ISSN 2229-5518

Secure Access of RFID System

Salim G Shaikh and Shankar D Nawale.

Abstract— Radio Frequency Identification (RFID) is a wireless technology; it considered the way to replace the barcode, RFID used for the purposes of automatic identification and tracking of object attach with tag. 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. While implementing the RFID in various applications we have to consider security and privacy risk in RFID adoption. Until now, many researches on the RFID's security and privacy were proposed. In this paper, we describe security model of the tag and Reader by using the Reader ID and Tag ID and 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.

Index Terms— Reader-ID, Tag-ID, hash-based protocol, RFID, Secure Access Control,WSRE Scheme,Chien Scheme,TripleDES.

1 INTRODUCTION

Radio Frequency Identification (RFID) technology, one of the forerunners of pervasive computing, is widely regarded as the successor of optical bar codes. Industries of manufacturing, supply chain management, and inventory control can benefit this technology to help reduce the costs wherever bar codes used to dominate.

The use of RFID in tracking and access application first appeared during the 1980s [1]. At the end of the 1980s, the major growth of contactless smart cards has been use passive tags, especially in access.

The use of RFID tags has been rapidly increased since the largest retailer in the United States; Wal-Mart mandated their use in 2003 for its top 100 suppliers [1]. With RFID, wireless automatic 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.

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 range 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 [2].

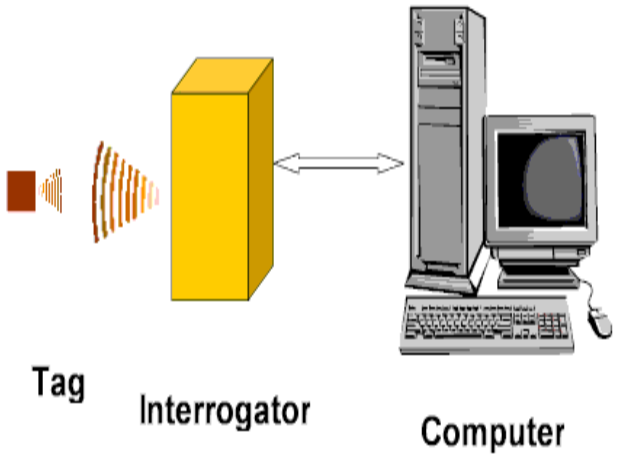


Fig. 1 A Typical RFID System

Active tags contain an on-board power source, such as a battery, as well as the ability to initiate their own communications; possibly with other tags. Semi-passive tags have a battery, but may only respond to incoming transmissions. Passive tags receive all power from the reader and necessarily cannot initiate any communications. [3]

A tag's power source determines both its range and cost. Passive tags are the cheapest to manufacture and incorporate into packaging, yet have the shortest read range. Semi passive tags have moderate range and cost, while active tags have the greatest range and cost. Semi-passive and active tags' on-board power source may also power a clock or integrated sensors. Refer to Table 1.1 for a comparison of the various tag types.

- *Author Shaikh Salim is currently pursuing masters degree program in Computer Engineering in Sinhgad Institute of Technology, Loanvala in pune University, India, PH-09960726716. E-mail: shaikhsg2@gmail.com,*
- *Co-Author Shankar Nawale is Guide and currently Head of the deparment Telecommunication Engineering in Sinhgad Institute of Technology, Loanvala India, PH-02114 407475. E-mail: shnkarnawale125@rediffmail.com.*

Power/ Types of Tag	Passive	Semi-Passive	Active
Power source	Passive	Battery	Battery
Transmitter	Passive	Passive	Active
Max Range	10M	100M	1000M

2 PRIVACY AND SECURITY ISSUES IN RFID SYSTEM

2.1 Review Stage

The threat to user privacy is a major hurdle to the expansion of RFID industry. In many adopted RFID systems, the tag responds the reader's query with its unique serial number, without verifying the reader's authenticity. This unique number can act as a clue for the adversaries to identify the tag carrier, thus threatening the user privacy [2].

While RFID system provides numerous benefits and performance in supply chain management [4], RFID tags may generate security and privacy risks to both organizations and individuals. 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[4].

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 [5]. These traditional attacks will find out in using RFID tag and reader communication and system application.

embed the images in the paper itself. Please don't send the images as separate files.

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 neighbour 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 cheaper 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.

3 REVIEW LITERATURES.

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.* [2] 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.).

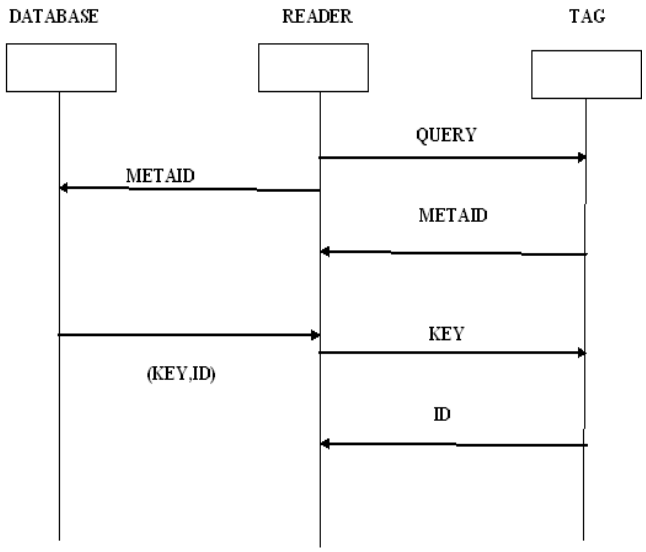


Fig. 2 WSRE hash-based access control scheme [2]

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.

3.2 Review the Chien's scheme

To prevent the man-in-the-middle attack, Chien [6] 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 RFIDTag.

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 $t = H(Key \oplus date)$ and sends t to the Tag.

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

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

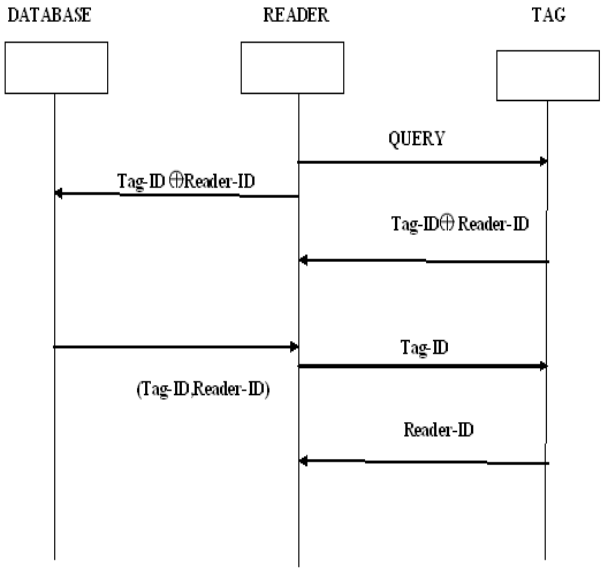
4 Proposed Algorithms.

In this paper, we proposed security algorithms between tag and Reader. According to our proposed algorithm we can secure the RFID tag information in two ways:
1) Firstly we could encrypt the tag 24 bit data using a private key at the tag side and at the database end. This private key would be burned on the microprocessor chip of the tag by the manufacturing company and its algorithm will be known only to the company. This encrypted data when send to the Personal computer (database) through the reader will be decrypted by using the same algorithm along with the private key and checked with the database entry. In this way the authentication of the tag could be maintained.
2) Secondly, we would also provide the security from attacks such as "man in the middle attack" by converting the tag 24 bit data into 30 bit (or more). This would be done using the reader unique id (like the MAC address of a computer). While sending the tag data to the database the reader would attach its own unique id with it. On the back end the tag data would be checked along with the reader id. If the AND operation gives positive result (both are valid) then only further action would be taken otherwise message would be shown reporting the attack (or un-authentication).
We are trying to implement this proposed algorithm by designing 3 applications (1 for tag, 1 for reader, 1 for database). These 3 applications being independent from each other will provide a simulated environment for the RFID technology. The algorithm would be implemented in the applications and the applications would communicate as the real system. The simulation will work as follows:

1) The user will input a 24 bit alphanumeric value in the tag application.
2) The reader application will have a SCAN button. On clicking this button the reader application will read

the tag data, attach its unique id, encrypt the 30 bit data and pass this data to the database application.

3) On the database end (3rd application) decryption would be performed. The database would divide the 30 bit data into 24 bit (tag data) and 6 bit (reader id).
4) If both values are correct then message would print showing successful completion.
5) If any of the 2 values is wrong then proper message would be shown regarding the fake value of Tag or Reader.



5 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 anonymity of our proposed paper as following

A) Anonymity: In our paper, we transfer encrypted Message instead of plaintexts on communications. By eavesdropping, attackers could get Encrypted messages.

B) Security attack: by applying the proposed scheme we overcome the men–in-the middle and reply attack by encrypting the Reader ID and Tag ID.

6 Conclusion.

In conclusion, information in tags can be protected from being read by unauthorized readers through the authentication procedures in the proposed scheme by encrypting the Reader ID and Tag ID. There are 24bit Tag ID and we add the 6 more bit as Reader-ID in this way we encrypts the 30 bit data using the triple DES Algorithms and enhance the security and authentication done on both way on Tag Side and Reader Side 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.

References

[1] Stephen August Weis," Security and Privacy in Radio-Frequency Identification Devices", Massachusetts Institute of Technology Department of Electrical Engineering and Computer Science on May9,2003.

[2] 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.

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

[4] Yu-Chih Huang ,"Secure Access Control Scheme of RFID System Application", 2009 Fifth International Conference on Information Assurance and Security , 978-0-7695-3744-3/09 $25.00 © 2009 IEEE.

[5] Zhaoyu Liu and Dichao Peng, "A Secure RFID Identity Reporting Protocol for Physical Attack Resistance", JOURNAL OF COMMUNICATIONS, VOL. 1, NO. 4, JULY 2006

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