Design and Analyses of Security Mechanism with Low Cost RFID Tag

김정태
목원대학교

저비용 RFID 태그를 위한 보안 메카니즘의 분석 및 설계

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

요 약

RFID technique has been applied in high-security and high-integrity settings such as national defense, healthcare, and citizen identification. We proposed especially the privacy of sensitive data, various cryptographic techniques applicable to low-cost RFIDs in order to enhance the security of RFID.

Ⅰ. Introduction

Research and development in RFID has been focused on hardware and firmware components such as active and passive RFID tags, readers, and embedded software, for the purpose of its deployment in specific application domains. RFID is being incorporated in supply chain management, giving enterprises a real time view on the location and integrity of their inventories. RFID technology is used in a location sensing prototype system for locating objects inside buildings. The main challenge of low-cost RFID tags is that they are not able to process any kind of access control mechanisms on the data stored. This feature of the low-cost RFID tags provides a query response of any reader without authentication, and hence clandestine scanning of the tags is a possible threat. On the other hand, low-cost tags are normally deployed in a wide area. As a result of the deployment, private information may disclose through the tags they carry. For instance, tags on medicines may show what diseases a person has, and books include what are your interests. More ever, people never want to let others know the number and how much they have in their wallet, especially when walking alone in a street. RFID is a powerful technology with numerous application possibilities. It's also a technology that raises serious privacy and security risks. Several RFID features make it particularly vulnerable among information systems, including the wireless transmission between the tag and reader; the tag's low computational power, which is often insufficient for strong security measures; and the tag's small size, which means that people can carry one without their consent or even knowledge [1].

II. Related Work

A shared pseudonym between each tag and the back-end database is required [2].

Exclusive-or (XOR) operation is the main functional component that is needed. They suggest key update after each session to guarantee forward security. Vajda and Buttyań proposed a set of extremely lightweight tag authentication protocols based on XOR, subset, squaring, etc. Although they cannot prevent active tracking attacks, they present effective ideas for low-cost RFID tag design. Another utmost lightweight metric is based on the concept of one-time pad [3].

III. Security Risks and Privacy Threats

With the development of RFID technology, its data security and personal privacy issues become increasingly prominent, which become an obstacle to the further development of RFID technology. Therefore, how to improve its security and protect personal privacy have become a research focus. Currently, major security threats faced by RFID reader network system are as follows: eavesdropping, relay attacks, unauthorized tag reading, tag cloning, people tracking, relay attacks, jamming, back-end attacks.

A. Security Risks

As mentioned in the security objectives, if those objectives are achieved, following attacks can be alleviated. Attacks on tags/interrogators, Access-key or Cipher-text tracing, Eavesdropping,Spoofing, Man-in-the-Middle, Replay, Brute-force and Denial of Service will be evaluated by considering the fulfillment of the above security objectives. Each attack will be checked for full protection, partial protection and no protection by evaluating the achievement of the list of basic security objectives under each attack.

B. Privacy Threats

Privacy threats can be crucial to two parties: Corporate Privacy and Personal Privacy. Each party is vulnerable to specific threats. In addition to the security protection, each privacy objective should be achieved to protect the corporate privacy threats: Corporate espionage threat and Competitive marketing threat, and also the personal privacy threats: Action threat, Association threat, Location threat, Preference threat, Constellation threat, Transaction threat. Each threat is checked against the above privacy objectives and evaluated for the fulfillment as fully protected, partially protected, not protected and not applicable.

IV. Conclusion

RFID technology presents a number of advantages, but also opens a huge number of security problems that need to be addressed before its successful deployment. In this paper, we have Analysed of security risks and privacy threats.

References

[1] Pawel Rotter, "A Framework for assessing RFID System Security and Privacy risks", IEEE CS, pp.70-77, 2008.

[2] Hung-Min Sun and Wei-Chih Ting, "A Gen2-Based RFID Authentication Protocol for Security and Privacy", IEEE Tran. on Mobile Computing, v.8, n. 8, Aug. 2009, pp.1052-1062.

[3] Vajda and L. Buttyań, “Lightweight Authentication Protocols for Low-Cost RFID Tags,” Proc. Second Workshop Security in Ubiquitous Computing (Ubicomp ’03), Oct. 2003.

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)