Chapter 4

A Security Framework for Networked RFID

Harinda Sahadeva Fernando
Deakin University, Australia

Jemal Abawajy
Deakin University, Australia

ABSTRACT

In the last decade RFID technology has become a major contender for managing large scale logistics operations and generating and distributing the massive amount of data involved in such operations. One of the main obstacles to the widespread deployment and adoption of RFID systems is the security issues inherent in them. This is compounded by a noticeable lack of literature on how to identify the vulnerabilities of a RFID system and then effectively identify and develop counter measures to combat the threats posed by those vulnerabilities. In this chapter, the authors develop a conceptual framework for analysing the threats, attacks, and security requirements pertaining to networked RFID systems. The vulnerabilities of, and the threats to, the system are identified using the threat model. The security framework itself consists of two main concepts: (1) the attack model, which identifies and classifies the possible attacks, and (2) the system model, which identifies the security requirements. The framework gives readers a method with which to analyse the threats any given system faces. Those threats can then be used to identify the attacks possible on that system and get a better understanding of those attacks. It also allows the reader to easily identify all the security requirements of that system and identify how those requirements can be met.
Radio Frequency Identification (RFID) is an automatic identification technology that is based on a contact-less, proximity based communication method (radio waves). The potential applications of RFID systems are diverse and RFID networks already exist in a large range of environments and applications. The proliferation of RFID networks has been rapid in the last decade (Schuster, et al., 2007). One specific area in which the use of RFID technology has become increasingly popular is in massively networked logistics applications such as global supply-chain management systems. The use of RFID tags instead of barcodes allow for the automated identification and tracking of the tagged objects. In addition RFID systems can generate a vast amount of transactional data concerning the tagged objects that can then be shared in real time with the other partners of the system. But, as with all technologies there are a number of issues that prevent its widespread adoption. In RFID the main current barrier to adoption is the large number of security concerns about networked RFID systems and the additional performance overhead placed on the system when generating and sharing such a vast quantity of data.

Networked RFID systems are a relatively complex type of RFID system. This complexity arises from some of its features such as wireless communication, mobile data containers (RFID tags), highly distributed nature and the presence of multiple independent entities that are authorized to access the system. Due to its wireless communication method and distributed nature networked RFID systems are vulnerable to a great number of malicious attacks at the edge of the system (tags, readers and wireless communications). These attacks can range from simple ones such as passive jamming and eavesdropping to more sophisticated attacks such as physical cloning of tags, man in the middle attacks and even RFID malware (Karygicmnis, et al., 2006). In RFID systems these threats can be mounted either through physical or logical access to system components. In addition, networked RFID systems can be attacked by internal partners as well as external attackers. Therefore the security threats and attacks that are faced by RFID networks are both numerous and extremely diverse. To successfully manage and eliminate all these different types of threats a large number of security requirements must be implemented.

Due to the large number and different types of attacks and threats facing a RFID system, fully securing it is a very complex task. This task is made even more difficult by the number of different components that must be protected and the large number of security concepts that must be upheld. Currently one of the biggest barriers to the widespread adoption of networked RFID systems is the unresolved security issues inherent in them (Juels, 2006). Without a proper security framework to reference most companies have no method with which to reliably access the vulnerabilities of their system. Nor do they have a method with which to decide how best they can remove those vulnerabilities and fully secure their RFID systems. Due to this fear over RFID system security most companies are still reluctant to implement RFID based solutions even though the benefits they pose are great. Therefore the need for a RFID security framework that will allow developers to successfully identify, manage and secure against the threats and attacks faced by RFID systems is currently very acute. But if such a framework is to be successfully developed a few challenges must first be overcome. Networked RFID systems, while seemingly similar to normal networked systems, differ quite significantly from them. Therefore the most important challenge is analysing how the security requirements of networked RFID differ from the security requirements of typical networked systems.

There is a currently number of security frameworks that are available in literature. But a majority of the current existing security frameworks are aimed at general networked systems (Jeong &
Related Content

Security Issues and Challenges Related to Big Data
www.igi-global.com/chapter/security-issues-and-challenges-related-to-big-data/196041?camid=4v1a

Mobile World Wide Web Content
Wen-Chen Hu (2009). Internet-Enabled Handheld Devices, Computing, and Programming: Mobile Commerce and Personal Data Applications (pp. 139-161).
www.igi-global.com/chapter/mobile-world-wide-web-content/24701?camid=4v1a

OODM: An Object-Oriented Design Methodology for Development of Web Applications
www.igi-global.com/chapter/oodm-object-oriented-design-methodology/22974?camid=4v1a

Mobility Protocols
www.igi-global.com/chapter/mobility-protocols/16867?camid=4v1a