2009 Fifth International Conference on Information Assurance and Security

Secure Access Control Scheme of RFID System Application

Yu-Chih Huang
Department of Information Management,
Tainan University of Technology
Tainan, Taiwan
e-mail: t00232@mail.tut.edu.tw

Abstract -- Radio Frequency Identification (RFID) is a contactless technology, it considered the way to replace the barcode, since the barcode is data read with line of sight and limits the utility for item-level of logistic and supply chain application in the future. RFID is intimate linking real and virtual also creates considerable security and privacy risk in RFID adoption. Until now, many researches on the RFID's security and/or privacy were proposed. In this paper, we surveys the literature of hash-based access control scheme and propose an effective scheme to enhance the security and privacy about the passive RFID tag.

Keywords : hash-based protocol, RFID, Secure Access Control

I. INTRODUCTION

RFID is an automatic identication technology that uses a tag embeded in the target entity to mark it with a unique code. The technology has a history of over 70 years, a very brief history of RFID is the so-call Identify Friend or Foe(IFF) system, first introduced in WWII and still in use today to identify friendly or enemy aircraft. The use of RFID in tracking and access application first appeared during the 1980s. At the end of the 1980s, the major growth of contactless smart cards has been use passive tags, especially in acess control and ticking. The use of such tags has rapidly increased since the largest retailer in the United States, Wal-Mart mandated their use in 2003 for its top 100 suppliers.With RFID, wireless automatice identification takes a very specific form: the object, location, or individual is marked with a unique identifier code contained with an RFID tag, which is in some way attached to or embedded in the target. RFID is not a single product but a comprehensive system, a typical RFID system include three basic elements: RFID tag(transponder), reader(transceiver) and back-end application system(or database), which demands the support of the computer network. A typical RFID system is shown in the Figure 1.

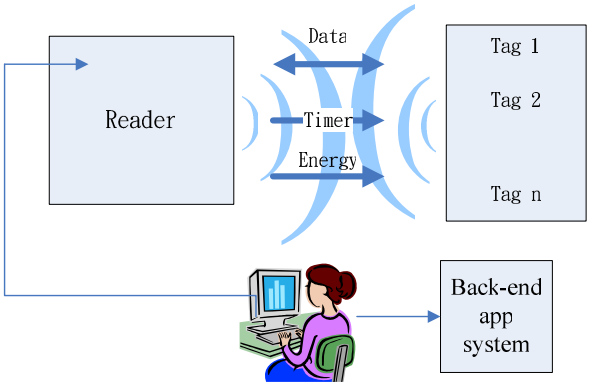

Fig. 1 A typical RFID system

Most RFID tags are passive means that they are battery-less and they obtain power to operate from the reader. When an RFID reader emits a radio signal , tags in vicinity respond by transmitting their stored data to the reader automatically, and from a rang of several meters. However, the barrier that the RFID system is facing presently is the issue of possibility of data security and privacy violation which could be as a result of illegal access.

While RFID system provides numerous benefits and performance in supply chain management[1], RFID tags may generate security and privacy risks to both organizations and individuals[2]. Since RFID is a wireless automatic identification and data capture technology, with unprotected tags could be monitored and tracked by business competitors or attackers. The privacy issue is involving many areas such as policies, security and law enforcement agencies. A criteria for evaluating a RFID system's privacy implies providing anonymity and unlinkability[3].

1. *Kill command*[4]
   The standard mode of operation proposed by the Auto-ID Center is indeed for tags to be killed upon purchase of the tagged product.

2. *Faraday cage approach*
   An RFID tag may be shielded from scrutiny using what is known as a Faraday cage a container made of metal mesh or foil which is impenetrable by radio signals (of certain frequencies).

978-0-7695-3744-3/09 $25.00 © 2009 IEEE
DOI 10.1109/IAS.2009.223

3. *The active jamming approach*
An active jamming approach is a physical means of shielding tags from view. In this approach, the user could use a radio frequency device which actively sends radio signals so as to block the operation of any nearby RFID readers.

4. *The blocker tag approach* [5]
The blocker tag is the tag that replies with simulated signals when queried by reader so that the reader cannot trust the received signals.

However, some thieves have been using foil-lined bags in retail shops to prevent shoplifting-detection mechanisms. The active jamming approach could be illegal for example if the broadcast power is too high it could disrupt all nearby RFID systems and not that alone it could be dangerous and cause problems in restricted areas like hospital and in the train. The blocker tag approach, like active jamming, it may affect the other legal tags [5]. Unprotected tags may have vulnerabilities to eavesdropping, traffic analysis, spoofing or denial of service.

In following, we briefly introduce some traditional attacks on security issue, such as the man-in-the-middle attack, the replay attack, the forgery attack, the stolen smart card attack, the denial of service attack, and some attacks, such as, Denning-Sacco attack and guessing attack discussed in [6]. These traditional attacks will find out in using RFID tag and reader communication and system application.

1. *Man-in-the-middle attack*
The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims, the sender(s) and the receiver(s), and relays messages between them, making them believe that they are talking directly to each other, but in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances.

2. *Replay attack*
A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it.

3. *Forgery attack*
Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive. Since the RFID handheld reader devices remote access network is an open environment, any malicious neighbor could forgery the communication traffic on the network.

4. *Spoofing attack*
A thief may replace a valid item with a fake label or replace the label of an expensive item with that of a fake label with data obtained from a cheaper item. Thus the lack of a means for authentication allows an adversary to fool a security system into perceiving that the item is still present or this may fool automated checkout counters into charging for a cheapter item.

5. *Denial of service attack*
A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users.

II REVIEW LITERATURES

2.1 Review the WSRE scheme

To accepting the resource limitations of low-cost RFID tags and prevent unauthorized readers from reading tag contents, the simple RFID access control scheme (for short WSRE scheme) based on the one-way hash function and randomized method proposed by Weis *et al.* [7] in 2003. The WSRE scheme is illustrated in Fig.2 and the operation procedure as following.

Step 1. The Reader sends the query signal to the RFID Tags.
Step 2. The RFID Tag responds the *metaID* data to Reader, where the *metaID* is the hash of a random key, i.e., *metaID* =H(*Key*).
Step 3. Database will look up the appropriate key in the back-end database after he receives the *metaID* data from the reader and finally transmits the *Key* to the Tag through the Reader.
Step 4. The Tag computes the value of H(*Key*) and compares it to the stored *metaID*. If these values are equal, the tag will give its ID to the Reader.

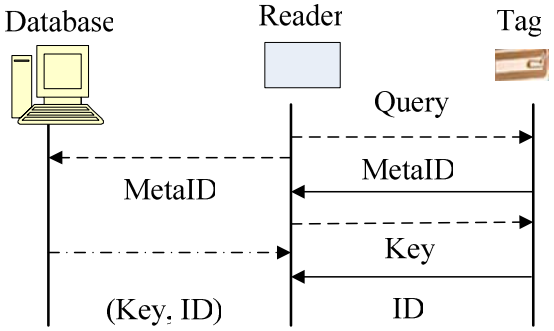

Fig. 2 WSRE hash-based access control scheme[7]

In this paper, there discuss the security of WSRE scheme from two ways of the information transitions by wire channel between Reader and Database and by wireless channel between Reader and Tags. The attacker can not receive or control the any data (such as MetaID, Key and ID) in this way. However, the data is transmitted by the wireless channel between Reader and Tag. Therefore, the data (such as Query, MetaID, Key and ID) can be eavesdropped or attacked by the man-in-the-middle attack. That is to say, the attacker can be impersonated the spoofed reader and the attack's procedure as following steps.

Step 1. The Tag will response the true *MetaID* to him when the Tag receive the require query from the attacker.

Step 2. The attacker can retransmit the true *MetaID* to the Reader and the Reader also gets *Key* and **ID** from the Database.

Step 3. The attacker can find the secret data *Key* from Reader and he retransmits the *Key* to the Tag.

Step 4. The Tag computes the value of H(*Key*) and compares it to the stored *metaID*. If these values are equal, the tag will give its ID to the attacker.

Finally, the attacker can get the secret *Key* and ID from the Tag. In other words, the man-in-the-middle attack is successful, the system security is failed.

2.2 Review the Chien's scheme

To prevent the man-in-the-middle attack, Chien [8] proposed a lightweight method to enhance WSRE weakness in 2006 and his scheme is shown in Fig.3. The operation procedure as the following step:

Step 1. The Reader sends the query signal to the RFID Tag and then the RFID tag sends the *metaID* and *date* to Reader, where *metaID* =H(*Key*). At the same time, the *date* data must be restored in RFID Tag.

Step 2. Database will look up the appropriate key in the back-end database after he receives the *metaID* data from the Reader and finally transmits the *Key* and ID to the Reader.

Step 3. The Reader computes the value of t = H(*Key*⊕*date*) and sends t to the Tag.

Step 4. The Tag computes the value of H(*Key*⊕*date*) and compares it with t. If these values are equal, the tag will give its ID to the Reader.

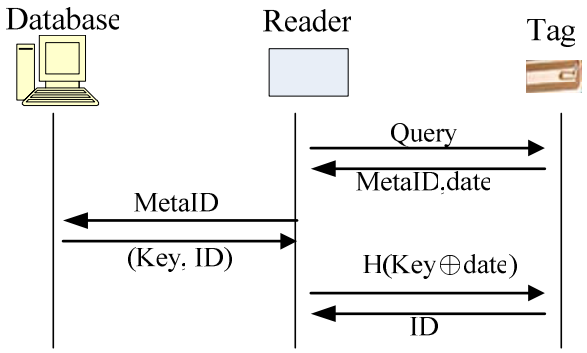

Fig. 3 The Chien's scheme[8]

However, the attacker can be eavesdropped and spoofed reader and replay to read the Tag ID in the date.

III PROPOSED SCHEME

In this paper, we propose a time efficient hash-based access control scheme using timestamp (includes date and time) and hash function to encode the message. It provides a solution to prevent replay attacks. The proposed scheme is showing in Fig. 4.

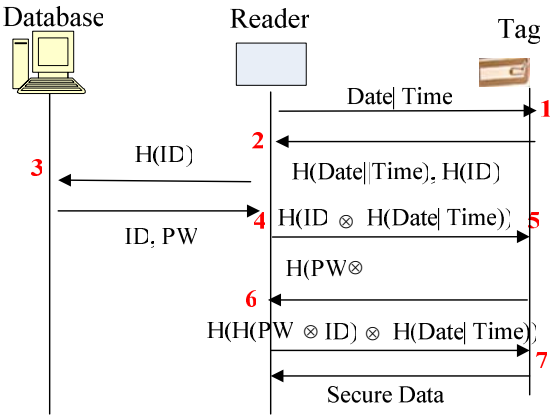

Fig. 4. The time efficient hash-based access control scheme

The detail of the proposed scheme is showing as following:

Step 1. The reader retrieves current system timestamp (date||time) and sends the timestamp to the tag. The tag then replies H(date||time) and H(ID) to the reader and stores (date||time) for further operations; where H(·) is a hash function and '||' denotes string concatenation operator.

Step 2. After receiving H(date||time) and H(ID), the reader confirms the timestamp. If it holds, the reader stores H(date||time) for further operation, then he queries H(ID) to the database server.

Step 3. After receiving the query H(ID) from the reader, the server queries H(ID) to database and retrieves corresponding relation. The server then replies the corresponding ID and PW to the reader from secure channel.

Step 4. After receiving the reply ID and PW from the server, the reader computes H(ID ⊗ H(date||time)); where '⊗' denotes XOR operator. The reader then sends H(ID ⊗ H(date||time)) to the tag.

Step 5. After receiving H(ID ⊗ H(date||time)), the tag verifies whether H(ID ⊗ H(date||time)) is correct. If it does, the tag replies H(PW ⊗ H(date||time)) to the reader.

Step 6. The reader verifies whether H(ID ⊗ H(date||time)) is correct. If it does, the reader computes and replies H(H(ID ⊗ PW) ⊗ H(date||time)) to the tag.

Step 7. The tag verifies whether H(H(ID ⊗ PW) ⊗ H(date||time)) is correct. If it does, the tag authenticates the reader and replies the secure data.

IV SECURITY ANALYSIS AND DISCUSSION

Since passive RFIDs are popularly used in various fields, to protect the personal privacy and the data secrecy, it is necessary to prevent the tag be accessed from illegal readers. We discuss mutual authentication and anonymity of our proposed paper as following:

a. Mutual authentication: To achieve mutual authentication, there are hashed messages: H(date||time), H(PW ⊗ H(date||time)), H(ID ⊗ H(date||time)) and

$H(H(PW \otimes ID) \otimes H(date||time))$, transferring between the reader and the tag in our scheme. Assume that an attacker has collected above messages and wants to impersonate the tag. Then the tag sends $H(PW \otimes H(date||time))$ to the reader. But because the timestamp is changing, $H(date||time)$ is changing too. The attacker then cannot pass the verification and he cannot get $H(ID \otimes H(date||time))$. So, the replay attack is failed.

b. Anonymity: In our paper, we transfer hashed messages instead of plaintexts on communications. By eavesdropping, attackers could get hashed messages: $H(date||time)$, $H(PW \otimes H(date||time))$, $H(ID \otimes H(date||time))$ and $H(H(PW \otimes ID) \otimes H(date||time))$, but not the plaintext ID and PW. So, the proposed scheme provides anonymity.

c. Replay attack: Since there is no clock generator in passive tags, in our scheme, we propose a time efficient scheme to retrieve current timestamp by the reader. By confirming the timestamp, the proposed scheme blocks the threats of replay attacks. Simultaneously, the secure transfer between the tag and the reader prevents eavesdropping, data collection, and malicious behaviors.

V CONCLUSION

In conclusion, information in tags can be protected from being read by unauthorized readers through the authentication procedures in the proposed scheme. The time efficient hash-based access control scheme blocks the threats of replay attack and man-in-the-middle attack. It is very imperative to protect unauthorized access to the tag in order to prevent the violation of privacy and confidential information stored in it.

REFERENCE

[1] I. Bose and R. Pal, "Auto-ID: Managing Anything, Anywhere, Anytime in the supply Chain," Counications of ACM 48(8) 2005,pp. 100-106.

[2] F. Thiesse, Managing Risk Perceptions of RFID, Auto-ID Labs White paper WP-BIZAPP-031, 2006.

[3] D.C. Ranasinghe, D.W. Engels, P.H. Cole, "Low-cost RFID system: Confronting Security and Privacy," Paper presented to Auto-ID Labs Research Workshop, 2004.

[4] Auto-ID Center, "Draft protocol specification for a 900 MHz class 0 radio frequency identification tag," 23 Feb. 2003.

[5] A. Juels, R. Rivest, and M. Szydlo, "The blocker tag: selective blocking of RFID tags for consumer privacy," Proceedings of CCS 2003, Washington D.C., pp. 103-111.

[6] E. J. Yoon, E. J. Lee, and K. Y. Yoo, "Cryptanalysis of Wang et al.'s remote user authentication scheme using smart cards," 15th International Conference on Information Technology: New Generations, 2008.

[7] S. Weis, S. Sarma, R. Rivest and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in 1st Intern. Conference on Security in Pervasive Computing (SPC), Boppard, Germany, March 2003, pp. 12-14..

[8] H.Y. Chien, " Secure Access Control Schemes for RFID systems with Anonymity," Proceedings of the 7th International Conference on Mobile Data Management(MDM 2006), 2006 p.96.