Research and Design of a Security Framework for RFID System

Jung-Tae Kim
Mokwon University

RFID 시스템의 보안 프레임 구조를 위한 설계 방법에 대한 분석

김정태
목원대학교
E-mail : jtkim5068@gmail.com

요 약

Given the security and privacy problems in the application of Radio Frequency Identification(RFID), this paper is proposed a kind of novel security framework, aiming to find a better mechanism in security and privacy problems. This paper reviews the relative work of RFID security mechanisms, then, the overall design scheme and modularized implementation of a secure RFID system based on trusted computing technologies is presented .

Ⅰ. Introduction

RFID is expected to be the basic technology for ubiquitous network or computing, and to be associated with other technology such as telemetric, and sensors. Recently, the wide deployment of RFID systems in a variety of applications has raised many concerns about the privacy and the security[1].

II. Current RFID Technology Development

Hardware components are common to all RFID applications while different software leads to different RFID application. Major issues in RFID hardware include product miniaturization, cost reduction, large production, etc. Some companies, such as German Siemens, speeded up the development of RFID chips to enrich their products and to meet users' needs. The integration density of current UHF RFID chips has been greatly increased. The new Generation 2 (Gen-2) RFID tags quickly replace old generation tags and have a dominant share on the RFID application market. Fujitsu developed the first RFID tag with 64KB memory which has been successfully adopted in aviation industry owing to its high access speed and large storage. The price of RFID readers are monotonically decreasing while the capacities of RFID readers are enhancing, in recent year. Microsoft issued the BizTalk Server which integrates the RFID with Microsoft product application. As RFID systems becoming an important part of everyday life, sensitive and private information may be stored in RFID tag. This security threat becomes more serious and puts a severe limitation to the promotion and deployment of RFID applications. However, owing to the limitation of space and cost of a RFID tag, RFID tag

usually does not equip with high power security mechanism. RFID tags are frangible to attack. Without appropriate security, anyone could read, alter and delete data on the RFID tags with a RFID reader/writer. Moreover, RFID tags are easy to clone. This is a big threat to access control systems. Now, a number of security measures are available for applications. For example, the ISO standard 15693 for data authentication is adopted in bank card authorizations and building access control systems. However, all security measures have some shortcoming and it has become a hot research topic in RFID[1].

III. Privacy and Security

Any emerging technology is bound to succeed if it meets the privacy and security concerns of the masses.

A. Privacy

In RFID system privacy falls under the realm of two domains; personal or individual's privacy and the manufacturer's privacy. Privacy could be compromised if personal information such as sizes of clothes worn by a woman, or RFID compliant items are known through readers deployed at various places. Also individuals could be tracked through their personal belongings and revealing of information such as credit card number or of the movie watched through the theatre ticket in the individual pocket do have some strength but not strong enough to curtail the growth of technology which can accrue enormous benefits. A study conducted by university of Florida in 2001 found that $ 5.8 billion (US) worth of inventory was lost due to administrations errors. The use of RFID for tracking the movements of inventory can save hundreds of million or even billions of dollars. Manufacturers have shown concern on spying by their counter parts to know the number of items they have marketed or sold in a store. Surely enough, the concerns are genuine. Privacy groups have made and are making inroads to overcome the said issues. Some suggested approaches to over come afore said issues are The "Kill Tag" Approach, The Faraday cage approach, The Active Jamming approach, The Smart RFID Tag approach, The Re-encryptions approach, Silent Tree Walking, Regulations Approach and The Blocker Tags[2].

B. Security

RFID has its peculiarities on account of its small size therefore all encryptions rules cannot be applied on it as done in other technologies. RFID tags have very rudimentary computational abilities as these are just small unpowered microchips. Relatively costly tags around 50 cents per tag are capable of some limited symmetric key cryptography. There are various forms of threats which could endanger the RFID system deployed in various applications. Some of those are:

The Danish company RFIDsec recently announced their first commercial launch of a secure RFID system, aptly called "RFIDsec". The RFIDsec Secure Protocol implements following features:

Compliant with EPC Gen-2 specifications operating in the standard protocol custom command space.

Strong encryption - all communications can be encrypted, making "listening in" a useless activity.

One-step authentication - the tag can remain silent, and hence unnoticed, until the reader that emits the "wake up" signal has been authenticated.

Support for advanced access management - making it possible to "partition" the chip memory and define different access rights for different parties for different parts of that memory.

It is essential to mention here that a "master key" is part of this functionality, making it possible to transfer full access control of the tag and all data on it to the customer at the POS when a tagged item is bought by him.

IV. Security Framework

We analysed a security framework in RFID system which guarantees that the reader will comply with a specific security and privacy policy[3].

A. A RFID security framework

RFID security framework contains three components: some RFID tags, trusted RFID readers that remotely stores and retrieves data using RFID tags or transponders, and a trusted server which contains privacy and security information. Addition to these, there is a database that stores product information, tracking logs, or key management of data. According with the following main steps to read the tag data when a tag arrives in the proximity of the reader:

A. A Request Verification

A request to read data is sent to the RFID trusted reader management module. This request is forwarded to the TPM, which verifies that the reader is still valid.

B. Trustsed Reader Verification and Configuration

The reader then sends back the request(including Trusted Agent ID) to the TS and the trusted policy engine is executed. There two cases: First, if this is the first request, the trusted agent ID is all zero, TS will assemble trusted agents and send to reader. At the same time, the Agent Id will be registered in ANS. The trusted agents will implement the readable and security policy initialization for the reader. Second, if this is not the first request, TS will check ANS, if the trusted agent ID is still valid and the privacy policy do not need to be updated. TS sends back the response and authorization to the reader. Else, TS sends back the trusted update agent and authorization to the reader.

C. Access and Execute

The TR then read and sends back the tag data to the TS. Meanwhile, a log is created for each reading operation.

V. Conclusion

RFID is becoming increasingly prevalent as the price of the technology decreases. A primary RFID problem concern is security threats against RFID system. We describe a way to design the RFID security framework to allow for maximum flexibility in changing privacy and security

References

[1] Dong-liang Wu, "A brief Survey on Current RFID Application", Proceedings of the Eighth International Conference on Machine Learning and Cybernetics, Baoding, 12-15 July 2009, pp.2330-2335

[2] A. Juels, RFID Security and Privacy: "A Research Survey,Selected Areas in Communications", IEEE Journal on Publication Date: Feb. 2006 Volume: 24, Issue: 2 On page(s): 381- 394

[3] Yan Fang, Liu BingWu1, Huo LingYu1 ,Yang Xi, "Research and Design of a Security Framework for RFID System",2010 International Forum on Information Technology and Applications, pp.443-445

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number:2010-0024133)