Chapter 3.14
RFID Systems:
Applications vs. Security and Privacy Implications

Dennis M. L. Wong
Swinburne University of Technology, Malaysia

Raphael C.-W. Phan
Swinburne University of Technology, Malaysia

ABSTRACT

In this chapter, we discuss the business implications, as well as security and privacy issues, of the widespread deployment of radio frequency identification (RFID) systems. We first describe, in more detail, the components that make up an RFID system to facilitate better understanding of the implications of each, and then review the commercial applications of the RFID. We then discuss the security and privacy issues for RFID systems and what mechanisms have been proposed to safeguard these. The topics discussed in this chapter highlight the benefits of using RFIDs for user convenience in ubiquitous and pervasive commercial services and e-businesses, while maintaining the integrity of such systems against malicious attacks on the users' security and privacy. This is vital for a business establishment to coexist with peers and remain competitively attractive to customers.

INTRODUCTION

Radio frequency identification (RFID) systems are gaining worldwide popularity for supply-chain management and tracking of goods, as well as for access control in distributed systems, toll systems, car immobilizations, and so forth. There are ongoing research and development (R&D) efforts everywhere in integrating RFID into available technology sectors, including e-business. Some have envisioned that RFID technology will revolutionize the world that we see today, bringing pervasive and ubiquitous systems to the forefront of everyday applications (Stanford, 2003).

Cryptologists and security researchers are also predicting the explosive growth of RFID technology. For instance, Adi Shamir, coinventor of the popular RSA encryption method (Anderson, 2001; Menezes, van Oorschot, & Vanstone, 1996; Stallings, 1999;) commented on the vast potential of RFIDs during his invited talk (Shamir, 2004) at the Asiacrypt 2004 conference attended by security researchers around the world.

With the soon to be widespread use of RFID systems, and their seamless integration into our daily chores, comes the issue of security and privacy. As with other personal data related applications, for example, Smart-Card, Web-based Transaction, and so forth, there are doubts on exactly how safe is an RFID system, from the aspect of information security? To what degree can one entrust his/her personal data, ranging from biodata to financial information, with RFID-based systems? The contactless nature of RFIDs, which is the main advantage of the technology, incidentally, is also the largest vulnerability, where much like the wi-fi technologies, there is no guarantee that the transmission medium cannot be eavesdropped upon.

The idea of automatic identification has been long established in the commercial sector, and the usage of bar-code scanning in the point-of-sale system is probably the most successful example one can openly observe. Consider this scenario: You have decided to purchase some groceries, so you gather them and bring them, in a basket, to the checkout point. The cashier scans through the goods using, probably, an infrared scanner; the price is then automatically displayed in the cash machine. Now, imagine a different scenario: you are carrying a basket with a tiny LCD display; once you put an item into the basket, the LCD screen immediately shows you the price of the item and perhaps a subtotal of your purchase. Once you arrive at the station, you are readily presented with an invoice, where you just need to acknowledge the transaction (say signing), and the bill will be automatically debited from your local bank account. The above scenario might be coming to a local retail branch near you, and the enabling technology behind this vision is the emerging RFID technology.

However, RFID technology is not new, and it has been in existence for decades. Its profile has been raised several folds recently, and there are several factors that account for this change, among which, a major reason is the successful deployment of RFID technology in the commercial sector. In supply-chain management, RFID tags have been envisioned by many to replace the bar-code labeling system, which has been in use since the early 1970s, as the new tool for automatic identification. The latter system is now becoming a bottleneck for big enterprises that have gigantic volumes of transactions. The fact that RFID is contactless enables the technology to be used in a ubiquitous and pervasive environment.

Incidentally, the U.S. Department of Defence (DoD) and Wal-Mart, a key retail giant in the U.S., have recently (ZIH, 2005) required all suppliers to be compliant with RFID technology by January 2005. Other major retail chains, for example, Target and Albertsons, have also mandated the same move. Such requirements imply that if the suppliers are not "RFID compatible," then they will not be getting any contracts from these retailers. Besides the retail sector, local governments have also been playing a key role in the deployment of RFID technologies. In Malaysia, the Malaysian citizens have been using RFID-based technology in their e-passports (Juels, Molnar, & Wagner, 2005) since the end of last century. Although unaware by many, the e-passport contains an identification chip that enables Malaysians to gain easy and quick access at Immigration Control points. In the U.S., the Defense Department is using RFID to administer their military shipments. For local authorities, libraries around the world are also deploying RFID in monitoring the transactions of their collections. Library users would not have to worry about library operation hours: as long as they drop the loaned items in