Amy M Ostrom
LIS999 – Independent Study: RFIDs
Advisor: Kristin Eschenfelder

RFIDs : Contactless IDs in the Modern Library

Auto-IDs

Look on the back of a package and see a barcode, scan a card to draw some money from an ATM, or speak into a voice identifier to gain access to a building. These all have a common trait of identifying an object whether it is a person or an item and are known as auto IDs. Several types of auto IDs exist, the oldest being the use of *Optical Character Recognition* (OCR) that could be read by machine as well as the human eye. *Barcodes* have held as the most widely used auto ID system for two decades now making quick scanning by optical lasers possible. *Biometric* ID systems require either voice identification or fingerprint ID and are used primarily for security access measures and identification of humans.

Auto ID systems that come in the form of a plastic card began in 1984 with the introduction of the *smart card*. They require contact, typically done by swiping it through a card reader, in order to access the data stored on it. Two types of smart cards exist based on their functionality – memory and microprocessor. The memory card simply holds data needed for something such as a prepaid phone card. A microprocessor smart card can actually produce small mathematical computations. Smart cards unfortunately wear down due to the physical contact needed in order to read the data, so in 1999 an organization known as the Auto-ID Center was created that developed a contactless smart card known as a Radio Frequency ID, or RFID for short, accurately named so for its method of transmitting data. In RFIDs, the speed is increased, the life duration expanded, and accuracy improved greatly due to its nonphysical indirect environment (Finkenzeller, 2003).

RFID Components

An RFID system consists of two components, the transponder and the reader. The transponder, also known as a tag, is what is placed on the object needing identification, such as a DVD or book. They come in many different shapes and styles and vary in the way they transmit their data to the reader. Tags can either be read only, write once read many, or read write. Read write tags are the most preferred among libraries as data stored on the tag can be updated. A transponder consists of two parts, the coupling and the chip. The chip is extremely small and contains the actual data and processor while the coupling is the antenna, which typically appears coiled, used to transmit to the reader. These two components sit in housing that can be made of many materials such as plastic, glass, metal, etc. Libraries prefer a paper-thin housing that can be "stuck" to the inside cover of a book or media box.

The reader is the second component of an RFID system, and is the unit connected to a computer that will read the transponder within a certain distance depending on the type of system in use. It does this with assigned radio frequencies, of which most libraries use the high frequency 13.56MHz band although a low frequency band does exist for library use at 125 KHz (Ayre, 2004). The reader not only reads the data on a tag and performs a certain task; it can provide power to the chip. This is necessary with a passive transponder that has no alternative power source than what is provided by the

reader when the tag is within the RF field range, also known as the interrogation zone. An active transponder will have auxiliary power such as a battery, making the tag bulkier and shortening the tag's overall lifespan to that of the battery's. Libraries are more interested in the passive transponders as they are smaller, less expensive, and have an unlimited lifespan.

Boss (2004) lists one more component for an RFID system as the docking station that connects the reader data to the library's automated system. This is the important connection between the RFID system and the ILS (Integrated Library System) that already exists within the library. The software found on this docking station houses a database for transactions that is able to produce reports. Two protocols have been developed for communication between the ILS and RFID software: SIP2 (Standard Interchange Protocol) and NCIP (National Circulation Interchange Protocol). NCIP was developed in 2002 to make up for the shortcomings of the original SIP2 protocol, but it has yet to be completely integrated into all vendors' systems (Ayre, 2004). Thomas, Schaper, and Ford (2004) describe their difficulties with SIP as well and resolved to use a "SIP-less" European system instead.

EPC Global Network and Libraries

Currently libraries are the largest users of RFIDs at an item level. Most of the commercial uses involve a "slap and go" method by applying tags to a unit being shipped rather than to all the individual items inside that unit. This improves shipment pattern monitoring at the unit level, decreasing unit loss rate and overall time spent on inventory checks. An organization known as the EPC Global Network manages the network these business RFIDs transmit their data over. Libraries would not be able to run their data across this network like businesses because of a protocol the EPC Global Network requires to "kill" a tag after it reached its final destination in the shipping procedure, thus rendering the tag completely useless. However, such a network would be extremely useful if widespread implementation of the RFID tag occurred for uses such as interlibrary loan and document delivery, as the network's powerful tracking system is why most businesses are increasingly applying RFID technology in their shipping procedures. Unlike business organizations, libraries are not interested in monitoring a one time shipment, but rather would like to track the "movement" of an item over its lifespan. Hence, while the EPC Global Network is quite important in the business realm, it is detrimental in the basic needs of tracking for a library. Open source software is currently under development called RadioActive that may lead to the development of a more robust network that could allow for the inclusion of library data transmissions.

Corporate vs. Library RFID Needs

Then on-profit status most libraries fall under is a large factor in its RFID needs and resources for implementing them. Corporations are using RFID prominently with recently produced units with finite destinations where library must not only tag recent acquisitions but must also purchase enough tags to re-identify each item already owns with infinite usage of materials in mind. Companies have finite destinations because RFID tag use is primarily implemented to improve the efficiency of transporting materials from its manufacturer's warehouse to a store's backroom. Quite the opposite of its commercial counterpart, library RFID tags are less finite with no "final destination" and must be functional. At any time the item is queried by a reader or wand. Because of this, tags implemented in libraries must last much longer and perform several functions. The most essential of these functions is identification commonly accomplished with an

alphanumeric string known as a barcode. It may also contain extensive details such as title and author information. Corporate RFIDs will also contain similar basic data on a short term basis.

Another feature not typically enabled at the unit level in the corporate RFID tagging system is the use of the security bit. One bit can be assigned to identify whether the item is checked in or out by using a simple true/false statement represented by a 0 or 1 (off or on). When the tag enters an interrogation zone the security bit will then be checked for its status, similar to the tattle tape magnetization at security gates. This one-bit security system may be supplemented or replaced by using a database containing the check out status of an item. Using this method would require the reader to acquire the item's serial number from the transponder, and then to query the database using the serial number. This alternative system is more time consuming as it must indirectly access this data from a database via multiple transmissions instead of reading it directly from the tag.

Advantages

In 2003, Karen Schneider gave a report to the California Senate's Committee on Energy and Utilities summarizing the current benefits and problems with incorporating an RFID system in the library. Comparing her list with those provided by Boss (2004) and Smart (2004) provide a fairly comprehensive list.

A very big benefit to becoming more automated by using an RFID system is the amount of injury reduction to the staff caused by repetitive motions due to checking in and out materials among other duties. Smart's article gives an example of the statistics found at the San Francisco Public Library, where a reported 768 "risky motions" were performed each hour by the circulation staff. The lost staff time and costs caused by these injuries over a three year period totaled 260 missed work days, 500 hours adjusting duties to accommodate for injuries, and a large sum of $265,000.

Another large advantage that contributes to the reduction of repetitive motion injuries is the simplified self check-in and check-out capabilities. This is possible because once the patron enters the interrogation zone, the reader finds the transponder and can change the status of those linked database records once the patron has scanned in his/her card. Smart emphasizes the impact of this ability not only on the staff and their benefits, but on the "wow" factor of the patrons when they are able to set a pile of books down and have a computer screen "automagically" read and display all of the titles. Without the need to directly position a barcode underneath a laser greatly reduces the amount of time down to a seemingly simultaneous check out as well as makes it easier overall. Having self check-in and check-out windows also empowers the patron, ensuring them that materials are properly checked in (or at least cannot directly accuse the staff) and gives them a sense of freedom.

The next highly useful feature of an RFID system is the ability to streamline inventory management. Many hours can be spent with staff combing the stacks to ensure materials are in proper order, and so many libraries are unable to do any sort of inventory checking at all. Shelf-reading can be greatly simplified by using a portable reader also known as a wand. This wand can read all of the transponders on a shelf as it is waved past them and register what materials are out of order or missing. For example, California State University, prior to the RFID system taking inventory was inconceivable. However, using the new inventory wand, librarians are able to inventory about 5,000 books an hour. This is very cost effective, since books declared lost or missing (especially when the book is simply misshelved) need to be replaced thus becoming very

expensive. The University of Nevada, Las Vegas reported to have found 500 lost materials in its 600,000 item collection, a savings of nearly $40,000 in replacement fees. California State University, in a partial inventory, reported to find at least 300 missing items. Hence, inventory checks increase catalog accuracy and reliability while lowering unnecessary replacement fees.

A possible addition that increases reliability while lowering repetitiveness in work duties is one not widely used. This is the costly automated materials handling. Essentially, a conveyor belt is installed at the base of a book drop and immediately processes all the materials placed in it by the patron without any human supervision. With the RFID tags, the built in readers on the conveyor belts are able to read whether a book needs to be sent to a different location or where in the library the item needs to go. Several carts are set up for each type of item and mechanical arms push the items down the correct conveyor belts to be sorted onto a cart.

Overall, by automating the library with one or many of these features reduces the human labor involved in the basic needs of the library, allowing for public service to become the primary prerogative for the actual library staff rather than materials processing.

Disadvantages

As with the advantages, Schneider, Boss, and Smart point out several disadvantages to installing an RFID system. The predominant problem is cost. Boss' article provides a basic budget plan for a library looking at installing RFID technology, although costs vary greatly based on features a library wants, the types of tags they choose, the size of a collection, and the amount of staff or volunteers they can find in order to implement the new tags. Cost of tags can vary anywhere between $0.40 and $1.00 per tag, still very expensive at a per tag level. Other mandatory costs include a temporary converter station, staff stations (approximately $2,500 each), exit sensors (about $4,000 each), inventory wand ($4,500), a server or docking station ($15,000), and a number of hours to convert from barcodes to tags. Since about three tags can be converted a minute, a small library can do this using about 250 hours where a larger library can see putting at least 1400 hours of labor towards conversion alone. Boss estimates that small libraries with about 40,000 items should budget at least $70,000 towards the project while large libraries of at least 250,000 items should look at a budget no less than $333,500. During a time of financial difficulty for most libraries, this particular route may not seem to be the most logical. Smart suggests looking at ROI (return on investment) to calculate out whether the short term costs of installing the RFID system are greater or less than the long term costs caused by repetitive motions and lost materials among other things. Others feel they can find more effective means of spending money such as buying newer furniture, attending conferences, or conversion of classification systems (Ferguson, 2004).

Another huge concern and arguably the largest problem is the perceived invasion of privacy. Two things Boss wanted to clarify about this particular issue is that patron information is not directly stored on the transponder, and that whatever data is directly stored on the transponder could be read once the item left the library. This particular concern correlates with the possibility of tracking each patron's reading habits and/or hotlisting particular library materials, both issues being huge security flaws that Molnar and Wagner describe in detail and are major arguments privacy advocates use (Heining, 2004). Concern of hotlisting and tracking exists at multiple levels; individuals might

invoke this peeping as well as institutions or even the government. Because the 13.56 MHz radio frequency can be replicated by other portable devices such as PDAs, the authors fear that people may program handhelds to read data residing on tags, in essence tracking and hotlisting from an external source that may cause even greater concern (Molnar and Wagner).

Even the one-bit security data is at risk as it can inform the exit sensors whether the item is checked in or checked out. If a person was able to manipulate this one bit from a 0 to 1, it would not set off the security alarms similar to demagnetizing the tattle-tape in the binding of a book. One way to protect against such attacks is to have the exit sensors send a query to the circulation database to check its status there rather than on the tag. This, as mentioned before with authentication keys, increases the response time length invariably decreasing the efficiency of the security feature. Other security issues that arise from using radio frequency is that wrapping the item in tin foil will essentially "wet" the frequency waves so the reader cannot find the transponder. This particular issue should especially concern the library as tin foil is not difficult to get into the library.

Another very serious security flaw that Molnar and Warner point out is the use of read write tags without protecting the data contained on the tags. Without locking the information with some sort of encryption key, anyone with some basic knowledge as to how encryption and data transfer work could hack into a tag and erase the data, and can even go a step further by locking it after erasing the data, rendering the tag useless. According to statements made throughout their report, security and RFID technology have not developed enough for mass implementation in the library due to the costs of upgrading after converting to RFIDs (mentioned in more detail later).

Another concern that is similar to wrapping an item in tin foil is simply removing the RFID tag all together. While similar issues arise with barcodes and the use of tattle-tape, many patrons are unaware that it is the tattle-tape in the binding that sets off the security alarm and not the barcode. With RFIDs, the transponder is very visible as it is typically attached to the inside of the back or front cover of a book. Simply removing this renders the tag useless to the item.

A combination of expense and outdated software and hardware comprise of another concern RFIDs introduce. Because many flaws do still exist mostly in security, transponder software and hardware upgrades will most likely occur. The cost of converting from a barcode system to an RFID system is expensive to begin, and then for a library to have to upgrade all of its materials again would be a great set back and detrimental for many of the benefits RFIDs bring such as lowered labor hours. Libraries have been warned to be very cautious in making a decision to move to this new system, and to wait while these upgrades are verified and implemented by transponder manufacturers.

Issues outside of the actual RFID system itself deal with a lack of staff knowledge, training, and understanding of the security issues and general mechanics of an RFID system. While it is fairly safe to assume most of the active librarians have either been brought into the profession using the barcode standard system of today or else became accustomed to it over the years, virtually no librarians have had extensive training and contact with RFID systems. While some companies provide training to library staff, comfort with the new technology is low. Because it is such a new technology, many concerns arise with the extended lack of interoperability with other libraries and organizations for services such as interlibrary loan. Essentially, if only one branch

upgrades its technology, it becomes an outcast to its other branches as its identification tags are unreadable by their scanners.

One final issue mentioned is how dependent the library is on legislation at the local, state, and national levels. With recent acts such as the PATRIOT Act and other anti-terrorism bills, libraries are increasingly susceptible to privacy intrusion. Although this issue extends beyond RFID systems, the increased tracking and hotlisting ability RFID tags provide enhance the legislature's ability to misuse the technology. Ayre (2004) sees librarians as being extra cautionary in protecting patrons' information with this recent legislation, but then contradictory by increasing tracking capabilities.

Current Library Implementation

So far, approximately 200 libraries around the world have implemented some degree of RFID technology. Of that, about 130 of them exist within North America. Most of the libraries that have begun implementing the new system are small branch libraries (Ayre, 2004). In North America, six companies produce RFID systems and provide varying degrees of other services. Different RFID tag manufacturers include Bibliotheca, Checkpoint, ID Systems, Libramation, 3M and TAGSYS (Tech Logic, Vernon, and VTLS). Of all the companies mentioned, only Tech Logic provides the most comprehensive product catalog for self check-in/check-out machine systems that work for all brands of RFID systems (Boss, 2004).

Overall, it is very apparent that many benefits arise from using RFID systems in libraries, especially if in measuring the ROI it balances out the short term high expenses to the long term savings or even returns a surplus. However, current security flaws as noted in detail by Molnar and Wagner provide significant evidence that libraries should hesitate or at least be very cautious in choosing to switch their systems before tags strictly manufactured for library use are standardized and security holes fixed. Implementation can only be determined at a library level as each library is unique in its needs and resources.

Bibliography

Ayre, L.B. (2004 August 19). Position Paper: RFID and Libraries. Retrieved 11/14/2004 from http://www.galecia.com/included/docs/position_rfid_permission.pdf

Boss, R.W. (2004 May 14). RFID Technology for Libraries. Retrieved 9/13/2004 from http://www.ala.org/ala/pla/plapubs/technotes/rfidtechnology.htm

Ferguson, A.W. (2004 June), "Back Talk – RFID." *Against the Grain*. v. 16, no. 3. p. 93-4.

Finkenzeller, K. (2003). RFID Handbook : Fundamentals and Applications in Contactless Smart Cards and Identification. 2nd ed. John Wiley & Sons : West Sussex, England.

Heining, A. and Case, C. (2004 October 5). Are Book Tags a Threat? *Christian Science Monitor*. v. 96, iss. 218. p.17.

Molnar, D, and Wagner, D. (2004 June 8). Privacy and Security in Library RFID: Issues, Practices and Architectures. Retrieved 10/20/2004 from http://www.cs.berkeley.edu/~dmolnar/library.pdf

Schneider, K. (2003). RFID and Libraries: Both Sides of the Chip. Testimony presented at Committee on Energy and Utilities, California Senate, 11/20/2003. Retrieved from http://www.senate.ca.gov/ftp/SEN/COMMITTEE/STANDING/ENERGY/_home/11-20-03karen.pdf

Smart, L. (2004 October 15). Making Sense of RFID. *Library Journal*. Retrieved 11/20/2004 from http://www.libraryjournal.com/article/CA456770

Thomas, S, Schaper, L, and Ford, R. (2004 October 15). Fayetteville's Quest. *Library Journal*. Retrieved 10/20/2004 from http://www.libraryjournal.com/article/CA456765