Practical Issues of Cryptography for RFID Privacy with Lightweight Mechanism

김정태

목원대학교

경량화 기법을 가진 RFID 보안을 위한 암호학적 구현의 문제

Jung-Tae Kim

Mokwon University

E-mail : jtkim5068@gmail.com

요 약

Using carefully assembled sets of IDs based on the cryptographic principle of secret shares, we can create RFID tags that yield virtually no information to casual "hit-and-run" attackers, but only reveal their true ID after continuous and undisturbed reading from up-close something that can hardly go unnoticed by an item's owner. In this paper, we analyses the practical issues of cryptography for RFID privacy with lightweight method.

Ⅰ. Introduction

RFID industry is actively developing international standards to meet the security and privacy needs, such as the Advanced Encryption Standards(AES). Different industries are meanwhile trying to design advanced authentication systems. This task is challenging as there are currently over 500 tags types available where different tags need different levels of security. RFID tags fit into generally three categories.

1. Logistical applications that require quick reading and very low security. These devices are used in shipping and receiving.
2. Consumer applications that requires high end security but no bulk reading capabilities. These are found in smart cards.
3. Vertical applications that need special security features tailored for specific use.

A good example is those RFID tags used in casino poker chips. In a typical system, RFID tags are attached to objects to be monitored. Each tag has a certain amount of internal memory is stored. This includes information about the object such as serial number, product composition, and so on. When a tag passes through wireless signals generated by a reader, it transmits this information to the reader, thereby identifying the object. Tags have a small capacity of memory in a range of formats such as Read-Only, Write Once Read Many, and Read/Write [2].

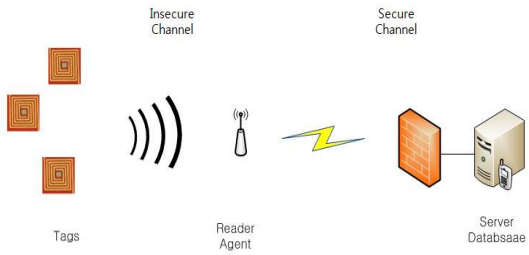

Fig. 1 Configuration of Basic RFID system

II. Trends of technology

RFIDs come in various sizes and may have different functionalities. These devices are currently in use by some major corporations as well as the government agencies for several reasons,

- Security/Access Control
- Supply Chain Management
- Fixed-Assets Tracking
- Toll Collecting
- Rental Items Tracking
- Baggage Handling

We present a list of general security goals as follows.

- Privacy:
- Protection against tag spoofing or cloning:
- Protection against impersonation attacks:
- Policy enforcement and access control:
- Transferability and tag release:
- Simplicity and efficiency:

In respect of market popularization consideration, the cost of RFID tag plays an important role. Based on the computational cost and the operations supported on tags, the RFID authentication protocols divide into four classes as follows [3].

(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.

III. RFID Threats

RFID threats can be broadly classified into following groups. a) inside supply chain b) transition zone and c) outside supply chain. Threats can also be classified into following groups depending on the type of organization/group. it affects a) Corporation b) Individuals and c) Other organizations[2].

A. Personal Privacy Threats:

Further groups the Individual privacy threats into following types

B. Association Threat: Vendors can associate a particular purchase with an individual by unsolicited reading of the RFID tags carried by that individual. RFID technology assigns unique id to each instance of the product. For example a vendor can associate a particular instance of coke bottle to an individual thereby creating a association between them.

C. Location Threat: An individuals` location can be determined by surreptitiously placing readers at specific locations. An individual carrying a unique tag can be monitored by the readers and his location revealed by correlating the unique id with the vendor database.

D. Preference Threat: A vendor/adversary can scan the RFID tags to reveal an individual`s personal preference. They can use this information to push advertisements to that individual through various channels. Unauthorized person can scan items with high value to pick up a potential victim for his crime.

E. Constellation Threat: Adversaries can use “constellation” (group) of tags carried by an individual to track his location. These unique individual tags can be a “signature” for an individual. He can be tracked on basis of this “signature.

F. Corporate espionage threat: Competitors

can gather data about supply chain remotely. Such data is most protected data in supply chain industry.

IV. Security Requirements

We consider privacy, cloning resistance, forward secrecy, and untraceability as the fundamental security requirements of RFID privacy-preserving authentication [3]. In RFID systems, a private authentication protocol should meet the above security requirements.

A. Privacy: Any user's private information should not be leaked to any third party during authentication.

B. Cloning resistance: All the valid tags should not be faked or impersonated. Replay attacks, in which adversaries may repeat the messages sent before to victims tag or readers, should also be infeasible to the authentication procedure.

C. Forward secrecy: Achieving forward secrecy is that keys stored in a compromised tag cannot reveal the previous outputs of this tag.

D. Untraceability: A tag should have no correlation with its authentication messages for avoiding tracking.

V. Security and performance Analysis

We make a comparison of protocol in terms of computational, storage and communication overhead.

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

We should analyses security analysis and performance evaluation to evaluate security analysis

- Protect user's privacy.
- Obtain mutual authentication.
- Resist impersonation attack.
- Forward secrecy.
- Resist de-synchronization attack.
- Resist replay attack.

VI. Conclusion

Authentication is an important requirement for many RFID applications. However, most of the authentication mechanisms always too complex on computation or need large memory space such that they are not suit for low-cost RFIDs. In this paper, we survey a security requirements and threats for ultra-lighweight RFID mutual authentication protocol.

References

[1] Ari Juels, "RFID security and privacy: A research survey," In IEEE Journal on Selected Areas in Communication, 2006.

[2] Garfinkel Simson,Juels Ari and Pappu Ravi, "RFID Privacy: An Overview of Problems and Proposed Solution", IEEE Security and Privacy Magazine, April-May 2006

[3] 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.

[4] Y. Z. Li, Y. B. Cho, N. K. Um, and S. H. Lee, "Security and Privacy on Authentication Protocol for Low- Cost RFID," CIS 2006, LNAI, vol. 4456, pp. 788 794, 2007.

[5] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags," RFID Privacy Workshop 2003, MIT, MA, USA, 2003.