Chapter 15
Survivability in RFID Systems

Yanjun Zuo
University of North Dakota, USA

ABSTRACT

There has been an increasing popularity of Radio Frequency Identification (RFID) techniques in various applications. A tiny RFID tag is attached to a mobile object, which can be scanned and recognized by a hand-held reader (e.g., a PDA, a mobile scanner). RFID offers opportunities for real-time item tracking, human identification, and inventory management. For applications using low-cost RFID tags and hand-held devices, however, various risks could threaten their abilities to provide essential services to users. In this chapter, survivability issues related to RFID systems are studied. For mission-critical systems empowered by the RFID technology, any interruption of essential services, even for a short period of time, is not acceptable. Hence, survivability must be provided to ensure that the critical services can be continuously delivered, despite malicious attacks and system failures. Our main contribution is a study and survey of survivability enhancing techniques in face of the special challenges that limited computational capacities, high mobility, and sensitive nature of RFID devices pose.

INTRODUCTION

Radio Frequency Identification (RFID) is a wireless technology for automatic item identification and data capture. It uses radio signals to identify a product, animal or person. Many retailers and wholesalers use RFID systems to manage product shipments and inventory tracking. Major retail chains such as Wal-Mart and Target have mandated that all suppliers introduce RFID. RFID have also been used in critical information systems in military, healthcare, and crisis management. The US Department of Defense has ordered that all shipments to its armed forces be equipped with RFID tags (Li & Ding, 2007). The UK armed forces adopted RFID in 2003 (Roberts, 2006).

There are three types of major components in a RFID system: tags, readers, and a backend server.

DOI: 10.4018/978-1-61520-761-9.ch015

A tag is physically attached to an item with a unique identification. A reader is a device that can recognize the presence of RFID tags and read the information supplied by them (Glover & Bhatt, 2006). It can be a PDA, a mobile phone or any kind of devices capable of communicating with an RFID tag. To obtain data from a tag, a reader first queries the tag and then forwards the received identity information to the backend server, which maintains a database of tag entries. After being authorized, the reader can obtain more detailed information about the tag. An RFID reader and the backend server communicate through a secure channel. Since the backend server and the readers can be secured using standard security mechanisms (e.g., public key cryptography), we assume that they are secure and trustworthy. In this chapter, we focus on the survivability enhancing techniques for low-cost RFID tags, which have limited computing and memory resources for security.

Although RFID systems provide numerous benefits for automatically identifying object items in a wide range of applications, they imply security concerns. Military RFID tags could be attacked by enemy forces. Supply chain RFID tags could be scanned by competitors for sensitive logistic information. RFID enabled passports may release personal data if not appropriately protected.

Various mechanisms have been developed to enhance the security of RFID systems. But, no guarantee can be offered for RFID security and privacy. In this chapter we address the issue of survivability for a RFID system and survey the potential survivability enhancing techniques in the literature. The objective of RFID survivability is to ensure that a RFID system provides essential services to users even in presence of malicious attacks and/or system failures. The major challenge for the survivability of an RFID system is the limited resources (e.g., memory, computing power, and area space) of RFID tags for security.

In the following discussions, we first present the background of system survivability and RFID security and privacy. Then, according to the unique features of RFID systems and the threat model, the survivability requirements for RFID systems are specified. Next, the survivability enhancing techniques in the literature are classified and discussed. Those techniques are presented from several perspectives such as preventive, protective and reactive, and recovery-oriented. Finally, future research directions on RFID survivability are discussed.

BACKGROUND

Survivability

System survivability has been studied from different application areas and based on different abilities that a critical system should have. Various definitions ([Deutsch & Millis, 1988; Ellison, *et. al.*, 1997; Knight, *et. al.*, 2003; Hiltunen, *et. al.*, 2000], to cite a few) of system survivability have been proposed and most of them share some common understandings. For instance, survivability is widely understood as a system property, relating the level of services provided to the level of damage present in the system and operating environment; a survivable system must support the system's mission; operating in a hostile environment, a survivable system may offer degraded (but acceptable to users) services to users and have the ability to recover when the environment improves. Tarvainen (2004) identify a set of key properties that a survivable system should have: (1) a survivable system delivers essential services and maintains essential properties of those essential services, e.g., specified levels of integrity, confidentiality, performance and availability; (2) requirements of survivability are often expressed in terms of maintaining a balance among multiple attributes such as security, reliability, and modifiability; and (3) it is crucial to identify the essential services, and the essential properties that support them, within an operational environment.

Survivability requirements can vary substantially depending on the scope of the system, the functionalities of the system, operating envi-