Chapter 9
DoS Attacks on RFID Systems: Privacy vs. Performance

Dang Nguyen Duc
Auto-ID Lab Korea, KAIST, Republic of Korea

Kwangjo Kim
Auto-ID Lab Korea, KAIST, Republic of Korea

ABSTRACT
In this chapter, the authors discuss the impact of providing tag privacy on the performance of an RFID system, in particular the complexity of identifying the tags being queried at the back-end server. A common technique to provide tag privacy is to use pseudonyms. That is, for each authentication session, a tag uses a temporary and random-looking identifier so that it is infeasible for attackers to relate two authentication sessions. A natural question which should arise here is how the server can identify a tag given that the tag’s identity is changing all the time. This problem becomes even more serious when the shared secret key between a tag and the server is updated after every authentication session to provide forward privacy. In the first part of this chapter, the authors review different techniques to deal with this problem. They then point out that most of the existing techniques lead to vulnerability of the back-end server against Denial-of-Service (DoS) attacks. They illustrate some of these attacks by describing methods which attackers can use to abuse the server’s computational resources in several popular RFID authentication protocols. Finally, the authors discuss some techniques to address the privacy vs. performance dilemma so that DoS attacks can be prevented while keeping tag identification efficient.

9.1 INTRODUCTION
RFID is an emerging technology which promises many powerful applications in supply chain management, smart home appliances and ubiquitous computing, etc. The key idea is to attach to each and every object a low-cost, wirelessly readable RFID tag (by the so-called RFID readers). Each RFID tag carries a unique string, serving as an object identifier so that this identifier can be used as a pointer to look up detailed information on the corresponding object (at some database servers or simply referred to as a back-end server where all the detailed information on tagged objects are

DOI: 10.4018/978-1-4666-3685-9.ch009
stored and managed). The identifier that a tag carries is usually called the Electronic Product Code (EPC). Unfortunately, this very core operation of an RFID tag also causes serious security concerns. These concerns are two-fold.

- **Counterfeiting product**: When RFID is widely deployed, we will come to depend on it to recognize surrounding objects, especially merchandized objects. However, the object identifier stored in an RFID tag can be read by any compatible RFID reader. In addition, wireless communication is inherently insecure against eavesdropping attacks which might help attackers capture the object identifiers without querying the tags. Malicious parties can collect legitimate tag identifiers and create tags that emit the same identifiers. We call these tags *cloned tags*. The cloned tags can be placed on counterfeiting products to avoid being detected.

- **Consumer privacy**: The uniqueness and availability of object identifiers raise another side effect for consumers, their privacy. With the vision of RFID tags being everywhere, it will become common for a person to carry with him/her several RFID-tagged objects. Therefore, a malicious hacker equipped with a compatible RFID reader, can identify objects carried by RFID holders as well as trace their movements. For the rest of this chapter, we will use consumer privacy and tag privacy as two equivalent terms.

To deal with counterfeiting products, one can implement an authentication protocol between the reader and the tag so that fake tags are detected and malicious readers cannot collect useful information from legitimate tags. This can be done easily, even on low-cost hardware like RFID tags. Many RFID authentication protocols (Ohkubo et al. (2004)) which employ just a cryptographic hash function or other lightweight cryptographic primitives have been proposed so far. However, dealing with privacy issues is much more difficult. This is not because privacy is a new problem in cryptography. Rather, it is due to the cost of providing privacy which in some cases could require the back-end server to go through the whole tag database in order to identify a single tag. A common technique for providing privacy is to use pseudonyms for RFID tags instead of their true identifiers. That is, for each authentication session, a tag uses a temporary, random-looking identifier (thus, it is called pseudonym) so that it is infeasible for attackers to relate two authentication sessions, even of the same tag. However, if a tag emits a different identifier whenever it is queried, the back-end server will have difficulty in identifying the tag. This problem becomes even more serious when forward privacy is required. Forward privacy is a security notion which specifies that the privacy of a tag is still partially preserved even if the secret key of the tag is exposed. By partially preserved, we mean that the querying sessions which happened before the secret key exposure remain anonymous (or sometimes referred to as unlinkable). In other words, the privacy of the tag is guaranteed up to the point of the secret key exposure. To provide forward privacy, a common practice is to refresh the secret key after every querying session. Unfortunately, this could add additional burdens on the back-end server when identifying and authenticating a tag because the server has to take care of situations where the secret keys shared between the server and tags were inconsistently refreshed (we refer to this problem as *de-synchronization of secret*).

In this chapter, we will demonstrate how malicious parties can exploit the privacy-performance dilemma in several privacy-preserving RFID authentication protocols to abuse the back-end...
Related Content

Review of Situational Awareness for Computer Network Defense
[www.igi-global.com/chapter/review-situational-awareness-computer-network/62372?camid=4v1a](www.igi-global.com/chapter/review-situational-awareness-computer-network/62372?camid=4v1a)

A Step-by-Step Procedural Methodology for Improving an Organization's IT Risk Management System

Spatial and Temporal Position Information Delivery to Mobile Terminals Using Audio Watermarking Techniques
[www.igi-global.com/chapter/spatial-temporal-position-information-delivery/70289?camid=4v1a](www.igi-global.com/chapter/spatial-temporal-position-information-delivery/70289?camid=4v1a)

Addressing Covert Channel Attacks in RFID-Enabled Supply Chains
[www.igi-global.com/chapter/addressing-covert-channel-attacks-rfid/75518?camid=4v1a](www.igi-global.com/chapter/addressing-covert-channel-attacks-rfid/75518?camid=4v1a)