Analyse of Trade-off for Implementing RFID Tag to Enhance Security

김정태
목원대학교

보안성 향상을 위한 RFID 태그 구현시의 Trade off 분석

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

요 약

Most of the sources of security and privacy issues in RFID technology arise from the violation of the air interface between a tag and its reader. This paper will approach the security risk analysis is process from the perspective of the RFID tag life cycle, identify the tag usage processes, identify the associated vulnerability and threat to the confidentiality, integrity and availability of the information assets and its implications for privacy, and then mitigate the risks

Ⅰ. INTRODUCTION

An emerging application is ubiquitous applications. The use of RFID tags for anti-counterfeiting by embedding them into a product is widespread. Public key cryptography (PKC) offers an attractive solution to the counterfeiting problem but whether a public key cryptosystems can be implemented on an RFID tags or not remains unclear. RFID based on identification is an example of an emerging technology which requires authentication as a cryptographic service. This property can be achieved by symmetric as well as asymmetric primitives. Previous work considered only symmetric key algorithms such as AES. It is not clear whether public key algorithms can be implemented in constrained devices, such RFID tag, and still depends on the area, performance and power requirements in typical of these applications[1].

II. BASIC SECURITY CONCEPTS

Because of the susceptibility of wireless radio communications, security of wireless networks can be more easily compromised and may be vulnerable to a more diverse range of threats than wired networks. However, fundamental security requirements of wireless networks are almost identical to those of wired networks. The generic security requirements of wireless networks are as follows:

Confidentiality guarantees that communicated data is accessible only to the intended recipient(s).

Authentication provides the communicating parties with a way to verify their identity.

Integrity enables the recipient of a message to verify that a message was not altered while in the network.

Availability ensures that the system remains operational even in the presence

of malicious or faulty nodes. The common threat to availability is a denial of service (DOS) attack.

Non-repudiation facilitates the proof that a message was sent and received by the parties that actually sent and received the message, respectively, that is, to prevent the parties from repudiating the transaction after it is committed.

Sometimes presented by the media as the next technological revolution after the Internet, Radio Frequency Identification (RFID) aims to identify objects remotely, with neither physical nor visual contact. They consist of transponders inserted into objects, readers which communicate with the transponders using a radio channel and a database which contains information on the objects. Many cryptanalytic problems can be solved in theory using an exhaustive search in the key space, but are still hard to solve in practice because each new instance of the problem requires to restart the process from scratch. The basic idea of a time-memory trade-off is to carry out an exhaustive search once for all such that following instances of the problem become easier to solve. Thus, if there are N possible solutions to a given problem, a time-memory trade-off can solve it with T units of time and M units of memory[2].

A. Classic Cryptography:

Rewritable Memory: In 2003, Kinoshita proposed an anonymous-ID scheme. The fundamental idea of his proposal is to store an anonymous ID, E(ID), of each tag, so that an adversary can not know the real ID of the tag. E may represent a public or symmetric key encryption algorithm, or a random value linked to the tag ID. In order to solve the tracking problem, the anonymous ID stored in the tag must be renewed by re-encryption as frequently as possible.

B. 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[3]

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(CR) authentication system". 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.

III. Consideration of Performance

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

A. Security analyses

Confidentiality:

This is a mechanism to guarantee a tag's privacy. In real 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 can design 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

We can estimate and make a close comparison of protocol to compare performance in terms of computational, storage and communication overhead.

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

As mentioned earlier, the primary objective of ECC is to provide a ready-to-use, publicly available software package for ECC based PKC operations that can be flexibly configures and integrated into sensor network application. To achieve this goal, we follow several principles in the design and development of ECC.

1. Security
2. Portability
3. Resource awareness and configurability
4. Efficiency
5. Functionality

IV. Conclusion

We analysed the performance of security related to issues by means of information security and privacy. Neither a symmetric nor an asymmetric cryptographic deployment is necessarily with light weighted algorithm. Both have advantages and disadvantages and their relative suitability will depend on the application.

References

[1] Gildas Avoine, Pascal Junod, and Philippe Oechslin, "Time-Memory Trade-Offs: False Alarm Detection Using Checkpoints", INDOCRYPT 2005, LNCS 3797, pp. 183 196, 2005.

[2] Martin Feldhofer, "Strong crypto for RFID Tag, - A comparison of low power hardware implementation", 2007 IEEE, pp.1839-1842.

[3] Yong Ki Lee, etcs, "Elliptic Curve Based Security Processor for RFID", IEEE Transactions on Computers, v.57. n.11, pp. 1514-1526, NOV. 2008.

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)