Design of Security Primitive based on Hardware Architecture For RFID Tag

김정태
목원대학교

RFID 태그를 위한 하드웨어 구조에 기반한 보안 프리미티브 설계

Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@hotmail.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 read. 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 consideration of security analysis with cryptographic primitive based on hardware basis.

Ⅰ. Introduction

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. 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 overcome aforesaid 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 [1].

II. Related Work

Tags themselves have no access control function, thus, any reader can freely obtain information from them. As a result, an authentication (as well as authorization) scheme must be established between the reader and the tag so as to achieve the privacy issue of a RFID system. Another tag security issue related to the scenario such that since the communication between a tag and a reader is by radio, anyone can access the tag and obtain its output, i.e. attackers can eavesdrop on the communication channel between tags and readers, which is a cause of consumers' apprehension. So the authentication scheme employed in RFID must be able to protect the data passing between the tag and the reader, i.e. the scheme itself should have some kind of encryption capability. Unfortunately, public-key cryptography requires the tag to perform complex mathematical computations. Because low-cost RFID tags offer extremely limited resources, it could be problematic to implement a public-key authentication protocol while keeping the tag's cost low. As of this writing, the most compact implementation of a public-key encryption scheme is the elliptic-based public-key encryption cipher (ECC), which requires roughly 15,000 logical gates on a tag. Cryptographic primitives required to implement hash-based authentication schemes are more compact. The Secure Hash Algorithm 1 (SHA-1), for example, only requires approximately 4,300 gates, whereas the Advanced Encryption Standards (AES) symmetric cipher requires roughly 3,400 gates. An on-tag scheme requires the tag to implement at least one of these primitives. Yet, some argue that current RFID chips costing below US$0.50 dispose of only 2,000 to 10,000 logical gates, approximately 200 to 2,000 of which are available for security needs.5 Consequently, not enough resources are currently available to implement any of the proposed authentication mechanisms [2].

III. Security and Privacy

A reader needs to communicate with tags and an application system which processes the data from the reader. Generally we do not concern too much about the security between the reader and application system since we can use current secure techniques, rather than the security challenges and technologies between the reader and tags. Privacy is also a serious concern for customers, and it may be an obstacle for RFID application when customers privacy is not able to guarantee. People may carry objects with communicating readers without even realizing the existence of tags. Passive tags usually send data out without security authentication when they receive a signal from readers. The data may also link to other secret information and location message that should be protected. Fundamental security objectives as confidentiality, integrity, authentication and anonymity are not achieved in RFID systems without the supports from special security mechanisms. For example, confidentiality is defined as ensuring that information is accessible only to those authorized to have access. The communication between a reader and tags in RFID systems is not protected by secure mechanisms. Eavesdroppers may then obtain information during their communication. The data risk from a reader to tags means forward channel is higher than that from tags to the reader means backward channel since the different power ranges. The work power range in forward channel can be hundreds meters, but the range in backward channel usually is several mini meters. Tags memory can also read if there is no access limits. Proposals for RFID security and privacy are categorised in two groups: one is for low-cost tags that cannot perform any computations, and the other is for higher capability tags (active tags) which are able to do some limited cryptographic operations [1]. We focus on the security and privacy of low-cost RFID systems in this paper [3].

IV. Performance and Evaluations

We will compare our protocol to its counterparts which are based on the hash function in the aspects of computational cost, storage cost, communication cost and security [4].

A. Computational Overhead

The main restriction of the computational ability lies on the tags. In our protocol, tags only need hash and XOR calculation while its counterparts use the hash function, the keyed hash function, the pseudorandom number generator and the XOR operator. The number of gates available to low-cost tag is usually around 7.5 15Kgates in which the number of gates that can be used to implement cryptographic technology is around 2.5 5Kgates. The universal Hash algorithm can well satisfy the restriction of the computational ability, so we can apply it for the tags.

B. Storage Overhead

The tag only stores the information related to authentication such as key and the random secret number T. The other information is stored in the back-end server. Thus, our protocol could meet the potential storage constraints in a low cost RFID environment.

C. Communication Cost

The protocol only needs five steps to exchange the authentication information, including two steps between the back-server and the reader. This is acceptable for most of the RFID system environment. In addition, we only transmit half of the information in step 2 and step 5, so as to improve the efficiency of the transmission and economize the communication cost. So our protocol is more efficient in communication cost than other RFID authentication protocols.

V. Conclusion

We presented an cryptographic issues for efficient and secure RFID authentication protocol. And we estimated performance for security primitive based on computation, storage and communication overhead.

References

[1] Ari Juels. RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications, 24(2):381 394, 2006.

[2] Sarah Spiekermann and Sergei evdokimov, "Critical RFID Privacy-enhancing technologies", IEEE Computer and reliability societies, march/april 2009, pp.56-62

[3] Hua Wang, etcs, "Privacy Preserving on Radio Frequency Identification Systems", Proceedings of the 2009 13th International Conference on Computer Supported Cooperative Work in Design, pp.674-679

[4] H.Y. Chien, “SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity,” IEEE Trans. Dependable and Secure Computing, vol. 4, no. 4, pp. 337-340, 2007.

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:2011-0026950)