GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

CLASSIFICATION OF RFID THREATS BASED ON SECURITY PRINCIPLES

Dushyant Kumar Sahu[*1], Asit Xaxa[2],Atul Sahu[3]
Student,B.E.(ET&T), Kirodimal Institute of Technology, Raigarh (C.G.)[*1]
Student,B.E.(ET&T), Kirodimal Institute of Technology,Raigarh (C.G.)[2]
Lecturer, Department of Electronics & Telecommunication, Kirodimal Institute of Technology Raigarh(C.G.)[3]

ABSTRACT

This paper surveys recent technical research on the problems of privacy and security for radio frequency identification (RFID). RFID tags are small, wireless devices that help identify objects and people.Thanks to dropping cost, they are likely to proliferate into the billions in the next several years—and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While geared toward the non specialist, the survey may also serve as a reference for specialist readers.

Keywords-RFID,Tag,Transponder,Reader,Security ,Privacy.

I. INTRODUCTION

Overview

THE “Radio Frequency Identification (**RFID**) is an automatic identification system. RFID uses RF to identify “tagged” items .This data is then collected and transmitted to a host system using an RF Reader. The data transmitted by the tag may provide identification or location information, or specifics about the product tagged, such as price, color, date of purchase, etc.”

An introduction to RFID

Radio Frequency Identification (RFID) technology has existed for decades. The term RFID is generally used to describe any Technology that uses radio signals for identification purposes which, in practice, “means any technology that transmits specific identifying numbers using radio .” Over the years, RFID has been used in in a variety of applications, such as inventory management;this work was sponsored by the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall School of Law, U.C. Berkeley. It was funded in part by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: Cisco, ESCHER, HP, IBM, Intel, Microsoft, ORNL,

Qualcomm, Pirelli, Sun and Symantec. anti-theft monitoring of consumer merchandise, and the

Taggin of livestock . With previous applications, it is difficult to link information stored on an RFID transponder to a specific individual. In anti-theft monitoring and inventory management, for example, the transponder is meant for temporary use and is externally applied, and thus easily removed if one desires.

Today ,new applications for RFID embed RF technology in common objects, or “everyday” things used by individuals, such as library books, payment tokens, and government-issued identification . For example, contactless smart cards, used in some public transportation and other electronic purse applications, contain an embedded chip which uses RF technology to communicate identifying data to the card reader. While these new applications of RFID can offer benefits, such as general convenience and decreased transaction times, they alsopose new privacy and security risks for individuals which are not present with more traditional RFID applications.

II. RFID EVOLUTION

RFID technology has passed through many phases over the last few decades (see figure 1). The technology has been used in tracking delivery of goods, in courier services and in baggage handling. Other applications includes automatic toll payments, departmental access control in large buildings, personal and vehicle control in a particular area, security of items which shouldn’t leave the area, equipment tracking in engineering firms, hospital filing systems, etc.[4, 5]. Figure 1 shows RFID evolution over the past few decades.

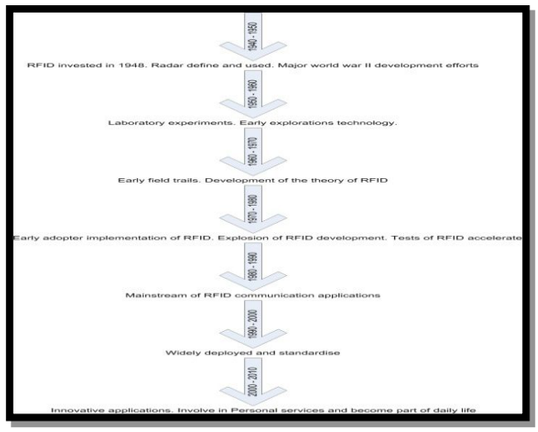

Fig. 1 RFID evolution: Over past the few decades adapted from [6]

III. HOW RFID SYSTEM WORKS

Most RFID systems consist of tags that are attached to the objects to be identified. Each tag has its own "read-only" or "rewrite" internal memory depending on the type and application . Typical configuration of this memory is to store product information, such as an object's unique ID manufactured date, etc. The RFID reader generates magnetic fields that enable the RFID system to locate objects (via the tags) that are within its range . The high-frequency electromagnetic energy and query signal generated by the reader triggers the tags to reply to the query; the query frequency could be up to 50 times per second. As a result communication between the main components of the system i.e. tags and reader is established .As a result large quantities of data are generated. Supply chain industries control this problem by using filters that are routed to the back-end information systems.

In other words, in order to control this problem, software such as Savant is used. This software acts as a buffer between the Information Technology and RFID reader Several protocols manage the communication process between the reader and tag. These protocols (ISO 15693 and ISO 18000-3 for HF or the ISO 18000-6, and EPC for UHF) begin the identification process when the reader is switched on. These protocol works on selected frequency bands (e.g. 860 – 915 MHz for UHF or 13.56 MHz for HF). If the reader is on and the tag arrives in the reader fields, then it automatically wakes-up and decodes the signal and replies to the reader by modulating the reader's field . All the tags in the reader range may reply at the same time, in this case the reader must detect signal collision (indication of multiple tags). Signal collision is resolved by applying anti-collision algorithm which enables the reader to sort tags and select/handle each tag based on the frequency range (between 50 tags to 200 tags) and the protocol used. In this connection the reader can perform certain operations on the tags such as reading the tag's identifier number and writing data into a tag.

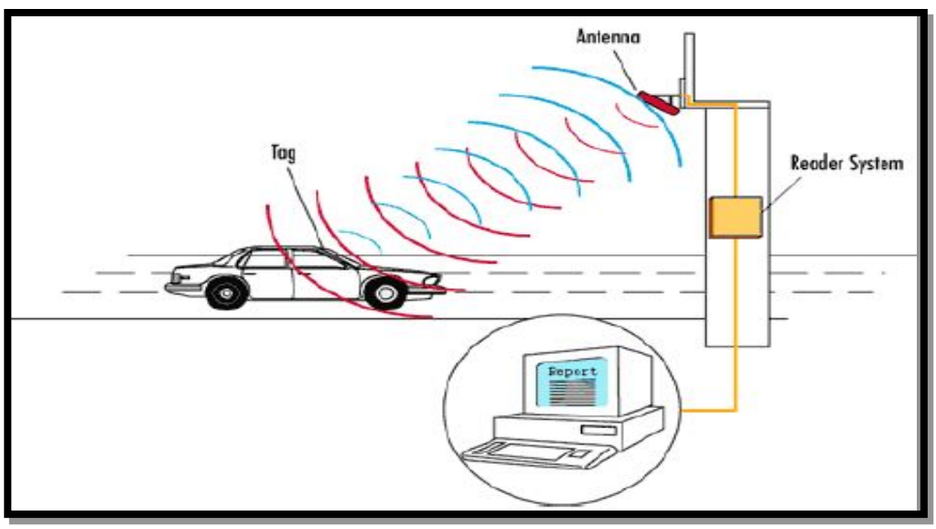

Fig. 2 A typical RFID SYSTEM [7]

IV. SECURITY AND PRIVACY ISSUE

With the adoption of RFID technology, a variety of security and privacy risks need to be addressed by both organization and individuals. The basic requirements for security have long been considered to consist of maintaining privacy (orconfidentiality), availability, and integrity. Recently non-repudiation has become equally important.While it is quite unlikely that any system can be made 100% secure, identifying the threats andassessing the risks are vital steps toward improving security RFID tags are considered "dumb" devices, in that they can only listen and respond, no matter who sends the request signal.

RFID privacy is already of concern in several areas of everydaylife.

• **Toll-payment transponders**: Automated toll-paymenttransponders—small plaques positioned in windshieldcorners—are commonplace worldwide. In at least onecelebrated instance, a court subpoenaed the data gatheredfrom such a transponder for use in a divorce case,undercutting the alibi of the defendant .

Passports: An international organization known as theInternational Civil Aviation Organization (ICAO) haspromulgated guidelines for RFID-enabled passports and other travel documents . The United States hasmandated the adoption of these standards by 27 "visawaiver"countries as a condition of entry for their citizens.The mandate has seen delays due to its technicalchallenges and changes in its technical parameters, partlyin response to lobbying by privacy advocates .

Human implantation: Few other RFID systems have inflamed the passions of privacy advocates like the Very Chip system . Very Chip is a human-implantable RFID tag, much like the variety for house pets. One intended application is medical-record indexing; by scanning a patient's tag, a hospital can locate her medical record. Indeed, hospitals have begun experimentation with these devices. Physical access control is another application in view for the Very Chip.

V. RFIDTAG

Passive RFID tags have no internal power supply. The minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the integrated circuit (IC) in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier signal from the reader. This means that the aerial (antenna) has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatters signal .The tag chip can contain nonvolatile EEPROM (Electrically Erasable Programmable Read-Only Memory) for storing data. Lack of an onboard power supply means that the device can be quite small: commercially available products exist that can be embedded under the skin.

There are three types of tags: the passive, semi-active and active. Semi-active tags have a combination of

active and passive tags characteristics. So, mainly two types of tags (active and passive) are being used by industry and most of the RFID system. The essential characteristics of RFID tags are their function to the RFID system. This is based on their range, frequency, memory, security, type of data and other characteristics. These characteristics are core for RFID performance and differ in usefulness/support to the RFID system operations. While considering these characteristics, figure 3 compares the active and passive tags.

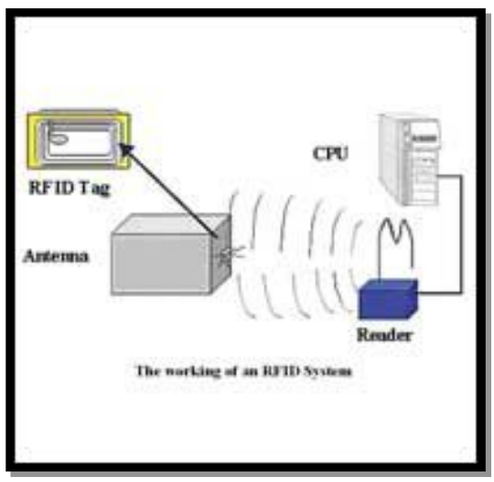

Fig.3 Working of an RFID System

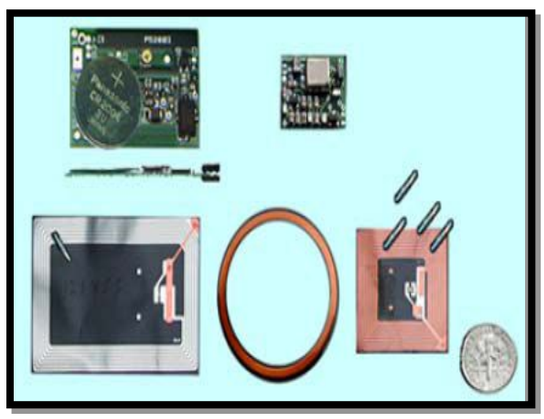

Fig. 4 Varity of RFID tags (various shape & sizes) [9]

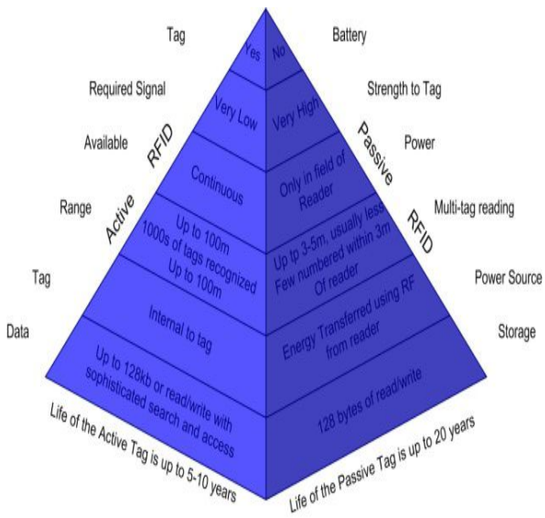

Fig. 5 RFID active and passive tags comparison

Tag Life

RFID tags last longer than barcodes because the technology does not require line-of-sight. Most RFID vendors claim a minimum of 100,000 transactions before a tag may need to be replaced (Boss 2004).

VI. THE RFID TAG INDUSTRY TODAY & ITS FUTURE

Given the choice of a cheap tag that costs a few cents and a secure tag, most end users will always go for the cheapest solution. However, as the number of RFID applications increase and include open loop systems with access from many parties, we can foresee that the current lack of security will be a major impediment in many solution designs. Our view is that Moore's Law - Intel co-founder Gordon Moore wrote in a 1965 article that the number of transistors on a chip would double every 24 months - and market drivers will soon enable security functionalities on low cost tags. The default choice of using cheap, unsecured tags must change if tag security can be seen to be a service-enabler and security management can be made easier and cheaper. We shouldn't forget that the security level for protection of a tag cannot be determined without any information about the final application. The security level is determined by the combination of the tag's protection and the security given by the characteristics of the physical car-key. The application also determines the value to the attacker and hence the capabilities that an attacker will bring to breaking the system.

VII. CURRENT RFID SECURITY CAPABILITIES

The key advantage of RFID technology over earlier technology, such as optical barcodes, includes the ability to identify objects without line of sight access. However an RFID system is more than a series of radio frequency tags. Any benefit relies on the system being capable of acquiring data from the tag and transforming that data into useful information for specific business processes.
The security of the radio interface is defined by the tag specification that is being read. Most tags (e.g. EPC C1G2) do not provide authentication to the reader, so the reader will accept whatever identifier or other memory values that are provided by the tag. These values are not processed by the reader, but passed to the host for collection and processing, limiting the facility to perform attacks on the reader by this interface.

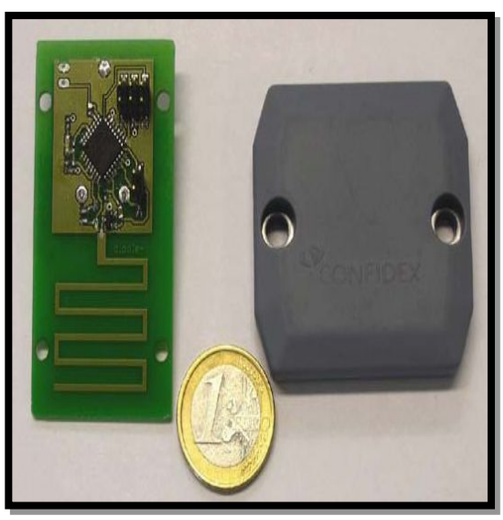

Fig 6:-Programmable semi-passive tag prototype (left) and a commercial encapsulated tag (right)

VIII. RFID SECURITY BENEFITS AND THREATS

Universally deploying RFID tags offers many potential security benefits, yet may expose new privacy threats. Otherwise intrusive or cumbersome security practices, such as airline passenger and baggage tracking, can be made practical by using RFID systems. Authentication systems already take advantage of RFID technology, for example car key-less entry systems. Embedding RFID tags as seals of authenticity in documents, designer products, and currency may discourage forgery. While RFID tags improve certain security properties in these applications, they may exacerbate privacy threats or pose new security risks. RFID systems are different from other means of identification because RF communication is non-contact and non-line-of-sight, whereas other means of identification are either contact-based or require line-of-sight. In other words, it is more difficult for the owner of the RF tag to physically impede communication with the tag. The promiscuity of RF tags is not unique; magnetic stripe cards, for example, are promiscuous, but we assume that the owner of the card takes the physical responsibility of preventing unauthorized users from physically accessing the card. Of course, the propagation characteristics of electromagnetic fields do limit the range from which passive RFID cards can be read. In fact, most tags operating at 13.56 MHz cannot be read from more than a meter away, and 915 MHz tags are difficult to read through most materials. Yet, as the information stored on the tag becomes more and more valuable, it is necessary to think through some of the security and privacy! related issues in RFID. We present such a discussion in this section, ending with a proposed approach.

- Airline passenger and baggage tracking made practical and less intrusive
- Authentication systems already in use (key-less car entry)
- Non-contact and non-line-of-sight
- Promiscuity of tags

Previous Work

The contactless interface and constrained computational resources of RFID devices present a unique set of characteristics most closely related to smart cards. Many relevant lessons may be gleaned from the wealth of smart card and tamper resistant hardware research. discusses a range of smart card protocols and analyzes cost and security trade-offs.

Security Goals

It is useful to state clear security goals when discussing security properties of various RFID designs. Tags must not compromise the *privacy* of their holders. Information should not be leaked to unauthorized readers, nor should it be 466 S.E. Sharma, S.A. Weis, and D.W. Engels possible to build long-term tracking associations between tags and holders.

IX. LOW-COST RFID ISSUES

With these security goals in mind, consider the security properties of passive factory-programmed, read-only tags. Each tag contains a unique identifier such as an EPC. While no more “promiscuous” than an optical bar code, automated monitoring of RF tags is possible. This basic design clearly violates the privacy goal since tracking tag holders and reading tag contents are possible if the tag is properly presented to a reader’s interrogation field. Neither tags nor readers are authenticated; therefore, no notion of trust exists either.

X. SOME APPROACHES TO RFID PROTECTION

Accepting short-term limitations on low-cost tag resources, we discuss a simple RFID security scheme based on a one-way hash function. In practice, a hardware optimized cryptographic hash function would suffice, assuming it may be implemented with significantly fewer resources than symmetric encryption. In this design, each hash-enabled tag contains a portion of memory reserved for a “meta-ID” and operates in either an unlocked or locked state. While unlocked, the full functionality and memory of the tag are available to anyone in the interrogation zone.

XI. FUTURE RESEARCH DIRECTIONS

While this candidate design partially satisfies some desired security properties, more secure implementations require several developments. One key line of research is the further development and implementation of low cost cryptographic 468 S.E. Sharma, S.A. Weis, and D.W. Engels primitives. These include hash functions, random number generators and both symmetric and public key cryptographic functions. Low cost hardware implementations must minimize circuit area and power consumption without adversely affecting computation time. RFID security may benefit from both improvements to existing systems and from new designs. More expensive RFID devices already offer symmetric encryption and public key algorithms such as NTRU . Adaptation of these algorithms for the low-cost (US$0.05-0.10), passive RFID devices should be a reality in a matter of years.

XII. EMERGING APPLICATIONS OF RFID

Tracking apparel: Marks & Spencer, one of the largest retailers in the UK, is tagging apparel items with ultra high frequency (UHF) tags beginning in Fall, 2003.

Tracking consumer packaged goods (CPGs): In 2003 UK Super market chain Tesco ran a three monthtest of “ Smart Shelve “ .The test wasperformed on DVDs stocked in Tesco's flagshipSand hurst store, near London, DVDs were taggedand programmed. Shelving units were equippedwith 13.56 MHz readers from Philipsemiconductors. The system put a time stamp nextto each movement of a product. So if a dozenDVDs left the backroom at 4:47 PM and never gotto

the shelf, the retailer could check who had access to the backroom at that time and focus theinvestigation on those employees that had access. This test was however capped at WallMart andGillette.

Tracking tires RFID Technology could be used in tire recalls." Instead of having to recall Persnationally or 'from the East Coast,' tire companies will be able to recall a bad lot from the twelve stores they were distributed to. We can only imagine how much money could be saved in such an example. Some analysts' projections anticipate auto-related RFID investments approaching as much as $2 billion by 2011. Michelin has developed a patent-pending RFID tire transponder, pictured below, which consists of a UHF RFID integrated circuit and two spring-wire antennas. Not only does the tag identify the tire, it actually monitors the tire temperature and pressure, using the kinetic energy from the tire to power itself as it rotates.

Tracking currency: The European Central Bank was moving forward with plans to embed RFID tags as thin as a human hair into the fibers of Euro bank notes by 2005, in spite of consumer protests. The tags could allow currency to record information about each transaction in which it is passed. Governments and law enforcement agencies hail the technology as a means of preventing money-laundering, black-market transactions, and even bribery demands for unmarked bills. However, It has yet to be implemented.

E Passports: In order to increase the security of United States travel documents, the Government has developed a new 'electronic passport' system. This will contain RFID tags: chips that will wirelessly send passport and biometric information to an inquiring RFID reader. This new passport system has already been deployed in October 2006. Except for Andorra, Brunei and Liechtenstein, allof the 27 countries whose citizens can travel to the 9 U.S. without a visa are now issuing "e-Passports," Reading a passport's RFID chip requires a password generated by scanning the machine readable data on the inside front cover. Additionally, a small shield in the front cover is supposed to only allow wireless passport reading when the booklet is open.

However A German computer security consultant has already shown in Aug 2006 that he can clone the electronic passports that the United States and other countries are beginning to distribute this year

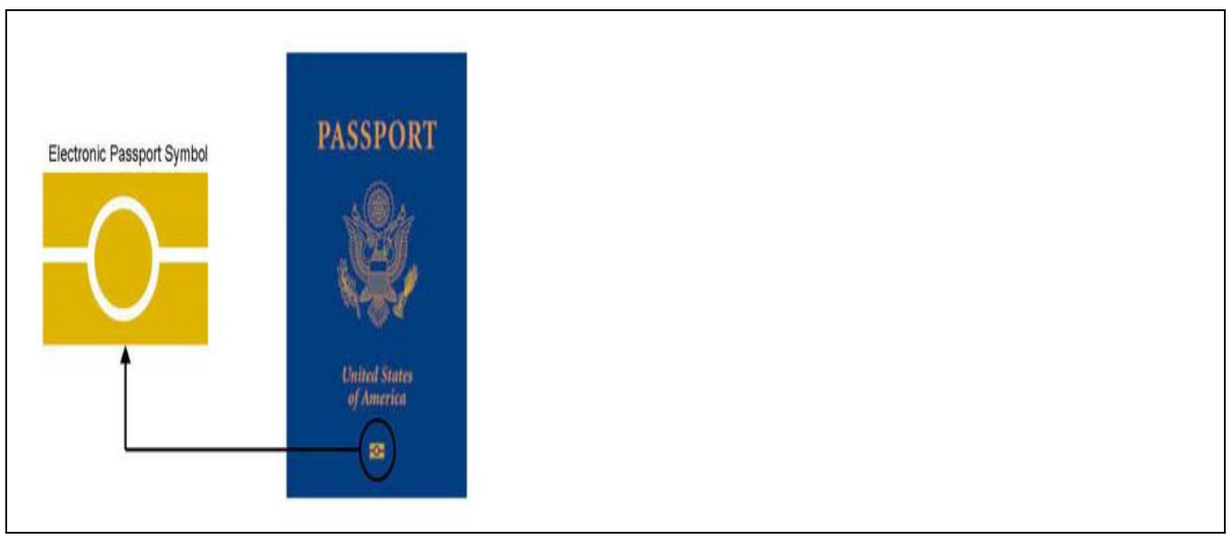

Fig7: E-PASSPORT

Reader Characteristics

The tag and the reader must comply with the same standard in order to communicate. If a tag is based on a proprietary design, a reader must support the same communication protocol to communicate with that tag. In many cases, if proprietary tags are used, only proprietary RFID readers from the same vendor can be used. Reader characteristics that are independent of tag

Power output and duty cycle,
Enterprise subsystem interface,
Mobility, and
Antenna design and placement characteristics include

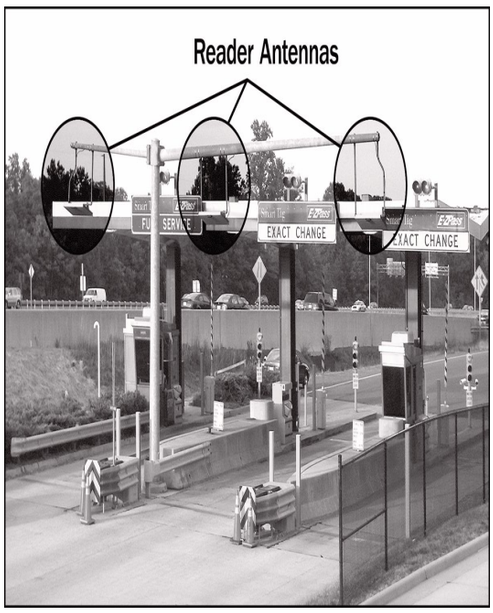

Fig 8:- Fixed Reader in Automatic Toll Collection Application

XIII. CONCLUSION

In this paper, we have considered the current state of RFID application in four important business-oriented application areas. We described potential benefits of an intensified use of RFID tags in these areas, and are coming up with an analysis of the causes that prevent this intensification. Eventually, this analysis should help researchers and industry to direct their efforts to advance RFID technology itself and its application. In order to identify the most pressing problems that promise the most advancement, if overcome, at a reasonable investment, we tried to judge the issues encountered in the four application fields according to additional criteria. In this paper we presented an overview of some of the security requirements for applications using RFID technology. We suggest a five step process to evaluate the security requirements of the RFID application and give some examples to show how the process might be used. Consideration of how the RFID technology itself can provide the desired level of security is one important step in the process of choosing the mechanism that will ultimately be used to make an application secure. Although some standards have been established, the ever-expanding use of RFID technology indicates there is an increasing need to improve standards and take all the steps necessary to provide security.

REFERENCES

[1] J. Bohn, "Prototypical implementation of location-aware services based on a middleware architecture for super-distributed RFID tag infrastructures", Pers Ubiquit omputing, (2008) Journal 12:155-166.

[2] J. Schwieren1, G. Vossen, "A Design and Development Methodology for Mobile RFID Applications based on the ID-Services Middleware Architecture", IEEE Computer Society, (2009), Tenth International Conference on Mobile Data Management: Systems, Service and Middleware.

[3] B. Glover, & H. Bhatt, RFID Essentials, O'Reilly Media, Inc, Sebastopol, (2006), ISBN 0-596-00944-5.

[4] K. Ahsan, H. Shah, P. Kingston, "Context Based Knowledge Management in Healthcare: An EA Approach", AMCIS 2009, Available at AIS library.

[5] S. Garfinkel, B. Rosenberg, "RFID Application, Security, and Privacy", USA, (2005), ISBN: 0-321-29096-8.

[6] L. Srivastava, RFID: Technology, Applications and Policy Implications, Presentation, International Telecommunication Union, Kenya, (2005).

[7] Application Notes, "Introduction to RFID Technology" CAENRFID: The Art of Identification (2008).