A Practical Approach for Enhancing Security of RFID Tag

You Wei Ko, Jeon Woo Nam, Yeong Beom Park, Jung-Tae Kim
Mokwon University

RFID 태그의 보안성을 향상시키기 위한 실제적인 접근 방법

고유위, 남전우, 박영범, 김정태
목원대학교
E-mail : jtkim5068@gmail.com

요 약

Radio Frequency Identification(RFID) has been considered as an key infrastructure for the ubiquitous society. However, due to the inherent drawbacks, RFID causes var- ious security threats like privacy problems, tag cloning, etc. This paper proposes a novel practical approach, which are fully conformed to EPCglobal RFID Gen2 standard, for enhancing security of currently used RFID Gen2 tags against the various security threats.

Ⅰ. Introduction

A basic RFID infrastructure consists of 3 major components: (1) tags,(2) a reader and its antenna, and (3) middleware application software. RFID tags are transponders that contain a chip and an antenna. The antenna receives radio signals from the readers while the chip is used to respond to the signals and to store information. Current tags are small enough to be embedded into physical objects for identification and tracking. Tags can be read only, write once/read many times or read/write. Security Requirements of Low-cost RFID Systems. To address the forementioned threats and privacy concerns a low-cost RFID system should satisfy the following security requirements:

A. Anonymity-Privacy: The values transmitted by a tag must not reveal any information about the product that it is attached to.

B. Privacy Location-untraceability: The values transmitted by a tag to a reader must not allow to an adversary to trace the product or the person that is carrying this tag[1].

Forward Security: The adversary must not be able to identify any previous transactions that a tag was involved in, even if he manages to obtain any secret values stored in the tag[2]. This property is referred as forward traceability. Protection against Tag spoofing-cloning: The adversary must not be able to spoof or to clone a legitimate tag, unless the tag has been tampered with.

C. Availability: The reader and thus the back-end system should always be in place to identify a legitimate tag[3].

II. Related Work

As illustrated in Fig. 1, a basic RFID system consists of six main components:[2]

RFID tag (transponder): The identification device attached to the tracked item.

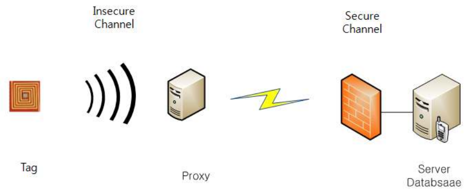

Figure 1. Block diagram of system configuration

1. A reader (transceiver): Handles radio communication through the antenna to detect the presence of RFID tags and read the information stored in them.
2. A reader antenna: A device which can be either stand-alone or integrated into the reader to enable two-ways RF communication between readers and tags,
3. RFID middleware: A software or dedicated hardware used to consolidate aggregate, process and filter raw RFID data received from multiple readers to generate useful information for enterprise applications.
4. Back-end RFID enterprise service: Receives filtered RFID data from the middleware and uses Application Programming Interfaces (APIs) to integrate these with existing enterprise applications
5. Network infrastructure: This is the backbone infrastructure to connect readers, middleware and the back-end data center.

Juels proposed privacy preserving schemes based on the tree-walking singulation scheme, that is the blocker tag and soft blocker tag[4]. Soft blockers simply show the privacy preferences of their owners to RFID readers. Most works about RFID security, especially authentication and privacy protection tried to facilitate the one-way hash function. Weis proposed hash lock scheme which utilized the metaID and a security key. Most of the previous works using the tag's cryptographic operations should not be applied to the low-cost RFID Gen2 tags and conformed to the Gen2 standard. Some schemes persisted to be conformed to the Gen2 standard also require the hardware-level of modifications since the ways where the tags and readers operate are totally different from the ways defined in the standard. We analysed DESL algorithm and its low-power, size optimized implementation aims at very constrained devices such as passive RFID tags. Providing cryptographic primitives[2] (esp. encryption) at extremely low cost is of paramount importance for securing RFID applications. Thus far, there have been two approaches for providing cryptographic primitives for such situations:

Optimized low-cost implementations for standardized and trusted algorithms, which means in practice in essence block ciphers such as AES

Design new ciphers with the goal of having low hardware implementation costs2 The best known light-weight AES implementation requires 3400 gates and draws a maximum current of 3.0µA

III. Enhancement of Security Mechanism

In order to enhance the security of RFID, especially the privacy of sensitive data, various cryptographic techniques have been proposed[4]. For example, "Hash-Lock" approach serves as a lock for a tag until a key or PIN is provided to unlock it. Re-encryption is a technique that re-encrypts a tag's content from time to time to avoid tracking, but the computation must be done by a trusted third-party due to the calculation overhead. Universal re-encryption is similar to the re-encryption approach except it uses public keys and the encryption is done locally on the tags using an extension of the El Gamal cryptosystem. Silent tree-walking is used to encrypt reader transmissions so that passive eavesdroppers “cannot infer the IDs being read”. Feldhofer et al. proposed a lightweight hardware implementation of a 128-bit version of the AES(Advanced Encryption Standard). Their design requires over 3500 gate equivalents considerably more than appropriate for basic RFID tags, but suitable for high-cost RFID tags. Juels and Weis proposed a lightweight authentication protocol called HB+. To implement HB+, tags have to generate random bits and compute binary dot products. The key lengths required for good security are as yet unknown, and the security model is limited[3].

Based on the computational cost and the operations supported on tags, the RFID authentication protocols divide into four classes as follows [4].

(1) The full-fledged class. The protocols such as an application on E-passport that need the support of conventional cryptographic functions, one-way hash function, or even public key algorithms.

(2) The simple class. The protocols is similar to the schemes that install pseudo random number generator or one-way hash function on tags.

(3) The lightweight class. The protocols that require a pseudo random number generator and simple functions like Cyclic Redundancy Code (CRC) checksum.

(4) The ultralightweight class. The protocols that only require simple bitwise operations (e.g. XOR, AND, OR, etc.) on tags. The tags of this class are suited for low-cost RFIDs.

Ⅳ. Conclusion

RFID technology can help automatically and remotely identify objects, which raises many security concerns. The authors review and categorize several RFID security and privacy solutions, and conclude that the most promising and low-cost approach currently attracts little academic attention. There is an urgent need to develop authentication protocols that are immune to attacks to allay fear among the ultimate consumers. Although there will probably never be complete security/privacy, it is necessary to identify possible threats and address them.

References

[1] Faouzi Kamoun. "RFID System Management: State-of-the Art and Open Research Issues" IEEE Transactions on Network and Service Management, V.6, N. 3, pp.190-205, Sep. 2009

[2] George Poulopoulos, Konstantinos Markantonakis, Keith Mayes, "A Secure and Efficient Mutual Authentication Protocol for Low-Cost RFID Systems", pp.706-p.711, 2009 International Conference on Availability, Reliability and Security

[3] S.A.Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Security in Pervasive Comp., volume 2802 of LNCS, pages 201-212, 2004.

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

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)