경량화 보안 기능을 가진 RFID 응용 분야에 대한 취약성 분석

김정태
목원대학교

Analyses of Vulnerability in RFID application with Lightweight Security Scheme

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

요 약

As RFID technology is becoming ubiquitous, the secunty of these systems gets much attention. Its fields of usage include personal identification, supply-chain management systems, and many more. Many kinds of RFID tags are available on the market which differ both in storage, and computational capacity. Since by standard IT means all the tags have small capacities, the security mechanisms which are in use in computer networks are not suitable. For expensive tags with relatively large computational capacities many secure communication protocols were developed, for cheap low-end tags, only a few lightweight protocols exist. In this paper we introduce our solution, which is based on the least computation demanding operator, the exclusive or function. By introducing two tags instead of one in the RFID system, our scheme provides security solutions which are comparable with those provided by the lightweight protocols. In the meantime, our scheme does not demand any computational steps to be made by the ta

Ⅰ. Introduction

RFID tags are categorized into two classes; passive and active. Passive RFID tags are powered by the signal received from reader. On the contrary, an active RFID tag is battery powered and has its own on-chip power source. Most RFID tags contain at least two parts [1]. One part consists of an integrated circuit used for storing and processing information, modulating and demodulating an (RF) signal, and other specialized functions. The second part consists of an antenna for receiving and transmitting the signal. Radio Frequency Identification (RFID) is widely adopted as an identification technology. While human beings are able to distinguish objects or other humans under difficult conditions, computing devices lack of this capability. From this point of view, RFID may be understood as a means of labeling objects to facilitate item automatic identification. RFID devices or tags are small chips joined to an antenna and designed to transmit data over wireless channels. By means of an RFID reader, tags are interrogated and their internal identifier or other resources, e.g. user memory, are accessed. Most RFID tags contain at least two parts. One part consists of an integrated circuit used for storing and processing information, modulating and demodulating an (RF) signal, and other specialized functions. Nowadays, RFID is one of the main technologies used to build ubiquitous systems. Recently RFID technology's potential has been recognized by ubiquitous computing researchers, in

implementing physical user interfaces. it becomes evident that information security gains more importance. It would be beneficial to have a generalized threat model that applies to all RFID applications. Okubo et al. proposed a hash-chain based authentication protocol which protects users' location privacy and anonymity. They claimed that their scheme provides not only strong forward security but also anonymity of tags. However, Li et al. have claimed that a hash-chain calculation must be a burden on low-cost RFID tags and give back-end servers heavy calculation loads in [2].

II. Security Mechanism

RFID and related security/privacy issues have been studied by researchers over the past few years, and these efforts have resulted in a stream of lightweight cryptographic protocols that purport to address different facets of related issues (e.g., Piramuthu, 2008). There is very little published research that address privacy/security issues that are specific to RFID tags in supply chains.[3]

One way hash function is a powerful and computationally efficient cryptographic tool. It fulfills not only the security requirements of RFID systems but also the functional and hardware implementation requirements. Two hash function schemes namely hash lock and extended hash lock schemes were introduced for mutual authenticating back-end server and RFID tags. The scheme provides tag's anonymity and privacy protection feature and blocks eavesdropping which can impersonate the tag as being authentic.[4] In the previous RFID authentication schemes. it is assumed that the communication channel between processing server and RFID reader is secure. The mechanism for channel protection is not provided and hence leaving an open and weak area to launch various kinds of attacks

1. Robust security feature
- Impersonation Attack
- Replay Attack
- Location Privacy Attack
- Forgery
- Denial of Service Attack
- Data Loss Attack
- Key anonymity & Intractability

Many protocols have been proposed for use in RFID systems. The following assumptions is as follows.

• An RFID system incorporates components of two types, namely a back-end server and RFID tags.

• Each server maintains a server database (DB) containing a set of values for each tag that it manages, and is combined with an RFID reader.

• Each tag has a rewritable memory which may be susceptible to compromise.

• The channel between the server and the tag is insecure, and communications are subject to eavesdropping or modification.

• An RFID protocol consists of three flows; typically, the first flow is a query from a server to a tag, the second is the reply of the tag to the server for tag authentication, and the third is the response from the server to the tag for server authentication.

• A server and a tag share secrets used for mutual authentication. They update the shared secrets synchronously whenever they perform a successful authentication session; a server updates tag secrets stored in its DB after receiving the second flow and having authenticated the tag, and the tag updates its stored secrets after receiving the third flow and having authenticated the server.

III. Security Analysis

The security design of the protocol

should not impede normal operations, and should prevent a malicious adversary from getting any information. We consider the following measures:

1. Secrecy/Authentication

The cryptographic methods used (for example the keyed Hash function H) correspond to the state of the art in industry today, and reasonably guarantee the secrecy of the message. Thus, we assure the recipient that the messages originates from valid sources.

2.Indistinguishability/Tracking/Passive

Replay Using a freshly generated random nonce with every message in the protocol, it is impossible to track the tag. Assume that an adversary pretends to be a genuine reader. He sends out a query, and receives a message back. Next time he sends a query, along with a fresh nonce, he receives a different message, so he cannot track the tag. Of course, with multiple tags in an area, tracking a specific tag without keys is extremely difficult if not impossible.

3. Forward Security

This means that the current key of a tag has been found, and can be used to extract previous messages (assuming that all its past conversations are recorded). Let's say the adversary somehow finds ki. The tag always communicates using a hash function. The adversary cannot use the key to decode any of the tag's messages because the one-way hash function H is considered computationally un-invertible. In other words, the adversary needs to have access to the hash digest table for lookups. So, he cannot decipher/recreate any past messages sent with previously used keys.

IV. Solutions of threat

There are a number of solutions proposed so far to solve the security problems and threats associated with the use of RFID systems. The fundamental principles and a critical review of every proposal can be summarized as follows.

- Kill Command: This solution was proposed by the Auto-ID Centerand EPCglobal. In this scheme, each tag has a unique password, for example of 24 bits, which is programmed at the time of manufacture. Upon receiving the correct password, the tag will deactivate forever.
- The Faraday Cage Approach: Another way of protecting the privacy of objects labeled with RFID tags is by isolating them from any kind of electromagnetic waves. This can be made using what is known as a Faraday Cage (FC), a container made of metal mesh or foil that is impenetrable by radio signals (of certain frequencies). There are currently a number of companies that sell this type of solution.
- The Active Jamming Approach: Another way of obtaining isolation from electromagnetic waves, and an alternative to the FC approach, is by disturbing the radio channel, a method which is known as active jamming of RF signals. This disturbance may be done with a device that actively broadcasts radio signals, so as to completely disrupt the radio channel, thus preventing the normal operation of RFID readers.
- Blocker Tag: If more than one tag answers a query sent by a reader, it detects a collision. The most important singulation protocols are ALOHA (13.56 MHz) and the tree walking protocol (915 MHz). Juels used this feature to propose a passive jamming approach based on the tree-walking singulation protocol, called blocker tag. A blocker tag simulates the full spectrum of possible serial numbers for tags.

• Bill of Rights: Garfinkel proposed a so-called RFID Bill of Rights that should be upheld when using RFID systems. He does not try to turn these rights into Law, but to offer it as a framework that companies voluntarily and publicly should adopt.

• Classic Cryptography:

– Symmetric Key Encryption: Feldhofer proposed an authentication mechanism based on a simple two-way challenge-response algorithm. The problem with this approach is that it requires to have AES implemented in an RFID tag.

– Public Key Encryption: There are solutions that use public-key encryption, based on the cryptographic principle of re-encryption.

• Schemes Based on Hash Functions: One of the more widely used proposals to solve the security problems that arise from RFID technology (privacy, tracking, etc.) is the use of hash functions.

– Hash Lock Scheme
– Randomized Hash Lock Scheme
– Hash-Chain Scheme

• A Basic PRF Private Authentication Scheme: This protocol uses a shared secret s and a Pseudo-Random Function (PRF) to protect the messages exchanged between the tag and the reader.

• Authentication Methods: The transponders should be validated before the system accept its data as a true value and starts to process it. A cloned transponder can be recognized by creating a "challenge-response (C-R) authentication system"4. This system will send a query to the transponder and according to response message, transponder will be authenticated and it's data will be processed. Using passwords or tag identifiers allow to authorize tags and easily track unathorized tags.

• Validation of SQL Queries: Against to the SQL injection attacks; a validator module can be included into the system. This module can be developed as a software which contains artificial intelligence characteristics. SQL attacks can be blocked by the control of this intelligent validator.

• Ban Mechanisms: To prevent a transponder to be used as a service blocker, frequent usage of transponder must be eliminated. This prevention can be made both using hardware and software systems.

V. Conclusion

Radio Frequency Identification (RFID) is a widely adopted identification technology. In this paper, we analyses vulnerability in RFID application with Lightweight Security Schems and present a general model for RFID-Systems containing logical entities. Taking this RFID-System model we categorized the security threats related to this model by the means of information security.

References

[1] 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.

[2] A. Juels "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[3] A. Juels, S. Garfinkel, and R. Pappu, "RFID privacy: An overview of problems and proposed solutions," IEEE Security and Privacy, vol. 3, no. 3, pp. 34–43, May/Jun. 2005.

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