Chapter 1
Computer System Attacks

Zhang Ning
XiDian University, People's Republic of China

ABSTRACT

The study of computer system attacks is an important part RFID security and privacy. This chapter provides a general overview of computer system attacks organized by target. Attacks on EPC entities - tags, readers, middleware, and back-end systems - are categorized and discussed, as well as wired link attacks. Countermeasures to the attacks are summarized and evaluated based on the discussion. The Denial of Services (DoS) attack is highlighted in the discussion.

INTRODUCTION

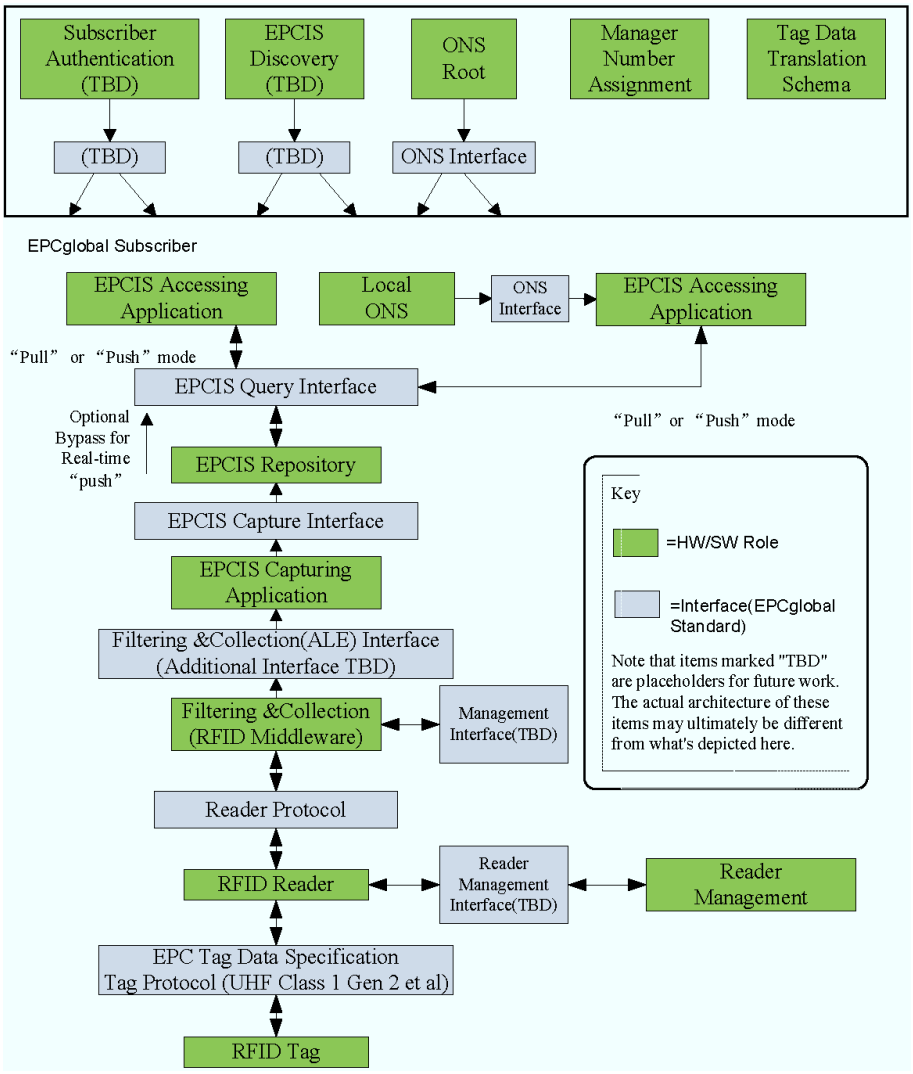
Security and privacy in RFID systems is a topic that deserves careful consideration. In this chapter, attacks can be various, especially, since RFID systems have a computer-driven back-end. Different sorts of computer system attacks are presented within the scope of RFID.

Throughout this chapter we will be considering the EPC Global network. EPC Global is an organization set up to achieve worldwide adoption and standardization of Electronic Product Code (EPC) technology. The main focus of the group is currently to create both a worldwide standard for RFID and the use of the internet to share data via the EPC Global Network.

According to the EPC Global framework, as in Figure 1, an RFID system consists of tags, readers, middleware and back-end. Any of these four entities or the communication paths between them can be the target of an attacker. We will do a comprehensive analysis of the computer system attacks on each entity and the wired link between middleware and the back-end. EPC Global network, by design, is also susceptible to DoS attacks. Our objective is to provide a reference for readers that acquaint them with computer system attacks on RFID systems.

DOI: 10.4018/978-1-4666-4707-7.ch001

Figure 1. The EPC global framework (Traub et al (2010))



ATTACKS ON TAGS

With wider usage of RFID, for instance, in many countries, new passports contain an RFID tag with an encrypted form of the data that is written in clear text on the passport, tag data security becomes our first consideration for security purposes. Generally, low-cost RFID tags (such as EPC Class-1 Generation-2 tags) have very limited resources, and may, therefore, not be able to support sophisticated security procedures based on encryption. This problem is exacerbated by the constant pressure from industry to develop ever cheaper tags. Surprisingly, these limitations may actually be an advantage to the security architect. Thus in RFID deployment, the most effective attacks are those on the tags and the ones resulting from the communications channel between tags and readers (wireless link attacks). We will discuss attacks on tag data in this section.