Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp69-74)

RFID Security and Privacy Concerns

S. Srinivasan[†], Akshai Aggarwal[*], Anup Kumar[†]
Computer Information Systems, Computer Science, Computer Engineering
[†]University of Louisville, Louisville, Kentucky, USA
[*]University of Windsor, Windsor, Ontario, CANADA
srini@louisville.edu, akshaia@uwindsor.ca, ak@louisville.edu

Abstract: - Radio Frequency Identification (RFID) technology is emerging as an important tool with applications in a variety of fields. The major concern regarding RFID is the ubiquitous nature of its deployment that extends far beyond the capabilities of any of the tools available today for monitoring any item without an RFID tag. Many of the applications envisioned have a legitimate use. However, this technology provides room for abuse of people's privacy. Moreover, since the communication between a RFID tag and its reader takes place in a wireless manner, issues concerning security of such a communication are also important. In this paper we briefly discuss RFID technology and its many positive uses; then we discuss the privacy concerns posed and the security considerations needed to alleviate doubts about the fair use of this technology. We have also specified additional security features that may be required to be incorporated in the tags and the associated readers so that privacy concerns can be addressed

Key-Words: - RFID, security and privacy, RFID tags, RFID transponders, RFID receivers, wireless monitoring

1 Introduction

Radio Frequency Identification (RFID) technology has been in existence for at least 60 years now. But until recently it has not been brought to wide-spread commercial use. The earliest use of RFID technology was during World War II when RFID tags were attached to aircrafts. RFID tags are slowly evolving as an alternative to the bar codes. Bar codes contain manufacturer-specific information rather than product-specific information. For example, a bar code on a Hershey's KitKat identifies the product with an ID unique to Hershey's. On the other hand, an RFID tag on a KitKat bar could contain not only the data about Hershey's but also the date of manufacture, the location where it was manufactured and who shipped it. Bar codes usually require human intervention in the form of scanning products with bar codes. An RFID is capable of being read in an automated manner. For example, in a supermarket warehouse, readers can be placed that can be activated remotely for scanning specific products such as toothpaste. This helps ensure that the product is not just in stock but in the place where it is supposed to be. This way the RFID tag helps monitor inventory effectively. Since in the case of bar codes, such information is not available, the inventory level is updated based on point-of-sale data. Unlike bar code readers, an RFID reader does not require a clear line of sight to the object that contains the RFID tag.

Businesses have relied on bar codes for a long time in order to keep track of inventory. The ever increasing commerce via the Internet demands more information to be made available on the Internet about the products and their shipping. In order to provide timely information, businesses are eager to have as much data as possible on the products and their availability in areas where they are most needed. RFID tags are capable of holding more information than a standard bar code and thus are capable of meeting this challenge effectively [4]. The U.S. Department of Defense, the world's largest retailer Wal-Mart and Procter and Gamble have announced plans for extensive use of RFID. Our goal in this paper is to address the capabilities of this technology and see how it would impact the communication security and people's privacy. The pertinent issues of RFID technology, which are required to be understood for addressing the privacy concerns, are stated in section 2. Section 3 gives the benefits of the RFID technology and the likely application areas. This helps one put the methods used for addressing privacy concerns in perspective. Section 4 specifies the privacy concerns and the methods used to ensure that privacy and confidentiality of data can be ensured. In section 5, we give the conclusions of the study and the future directions of our work.

2 RFID Technology

An RFID system consists of a transponder, a reader and an antenna. The transponder (transmitter – responder) device is commonly called the tag. The RFID reader is a transceiver (transmitter – receiver) that has the ability to transmit and receive radio signals over the air. RFID tags come in three different forms: active, passive, and semi-passive. The most common form of RFID tag is passive. Passive tags do not have an embedded power source and they hold up to two kilobits of data. Semi-passive and active tags could hold as much as 32 kilo bits of data. Semi-passive and active tags both have a power source in the form of a battery. The battery source in a semi-passive tag powers the circuitry when a reader interrogates the tag whereas in active tags, the battery source transmits data when interrogated. Active tags have the ability to automatically broadcast data such as GPS coordinates. Since active tags require battery power to broadcast its data, they have limited life. Majority of the tags are 'read only' tags. But the active tags could be 'read or write' tags. A typical RFID system is shown in Fig 1.

Every RFID transponder tag has a unique identifier. Both the passive and semi-passive tags respond to RF signals that come from a reader. The data stored in the tag is sent back to the reader in response to the RF signal. This method requires the reader to be within a short range of the tag. A single RF signal could elicit responses from multiple tags simultaneously. For example, a scan of the cargo bay of an aircraft full of RFID-tagged luggage would result in many of the tags sending their data back to the reader. An RFID reader is capable of processing hundreds of responses per second [20]. An active RFID tag is designed to send out data periodically to any readers that are within its range. An active tag has the ability to receive certain forms of information such as the GPS coordinates of its current location and broadcast the same to the readers. Clearly such a tag would help law enforcement keep track of potential terrorists.

The RFID tags as a stand alone entity may not be of such a great use and may not violate privacy laws. However, when combined with other forms of data such as the point-of-sale data including the method of payment or the data from a loyalty card could identify the person who holds a product containing a RFID tag. RFID tags use various frequencies to communicate their data. Table 1 illustrates the common frequencies in use for RFID and additional related data such as storage capacity and distance to a RFID reader [6]. Of these frequencies, the 915 MHz frequency band used in U.S. allows for the use of anti-collision algorithms to be used when multiple tags are involved [2].

Low-frequency RFID tags are the most commonly debated tags at this time. They use less power and consequently have shorter ranges. The reader signals in this case would be able to penetrate non-metallic objects such as packaging for a cloth. The higher frequencies are useful to scan objects at a distance. They are primarily used in air-to-air or air-to-ground communications [5]. At this time the active tags are primarily used by the U.S. Department of Defense and Wal-Mart.

Even though there is no universal standard at this time for RFID tags, an industry-driven standard called the Electronic Product Code (EPC) is being developed by EPCglobal [12]. EPC has at most 96 bits in length. The EPC standard calls for each tag to contain a header, a management number, an object class and a serial number. It is to be noted that at this time there are many tags that use proprietary technology and as such are not cross-functional with multiple readers. One of the organizations that is taking a leading role in standards is Alien Technology [19].

3 Benefits of RFID

RFID clearly has numerous benefits to offer the businesses and consumers. The major benefit for businesses is in the ability to efficiently manage inventory and thus reduce cost of goods sold. Wal-Mart introduced passive RFID tags in April 2004 to track pallets. When this method of tagging is extended to cartons in a pallet and to individual goods, the retailer is able to monitor the inventory more effectively. Such tags are especially useful in handling perishable products where a sell-by date could be effectively controlled and monitored. From a customer perspective, the embedded tag can help in receipt-free sales and returns as well as protect the customer from post-sale theft [5].

RFIDs are in use already in various forms. The most common of these applications is the automobile toll responders. These are usually of the semi-passive category of RFID tags. Another application is in the RFID-tagged automobile ignition keys as a theft deterrent [20]. A new application that is emerging in U.S. is called SpeedPass, that is used to refill gasoline in automobiles. Recently American Express has introduced a RFID-based ExpressPay system. MasterCard has introduced a similar system called PayPass. Both these systems are designed to help the consumers move through the retail shops faster and keep track of the card activities online. Another major application evolving in various countries is the E-passport, where an RFID tag is embedded in the passport. Sweden has already implemented this [7].

One of the common problems that many pet owners face is the disappearance of their pet. RFID tags have been implanted in over fifty million pets so that the lost pet could be returned to the owner. Use of RFID tags in smart appliances could help monitor the food quality as well as inventory in a refrigerator and control the wash setting in a washing machine, based on the types of clothes being washed. Likewise, shoppers in a supermarket need not wait in line at the check out counter. As items are placed or removed from the shopping cart, strategically located readers would monitor the products and tally the total and charge the customer's RFID-enabled charge card. This application has been tested by NCR Corporation. But the process needs refinement as, in some tests, products in nearby carts were billed to the wrong customer.

A major benefit of RFID tags is in the medical field where a large number of specialized activities are required to be monitored carefully for each patient. This scenario would also apply to people who need help with ordering and dispensing of medicine. Research work at Intel and the University of Washington in this area has considered the impact of RFID tags in medication compliance and the correlation of information from multiple tags [21]. Another area that has benefited most from RFID technology is supply chain management. In supply chain, the tags could be placed in enclosed tamper resistant units. This added feature provides convenience for tracking the item as well as security from cloning [10].

4 Privacy Concerns

RFID technology has the potential to uniquely identify the user by using a multitude of data associations. In the evolving ubiquitous computing environment, RFID joins Wi-Fi and Bluetooth technologies to form the core of "intelligence infrastructure" [22]. Electronic Privacy Information Center is helping in this regard by educating the consumers, the policy makers and infrastructure designers [8]. The major privacy concerns stem from the fact that when individual goods are tagged, the manufacturers, retailers, and marketers will be able to track the goods beyond the point-of-sale because they have associated data. Moreover, others with ulterior motives would be able to use readers and see who has what product. At present, with bar codes, a third party would not be able to gather any such data using a mere scanner. For example, a simple presence of an RFID tag in clothing could be used by an employer to capture data of all people arriving at a particular venue, such as a rally, and then compare it with data when employees arrive for work. The employer may use the data to discriminate or retaliate at employees who were at locations that the employer did not think of highly. Since such concerns are legitimate, both the U.S. Federal Trade Commission [18] and several state legislatures have started developing legislations to address potential abuse of this technology. As RFID is an emerging technology, there are not many real cases, available to illustrate these concerns. The objective of our study is that the users may choose the implementations so that the privacy concerns are adequately addressed. From a technology perspective, it is worth noting that at present the distance of the reader to the tag is less than than two meters in most of the cases and as such people will notice the use of any RFID reader [9]. For UHF tags, the reader can read from a distance of 6 meters.

At present passive RFID tags cost around 50 U.S. cents [3, 17]. The goal is to mass produce the tags at a cost of less than 10 U.S. cents. However the low cost tags may lack the necessary resources to have security features built-in them. This requires developing two types of passive tags – one lacking any security features and another with some security features. We expect that tags with no security features would be used with goods that are in heavy use, such as perishable food. Also, tags with security features may be used for expensive clothes and electronic devices. Over 500 million such tags have already been produced by Texas Instruments [11]. The privacy concerns can be addressed, by removing the tags or by "killing" the tags at the point-of-sale by disabling it.

Consider a typical scenario as depicted in Fig 2.

People with an RFID reader will be able to capture data of items that a person possesses at any time, including any medical devices implanted in the body, without the knowledge and permission of the individual. One way to protect such data could be in the form of a locking mechanism [20]. The RFID tag with security features could have a special bit turned on to indicate that it should respond with data, only to signals that address the security bit. The major problem with this solution is that the RFID tags and readers have not yet been standardized.

Another approach to ensuring privacy of information from the RFID tags is to use some form of individually identifiable number (IIN) on the product's physical tag. The manufacturer could add a three digit code similar to the Card Verification Value (CVV) in credit cards. Such a number would be visible only on the product tag and the reader must be able to accept an input of this kind before it can associate the Electronic Product Code with the necessary databases. The World Wide Web Consortium (W3C) has initiated a Privacy Preferences Project (P3P) to develop a framework for privacy policies [1].

4.1 Confidentiality of Data

The data from an RFID tag is accessed via wireless devices [13, 14, 15]. One way to protect such data is to encrypt it in some form. If a lock bit, that can be turned on or off using special signals from the reader, is used, the data would be delivered by the tag only if the bit is enabled to deliver the data..

There is potential for eavesdroppers to capture data transmitted wirelessly, be it encrypted or not. If the data is encrypted, the eavesdropper may simply capture the data and use it, along with other similarly captured data, for crypto-analysis.

One of the security concerns with RFID tags is cloning. An eavesdropper might capture the RFID tag from a pallet in transit with prescription medicines and place that tag in a new pallet of counterfeit medicine or for that matter any pallet containing no useful goods. This potential problem shows that the type of tag used in a pallet cannot be of the same type as one that might be placed on a perishable food item. Thus, a semi-passive tag would be more appropriate for a pallet where the battery power provided by the semi-passive tag could be used for activating a sophisticated circuitry that could perform handshaking functions for authentication. Yet another solution could be the use of IINs for pallets. In order to handle IINs there should be a separate mechanism for IIN value management. Clearly the IINs should not be visible from the pallet's tag as the cloner could benefit from such information. Instead, the IIN value could be placed in the bill of lading which the person attempting to substitute a pallet would not have access to. Thus, arriving at solutions requires a careful study of the procedures, through which the information in RFID tags could be abused. The technical solution discussed above is further enhanced by the availability of ultra small individual recognition security chips [16].

4.2 Methodologies for Mitigating Privacy Concerns

When tags are used by retailers, the tags must be disabled at the point-of-sale. The control functions of a tag may be encrypted so that functions like turning on or turning off of the locking bit can be operated by an authorized device only. Once a customer passes the point-of-sale, the control may turn off the reading process. Moreover the control may be asymmetric. While the turning off process may be usable from a distance, the turning on of the reading process may be possible through a device, which is kept only at a few inches from the tag. Skimming fabric, which hides the tag from a reader, should also become easily available to the user so that if a user should be interested, he should be able to disable the reading by hiding the tag behind such a fabric. By adding these techniques to encryption for confidentiality and INN bits, it should be possible to avoid invasion of privacy of customers. For valuable products GPS- aware active tags can be used with a database, which continuously monitors the product and stores the data in a database. This can issue an alert, if the product is sought to be mis-placed, cloned or stolen.

6 Conclusions

RFID tags have numerous benefits to offer. The RFID industry and the users could benefit a lot by establishing a set of international standards so that one need not worry over international jurisdictions for any litigation. The privacy concerns about the possible abuse of RFID tags are genuine. But suitable technologies and policies can be put in place to protect the privacy rights of all the stake-holders. In this paper, we have been able to work out the technological methods for addressing the privacy concerns. The protocols, for using the technological methods will have to be designed for each application so that the effectiveness of the technological methods is not jeopardized by weaknesses in protocols. Since the technology is still being developed and the protocols for each application have not been worked out, it is not possible to obtain the test results from a specific application. As the standardization process moves forward, and as application specific protocols are developed, tests on the methodologies developed in this study will have to be conducted.

References:

[1]. Floerkemeier, C., Schneider, R., Langheinrich, M. 2005. "Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols," Springer-Verlag LNCS, vol. 3598, H. Murkami et al, Editors.

[2]. Floerkemeier, C. And Lampe, M. 2004. "Issues with RFID usage in ubiquitous computing applications," Springer-Verlag LNCS vol. 3001, pp. 188-193, A. Ferscha et al, Editors.

[3]. Sarma, S.E., Weis, S.A., Engels, D.W. 2003. "RFID Systems and Security and Privacy Implications," Springer-Verlag LNCS vol. 2523, pp. 454-469, B.S.Kaliski et al, Editors.

[4]. Albrecht, K. 2002. "RFID: Tracking everything, everywhere,"http://www.spychips.com/rfid_overview.html. Accessed on Oct. 22, 2005.

[5]. Harper, J. 2004. "RFID Tags and Privacy: How Bar-Codes-On-Steroids Are Really a 98-Lb. Weakling," Competitive Enterprise Institute, vol. 89, June 21, Washington D.C.

[6]. IEEE Technical Policy Committee, "Developing National Policies on the Deployment of Radio Frequency Identification (RFID) Technology," Washington D.C., October 2005.

[7].Collins, J. 2005. "Sweden Switches to E-Passports,"http://www.rfidjournal.com/article/articleview/1942/1/1. Accessed on Oct. 22, 2005.

[8]. Electronic Privacy Information Center. http://www.epic.org. Accessed on Oct. 22, 2005.

[9].Alfonsi, B.J. 2004. "Privacy debate centers on radio frequency identification," IEEE Security and Privacy Magazine, vol.2, #2, Mar-Apr., p. 12.

[10].Raza, N., Bradshaw, V. and Hague, M. 1999. "Applications of RFID Technology," IEE Colloquium on RFID Technology, Oct. 25, pp. 1-5.

[11]. Texas Instruments. http://www.ti.com/rfid/. Accessed on Oct. 30, 2005.

[12]. EPC Global. http://www.epcglobalinc.org/. Accessed on Oct. 23, 2005.

[13]. Sarma, E.E., Weis, S.A., and Engels, D.E. 2003. "RFID Systems and Security and Privacy Implications," Springer-Verlag Lecture Notes in Computer Science, vol. 2523, B.S.Kaliski (Editor), pp. 454-469.

[14]. Finkenzeller, K. 1999. "RFID Handbook," John Wiley & Sons, New York.

[15]. Weis, S.A. 2003. "Radio-frequency identification security and privacy," MIT M.S. Thesis, Cambridge, Massachusetts, USA.

[16]. Takaragi, K. et al. 2001. "An ultra small individual recognition security chip," IEEE Micro, vol. 21, #6, 43-49.

[17]. Garfinkel, S. and Rosenberg, B. (Editors). 2005. "RFID Applications, Security, and Privacy," Addison-Wesley Publishers, New York.

[18]. US – FTC. 2005. "Radio Frequency Identification: Applications and implications for consumers," March. http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf. Accessed on October 29, 2005.

[19]. Alien Technology Corp. 2005. http://www.alientechnology.com. Accessed on October 28, 2005.

[20]. Juels, A. 2005. "RFID Security and Privacy: A Research Survey," RSA Laboratories, (condensed version to appear in IEEE Journal on Selected Areas in Communications).

[21]. Fishkin, K.P., et al. 2004. "A ubiquitous system for medication monitoring," Pervasive 2004.

[22]. Spiekermann, S. and Ziekow, H. 2005. "RFID: A 7-point plan to ensure privacy," http://lasecwww.epfl.ch/~gavoine/rfid/.Accessed on October 26, 2005.

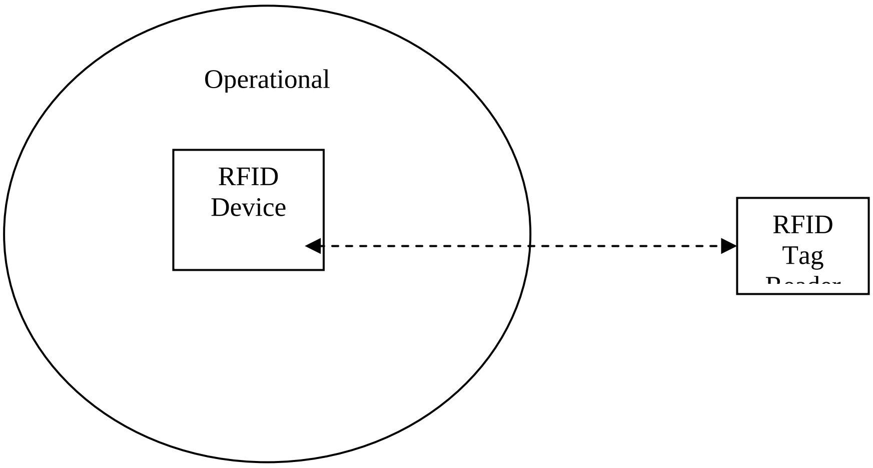

Fig 1. RFID system

Table 1. RFID tag frequencies, range and memory capacity.

Frequency Type	Frequency Range	Distance to Reader	Memory Capacity
Microwave	2.45 GHz (ISM band)	2 meter	Less than 1 Kbits
Ultra High Frequency	866 to 960 MHz	6 meter or more	1 Kbits
High Frequency	13.56 MHz	1.5 meter	256 bits to 4 Kbytes
Low Frequency	30 KHz to 300 KHz	1 meter	64 bits to 1360 bits

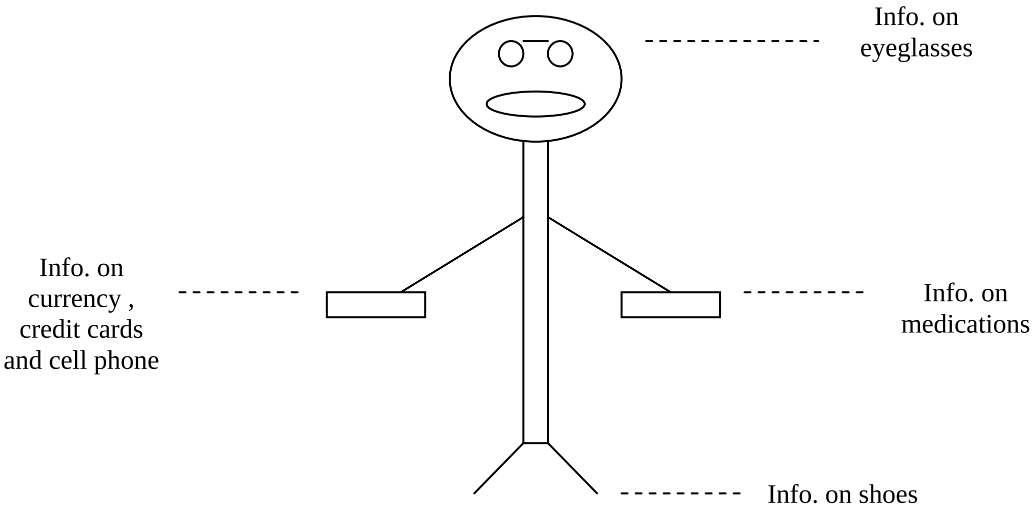

Fig 2. Multiple RFID tags on a person