication use heavy cryptography which seems to be impractical.

We mainly discuss Tan's work on which our work is based. We use subscript to specify a specific tag or reader and their information stored. For example, the j-th tag T_j stores its identifier id_j and secret t_j.

The access list L_i stored in the reader R_i specifies the tags' information the reader can access. The structure of L_i is shown as followed.

$$L_i = \begin{cases} f(r_i, t_1) : & id_1 \\ \dots \quad : & \dots \\ f(r_i, t_n) : & id_n \end{cases}$$

The protocol is illustrated as followed.

(1) $R_i \rightarrow T_j$: request

(2) $R_i \leftarrow T_j$: n_j

(3) $R_i \rightarrow T_j$: n_i, r_i

(4) $R_i \leftarrow T_j$: $h(f(r_i, t_j))_m$, $h(f(r_i, t_j)\| n_i\|n_j) \oplus id_j$

(5) R_i: checks L_i for matching $h(f(r_i, t_j))_m$

(6) R_i: determines $h(f(r_i, t_j))_m$, $h(f(r_i, t_j)\| n_i\|n_j) \oplus id_j$, to obtain id_j

In this protocol, lightweight hash function and XOR, instead of symmetric or asymmetric cryptographic algorithm, were applied. Tan et al has analyzed the protocol is free from the attack of Privacy, Tracking, Cloning, Eavesdropping, Physical attack and Denial of service (DoS).

III. OUR REVISED SERVERLESS AUTHENTICATION PROTOCOL WITH TAG AUTO-ADDING

Tan et al. have analyzed their protocol's security and thought the protocol provides privacy protection. They also thought it resists tracking and cloning attack and so on. However, this protocol does not adding new tag information to readers without CA authentication and back-end database support. In manufactory, products are made by great amount under some band and series of brand. It is easy to keep and store brand and series' information for both readers and tags authenticated by CA. But it is difficult and inefficiency to keep information for each product or goods due to huge quantity. If doing so, readers will spend a lot time searching list L_i.

In our protocol, two secrets, b standing for brand secret, and s, standing for series secret, are described as

b_j: brand secret unique by CA

s_j: series secret, unique by CA

t_j: tag secret, $t_j = f(id_j, s_j)$

So reader R_i authorized to access tags $T_1 \cdots T_n$, for series but not for specific product, will have L_i where

$$L_i = \begin{cases} f(r_i, b_1): & s_1 \\ \ldots & : \ \ldots \\ f(r_i, b_n): & s_n \end{cases}$$

Reader owned all brands and series' secrets, which can be used for two-way authentication.

(1) $R_i \rightarrow T_j$: request

(2) $R_i \leftarrow T_j$: n_j

(3) $R_i \rightarrow T_j$: n_i, r_i

(4) $R_i \leftarrow T_j$: $h(f(r_i, b_j)||n_i||n_j) \oplus s_j$

(5) R_i: calculate $h(f(r_i, b_j)||n_i||n_j) \oplus s_x$, search each s in L_i, for matching $h(f(r_i, b_j)||n_i||n_j) \oplus s_j$ to obtain s_j

(6) $R_i \rightarrow T_j$: n_i', $h(f(r_i, b_j)||n_j)$, n' is a new random number generated by R_i

(7) T_j: checks if $h(f(r_i, b_j)||n_j)$ is correct. If not, refuses R_i

(8) $R_i \leftarrow T_j$: $h(f(r_i, b_j)||n_i'||n_j) \oplus id_j$, $h(f(r_i, b_j)||n_i'||n_j) \oplus t_j$

(9) R_i: determines $h(f(r_i, b_j)||n_i'||n_j)$ to obtain id_j, t_j

(10) R_i: if t_j equal to $f(id_j, s_j)$, authorized to access T_j

Where n_i, n_j are random numbers generated by R_i and T_j respectively. T_j sends its s_j a $h(f(r_i, b_j)||n_i||n_j) \oplus s_j$ to protect s_j. An unauthenticated reader cannot obtain s_j since he does not know $f(r_i, b_j)$, and hence the $h(.)$ value. This is a form of tag authenticating reader. The reader checks L_i for matching entries. If there are no matching, then either the RFID tag is a fake, since it is not able to generated a correct $f(r_i, b_j)$, or that it is a tag that R_i is not authorized to access the tag, thus no information of the t*ag* appearing in L_i. If there is a match, the reader then uses the random numbers n_i and n_j to obtain $h(f(r_i, b_j)||n_i||n_j) \oplus s_j$ and s_j. If the s_j received from the tag does not match entry in L_i then again authentication fails. Different random n_i and n_i' are used in two queries, which mean that $h(f(r_i,b_j)||n_i||n_j)$ changes to avoid tracking attack.

IV. PERFORMANCE EVALUATION

The proposed protocol based on Tan protocol makes it possible for readers to access new tags while computation and storage increase. But compared with regular method of adding tags by CA and back-end database, it is acceptable. Compared with the traditional back-end server-based authentication protocols, this protocol has been improved in terms of safety and efficiency. Table 1 compares computation and security performance among our work and other typical protocols. H stands for the implementation of a hash function, G executing a pseudo-random number function, l the length of the hash function, g length of the pseudo-random number, d for the reader or the tag id's length, n representing the number of product tag, n' number of brand series and $n' \ll n$。

V. CONCLUSION

Based on the existing authentication protocol analysis and summary, a secure RFID mutual authentication and security protocol is proposed, in terms of improved efficiency and safety of traditional RFID authentication protocol having. The result indicates our protocol can provide tag auto-adding, mutual authentication and privacy protection, resisting attacks. Next target is to make further improvements to the work, to reduce the amount of computation and communication between reader and tag. Together with the development of anti-counterfeiting technology and networking technology, commodity security and privacy protecting will be achieved.

TABLE 1 COMPARISON OF THE EFFICIENCY AND SECURITY(√ : SECURE, × : NOT SECURE)

Protocols	Computation(times)				privacy leaking	tracing	Cloning	Denial-of-service	Data synchronization
	Reader	*Tag*	*Back-end database*	*Communication*					
Tan protocol[2]	$nH + G$	$3H + G$	0	$h + m + 2g + d$	√	√	√	√	√
Proposed protocol	$(n' + 3)H + 2G$	$4H + G$	0	$4h + 3g + d$	√	√	√	√	√
Hash-Lock protocol[10]	0	0	0	6d	×	×	×	×	√
Randomized Hash−Lock protocol[11]	nH	$H + G$	0	$h + g + (n + 1)d$	×	√	×	×	√
Hash chain protocol[12]	0	2H	nH	$2h + d$	×	√	×	×	×
Hash-based ID variation protocol[13]	0	3H	$(2n + 1)H + R$	$6h + 2g + 2d$	√	×	×	×	×
Distributed RFID Challenge-Response protocol[14]	G	$2H + G$	$(n + 1)H$	$4h + 4g$	√	√	√	×	√
LCAP protocol[15]	G	2H	$(2n + 1)H$	$4.5h + 2g$	√	×	√	×	×

[1] Pang L, Li H, He L, et al. Secure and efficient lightweight RFID authentication protocol based on fast tag indexing [J]. International Journal of Communication Systems, 2013.

[2] Tan C C, Sheng B, Li Q. Secure and serverless RFID authentication and search protocols [J]. Wireless Communications, IEEE Transactions on, 2008, 7(4): 1400-1407.

[3] SowmyaMyneni, SatyajayantMisra, GuoliangXue, SAMA: Serverless Anonymous Mutual Authentication for Low-Cost RFID Tags[C], IEEE ICC 2011 proceedings.

[4] Kim Z, Kim J, Kim K, et al. Untraceable and serverless RFID authentication and search protocols[C]//Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011 Ninth IEEE International Symposium on. IEEE, 2011: 278-283.

[5] Lee C F, Chien H Y, Laih C S. Server‐less RFID authentication and searching protocol with enhanced security[J]. International Journal of Communication Systems, 2012, 25(3): 376-385.

[6] Safkhani M, Peris-Lopez P, Bagheri N, et al. On the security of tan et al. serverless RFID authentication and search protocols [M]. Radio Frequency Identification. Security and Privacy Issues. Springer Berlin Heidelberg, 2013: 1-19.

[7] Deng M, Yang W, Zhu W. Weakness in a Serverless Authentication Protocol for Radio Frequency Identification[M]//Mechatronics and Automatic Control Systems. Springer International Publishing, 2014: 1055-1061.

[8] Jialiang H, Youjun X, Zhiqiang X. Secure and Private Protocols for Server-less RFID Systems[J]. International Journal of Control & Automation, 2014, 7(2).

[9] Tian Y, Chen G L, Li J H. A Lightweight Serverless RFID Tag Search Protocol [J]. Advanced Materials Research, 2013, 684: 531-534.

[10] Sarma S E, Weis S A, Engels D. Radio-frequency-identification security risks and challenges[J]. Cryptobytes, 2003, 6(1):2-9.

[11] Weis S A, Sarma S E, Rivest R L, et al. Security and privacy aspects of low-cost radio frequency identification systems[M]. Security in pervasive computing. Springer Berlin Heidelberg, 2004: 201-212.

[12] Ohkubo M, Suzuki K, Kinoshita S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID[C]. Proceedings of the SCIS. 2004, 2004: 719-724.

[13] Henrici D, Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers[C]. Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on. IEEE, 2004: 149-153.

[14] Rhee K, Kwak J, Kim S, et al. Challenge-response based RFID authentication protocol for distributed database environment [M]. Security in Pervasive Computing. Springer Berlin Heidelberg, 2005: 70-84.

[15] Lee S M, Hwang Y J, Lee D H, et al. Efficient authentication for low-cost RFID systems[M]. Computational Science and Its Applications−ICCSA 2005. Springer Berlin Heidelberg, 2005: 619-627.

[16] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydlo, Securityanalysis of a cryptographically-enabled RFID device, in: USENIX SecuritySymposium, USENIX, Baltimore, Maryland, USA, 2005, pp. 1−16.