ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Challenges to Privacy and Risk Oriented RFID System Implementation in Libraries

Nitumika Gogoi

Lecturer, Centre for Library & Information Science Studies, Dibrugarh University, Assam, India

ABSTRACT: Library and information Professionals of the present decade have adopted and borrowed the characteristics those of the technologists and software professionals in the competition to conquer the sophistications of offline and online content providers as well as quest for existence in the digital milieu. This ultimately has enhanced their user service standards blended with auto service system on the part of the users. The users however are responding very well to this renovated image of the libraries and information centres (LICs). When viewed in this context of technological progress, Radio Frequency Identification (herein after RFID) implementation is hardly unique. The commercial deployment of RFID technology has captured every segment of the present market sector as well as specialized and security related applications. The LICs therefore are not lagging behind. They have started tagging every item in their possession with RFID tag, raising patron privacy concerns. As such in an item tagging regime, the ability to track tags raises the possibility of surveillance of library patrons and their reading habits. Through this paper, an attempt is made to investigate the privacy risks in the libraries' use of RFID technology and methods for reducing such risks.

KEYWORDS: RFID, privacy, eavesdropping, collision avoidance, password management

I. INTRODUCTION

The best way of making a system secure is by knowing how it can be attacked. Therefore, an RFID compliant library is no exception with a large number of readers thronging in and out of it in need of books possessed by the library. The RFID technology is a pervasive technology because leakage of information is a major defect that occurs when data sent by tags reveal sensitive information about the labeled items. Information products labeled with insecure tags reveal their memory content when queried by readers. Usually readers are not authenticated while tags answer in a transparent and indiscriminate manner. The main purpose of RFID is automated identification of products and people. One of the biggest advantages of RFID over conventional systems such as bar codes is that neither line of sight nor physical contact is required for an object with an RFID tag to be identified, as is the case with bar codes where line of sight is required and smart cards, where contact is required and it is hoped to replace all techniques of optical identification.

II. LITERATURE REVIEW

Dai Yu (2011) in his case study on the Turku City Library on implementing RFID Technology in Library Systems focused on the management aspect of a library particularly the self service support system for patrons by introducing RFID system. Based on a comparative study between the barcode and RFID applications, it is stressed on the many benefits of RFID. However, challenges are many and are pointed out as those of tracking and hot listing. Moreover, depending on the strength of the RFID reader it is possible to either greatly hinder or completely block the tag signal by wrapping an item, embedded with several layers of aluminum or tin foil. This combined with a weak gate sensor, makes risk of item getting stolen quite high.[11] Syed Md Shahid (2005) considers RFID applications in circulation, tracking, inventorying and security of library materials as well as discusses on the various components of the RFID system in details followed by its installation features. At the same time, he states that it is important to educate library staff and library users about RFID technology before implementing a program.[12] Serge Vaudenay (2001) deals in preparing a model based purely on the security and privacy of the RFID tags and assumes a powerful adversary who can control all communications mandating the use of some public key cryptography techniques while discussing on tag corruptions and availability of side channels.[13] In a research project, David Alexander Molnar studies the security and privacy in deployments of RFID technology and propose novel mechanism for improving RFID privacy for library books and electronic passport and deals with private authentication. He also discuss broadly on the different eavesdropping ranges, repetitive stress injuries, streamline mechanism and RFID as an enabler for automatic sorting on book check-in.[14]

Seema Vasistha (2009) aims at extending RFID applications in an academic library keeping in view the scantiness of funds and scarcity of supporting staff. Moreover it is considered important for controlling management problems such as increasing theft, monopolizing reading materials, poor inventory accuracy, inadequate security control.[15] A. Narayanan et al. particularly studies the technical and scientific aspects of RFID system with in depth discussion on microchips, anti-collisions as well as tag classes that can be applied in library oriented RFID system and giving importance on its implementation in retrospective conversion and reader usage.[10] Dhanalaxmi M and Uppala Mamatha (2009) describes the different RFID modules that provide integration with Library Management System along with the positioning of the tags on the document that gives 100% readability of tags thus reducing time consumption. [9]

III. THE RFID SYSTEM IN A NUTSHELL

More generally, RFID system can be considered a non-contact method of using radio frequency electromagnetic (herein after RFE) waves with frequencies up to 2.5GHz, for communication between two remote entities. Data is stored in devices called RFID tags or transponders (each with a unique identification number), and is retrieved by readers or transceivers. The main purpose of RFID system is the automated identification of people and products. While the biggest stumbling blocks in the use of RFID system are the numerous and complex security threats that as well as privacy issues involved with RFID system.[1]

➢ An RFID system basically consists of three components:

1. The *RFID tag or transponder* (derived from transmitter/responder). It bears the information that identifies the person or object, and is carried or implanted. The information is usually in the form of an alphanumeric word. This information is called an identifier, and that of each tag is unique. Tags vary in size, and their size mainly depends on the size of the antenna on the tag.
2. The *RFID reader or transceiver* (derived from transmitter/receiver). It supplies energy to the tag in the form of RF electromagnetic waves. It then receives the signal from the tag. It usually contains an interface that allows it to communicate with a data processing system.
3. The *back-end infrastructure or data processing system*. This receives the information from the reader, and processes it by using the tag ID number of a product to identify it. The RFID reader and the back-end infrastructure are together called the reader system.

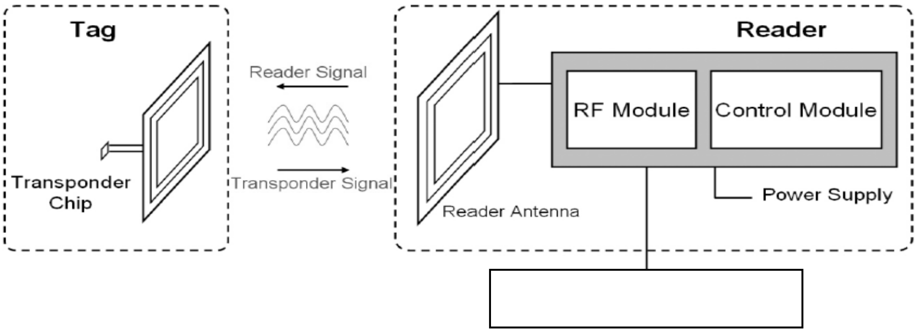

Figure1: Components of an RFID system

Whenever a tag comes into the vicinity of a reader, it receives a signal from the reader and transmits its unique key, enabling identification of the object or person carrying the tag. Clearly then the reader must be able to handle multiple tags at once. There are some cases, however where there is only one tag for a particular reader. Thus RFID systems are of two types – one to one and many to one.

➢ RFID tags can be classified into 3 types depending on their power consumption: passive, semi-passive and active.

- *Passive tags* have no internal energy source. The electrical energy required for the tag current is derived from the radio waves emitted by the reader. These tags are the smallest and cheapest, and thus are the most widely used. They also have a virtually unlimited lifespan.
- *Semi-passive tags* are similar to passive tags in that the energy required for transmitting the signal is still derived from the reader. However, these tags have a small battery for internal computations.
- *Active tags* do not require external power. They have an internal battery that is used for transmission of data as well as for transmission of the signal. As a result of the increased power, they can transmit data over a much larger range compared to passive tags. However, their relatively high cost means widespread use is not possible.

The tag which is most likely seen in the present libraries is the passive tag that replaces the barcode application in libraries because of their chip size.

➢ As for the concerned frequency of operation, RFID systems operate in several frequency bands. The low frequency (LF) band is 124-135 KHz. High frequency (HF) ranges from 3 MHz to 30 MHz, with 13.56 MHz being the typical frequency used for HF. Ultra HF ranges from 300 MHz to 1 GHz. Microwave frequency ranges upward from 1 GHz. A typical microwave RFID system operates either at 2.45 GHz or 5.8 GHz, although the former is more common. [2]

➢ Read range i.e. the maximum radius around a reader in which, if a tag is brought, the reader system can successfully read its identifier. Range depends on factors such as:

- Frequency of operation: Range increases with frequency. However, metal acts as a barrier to radio wave propagation, and reduces the range at higher frequencies.
- Transmitter power of the reader.
- Antenna size of reader and tags.
- Transmitter power of tags: This is applicable only for active tags.

Often, vendors of RFID readers are required to quote a range. They either quote it for standard tags e.g. tags manufactured according to ISO standard, or specify the tag particulars. The electromagnetic spectrum on which RFID resides is regulated by local governmental bodies. Global standards define it as the most efficient platform on which an industry can operate and advance. The International Organization for Standardization (ISO) and EPCglobal have been very active in developing RFID standards. The AutoID Center and its commercial offshoot, EPCglobal, have also defined specifications and standards. Most commercial applications, including library applications, today use the HF standards. RFID tags with the ISO Standard 15693 are the most common ones for library applications.[3]

IV. RFID SYSTEM IN LIBRARIES

Current standards (ISO 15693) apply to container-level tagging used in supply chain applications and do not address problems of tracking and hot listing. Next-generation tags (ISO 18000, August 2004) are designed for item-level tagging. The newer tags are capable of resolving many of the privacy problems of today's tags. The ISO 18000 standard is capable of establishing a more secure communication between the tag and the reader as well as can address applications under six categories:

1. Access control (keyless entry)
2. Asset tracking (self-check-in and self-checkout)
3. Asset tagging and identification (inventory and shelving)
4. Authentication (counterfeit prevention)
5. Point-of-sale (POS) (Fast Track)
6. Supply chain management (SCM) (tracking of containers, pallets, or individual items from manufacturer to retailer)

However, no library RFID products using the new standard are currently available. Libraries implementing RFID system today are using tags unsuited for item- level tagging. As such, privacy concerns associated with it poses an important impediment to libraries' use of RFID tags that contain static information that can be relatively easily read by unauthorized tag readers, allowing intervention of privacy issues described as "tracking" and "hot listing." Tracking refers to the ability to follow the movement of a book (or person carrying the book) by "correlating multiple observations of the book's bar code" or RFID tag. Hot listing refers to the process of building a database of books and their associated tag numbers (the hotlist) and then using an unauthorized reader to determine who is checking out items on the hotlist.

On the other hand, most RFID readers in libraries can read tags up to 16 inches away. Readers in library RFID systems are used in the following eight ways:

1. Conversion station where library data is written to the tags
2. Staff workstation at circulation used to check in and checkout materials.
3. Patron self-checkout station used to check out books without staff assistance.
4. Exit sensors verify that all books leaving the library have been checked out.
5. Patron self-check-in station used to check in books without staff assistance.
6. Book-drop reader checks in books when patrons drop them in the book-drop.
7. Sorter which is an automated system for returning books to proper area of library.
8. Portable reader which is a handheld reader for inventorying and verifying that items are shelved correctly.

Shelf Management
Check in/out station
Book Drop
Self Check in/out
Anti-theft Detection
Tagging

V. LIBRARY PROBLEMS ADDRESSED BY RFID

- Libraries are suffering from budget shortfalls as never before. With cuts to state and local governments, it is difficult for libraries to remain staffed and open. RFID is seen as a way to address the staff shortages by increasing the number of circulations that can be processed with less staff.
- Self-check systems have become very popular with both patrons and staff. RFID self-check systems allow patrons to check in or check out several books at a time. Self-check systems reduce the number of staff needed at the circulation desk.
- With RFID-enabled tools, inventory-related tasks can be done in a fraction of the time that it takes with bar code readers. A whole shelf of books can be read with one sweep of the portable reader, which then reports which books are missing or mis-shelved. For archives handling sensitive materials, the ability to inventory items without handling them is an additional benefit.
- Sorting can be accomplished automatically with RFID. For a book that is dropped into the book drop, the reader reads the tag and uses the automatic sorting system to return the book to the shelves, the stacks, or the hold area.
- Reduction of repetitive stress injuries (RSIs) among staff is another reason libraries are converting to RFID system. The repetitive motion associated with checking out books using optical scanners is believed to be more problematic than with RFID enabled scanners. It is still too early to determine whether RFID systems reduce the incidences of RSI injuries.

- Security is another aspect of library operations that may be greatly improved with RFID-based security systems. Rather than purchasing additional tags for security, libraries can use a single tag for identifying items and securing them. As patrons leave the library, the tags are read to ensure that the item has been checked out. Librarians also report that they can more easily retrieve lost or hidden items using the portable readers. At the session “Tiny Tracker: The Use of RFID Technology by Libraries and Booksellers.” Karen Saunders of Santa Clara City Library reported at that many DVDs were being hidden by patrons for their own use later. Using the RFID reader, staff located these lost items and returned them to circulation. The possibility of blocking the tag from being read by using foil or by removing the tag puts into question whether RFID is truly the best approach for library security. In addition, readers are already being developed that are capable of scrambling the data on tags.[4]
-

As has been mentioned above, the private authentication is one of the key technical challenges to be overcome in the present libraries’ RFID system. It is because we want tags to reveal their identity to authorized RFID readers, those owned by the library, so that the library can track books as they are checked in and out. For privacy, the tag must not disclose its identity until the reader has been authenticated; also, prudent key management requires that each tag hold a different symmetric key. The paradox is that a legitimate reader cannot authenticate itself until it knows which key to use, which requires knowing the tag's identity, but for privacy reasons the tag dares not reveal its identity to an unknown reader before that reader has been authenticated. Because the communication between reader and tag is wireless, there is a possibility for third parties to eavesdrop on these signals. One unusual aspect of RFID communication is an asymmetry in signal strength: because tags respond by passively modulating a carrier wave broadcast by the reader, it will be much easier for attackers to eavesdrop on signals from reader to tag than on data from tag to reader.

VI. INTRUSIONS TO THE RFID SYSTEM APPLICATIONS IN LIBRARIES

- *Detecting Tag Presence*

Current architectures do not prevent a reader from detecting a tag's presence. Detecting a new library RFID tag means someone or something moved a book into detection range, typically signaling the presence of a human being. Detecting human presence enables applications such as alarm systems, advertisements that respond when someone comes near, or real-time tracking of specific tags. The ability to detect a human presence might, in some cases, be considered an infringement on that person's privacy.

- *Static Tag Data and No Access Control*

It is seen that none of today's library RFID tags employ read passwords or other read access control. Because the bar code on the RFID tag remains same throughout its lifetime, the ability to read it at will enable several privacy risks.
First, the adversary may determine which library owns the book and infer the origin of the person carrying the book. In particular, bar codes for libraries with the Innovative bibliographic database have well-known, geographically unique prefixes. Vendors may also place library IDs on tags to prevent tags from one library from triggering readers at another. For example, police at a roadblock may scan for patrons from specific city libraries in predominantly minority areas and search them more carefully; this would raise issues of racial profiling.

Second, any static identifier can be used both to track and hotlist books. In book tracking, the adversary tracks a book by correlating multiple observations of the book's bar code. The adversary may not necessarily know the title and author of the book unless the bibliographic database is available, but the bar code can still be used to track the book's movements. Tracking the book's movements may mean tracking the movements of the person in possession of that book. Combined with video surveillance or other mechanisms, this may allow an adversary to link different people reading the same book. In this way, an adversary can begin profiling individuals' associations and make inferences about a particular individual's views.

In hot listing, the adversary has a “hotlist" of books in advance that it wishes to recognize; to determine the bar codes associated with these books, the adversary might visit the library to read tags present on these books. Later, when the adversary reads an RFID tag, it can determine whether that tag corresponds to a book on the hotlist. With current architectures, hot listing is possible; each book has a single static identifier which never changes over the book's lifetime.

Hot listing is problematic because it allows an adversary to gather information about an individual’s reading habits without a court order. For example, readers could be set up at security checkpoints in an airport, and individuals with hot listed books set aside for special screening. For another example, readers could be set up at the entrance to stores and used to tailor patron experience or target marketing; these readers would look almost identical to the anti-theft gates used today.

- *Collision-Avoidance IDs*

Even if RFID tags were upgrade to control access to bar codes using read passwords or some other form of access control, many tags can still be identified uniquely by their radio behavior.
In particular, many tags use a globally unique and static collision ID as part of their collision- avoidance protocol. This typically will allow unauthorized readers to determine the tag's identity merely through its collision-avoidance behavior.

- *Write Locks, Race Conditions and Security Bit Denial of Service*

In deployments with rewritable tags, some method must be used to prevent adversaries from writing to the tag. Otherwise, an adversary can commit acts of vandalism such as erasing tag data, switching the RFID data of two books or changing the security status of tags with “security bits."

Unfortunately, vandalism is a real threat to libraries, especially from people who feel certain books should not be available; it would be naive to expect such people to ignore RFID-based vandalism for long. Once locked, a piece of memory cannot be unlocked by any reader and so cannot be modified. While this would prevent an adversary from changing the bar code, this architecture makes implementing a security complicated. The page holding the security bit would need to be unlocked when a book is checked in or out, or else the status of the bit could not be changed. At the same time, nothing appears to prevent an adversary from changing the security bit to “not checked out" and then locking that page of memory. The resulting tag is then unusable, as the memory cannot be unlocked; physical replacement of the tag is required before the book can be checked out. We refer to irrevocable locking of the security bit as a security bit denial of service. In addition to the issues with implementing security bits, there is a privacy concern as well. If there exist any unlocked memory on the tag, an adversary can write its own globally unique identifier and track tags based on this ID. This attack could bypass other mechanisms intended to prevent tracking or hot listing of tags, such as rewriting tag. Therefore, care should be taken to always lock all unused memory on writeable library RFID tags. [5]

- *Tag Password Management*

The current deployments do not seem to use read passwords, but write passwords are employed. There are two natural approaches to password management:
a. Use a single password per site; or,
b. Endow each tag with its own unique password. [6]
If a single password is used for all tags, then a compromise of any tag compromises the entire system. In deployments that use writable security bits, the write password is used on every self- checkout; in systems with read passwords, exit sensors must use the read password every time a book leaves the library. In either case, passwords are available to a passive eavesdropper. Consequently, eavesdropping on a single communication reveals the password used by every tag in the system, a serious security failure. Once learned by a single adversary, a password can be posted on the Internet. Then, anyone with a reader can mount the attacks we have discussed. If different passwords per tag are used, then some

mechanism is required to allow the reader to determine which password should be used for which tag. Unfortunately, most obvious mechanisms for doing so, such as having a tag send an index into a table of shared secrets to the reader; provide tags with static, globally unique IDs. [7] These globally unique IDs allow tracking and hot listing of tags, which would defeat the entire purpose of read access control. We need a mechanism for reader and tag to authenticate each other without revealing the identity of the tag to adversaries. In fact, it is not clear how to achieve efficient private shared secret authentication, even with PC-class resources. Trying all passwords sequentially will take far too much time, since many libraries have hundreds of thousands of books. Thus, privacy appears incompatible with prudent password management.

VII. MEASURES FOR QUASI EXPURGATION OF ATTACKS ON RFID SYSTEM

Current library RFID tags do not prevent unauthorized reading of tag data. Therefore, information such as title, author, shelf location, patron information, or last check in/checkout time should in no circumstance be stored on library RFID tags. Further, such information is not needed; a pointer to a database is sufficient for all current and envisioned applications of library RFID tags, including collection management and item sorting. [8]

At the same time, both tracking and hot listing are possible whenever a static identifier is used. Therefore, if a static identifier is in place on the RFID tag, it is imperative to prevent unauthorized tag reads. However, it is supposed that static identifiers may include collision IDs that are not protected by access control mechanisms intended to protect tag data. Therefore to avoid tracking tags by collision ID, some mechanism for private collision avoidance must be used.

Apart from these justifications some measures find important status in the implementation of RFID system in LICs such as:

Integrating Software: With the preset Library Management Software. Care should be taken to integrate the library automation package while detailed tender specifications are drawn.

Training of Staff: Train the staff on various aspects of RFID technology. Proper demonstration of the system can be arranged by experienced vendors as well as librarians too should visit the library where the system is successfully running.

Performing Test Cases: To check out unit level and system level performance for accuracy.

Process Improvement: The errors found out from the test cases should be revisited to make the system perform accurately. Until sufficient confidence is gained with the system, old system in practice can be continued. [9]

VIII. CONCLUSION

RFID system bestowed with the capability to be reprogrammed is better than Bar codes and can help LICs accurately manage collections and extend their services. However, issues about reliability, interference and attacks on privacy and security issues need to be addressed further. Moreover, it is incumbent on librarians to educate the patrons about the possible abuses associated with RFID mainly for two reasons: because libraries have an interest in using the technology and because the threat to privacy posed by “ubiquitous computing” of which RFID is a part, is significant. [10]] In spite of the highlighted threats to RFID system in the present paper, these can be extenuated with the fact that RFID is that technology which provides the “right information to the right user at the right time and in the right personalized way in its entirety.”

REFERENCES

[1] Arjun Agarwal & Mala Mitra, ‘*RFID: Promises and Problems*’.
[2] Allied Business Intelligence (2002). *RFID white paper*. Oyster Bay, New York.
[3] R. Moroz Ltd. (2004, July). *Understanding Radio Frequency Identification (RFID) (Passive RFID)*. Markham, Ontario: R. Moroz Ltd. Retrieved August 4, 2014 from www.rmoroz.com/rfid.html.
[4] ibid. [3]
[5] Lori Bowen Ayre, *Wireless tracking in Libraries: Benefits, Threats and Responsibilities*. Retrieved on September 15, 2014.

[6] ibid. [5]
[7] Anonymous, *Privacy and Security in Library RFID issues, practices and architectures.* Retrieved on September 15, 2014
[8] ibid. [7]
[9] M. Dhanalaxshmi & Mamatha Uppala, RFID based Library Management System. Proceedings of ASCNT – 2009, CDAC, Noida, India, pp. 227 – 234
[10] Narayanan A., Sanjay Singh & Somasekharan M. *Implementing RFID in Library: Methodologies, Advantages and Disadvantages.* Scientific Information Resource Division, IGCAR
[11] Dai Yu, Implementation of RFID technology in Library Systems. Case study: Turku City Library in Bachelor's thesis in Business Information Technology
[12] Syed Md Shahid, Use of RFID Technology in Libraries: a new approach to Circulation, Tracking, Inventorying and Security of Library materials. Library Philosophy and Practices. V8 no.1
[13] Serge Vaudenay. On privacy models for RFID. ASIACRYPT 2007. International Association of Cryptographic Research
[14] David Alexander Molnar.Security and privacy in two RFID deployments, with new methods for Private authentication and RFID pseudonyms. Research Project. Dept. of Electrical Engineering and Computer Science, University of California, Berkeley.
[15] Seema Vasistha. Roadmap for RFID implementation in Central Library, PEC University of Technology. ICAL 2009: Technology, Policy and Innovations.

BIOGRAPHY

Ms. Nitumika Gogoi obtained MSc. in Mathematics from Dibrugarh University, Assam, India in 2004 and received the Masters degree in Library and Information Science from Indira Gandhi National Open University (IGNOU), India in 2008. She is presently working as a lecturer in the Centre for Library and Information Science Studies, Dibrugarh University, Assam, India.