Chapter 3
Security Issues for ISO 18000-6 Type C RFID: Identification and Solutions

Peter J. Hawrylak
The University of Tulsa, USA

John Hale
The University of Tulsa, USA

Mauricio Papa
The University of Tulsa, USA

ABSTRACT

Radio frequency identification (RFID) devices have matured to the point where they are now expanding beyond the retail supply chain and public transit fare management systems. RFID technology provides a low power and economical method to link remote sensors to larger control systems. In these cases, the RFID protocols provide the communication link between the sensor and larger control system. Security solutions designed for the retail and transit fare management systems are not sufficient for these new control systems. New avenues of attack are available, and attackers have different goals. Therefore, the security of these RFID protocols must be re-examined in order to identify those vulnerabilities that are not significant in the retail or fare applications, but could be exploited in these new settings. This chapter analyzes the ISO 18000-6 Type C protocol to identify potential security vulnerabilities. This protocol is one of the major RFID protocols for passive RFID systems.

INTRODUCTION

Radio frequency identification (RFID) devices are becoming pervasive in our world and play a key role in the deployment of the Internet of Things (IoT). This chapter focuses on security issues of the ISO 18000-6 Type C (International Organization for Standardization, 2010) protocol stack, which is based on the EPCglobal Gen-2 protocol (EPCglobal, 2008). This protocol stack is becoming particularly relevant in distributed process control systems, also known as SCADA (Supervisory Control and Data Acquisition)

DOI: 10.4018/978-1-4666-1797-1.ch003

systems. In particular, the ISO 18000-6 Type C protocol supports the use of sensors in SCADA systems used in the operation of various critical infrastructures such as the oil & gas industry and the electric power sector.

This chapter presents a brief introduction to RFID architectures and an overview of the ISO 18000-6 Type C protocol. Next, threats to RFID systems are described and analyzed in the context of the protocol stack, the messaging structure, and the state transitions of RFID network nodes. This analysis provides the basis to present interruption, modification, and fabrication attacks on such systems. In particular, a series of scenarios are presented to illustrate the relevance of security issues identified in this chapter. Possible solution paths and mitigation strategies for these issues are presented to help system users and designers mitigate the negative effects that these attacks may have. The chapter concludes with a section highlighting the security challenges facing RFID and the necessary areas of research to overcome these issues.

RFID BACKGROUND

RFID provides a means to remotely identify and monitor assets. Initially used for monitoring retail inventories, supply chain management, automatic toll collection (e.g. EZ-Pass), and keyless entry systems, RFID is now being coupled with sensors to monitor the asset's condition (Todd, Phillips, Schultz, Hawkins & Jensen, 2009; Law, Bermak & Luong, 2010). The attachment of sensors increases the value and applicability of the information provided by the tag. Wireless sensors offer many advantages for monitoring conditions in hard to access places and machinery because wiring is minimal and minimal infrastructure is required for wireless sensor systems. As a result, RFID systems are being investigated for use as the communication medium for edge devices to sense conditions for critical infrastructures such as the Smart Grid (next generation power grid). This increase makes RFID systems a target for or a tool in the use of a malicious cyber-attack. Thus, the security of the communication protocols employed to connect RFID devices together must be investigated.

RFID systems are comprised of four major components: RFID tags, RFID readers, RFID middleware, and backend software. The backend software controls the overall system and provides the repository of information for the tags. An enterprise resource planning (ERP) software package is one example of backend software. The RFID middleware sits between the backend software and RFID reader. Sometimes the RFID middleware is contained within the RFID reader itself. The RFID middleware provides the functionality of a device driver to link the RFID reader to the network and ultimately to the backend software, and filters or prunes the information sent to the backend software. This helps to reduce the amount of data transmitted over the network. The RFID reader is the edge device providing the last mile network connection between itself and the RFID tag. RFID tags are attached to the asset. RFID tags contain a unique identification number and possibly some additional memory that may read only or read-writable. Some RFID tags, termed a *license plate tag*, contain only the unique identifier that is used to access a record in a database maintained by the backend software. More advanced tags offer additional memory that can store or record additional information, such as expiration date or to track information over the asset's lifetime.

One general classification for RFID tags is based on how they are powered. There are three types of tags using this classification: passive, battery-assisted passive (BAP), and active. Passive tags have no on-board battery and must harvest their operating energy from the environment. A group of passive tags are shown in Figure 1.

The most common method is to harvest energy from the RFID reader's RF transmission. Other energy harvesting methods include thermal,