모바일 에이전트 기법을 이용한 RFID 시스템 구조의 분석

김정태
목원대학교

Analyses of RFID system architecture based on Mobile agent scheme

Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

RFID enabled credit cards are becoming increasingly popular as contactless credit cards. We envision a future where RFID credit cards will be used for online shopping. RFID system has tremendous potential to render electronic payments more secure than normal credit cards. The word RFID enabled credit cards may bring in mixed passion, enthusiasm and perhaps even rage! This is partly paranoia and partly reality. The reality is that an intruder can read RFID cards without the user even noticing it. This brings in a zone of discomfort and leads to paranoia. Certain interactivity should exist to bring back this comfort to the user. This paper tries to make an effort in that direction. In this paper we propose mobile phone based architecture for secured electronic payments using RFID credit cards.

Ⅰ. Introduction

An RFID system consists of several components: tags, tag readers, and application software. The tag contains a transponder with a digital memory storing a unique electronic identifier, as well as information about the object it's attached to. The reader consists of a transceiver, decoder, and antenna. The reader reads from and, if necessary, writes to the tag, relying on a signal it emits that activates the tag so it turns into a transmitter. Such automatic tag reading allows great amounts of data to be transmitted at once, speeding up operations while improving accuracy and productivity. The readings do not require direct contact or line of sight between tag and reader. Chiu et al. [1,2] has proposed a solution which eradicates central server and key management problem. They have proposed a solution for searching where a reader broadcasts a query and only the valid tag replies to that. The problem with their solution is that the tag needs to remind all the queries that it receives. This is not feasible for small tags with low memory. Moreover an adversary can query the tag the maximum number of times it can remember. Over the last several years, ubiquitous computing has been integrated into many aspects of our lives because of the evolution of radio frequency identification (RFID) and mobile phone technology. We define a single-use RFID as a networked processing device with the following features: an RFID to work actively, a limited number of data transfers, low-bit data transfer, and long-range radio-communication by VHF/UHF frequency. There are two key elements within a RFID system:

- RFID tag, or transponder, carries

object-identifying data.

• RFID reader, or transceiver, reads and writes tag data. Basically, the tag reader broadcasts a radio frequency signal to access information stored on the tags nearby. This information can range from static identification numbers to user written data or data computed by the tag. Radio frequency identification (RFID) is an automatic identification system that can remotely store and retrieve data about objects by using small devices called RFID tags. RFID systems consist of radio frequency (RF) tags and RF readers. Tag readers can question tags about their contents by broadcasting an RF signal, without physical contact. RFID systems always consist of three major components.

1. Reader/transceiver including antenna which communicates with the tag.
2. Tag/RFID label or Transponder which is placed on the object to be identified.
3. Application systems

II. Trends of technology

Authentication and privacy protection in mobile RFID are hot research topics among the researchers. Because of the very cost, however, its resources are extremely scarce and it is hard to have any valuable security algorithms in it. It causes security vulnerability, in particular cloning the tags for counterfeits. Mobile RFID service structure provides its services by associating the mobile communication network and the RFID application service network based on the RFID tag. The area to consider the security basically is the RFID tag, reader terminal area, mobile communication network area, RFID application service network area, and security issues like the confidentiality/integrity/authentication/permission /non-repudiation shall be considered in each network area. RFID technology increases the benefits of wireless information systems. In addition to great productivity gains, RFID systems may create new threats to the security and privacy of individuals or organizations. RFID tags may pose security and privacy risks to both organizations and individuals[3,4]. RFID has received a great deal of press in recent years, especially since the first business applications emerged and the world's largest retailers began to put the vision of smart items into practice. Although many companies have explored RFID and ERP technologies' value for tracking materials throughout the supply chain, few have reported on how RFID and ERP support their management and operation of assets and facilities[5,6]. RFID Infrastructure for Wireless Mobile Systems (RIWIS) project has been developed with the idea of creating a common RFID infrastructure that can be used with wireless/mobile information systems and making this infrastructure interoperable with standardized learning management systems in many countries. But the RFID applications used presently do not have very reliable security mechanisms. Most RFID cards are validated by comparing the card ID with the data stored in online database. In many mobile applications, network connectivity is unreliable, so it is hard to verify the card online directly.

III. Threats of attacks

Some well known attacks are as follows:

• Physical Attacks: Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others.

• Denial of Service (DoS): A common example of this type of attack in RFID

systems is the signal jamming of RF channels.

• Counterfeiting: There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.

• Spoofing: When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.

• Eavesdropping: In this type of attacks, unintended recipients are able to intercept and read messages.

• Traffic analysis: Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and can not be decrypted.

Effective RFID Security Protocols can provide protection against the described threats. Although RFID is a cheap and automated identification technology but still numerous good RFID security protocols hard to fit in the said domain because of the complexity of protocols against the limited/tight computational tag resources.

IV. Summary of requirements

Most of the works on RFID have developed a method of searching with the use of a central server. In essence whenever a reader tries to search a tag, it will do so by first making a contact with the central server for the authentication purpose. The Reader will only read the tag id and send it to the server for authentication. we summarize some essential operational and cryptographic properties for general RFID systems in order to clarify the issues of the paper.

• Scalability:

If the computational workload of an authentication protocol increases linearly as the number of the tags, the system is not scalable. Noting that most RFID applications should accommodate a large number of tags, e.g. a large library may have millions of books and each book should have a tag, the scalability is a critical property in RFID systems.

• Anti-cloning:

Since a large number of tags will be spread out in the RFID applications, an attacker may be able to capture a tag, investigate it by microscope probing [4], learn all the information in the tag, and make a counterfeit. However, an attacker should not be able to forge other tags except the cracked one. If a group of tags share secret information and a reader authenticates tags by the shared secret, it will be possible to clone some other tags with the learned secret. This will also cause the tracking problem since an attacker can decrypt the exchanged messages. Therefore, the secret information on a tag should be pertinent to the tag so that the other tags except the cracked one are still secure. One possible way to protect the secret stored in a tag is to use a secure memory [5]. However, it is not practical to store a long-term secret (a group key, shared secret among a group of tags and readers) in tags and to use it for authentication since only single cracked tag may endanger all the tags and readers having the shared secret. In this paper, assuming that an attacker is able to crack and reveal the secret in a tag, we define an RFID system secured against the cloning attack as long as the secret of a tag is pertinent to the tag and secured from passive or active skimming attacks.

• Anonymity:

RFID tags are supposed to respond with some message whenever they receive a query message from a reader. If the

responses are fixed or predictable by an attacker, it results in a privacy problem. An attacker is possibly able to track a tag, and hence its owner too, and collect data for malicious purpose. Therefore, the responses of tags should be randomized so that it is infeasible to extract any information in communications between a tag and a reader.

V. Security and performance Analysis

Some of the security properties of the proposed protocols are listed as below.

A. Security analyses

▪ Confidentiality: This is a mechanism to guarantee a tag's privacy. In our design, a tag's secret values will never be disclosed in clear during the protocol execution.

▪ Tag anonymity: As the ID of the tag is static, we should send it, and all other interchanged messages, in random wraps (i.e., to an eavesdropper, random numbers are sent).

▪ Tag/reader authenticity:

We have designed the protocol with both reader-to-tag authentication (due to messages A and B) and tag-to-reader authentication (due to message C). These are achieved via the shared and synchronized secrets at both sides, and the permanent hidden value (ID) as well.

B. Performance Analysis

In this section, we make a close comparison of protocol in terms of computational, storage and communication overhead.

- Computational overhead:
- Storage overhead:
- Communication overhead:

VI. Conclusion

We analyses a new type of simple and efficient authentication module with a new scheme that performs hash function just once rather than twice or more in existing scheme. It can be easily adopted on active RFID tags and reader with low cost. And, we analyses security and performance analysis for future work.

References

[1] M. Jo and H. Y. Youn, "Intelligent recognition of RFID tag position," Electronics Lett., vol. 44, no. 4, pp. 308–310, Feb. 2008.

[2] M. Rieback, B. Crispo, and A. Tanenbaum, "The evolution of RFID security," Pervasive Computing, IEEE, vol. 5, no. 1, pp. 62–69, Jan.-March 2006.

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags," RFID Privacy Workshop 2003, MIT, MA, USA, 2003.

[4] Y. Z. Li, Y. B. Cho, N. K. Um, and S. H. Lee, "Security and Privacy on Authentication Protocol for Low- Cost RFID," CIS 2006, LNAI, vol. 4456, pp. 788–794, 2007.

[5] P. Horster, M. Michels, and H. Petersen, "Authenticated encryption schemes with low communication costs," IEEE Electronics Letters, vol. 30, no. 15, pp. 1212–1213, 1994.

[6] F. Stajano, "Security fot Ubiquitous Computing," Halsted Press, 2002. feasibility (Periodical style)," IEEE Trans. Electron Devices, vol. ED-11, pp. 34–39, Jan. 2002.