Chapter 7.3
An Evaluation of the RFID Security Benefits of the APF System:
Hospital Patient Data Protection

John Ayoade
American University of Nigeria, Nigeria

Judith Symonds
Auckland University of Technology, New Zealand

ABSTRACT

The main features of RFID are the ability to identify objects without a line of sight between reader and tag, read/write capability and ability of readers to read many tags at the same time. The read/write capability allows information to be stored in the tags embedded in the objects as it travels through a system. Some applications require information to be stored in the tag and be retrieved by the readers. This paper discusses the security and privacy challenges involve in such applications and how the proposed and implemented prototype system Authentication Processing Framework (APF) would be a solution to protect hospital patient data. The deployment of the APF provides mutual authentication for both tags and readers and the mutual authentication process in the APF provides security for the information stored in the tags. A prototype solution for hospital patient data protection for information stored on RFID bracelets is offered.

INTRODUCTION

Radio Frequency Identification (RFID) refers to an Auto-Identification system comprised of RFID tags, RFID readers and the requisite RFID middleware that interprets tag information and communicates it to the application software. RFID tags contain specific object information in their memory, accessed via radio signal of an RFID reader. RFID tags contain a microchip capable of holding stored information, plus a small coiled antenna or transponder (Psion, 2004).

In the APF (Authentication Processing Framework) implementation (Ayoade 2005) an Omron's RFID tag "V720S-D13P01" was used. It is a passive tag that has read and write tag memory capability. The memory capacity of this tag is 112 bytes (user area). This means it has EEPROM/RAM memory capability. The reader used was manufactured by FEIG electronic (ID ISC MR 100). It has a frequency of 13.56 MHZ. This type of RFID system was used because its frequency has the widest application scope and it is the most widely available high frequency tag world-wide. Its typical read range is approximately 1m.

APF is a system that could allow many readers to read from and write to the RFID tags and it prevents unauthorized readers from reading information from the tags without the knowledge of the tags.

In a nutshell, APF prevents privacy violation of information in the RFID system. The APF system was developed based on the existing typical RFID system and will therefore work with the existing system.

In the RFID system, many proposals have been presented to solve common privacy and security problems, however, these proposals face one disadvantage or another, making them insufficient to completely address the problems in question. We agreed that a simple approach for dealing with the problem of privacy is to prevent readers from receiving data coming from tags (Avoine, 2004). However, as mentioned earlier, all the propositions to date have one disadvantage or another.

RFID technology can be used to collect a lot of data related to persons, objects or animals, thus there are data protection concerns. The first type of risks arises when the deployment of RFID is used to collect information that is directly or indirectly linked to personal data. In a digital world, collecting and analyzing personal data is a task that computers and agents can do diligently. This is an issue connected to ICT in general, rather than to RFID specifically. It is mainly the widespread use of RFID, and its use in mobile situations accompanying persons that could lead to unpredictable situations – and thus unpredictable threats (ECISM 2006).

A second type of privacy implication arises where personal data is stored in RFID tags. Examples of this type of use can be found in passports or RFID-based health records. The relative openness of the area where the application is deployed will greatly influence the options to illicitly access the data (ECISM 2006).

A third type of data protection implication arises from uses of RFID technology which entail individual tracking. As soon as a RFID-profile is known (because the tags are linked to personal data) the comings and goings of people could be followed. This is possible for company-level applications (e.g. by using access cards), but could theoretically also be used in tracking where you are. This could be in your car (if the car or clothes are tagged, as also indicated in the example), or in person, in public locations (ECISM, 2006). This could have implications for people who could come to harm if their health records were to be accessed such as in the case of HIV/AIDS, mental illness, past medical history or even pregnancy.

THE PROPOSED CONCEPT OF THE AUTHENTICATION PROCESSING FRAMEWORK

A framework that will authenticate readers before they can access the information stored in tags was proposed in (Ayoade, 2004). The proposed procedure is called Authentication Processing Framework - APF. The main concept of this framework is that tags and readers will register with the APF database which will authenticate readers prior to reading data stored on RFID tag. Implementing this kind of framework in the RFID system will alleviate security and privacy concerns.