Chapter 7.2
Privacy Issues of Applying RFID in Retail Industry

Haifei Li
Union University, USA

Patrick C. K. Hung
University of Ontario Institute of Technology, Canada

Jia Zhang
Northern Illinois University, USA1

David Ahn
Nyack College, USA

EXECUTIVE SUMMARY

Retail industry poses typical enterprise computing challenges, since a retailer normally deals with multiple parties that belong to different organizations (i.e., suppliers, manufacturers, distributors, end consumers). Capable of enabling retailers to effectively and efficiently manage merchandise transferring among various parties, Radio Frequency Identification (RFID) is an emerging technology that potentially could revolutionize the way retailers do business. With the dramatic price drop of RFID tags, it is possible that RFID could be applied to each item sold by a retailer. However, RFID technology poses critical privacy challenges. If not properly used, the data stored in RFID could be abused and, thus, cause privacy concerns for end consumers. In this article, we first analyze the potential privacy issue of RFID utilization. Then we propose a privacy authorization model that aims to precisely define comprehensive RFID privacy policies. Extended from the role-based access control model, our privacy authorization model ensures the special needs of RFID-related privacy protection. These policies are designed from the perspective of end

consumers, whose privacy rights potentially could be violated. Finally, we explore the feasibility of applying Enterprise Privacy Authorization Language (EPAL) as the vehicle for specifying RFID-related privacy rules.

INTRODUCTION

In present retail industry, retailers are under tremendous pressure to improve efficiency. One way to increase productivity is through the adoption of new technologies. History has revealed that retailers are the early adopters of Electronic Data Interchange (EDI) and Business-to-Business (B2B) e-commerce. The benefits of adopting these new technologies are obvious: reduced time to market and reduced cost associated with office and manufacturing floor automation. In recent years, Radio Frequency Identification (RFID) has caught significant attention in the retail industry. RFID is a generic term for the technologies that use radio waves to automatically identify individual items wirelessly. RFID is capable of enabling retailers to effectively and efficiently track the entire circulation process of items from suppliers to end users. It can provide identify, orientate, and trace objects directly and continuously. In addition, RFID is able to deliver information at real time. As a result, RFID is considered an emerging technology that potentially could revolutionize the way retailers do business. Among other examples, Wal-Mart mandated its top 100 suppliers to use RFID by January 2005 (Vijayan & Brewin, 2003); the U.S. Department of Defense also made a similar request to its military suppliers (U.S. Department of Defense, 2003).

Although it seems like RFID is a boon to e-commerce, the actual adoption of RFID in retail industry is quite slow (Bradner, 2005). Retail industry poses typical enterprise computing (Neogi & Ghosal, 2004) challenges, as a retailer normally deals with multiple parties belonging to different organizations (i.e., suppliers, manufacturers, distributors, end consumers). Nowadays, the focus of enterprise computing efforts of retailers mainly aims at suppliers. To date, there has been little work conducted on how to provide enterprise-level computing capability for individual customers. In addition to the security issue, one such capability we have identified is consumer privacy protection. There is a growing concern for data privacy among businesses and consumers due to the possible unwanted revelation of confidential or personal data stored within RFID devices.

Privacy is a state or condition of limited access to a person (Schoeman, 1984). In particular, information privacy refers to an individual's right to determine how, when, and to what extent personal information will be released to people or to organizations (Westin, 1967). To date, information privacy mainly aims to ensure the confidentiality of sensitive information. In other words, one major objective of enforcing privacy is to protect personally identifiable information (PII). Many authorization technologies can be applied to protect PII. However, information privacy contains other privacy concepts, such as purpose and obligation (Fischer-Hubner, 2001). In more detail, authorization focuses on preventing unauthorized users from accessing sensitive information, while privacy focuses on managing authorized users to use information effectively and to achieve an organization's strategy within necessary constraints (Bucker et al., 2003).

In addition, privacy control does not focus on individual subjects. A subject releases his or her data to the custody of an enterprise with an agreement to the set of purposes for which the data may be used. In the U.S., the Privacy Act of 1974 requires that federal agencies grant individuals access to their identifiable records that are maintained by the agency, ensure the accuracy and timeliness of existing information, and limit the collection of unnecessary information and the disclosure of identifiable information to third