Analyses of Light-weight Protocol for Tag Security in RFID System

김정태
목원대학교

RFID 시스템에서의 태그 보안을 위한 경량화 프로토콜 분석

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

요 약

Most of existing RFID authentication protocols either suffer from some security weaknesses or require costly operations that are not available on low-cost tags. In this paper, we analyzed the security mechanism of a lightweight authentication protocol.

Ⅰ. Introduction

RFID (Radio Frequency Identification) is an automatic identification technology to remotely store and retrieve data. A typical RFID system is composed of RFID tags, RFID readers and a back-end server. The reader forwards the tag response to a back-end server. The back-end server has a database of tags and can retrieve detailed information regarding the tag from the tag response. Recently, the wide deployment of RFID systems in a variety of applications has raised many concerns about the privacy and the security. An RFID tag can be attached to a product, an animal, or a person for the purpose of identification using radio waves. For any possible reasons, an adversary may perform various attacks such as eavesdropping, traffic analysis, spoofing, disabling the service, or disclosing sensitive information of tags, and hence infringes people's privacy and security [1].

II. Related Work

Although there have been many works devoted to design security mechanisms for low-cost RFIDs, most of these works require the tags to be equipped with costly operations such as one-way hashing functions, which are still unavailable on low-cost tags. Contrary to these works, the schemes do not require the support of hashing functions on tags. However, the schemes have been reported to show some security weaknesses. Recently, Li et al. [2], based on only bitwise XOR (□), the Partial ID concept and pseudo random numbers, proposed a lightweight RFID authentication protocol for low-cost RFIDs. Different from most of existing solutions which used conventional cryptographic primitives (encryptions, hashing, etc), this protocol only used simple operations like XOR and substring [3].

III. Enhancement of Security Mechanism

Many proposals have been proposed to satisfy the security requirements in order

to resolve the privacy problems. In this section, we have divided the previously proposed protocols into two categories [4].

A. Hash Function Based Security Protocol

Hash-lock protocol and the randomized hash-lock protocol proposed by Weis et al., the hash-based ID variation protocol proposed by Henrici et al., and the hash chain protocol proposed by Okubo et al. are the most interesting and efficient protocol based on hash function. However, these methods are proven to be unsecure and not efficient in those three security requirements aspect.

B. Arithmetic Calculation Based Security Protocol

To design a security protocol based on simple encryption algorithms in order to fulfill the low implementation needs, Juel et al. proposed minimalist cryptography using one-time pad scheme for low-cost RFID system and a HB algorithm based protocol. However, one-time pad based protocol did not fulfill the implement cost limitation and several security problems of the HB algorithm based protocols have been verified recently.

C. Simple Operation

Another issue related to the design of RFIDs is the computational effort required at the tag side. This is because most common tags are passive devices in the sense that they derive electrical power from the signals sent by a reader [5].

Peris-Lopez et al. initiated the design of the so-called ultra-lightweight RFID protocols, which involve only simple bitwise logical or arithmetic operations like exclusive-OR (XOR), OR, addition, subtraction, bit rotation, and so forth[5]. In particular, Chien presented the SASI protocol, which is designed to offer better security than previous protocols of Peris-Lopez et al. SASI is claimed to achieve a list of security properties, including resistance to tracking, i.e., untraceability.

IV. Conclusion

In this paper, we analyzed the security of the lightweight protocol to apply for light-weight mutual authentication. We should consider requirement for implementing which is one of its design objectives.

References

[1] Chien, H., & Chen, C. Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards. Computer Standards &Interfaces, 29(2), 254 259. 2007.

[2] Hung-Yu Chien and Chen-Wei Huang, "A Lightweight Authentication Protocol for Low-Cost RFID", Journal of Sign. Process Syst.,DOI 10.1007/s11265-008-0281-8, 2008

[3] Shijie Zhou, etcs "A lightweight anti-desynchronization RFID authentication protocol", Inf Syst Front, DOI 10.1007/s10796-009-9216-6, 2009

[4] Jung-Hyun Oh, etcs, "A Secure Communication Protocol for Low-cost RFID System", Seventh International Conference on Computer and Information Technology, pp.949-954, 2007.

[5] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, “EMAP: A Efficient Mutual Authentication Protocol for Low-Cost RFID Tags,” Proc. OTM Information Security Workshop (IS ’06), pp. 352-361, 2006.

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)