Unified Modeling for RFID Privacy to Enhance Security Issues

김정태
목원대학교

보안성 문제를 개선하기 위한 RFID 보안성에 대한 모델링 기법

Jung-Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

요 약

RFID technology can help automatically and remotely identify objects, which raises many security concerns. We review and categorize several RFID security and privacy solutions, and conclude that the most promising and low-cost approach currently attracts little academic attention. We therefore concluded that, from a privacy perspective, the user scheme is an important strategy for meeting the consumer's needs. Furthermore, we call for the privacy research community to put more effort into this line of thinking about RFID privacy.

Ⅰ. Introduction

As the Unified Modeling Language (UML) sequence diagram in Figure 1 shows RFID security and privacy model , this form of authorization process involves a reader directly addressing an object's tag to ask for permission to read. If a system authorizes it, then the reader gains access to the tag's content. An early and relatively simple example of this kind of technology is the randomized hash-lock procedure, which relies on a hash function implemented by the tag's circuitry such as (a) on-tag, (b) agent, (c) user schemes and (d) password model. The user has more control over privacy because he or she has the opportunity to authenticate requests, thereby giving the tag explicit permission to release its data. Each proposal involves trade-offs concerning security levels, tag cost, key management complexity, and user transaction cost.

II. Related Work

Furthermore, each solution achieves a different level of user control. 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 [3].

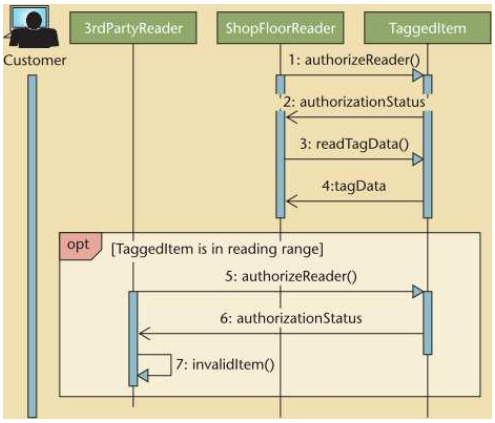

Fig 1. RFID security and privacy model

III. Requirement of Security Mechanism

We describe several common attacks on RFID system in the following.

- Access control
- Tag anonymity
- Protection against traceability
- Reply attack prevention
- Synchronization analysis
- Eavesdropping resistance
- Impersonation resistance
- Data integrity

A low-cost RFID system should satisfy the following security requirements:

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

2) 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.

3) 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. This property is referred as forward traceability.

4) 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.

5) Availability: The reader and thus the back-end system should always be in place to identify a legitimate tag.

IV. Conclusion

In this paper we have reviewed and analyzed previous RFID protocols in order to highlight the importance of trust in communication between back-end server, RFID reader and tags.

References

[1] PawelRotter. A Framework for Assessing RFID System Security and Privacy Risks. IEEE Pervasive Computing, pp.70-77, June 2008.

[2] Ari Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications, pp.381-394, February 2006

[3] Sarah Spiekermann and Sergei evdokimov "Critical RFid Privacy-enhancing technologies", IEEE Security & Privacy, March/April 2009, pp.56-62.

[4] Garfinkel,S.L., Juels,A., Pappu,R. "RFIDprivacy: an overview of problems and proposed solutions", Security & Privacy, IEEE, v. 3, n3, May 2005, pp.34-43

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)