An Approach to Security and Privacy of RFID Systems in Anti-Desynchronization

Min-Hua Shao
Department of Management Information Systems, National Pingtung University of Science & Technology, Pingtung, Taiwan 91201

Summary
Radio-frequency identification (RFID, for short) is regarded as a fundamental technology for ubiquitous services and thus a growing security and privacy concern goes along with its applications integrated into everyday life, often in an invisible way. The possible abuse of RFID's tracking capability raises threats to user privacy. It has inspired lot of research interest, but many measures bring about a very challenging risk, that is, synchronization. Failure to keep changes of the shared secret in step between the tag and the back-end server will cause RFID system out of action. This paper presents an effective privacy-preserving protocol by means of commutative cipher to obviate the possibility of the mistake. In the proposed scheme, the tag output associated to the fixed secret identifier is dynamic at every session to conduct mutual authentication with reader-to-tag and tag-to-reader in turn. Therefore, our work is robust against desynchronization attacks and other security attacks, such as cloned use and man-in-the-middle attack, as well.

Key words:
Desynchronization, Mutual authentication, Untraceability, Counterfeiting, RFID.

1. Introduction

RFID is an automatic identification method, counting on storing and remotely retrieving data via RFID tags or transponders. In a prospective ubiquitous-computing environment, RFID tags will be attacked to or incorporated into all kinds of products, physical objects or person for the purpose of identification using radio waves, and could grow into a fundamental facility as a base for ubiquitous services. Obviously, only if secure enough to ensure personal data privacy is guaranteed can retailers implement and consumers trust and confidently use the technology on a mass scale [1-2]. Therefore, the treatment of privacy and security for RFID has inspired a variety of work [3], and there are three major types of approaches to address this technical problem: hash-chain scheme, anonymous-ID scheme, and internal re-encryption scheme. Ohkubo et al. [4] made a clear survey of their functionality according to privacy level, tag cost, and scalability. The comparison result is summarized as follow: The hash chain ensures strong privacy and low cost but limited scalability; Anonymous-ID guarantees low cost and greater scalability but limited privacy; Internal re-encryption assures strong privacy and greater scalability but high cost. Whatever approach is taken, untraceability is received the growing attention to privacy protection for RFID-embedded commercial services. The possible abuse of RFID's tracking capability raises threats to user privacy [5]. Previous works [6-10] dealt mainly with untraceability as the refreshment of the shared secret between the tag and the reader or the back-end server; but this suffers severely from adversarial attacks, including counterfeiting, man-in-the-middle attacks, etc. In other words, it will most likely fail to carry out mutual authentication later on account of desynchronization. Due to this, we propose a new methodology for untraceability with commutative cipher in which the tag output associated to the constant secret identifier is not fixed. Therefore, the proposed scheme has no trouble about the maintenance of synchronization.

The rest of this paper is organized as follows. In Section 2, we discuss security properties and preliminary concepts used in this paper. Section 3 presents the proposed authentication protocol for the betterment of privacy protection. Section 4 gives a security analysis of our new scheme thoroughly. Section 5 then concludes the paper with a summary of our achievements.

2. Preliminaries

Before starting our approach, we set out the requirements that such protocols should meet. Firstly, the detailed treatment of security and privacy concerns for RFID is described in Section 2.1. Then, for completeness and readability, cryptographic primitives used in our scheme are obvious and briefly summarized in Section 2.2.

2.1 Security Properties

As discussed in [9-15], the following set of security properties on RFID system are incorporated and extended:

(i) Mutual Authentication: The property permits the reader and the tag in a communication to verify the identity of the other, that is, reader-to-tag authentication and tag-to-reader authentication.
(ii) Item Privacy: Only authorized devices can understand the contents or price of a tagged item even though EPC code is revealed.

Manuscript received April 20, 2010
Manuscript revised April 20, 2010

(iii) Spoofing and Cloning: A spoofing attack happens to a situation where a fake reader or tag successfully masquerades as a genuine one by falsifying data and thereby gaining an illegitimate advantage. The tag cloning attack often accompanies the attack where tags are replicated from data transmitted by the tag.
(iv) Untraceability and Forward security: User privacy is always a matter of concern. Untraceability provides the treatment of the anonymity of the unique identifier; and further, forward security ensures that data transmitted today will still be secure in the future even if the tag is compromised.
(v) Synchronization: The requirement is in connection with untraceability protection of using no single and fixed identifier of the tag. Thus, synchronization is required to consistent the identifier kept in the tag with the related one hold at the back-end server.
(vi) Scalability: The computational complexity of conducting an exhaustive search for tag identification is the key to scalability. Similarly, poor performance is usually arisen from that tag output is not fixed.

2.2 Cryptographic Primitives

Fast hash functions and limited symmetric-key cryptography are more suitable for RFID application system, where computational speed and lower power consumption are important [16-18]. In our scheme we exploit a commutative encryption algorithm, a kind of symmetric key cryptosystems, denoted by CE. The operational property in CE has to satisfy the following requirement:

$$CE(k_1, CE(k_2, m)) = CE(k_2, CE(k_1, m))$$

$$CE^{-1}(k_1, CE^{-1}(k_2, c)) = CE^{-1}(k_2, CE^{-1}(k_1, c))$$

where

$CE(.)$	=	a commutative encryption function
$CE^{-1}(.)$	=	a commutative decryption function
m	=	message being protected
c	=	a ciphertext of the message m
$k1, k2$	=	symmetric secret keys

Obviously, the commutative property is not existed in every symmetric key cryptosystem, i.e., DES or AES [2]. The XOR operation is a simple instance to show the concept. A more secure and practical design for a commutative cipher can refer to [20].

3. The Proposed Scheme

In the model of the proposed scheme, three different roles involved in RFID system are as follows.

(i) T: The wireless tag is comprised of an IC chip and antenna, and is a transponder to react to a wireless probe from the RFID reader.
(ii) R: The wireless reader transmits a radio frequency probe signal to T within power range, retrieve data from T and then send it to the back-end database.
(iii) S: The back-end server has a database which maintains product-related information such as identifier and shared secret, and is able to discover the blind identifier of T forwarded by R in a secure communication channel.

The notations for operations are defined below.

ID	Pseudo-EPC code of *T*
K	The secret key is hold by an authorized S
C	A cipher of *ID* using *K* in cryptosystem *CE*
R	A secret key is generated randomly by *T*
U,W	Temporal outputs are used for operation *CE(.)* and $CE^{-1}(.)$, respectively.
TS	Timestamp generated by *S*
TS_{last}	A recent *TS* received by *T*
$H_{ID}(.)$	A *HMAC* function and its secret key *ID*
h_{TS}	The output of a *HMAC* function

3.1 Initialization Phase

Any *T* has three non-volatile memories *ID*, *C* and TS_{last} which are initialized into *T*'s memory by the product owner during manufacturing process. In which, *ID* is a unique ID number that can be produced by one-way hash function or the other encoding schemes to identify a valid *EPC* code. $C = CE(K, ID)$ is the key to authenticate *R* (and *S*) to *T* through conducting a similar challenge-response procedure. TS_{last} is assigned the value 0 at the initialization phase, and is used for the purposes of protection against replay attack. S has a unique access key *K* that signifies the authorized entity such as the product owner, and maintains a time clock for *T-to-R/S* authentication without synchronization problem. In addition, S also keeps two fields in the database: *EPC* code and its *ID*.

For clarity of exposition, a common assumption we make here is that there is a secure channel existed in between *R* and *S*. That is, *S* can know an authorized *R* from an unauthorized one in our scheme.

3.2 Implementation Phase

To carry out the tag identification by the authorized devices, T, R and S conduct the following steps visualized in Table 1.

(i) *R* signals a query message to neighbor *T* continuously, and requests *T*'s response.

(ii) Upon sensing query from *R*, *T* generates a secret key *R* randomly, retrieves *C*, computes a commutative cipher operation $U = CE(R, C)$, and then sends *U* to *R*. It is a challenge-response process of conducting *R/S-to-T* authentication in which *U* can be treated as a special nonce.

(iii) After receiving the response from *T*, *R* forwards *U* to *S*. Only the authorized *S* can use the correct access key *K* to decrypt *U*, that is, $W = CE^{-1}(K, U)$. After that, *S* generates a timestamp *TS* to challenge *T*, and then deliver *W* and *TS* to T with the help of *R*.

(iv) When *T* receives *R/S*'s answer, it computes the last decryption $ID' = CE^{-1}(R, W)$, checks if $ID' == ID$ and $TS > TS_{last}$, and rejects the case if any of them is invalid. After *R/S*'s authenticity is assured, *T* has to authenticate itself to *R/S* and tells *R/S* who it is. *T* calculates $h_{TS} = H_{ID}(TS)$, assigns *TS* to TS_{last}, and sends h_{TS} and *TS* to *R*.

(v) Upon receiving the response, *R* forwards h_{TS} to *S* in order to disclose *T*. Firstly, *S* compares received and sent *TS* and checks its use in lifetime. If the verification holds, *S* calculates $h'_{TS} = H_{ID}(TS)$ for each *ID* in the list of pairs (*EPC code*, *ID*) and checks if $h'_{TS} == h_{TS}$. When a match is found, *S* can collect the associated *EPC code*. Otherwise, *S* aborts the authentication procedure.

Table 1. The Efficient Privacy-preserving Protocol with mutual authentication

$R \rightarrow T$:	Query
T:	generate *R* and compute $U = CE(R, C)$
$T \rightarrow R \rightarrow S$:	*U*
S:	compute $W = CE^{-1}(K, U)$ generate *TS*
$S \rightarrow R \rightarrow T$:	*W*, *TS*
T:	compute $ID' = CE^{-1}(R, W)$ if $ID' == ID$ and $TS > TS_{last}$ then calculate $h_{TS} = H_{ID}(TS)$ $TS_{last} \leftarrow TS$ else output "unknown reader" and halt
$T \rightarrow R \rightarrow S$:	TS, h_{TS}
S:	if $TS(received) == TS(sent)$ and *Lifetime(TS)* then calculate $h'_{TS} = H_{ID}(TS)$ else halt if $h'_{TS} == h_{TS}$ then retrieve EPC code else output "unknown tag" and halt

4. Security Analysis and Discussion

Recall that we have set up six design goals in Section 2.1. All of them are achieved by the proposed scheme.

(i) Mutual Authentication. The series of the first two communications presents a challenge-and-response procedure and its closing provides *R/S-to-T* authentication. The completion of the last communication goes along with a successful *T-to-R/S* authentication.

(ii) Item Privacy. The proposed scheme has filled all requirements for item privacy: only *S* has *EPC code*, *T* doesn't have *EPC code*, and *ID* is not a *EPC code* itself. No useful data is released by a tag participating in the protocol.

(iii) Spoofing and Cloning. The secret key *K* only known by the authorized *S* can be effective against attacks on the tag where the attacker masquerades as a valid reader. Besides, the authenticator h_{TS} can prevent from attacks on the reader where a counterfeit tag is given. In our scheme, h_{TS} made up of the secret *ID* and *TS* under s secure *HAMC* function is intended for use only once and has a very short lifetime. Therefore, the threat of an opponent stealing the authenticator for presentation later is countered.

(iv) Untraceability and Forward Security. In general, a common countermeasure for traceability attacks is to employ random session identifiers through, i.e., secure one-way hash functions. Unfortunately, it may result in desynchronization later. Our work provides a variable tag output *U* related to the constant *ID* and thus has no problem about refreshment of the secret *ID* in *T* and *S* at the same time; and further, forward security is guaranteed as randomized secret key *R* expose to an adversary.

(v) Synchronization. As noted above, previous efforts tried to satisfy untraceable authentication at the risk of losing synchronization. The proposed scheme exploits commutative cipher to get rid of the treatment of synchronization in which the tag output is not fixed but the secret *ID* is always kept static at every session. This is the most significant contribution in our work.

(vi) Scalability. HAMC should execute in approximately the same time as the embedded hash function. It's time complexity of matching computations is acceptable in the related studies. Particularly, the burden of timestamp services has been put on *S* rather than on *R* and/or *T*. The treatment is reasonable because the back-end server has a great capacity to take on heavy loading. The cost of keeping the facility can also be regarded as a part of an investment in the

business. Additionally, the tag *T* only deals with the refreshment of TS_{last} and the functionality required of the reader *R* is minimal and applicable in common use.

5. Concluding Remarks

The treatment of synchronization is tough work for the variable-secret (ID) approach due to untraceability. It is easy to have the RFID tag fail to authenticate itself to the authorized reader and server through a variety of adversarial attacks such as spoofing, cloning, and man-in-the-middle attacks. In this paper, we propose an effective countermeasure against desynchronization besides accomplishment of other design goals. In exact speaking, the proposed scheme is not required to deal with synchronization of the secret ID kept in the tag and the back-end server because it is fixed all the time. The tag output associated to the secret ID, however, is dynamic for running sessions to fulfill mutual authentication. Obviously, commutative cipher may ultimately provide better assurance to privacy protection for RFID. As compared with its more common applications, we are able to simplify the use of such primitives in our protocol.

Acknowledgments

The author would like to thank the anonymous reviewers for their valuable comments and suggestions. This paper was supported in part by the National Science Council, Taiwan, under contract NSC 98-2410-H-020-007-MY2.

References

[1] Knight, W. (2006) RFID-another technology, another security mess? Infosecurity Today, May/June, 35-37.
[2] Karygiannis, T., Eydt, B., Barber, G., Bunn, L. and Phillips, T. (2007) Guideline for Security Radio Frequency Identification System. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Retrieve December 10, 2007 from the World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf
[3] Ayoade, J. (2007) Roadmap to solving security and privacy concerns in RFID systems. Computer Law & Security Report, 23, 555-561.
[4] Ohkubo, M., Suzuki, K. and Kinoshita, S. (2005) RFID privacy issues and technical challenges. Communications of the ACM, 48(9), September, 66-71.
[5] Avoine, G. and Oechslin, P. (2005) RFID traceability: a multilayer problem. Proceedings of Financial Cryptography, 28 February-3 March, Roseau, Commonwealth of Dominica.
[6] Ohkubo, M., Suzuki, K. and Kinoshita, S. (2003) Cryptographic approach to privacy-friendly tags. Proceedings of RFID Privacy Workshop, MIT.
[7] Dimitriou, T. (2005) A lightweight RFID protocol to protect against traceability and cloning attacks. Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 5-9 September, pp.59-66.
[8] Gao, X., Xiang, Z., Wang, H., Shen, J., Huang, J. and Song, S. (2004) An approach to security and privacy of RFID system for supply chain. Proceedings of the IEEE International Conference on E-Commerce Technology for Dynamic E-Business, 15 September, pp.164-168.
[9] Seo, Y., Lee, H. and Kim, K. (2006) A scalable and untraceable authentication protocol for RFID. Proceedings of EUC Workshops 2006, LNCS 4097, pp.252-261. Springer-Verlag, Berlin.
[10] Yang, M.H., Wu, J.S. and Chen, S.J. (2008) Protect mobile RFID location privacy using dynamic identity. Proceedings of ICCI'08, Stanford, CA, 14-16 August, pp.366-374.
[11] Ayoade, J. (2006) Security implications in RFID and authentication processing framework. Computer & Security, 25, 207-212.
[12] Juels, A. (2006) RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications, 24(2), 381-394.
[13] Roberts, C.M. (2006) Radio frequency identification. Computer & Security, 25, 18-26.
[14] Knospe, H. and Pohl, H. (2004) RFID security. Information Security Technical Report, 9(4), 39-50.
[15] Song, B. and Mitchell, C.J. (2007) RFID Authentication protocol for low-cost tags. Proceedings of WiSec'08, Alexandria, Virginia, USA, 31 March-2 April, pp.140-147.
[16] Zhang, L., Zhou, H., Kong, R. and Yang, F. (2005) An improved approach to security and privacy of RFID application system. Proceedings of International Conference on Wireless Communications, Networking and Mobile Computing, 23-26 September, pp.1195-1198.
[17] Aigner, M. and Feldhofer, M. (2005) Secure symmetric authentication for RFID tags. Proceedings of Telecommunication and Mobile Computing Workshop, 8-9 March, Graz, Austria.
[18] Feldhofer, M., Dominikus, S. and Wolkerstorfer, J. (2004) Strong authentication for RFID system using the AES algorithm. Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, LNCS 3156, pp.357-370.
[19] Schneier, B. (1995) Applied cryptography: protocols, algorithms, and source code in C. 2nd Edition, Wiley.
[20] Bao, F., Deng, R.H. and Feng, P. (2001) An efficient and practical scheme for privacy protection in the E-commerce of digital goods. Proceedings of ICISC 2000, LNCS 2015, pp.162-170. Springer-Verlag, Berlin.

Min-Hua Shao is an Assistant Professor with the Department of Management Information Systems at National Pingtung University of Science & Technology, Taiwan. She received her BCS degree from National Yunlin University of Science & Technology, Taiwan, in 1996, MS degree in information management

from National Chengchi University, Taiwan, in 1998, and Ph.D. degree in Information Management from National Chiao Tung University, Taiwan, in 2005. Her research interests include computer and network security, cryptographic protocol, mobile communications security, and trust and privacy issues over electronic and digital commerce.