Chapter 58
Malware Protection on RFID-Enabled Supply Chain Management Systems in the EPCglobal Network

Qiang Yan
Singapore Management University, Singapore

Yingjiu Li
Singapore Management University, Singapore

Robert H. Deng
Singapore Management University, Singapore

ABSTRACT

As RFID-enabled technology is becoming pervasive in enterprise systems and human life, it triggers significant concerns over the malware that can infect, damage, and even destroy RFID-enabled network systems. RFID malware can spread malicious codes or data quickly to a large number of RFID systems via RFID read and write, which are pervasive operations on RFID tags that are transported from one RFID system to another. To address this concern, this chapter uses RFID-enabled supply chain management systems in the EPCglobal network as a case study to demonstrate the important issues in RFID malware protection. This case study shows that although there are fundamental difficulties in preventing RFID malware from entering the systems, the behaviors of RFID malware resemble traditional malware after it enters the systems. Based on this characteristic, the security threats of RFID malware can be effectively controlled.

INTRODUCTION

RFID is an automated data collection technology that uses radio frequency waves to transfer data between a reader and an RFID tag to identify, track or locate the physical item to which the tag is attached. Since RFID technology improves the automation processes significantly, it works its way into many enterprise systems like supply chain management systems. The market value of RFID technology keeps growing even under the current global financial crisis. According to a market report from IDTechEx (Das & Harrop (2009)), the value of the entire RFID market was $5.56

DOI: 10.4018/978-1-4666-4707-7.ch058

billion in 2009, up from $5.25 billion in 2008; by 2019, the market value of RFID technology is predicted to grow over five times to exceed $27 billion, and the number of RFID tags sold yearly will increase over ten times to exceed 100 billion. If we further consider the trends of integrating RFID systems over the Internet ("The Internet of Things"), the future large-scale deployments of RFID-enabled network systems are very likely to become attractive targets for malware developers.

As an emerging threat to high value RFID applications, RFID malware got the attention of the industry and the public after the first proof-of-concept RFID malware was reported in 2006 (Rieback, Crispo & Tanenbaum (2006)). It was classified as a long-term threat in the latest IT security threat report from Gartner (Pescatore, Young, Allan, Girard, Feiman & MacDonald (2008)). Compared to other long-term threats, the RFID attack was placed at the earliest position, which means that the threats of RFID attacks were the most imminent. Gartner further identified the biggest risk associated with RFID applications as:

RFID systems, especially readers, were developed without security in mind(Pescatore, Young, Allan, Girard, Feiman & MacDonald (2008), p. 20)

Hence, reading RFID data from ubiquitous acquisition points without proper security protection will incur high risks and pose serious threats to enterprise IT security. In addition, as RFID readers are integrated into personal devices such as PDAs or mobile phones, and more RFID applications are developed on these devices, RFID malware will eventually penetrate into our daily lives.

These potential threats have motivated us to provide a comprehensive investigation of RFID malware protection. We use RFID-enabled supply chain management systems in the EPCglobal network as a case study. This kind of systems is one of the most important enterprise applications of RFID technology. RFID technology has been widely envisioned to have significant impact on modern supply chain management as an inevitable replacement of barcodes in the near future. EPCglobal network[1], the de-facto industry standard for RFID-based trading systems, further integrates RFID technology with Internet and networking technology, to enable contactless information collection, integration, sharing and querying in real time over the Internet.

To demonstrate the important issues on RFID malware protection for RFID-enabled supply chain management systems, we describe and analyze a demo security system, RFscreen. It is designed to detect and filter out generic RFID malware by protecting critical points on each layer of an RFID-enabled supply chain management system. Our analysis on RFscreen shows that there are fundamental difficulties in preventing RFID malware from entering the systems. But after it enters the systems, it behaves similarly to traditional malware whose threats can be effectively detected and prevented.

This chapter aims to provide the necessary background and a comprehensive analysis of RFID malware for RFID-enabled supply chain management systems. The background section describes the EPCglobal network architecture, the capabilities of current RFID infrastructure, and the basic characteristics of RFID malware. The remainder of this chapter is devoted to the analysis of the potential security threats of RFID malware and the design of corresponding countermeasures.

BACKGROUND

This section first introduces the background knowledge of RFID-enabled supply chain management systems specified by the EPCglobal network. After that, we describe the basic characteristics of RFID malware.