Computer Standards & Interfaces 44 (2016) 110–116

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Design and analysis of secure mechanisms based on tripartite credibility for RFID systems

Baojiang Cui [a,b,1], Ziyue Wang [a,b,*], Bing Zhao [c], Xiaofeng Chen [d]

[a] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China
[b] National Engineering Laboratory for Mobile Network Security, China
[c] China Electric Power Research Institute, Beijing, China
[d] School of Telecommunications Enginnering, Xidian University, Xi'an, China

ARTICLE INFO

Article history:
Received 22 January 2015
Received in revised form 8 May 2015
Accepted 3 June 2015
Available online 12 June 2015

Keywords:
LLRP
RFID
Authentication
Security
MAC

ABSTRACT

The number of applications for RFID systems is growing rapidly. Due to the conflict between large-scale use of RFID technology and inadequate security-related research, this paper proposes secure mechanisms based on tripartite credibility consisting of an enhanced security mechanism of LLRP and a tag participation third-party authentication mechanism. This paper first introduces relevant information about RFID systems and then details design and implementation of the proposed secure mechanisms. Finally, this paper evaluates the performance of the proposed mechanisms in terms of storage complexity, communication cost and computational cost and analyzes the security advantages compared to those of previous research.

1. Introduction

Radio frequency identification (RFID) is a non-contact automatic identification technology that identifies targets to obtain relevant data using radio frequency signals without manual intervention in a variety of harsh environments [1]. Compared with other means of identification, RFID can identify multiple targets, moving targets and long-range targets. It has the advantages of robustness against moisture, dust and smoke. Currently, with the development of modern electronic technology, the emergence of low-power miniaturized chips promotes the rapid development of RFID applications [2]. RFID technology is now involved in all aspects of daily life, being widely used in various fields including production, manufacturing, retail, logistics, transportation, medical, inventory control and asset management to improve management efficiency [3].

In general, an RFID system consists of the tag, the reader, and the client. The tag, which is placed on the target, has a certain storage and computation capacity. As the tag stores the identity and special information of targets, it is the real data carrier in the RFID system. The reader exchanges data with the tag using a radio frequency signal. The essential function of the reader is to provide a means for data transmission with the tag. In addition, it offers some fairly complex functions, including signal state control, parity error checking and correction [4]. The client is simply accepted as a database system that is mainly used for storage, information processing and management of the RFID system. Generally, the client replies to queries from the reader through wired or wireless channel transmission.

EPCglobal is an RFID standard research institution jointly organized by UCC and EAN, and it has excellent speed, depth and breadth in setting global RFID standards [5]. Since its earliest days, EPCglobal has been committed to establishing a set of neutral, open and transparent global standards. EPCglobals goal is to solve the transparency and traceability of the supply chain [6]. Transparency and traceability mean that in the supply chain, all partners can understand the information on each individual item, including location, production date and so on. Low Level Reader Protocol (LLRP) is a protocol interface standard recently set by EPCglobal as the communication standard between RFID readers and clients [7].

LLRP is called low-level because it provides control of RFID air protocol operation timing and access to air protocol command parameters [8]. LLRP provides the formats and procedures of communication between a Client and a Reader, whose minimum unit is called messages [9]. Clients send messages including requests for capability discovery, device configuration, access operations, and inventory management to readers. Similarly, readers send messages such as the results of RF surveys, acknowledgements, access and inventory operation results to clients [10]. There is no mechanism for retransmission or re-request because LLRP is an application layer protocol. Consequently, maintaining

* Corresponding author.
E-mail address: princeyue@bupt.edu.cn (Z. Wang).
[1] This author is the first author.

http://dx.doi.org/10.1016/j.csi.2015.06.003
0920-5489/

the consistency of the readers status recorded by clients and real status is a prerequisite for the system to work properly.

As RFID technology is applied in more fields, the expectations for RFIDs development become higher [11]. RFID technology is currently in a rapidly rising period, and the technology is widely recognized to be one of the most promising application technologies of this century. Furthermore, a number of countries attach importance to RFID technology, hoping to develop it into a significant industry [12]. It is worth mentioning that Cisco predicts the global manufacturing sector will have 13.5 billion assets to apply to Internet of Things applications by 2022. The development of RFID technology has been in progress for more than 50 years, and the variety of RFID products will become increasingly diverse with advancing technology [13]. Therefore, the development of RFID technology will lead to new progress in a variety of areas such as the tag, the reader, application systems integration, middleware platform, and standardization.

Because the designers did not consider the security issues of RFID systems at the beginning, phenomena such as malicious tag damage, smart card copying, and mobile payment terminal impersonation appear frequently [14]. In particular, the leakage of military information and commercial secrets from RFID systems may cause serious consequences. RFID system security issues must be addressed urgently because security has become the bottleneck restricting the development of RFID technology [15]. The data exchange between the reader and the tag is carried over insecure wireless channels. Accordingly, attackers can easily intercept data exchange information to counterfeit the identity of communicating parties. There are also some security threats in LLRP, which is used between the reader and the client. For instance, the lack of sender authentication may cause security threats, and version negotiation error leads to interaction failure. This article improves the RFID security mechanism to address some of these security issues [16].

2. Related works

Due to the common uses of RFID, security and privacy can have a significant impact on the development of RFID systems. Thus, as a part of the RFID system, enhancing the security mechanism of LLRP is very important. In the past few years, some researchers have done excellent work on the applications of LLRP, but few have paid attention to security.

The first work on LLRP was a class library for the LLRP specification. It was developed by Joe Hoag from the University of Arkansas. The library, which is written in Java, can conveniently encode/decode LLRP messages to/from their corresponding binary representation. Later, a LLRP Reader Agent [17] was developed with the help of this library. This agent has the popular characteristic of being able to communicate with any LLRP Reader. Therefore, it is integrated into an agent-based RFID middleware application called TagCentric.

Beginning with Sana Qadir and Mohammad Umar Siddiqi, researchers have turned their attention to the security requirements of LLRP. Reference [18] summarizes the existing work that has been done on LLRP. It also assesses the security vulnerabilities of LLRP and discusses possible security solutions. Then, it presents the TLS-LLRP endpoints that use TLS to establish a secure LLRP connection, details the metrics selected to indicate performance and outlines the experimental procedures accordingly.

Reference [19] acknowledges that there is no significant fault-tolerant mechanism that considers the protocols behavior, and it proposes an approach that monitors RFID failures resulting from misconfiguration errors of the LLRP protocol using the logging system of this protocol. The authors have identified all RFID failures to consider and found their associated causes in LLRP misconfigurations. The causes are recorded in a knowledge model. A log file analyzer uses this knowledge model to address the detected failure.

In the exploratory research of reference [20], various protocols for authentication and cryptography in low-cost RFID are investigated and qualitatively compared in terms of output and results.

Hash lock is commonly employed by several protocols to improve the security and privacy of RFID authentication. Reference [21] is a survey that closely examines those protocols in terms of their focus and limitations. The hash-lock method is used in various ways in these RFID authentication protocols to address the security and privacy problems of RFID technology.

In reference [22], after highlighting goals and problems, an approach called Triggered Hash Chains is proposed to address the problems. The approach combines the concepts of two very different, widely known RFID protocols, i.e., the Hash-based ID variation approach and the Hash chain approach. The resulting proposal joins the advantages of both protocols. The approach is evaluated using a variety of practically relevant criteria.

Based on all of the above research, this paper proposes secure mechanisms based on tripartite credibility for RFID systems that combine an enhanced secure mechanism for LLRP with a tag participation third-party authentication mechanism, analyzing the advantages of the new approach compared to previous work.

3. Security assessment of RFID

The specifications already include security features or have recommended the ideal security practice [23] as EPCglobal is intended to provide its users the services of security and privacy. However, any supply chain management system built using current RFID components is vulnerable to certain security threats because manufacturers simply do not adopt any of the recommended security features.

Most RFID systems do not apply any security mechanisms, and messages are transmitted without being checked or encrypted [24]. The main reason for this lack of security is that such features are considered to be possible to ignore or add in the future as they can severely degrade system performance [25].

In view of this special circumstance, reference [26] indicates the most serious threats in an intra-enterprise scenario where RFID operates to be the following: tag sniffing, malicious or compromised Readers, spoofing, eavesdropping, replay and man-in-the-middle attacks on the communication channel between Reader and Client or between Reader and Tag.

Due to the features of LLRP [27], there are still threats such as interactive failure resulting from wrong version negotiation and protocol shutdown resulting from a malicious Reader [28].

Based on the security features above, the following security services should be implemented in LLRP:

- Reader-Client mutual authentication and authorization;
- Lightweight data encryption;
- Integrity verification and privacy protection of messages;
- Increasing the tolerance of failure in the negotiation process caused by parameter errors, to enhance protocol robustness.

4. Preliminary knowledge

The notations in Table 1 are used in this paper to describe the security mechanisms.

Notably, in following the discussion of an enhanced secure mechanism for LLRP, notation A is used to represent the Reader identifier instead of ID_A to simplify the representation. However, in the tag participation third-party authentication mechanism, notation ID_A is used to represent the Reader identifier to distinguish it from the ID of the Tag.

In addition, because various security keys can be derived from the same initial key, for example, K_0 for authentication is generated by $f(K, 0)$ and K_1 for encryption is generated by $f(K, 1)$, this paper simply