Analyses of Privacy and Vulnerability with Light-weight RFID System

인병준, 박영범, 남전우, 김정태
목원대학교

저용량 RFID 시스템에서의 보안 및 취약성 분석

Byung-Jun Ahn, Young-bum Park, Jun-woo Nam, Jung Tae Kim
Mokwon University
E-mail : jtkim5068@hotmail.com

요 약

We analysed privacy, attack model and vulnerability with light-weight RFID System. A specific system's vulnerability depends on its implementation and the applied countermeasures. We can build an RFID system with a satisfactory security level even in a high-risk application area. To do so, however, we must pay attention to the implementation of proportional security measures.

Ⅰ. Introduction

Nowadays, RFID is one of the main technologies used to build ubiquitous systems. Recently RFID technology's potential has been recognized by ubiquitous computing researchers, in implementing physical user interfaces. With the upcoming of NFC technology, which allows embedding RFID readers in commercial mobile phones, the number of RFID based systems will increase dramatically. It is possible to move the location of the data from the database to the transponder. Having these shifts in mind it becomes evident that information security gains more importance. It would be beneficial to have a generalized threat model that applies to all RFID applications. To achieve this, a common abstract model for RFID applications will be needed [1].

II. Related Work

RFID tags suffer from variety of attacks: (1) physical invasive attack, where an adversary can physically compromise the inlay of an RFID tag and read the memory for any information; (2) side channel attack, where an adversary uses timing analysis, power analysis or electromagnetic analysis to get tag information; (3) jamming attack, where an adversary blocks all RF channels between reader and tags; (4) spoofing attack, where a man-in-the-middle can impersonate a legitimate tag; (5) eavesdropping, where an attacker is able to intercept messages sent between reader and tags; (6) cloning attack, where an attacker writes the information of a compromised tag to a set of new tags [2].

III. Analysed of Security Mechanism

We analyze the protocol to evaluate whether the protocol satisfies the security

requirement, such as confidentiality, anonymity, availability, privacy, de-synchronization resistance, location privacy and forward security.

(1) Data Confidentiality and Integrity

A malicious reader can eavesdrop the communication between the tag and the reader, trying to obtain useful information. All the secret contents are hidden by the hash function in our protocol. Because of the irreversibility of the one-way hash function, attackers cannot get any information from the intercepted message. In addition, we link the tag's serial number C, which is embedded in the tag, to the authentication information to ensure the data integrity. Any modification of the information can be detected because of the collision-resistance of the hash function.

(2) Tag Anonymity

In the initial state, the tag and the back-end server share the key. It is random and anonymous in each session because it will update randomly after the protocol process is successfully completed. The tag's identification information is always hidden by the random secret key. So if the adversaries don't know the secret key, they cannot know the identification of the tag.

(3) Availability

Any RFID system can easily be disturbed by frequency jamming. But, denial-of-service attacks are also feasible on higher communication layers. The so called "RFID Blocker" exploits tag singulation (anti-collision) mechanisms to interrupt the communication of a reader with all or with specific tags.

(4) Man-in-the-middle Attack Prevention

An adversary in RFID may exploit the vulnerabilities of the wireless channel to launch man-in-the-middle (MIM) attacks. In this attack, the malicious entity intercepts the communication between an RFID tag and the reader by falsely pretending to be the authentic reader and/or the tag.

(5) Replay Attack Prevention

Since the reader challenges the tag with the random number r, the replay attack to the reader can be prevented. Thus the adversary cannot spoof the tag and pass the authentication.

(6) De-synchronization Resistance

The adversary can hamper the communication between a reader and a tag which can bring system to a mess. The de-synchronization resistant mechanism discussed previously makes the protocol meet this requirement.

(7) Location Privacy

The tag's tracking attack consists on the tracking of the behavior of the owner of a tag. A tag reader at a fixed location could track RFID-tagged products carried by people passing by. Correlating data from multiple reader locations could even track the movement. An adversary can track the tag whose response information remains invariant in all transmissions.

(8) Forward Security

It means to protect the past communications from a Tag even assuming the Tag be compromised some day.

IV. Analyses of Attacks Models

We briefly discuss about attack model to describe vulnerability.

A. A Variety of Attacks

Some well known attacks are [3]:

Physical Attacks: Some examples of physical attacks are probe attacks, material removal through shaped charges or water etching, radiation imprinting, circuit disruption, and clock glitching, among others.

Denial of Service (DoS): A common example of this type of attack in RFID

systems is the signal jamming of RF channels.

Counterfeiting: There are attacks that consist in modifying the identity of an item, generally by means of tag manipulation.

Spoofing: When an attacker is able to successfully impersonate a legitimate tag as, for example, in a man-in-the-middle attack.

Eavesdropping: In this type of attacks, unintended recipients are able to intercept and read messages.

Traffic analysis: Describes the process of intercepting and examining messages in order to extract information from patterns in communication. It can be performed even when the messages are encrypted and can not be decrypted.

B. Attack Models

we can classify attack models achieving such goals [4].

Passive Attack. It is classified into a passive attack if an adversary can just eavesdrop and collect the exchanged messages between a reader and a tag but cannot inject and modify an answer to a reader(or a tag)and have no ability to make a physical attack to a tag. For example, tracing through eavesdropping is included in this passive attack.

Active Attack. We define an active attack as injecting/modifying/blocking answer as well as eavesdropping. In this attack it is possible to impersonate a tag. Still an active attack does not include a physical access to a tag. DoS attack or spoofing attack belongs to this attack.

Tag-compromising Attack.

We define a tag-compromising attack as an attack where an adversary captures a tag and obtains a secret information in the tag. It is important that a compromised tag does not affect non-compromised tag in security point of view. It is noted that this attack includes passive and active attacks.

IV. Conclusion

Taking this RFID system model, we categorized the security threats related to this model by the means of information security. The main advantage of having a general threat model is that a systematic security analysis of RFID systems can be done and it is possible to compare the security of different RFID systems.

References

[1] Thomas Schaberreiter, "An Enumeration of RFID Related Threats", The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp.381-389, 2008.

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

[3] Li Lu, Yunhao Liu and Xiang-Yang Li, "Refresh: Weak Privacy Model for RFID Systems", IEEE INFOCOM 2010.

[4] Hwaseong Lee, etcs, "Trapdoor-based Mutual Authentication Scheme without Cryptographic Primitives in RFID Tags", Third International Workshop on Security Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2007).

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)