Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

April 2016, 23(2): 31–37
www.sciencedirect.com/science/journal/10058885

The Journal of China Universities of Posts and Telecommunications

http://jcupt.bupt.edu.cn

Research on a provable security RFID authentication protocol based on Hash function

Yu Yinhui (✉), Zhang Lei

College of Communication Engineering, Jilin University, Changchun 130012, China

Abstract

Research on existing radio frequency identification (RFID) authentication protocols security risks, poor performance and other problems, a RFID security authentication protocol based on dynamic identification (ID) and Key value renewal is proposed. Meanwhile, the security problems based on Hash function RFID security authentication protocol in recent years have been also sorted and analyzed. Then a security model to design and analyze RFID protocols is built. By using the computational complexity, its correctness and security have been proved. Compared with the safety performance, storage overhead, computational overhead and other aspects of other protocols, the protocol for RFID has more efficient performance and ability to withstand various attacks. And the C# programming language is used to simulate the authentication process on the visual studio platform, which verifies the feasibility of the protocol.

Keywords mutual authentication protocol, provable security method, Hash function, RFID system

1 Introduction

RFID is a non-contact automatic ID technology. Through wireless communication, RFID uses radio frequency to transfer information between the tags and the readers [1]. Nowadays, RFID system is widely applied to manufacturing, logistics and transportation, etc. However, with the rapid development of RFID technology, the problems of security risks and poor performance hinder the development of RFID.

In order to improve the integrity, authenticity, privacy, and other functions for transferring information in the RFID system, experts have proposed many solutions [2]. In 2004, Weis et al. proposed the random Hash-Lock protocol. However, because the Key shared between the tag and the back-end server is sent in plaintext, the system is vulnerable to track, counterfeit attack, replay attack and other attacks. In 2008, Lee et al. [3] proposed the security protocol. Although it can resist the counterfeit attack, it fails to guarantee the forward/backward security and defend against the replay attack. In 2009, Ding et al. [4] proposed a Hash-based security authentication protocol (HSAP). Although the protocol can resist the counterfeit attack, replay attack and de-synchronization attack, it ignores the forward/backward security and the problems about transferring the ownership of tag. In 2010, Luo et al. [5] proposed a security protocol supporting the tag ownership transfer. The analysis shows that the protocol is of high cost in communication, heavy server computing and poor scalability.

This paper proposes a RFID security authentication protocol based on dynamic ID and Key value renewal. Compared with other protocols, the scheme can not only effectively protect the privacy security of RFID system and reduce the storage capacity, communication and computational load between the parties, but also its correctness and security are proved by using the provable security methods.

2 RFID system security design and demand

2.1 Security model

A typical RFID system is composed of RFID tags, RFID

Received date: 16-03-2016
Corresponding author: Yu Yinhui, E-mail: yuyh@jlu.edu.cn
DOI: 10.1016/S1005-8885(16)60018-3

readers and a back-end server. In RFID system, communications between server and reader generally takes place through a secure channel. However, communications between reader and tag usually occurs via wireless communication which is regarded as an insecure channel. In the process of building RFID security model, the system is often divided into two parts, namely the tag and reader (the reader and server are considered as the whole). The attacker A may control the radio channel and have the ability to acquire, block, replay and tamper with the message, which can also initiate a session with any entity in the process of implementation of the protocol at any time.

This paper presents the process of untraceable privacy model for the RFID authentication scheme [6–7]. It needs to use oracle query method to model the ability of the attacker A in detail. T expresses the tag, R does the reader, and the protocol between them is expressed by P. Both the tag and the reader can initiate a number of instances of P in the protocol, and Π_{T}^{i} expresses the ith tag instance, Π_{R}^{j} does the jth reader instance, An attacker A is able to implement the following oracle queries in the process of authentication protocol.

Execute($\Pi_{\mathrm{T}}^{i}, \Pi_{\mathrm{R}}^{j}$) It describes an instance that the attacker A executes the protocol between the tag and the reader, and the attacker A can get the full information.

SendTag($\Pi_{\mathrm{T}}^{i}, m_1$) It describes that the attacker A sends a message to the tag via the forward channel, and receives the response of the tag.

SendReader($\Pi_{\mathrm{R}}^{j}, m_2$) It describes that the attacker A sends a message to the reader via the reverse channel, and receives the response of the reader.

Corrupt(Π_{T}^{i}) It describes that the attacker A has the ability to bribe a tag, which leads to leak the secret information.

Test(Π_{T}^{i}) It describes that the attacker receives the secret information（ID, Key）from the Corrupt(Π_{T}^{i}), and it used to weigh the security of the statement of the Π_{T}^{i} instance. According to the toss of a coin b, if b=1, it returns the (ID, Key). If b=0, it returns a random number (the equal length of the tag's secret information).

RFID security object not only guarantees that the tag's secret information is not leaked, but also guarantees the tag's untraceable privacy. Therefore, it is necessary to ensure that T_0 and T_1 are not recognized and distinguished from all tags, and the following assumptions are defined.

Any attacker A implements the Test(Π_{T}^{i}) query for the authentication protocol P instance. The final result is $b' = b$, and then the event is defined as the identification of successful event $S(A)$. That an attacker identifies any two tags T_0 and T_1 is defined as the advantage of the successful identification, which can be mathematically written by

$$I\ (A)=2\Pr[S(A)]-1 \tag{1}$$

Untraceable privacy is defined by privacy games that contain an attacker, the tags and readers. The process is as follows.

In the first stage, the attacker A can send any Execute, SendTag, SendReader, Corrupt queries.

In the second stage, the attacker A selects a fresh session from the process of executing the privacy game, and sends a corresponding Test(Π_{T}^{i}) query to the session. It depends on a random bit $b \in \{0,1\}$, and sends $T_b \in \{T_0, T_1\}$ to the attacker. And then the attacker A continues to carry on any Execute, SendTag, SendReader, Corrupt queries.

In the third stage, after the attacker A get a result (b') of the output in the privacy game, the result is treated as a speculation of the b value.

2.2 RFID system security demand

1) Tags are low-cost and resource constrained. The tag is passively powered, so all the tags are highly resource constrained with limited computation power, storage capacity, and communication capability. Therefore, the selection of the password mechanism is limited. In our protocol, every tag needs to have only one Hash function, $H(x)$ and the XOR operation capability.

2) Reliability. When the RFID authentication scheme is designed, it can not only resist all kinds of common authentication attacks—counterfeit, replay and de-synchronization attacks, but also it is necessary to establish an effective security model to ensure that the real identity of user tags, the geographic location and other important information are not stolen and located.

3) Provable security. When the security protocol authentication scheme is designed, the relevant description of the protocol, the algorithm of reasoning and the insecure communication system, are very difficult to ensure that the authentication protocol is safe and effective. So its