RFID & Privacy within Libraries – Myths, Misconceptions and The Future

No subject has so polarised libraries in recent years as the potential risk to personal privacy brought about by the introduction of Radio Frequency Identification (RFID) systems. Particularly in the United States of America has the debate become fierce with lobby groups attempting to stop libraries migrating to this new technology.

It can be extremely difficult for Australian libraries to accurately gauge the risks to the privacy of their borrowers in the context of rhetoric which at times borders on the hysterical and is often misinformed. The RFID application space is vast and spans multiple technology platforms and standards of which libraries are but a small part. Observations made regarding one application are not necessarily valid in another application. The goal of this paper is to provide an overview of the perceived threats, to probe their technical feasibility and to present a clear picture of what may and may not be done by libraries to mitigate the risk that actually exists. The current RFID standards are also examined in the context of privacy and their limitations are weighed.

The paper concludes by exploring what could be done in the future by commercial RFID vendors to maintain compatibility with standards while maximising the data security and therefore borrower privacy of their systems.

1. Introduction

"RFID Should be restricted by the state – Radio Frequency ID can be a boon, but who is tracking the trackers?" This headline appeared above an article (Mather and Wiebell, 2005), in *Information Age*, the bi-monthly journal the Australian Computer Society. The authors went on to discuss scenarios where RFID transponders could potentially compromise the privacy of those who possessed them, including "tiny tracking devices the size of a grain of dust" which may be embedded in articles of clothing etc and used to track their unsuspecting wearers.

In the United States of America we have seen lobby groups formed with the goal of keeping RFID out of specific libraries (O'Connor, 2005; EFF, 2005). Commentators have urged us to delay the implementation of RFID in libraries until the privacy problems are solved (Ayre, 2005), or to drastically limit the amount of data stored on RFID tags used in libraries (ibid).

Much of the debate is conducted in an emotive fashion. Often the level of understanding regarding RFID technologies is minimal on the part those involved. How then are we to judge the nature and seriousness of the problem? In this paper I will attempt to disassemble the various components of concern and analyse which threats are realistic and which might be imagined. In many cases, this can be done by reference to the technology

platform on which library RFID systems are based. The paper also considers the vulnerabilities inherent within the standards on which current library RFID systems are built. The paper progresses by listing the perceived threats, considering the current technology platform employed within library RFID, and then analysing the threats in the context of this platform. The discussion is framed by the library application of RFID and the specific concerns that might apply to the privacy of library users following an implementation of RFID technology.

2. Privacy / data security concerns

Broadly, the most common discussions regarding privacy threats due to reduced data security in RFID systems can be sorted into two categories. The threats in each category are presented as an overview and then are considered separately in more detail.

1. Threats involving the privacy of the borrower
    - Tracking
    - Hotlisting
    - Profiling

2. Threats involving the library's collection
    - Theft of library material
    - Digital vandalism
    - Tag-based viruses

2.1 Overview of threats involving the privacy of the borrower

The threats in this category all have a common theme; an antagonist (government, terrorist, criminal, corporate etc) uses RFID technology in a covert manner to read data from tagged library items carried by the individual. The data is then used in several ways determined by the specific threat. In the case of *tracking*, data from the RFID tag is used to monitor the whereabouts or movements of a specific individual. A scenario has been suggested (Albrecht, 2006) where RFID systems become ubiquitous within society (perhaps due in part to extensive RFID use by the retail sector) and enable an antagonist to make multiple observations of an individual by means of the RFID tags carried, including those contained in library material. These observations may be correlated with observations of other individuals to determine associations between persons. The observations may also be used to track locations visited by individuals on specific days or at specific times.

In the case of *hotlisting*, the antagonist's intention is to match individuals with known RFID identifiers. An example often given relates to the ability to scan individuals at airports before they board an aircraft (Molnar and Wagner, 2004). In this scenario, an RFID antenna is configured as part of the security screening process and individuals with specific library material or material borrowed from specific institutions are diverted for additional attention by the security staff. Another scenario involves a covert RFID antenna at a public

library, linked to a tiny camera which records the image of individuals who exit the library carrying specific material types or titles. It has been suggested that the use of almanacs can be an indicator of terrorist preparations and so individuals using or borrowing this type of material may be subjected to closer scrutiny (CNN, 2003).

The third threat, *profiling*, involves correlating specific types of library material with typically demographic, ethnographic or religio-political information regarding the borrower. One scenario sometimes presented as an illustration of this threat is the occasion when a law enforcement officer pulls over a vehicle with several passengers (Molnar and Wagner, 2004). Using a portable scanner, the officer determines that library items from a specific library are present in the vehicle. The library in question may have a particular religious affiliation or be located in an area where persons of interest to the law enforcement officer are known to reside. In this case, merely possessing an item from such a library might result in closer scrutiny of the individuals. Alternatively, individuals from specific ethnic backgrounds may trigger an alarm from covert observations when they have specific types of library material in their possession.

Another form of profiling consists of determining the reading habits of individuals by scanning the RFID tagged items in their possession without them being aware of it. There are anecdotal stories that appear in the popular media occasionally describing how the library material in a household might be scanned by government agents hovering in a helicopter or located in a van across the street. Perhaps even perched, sniper-like, on the roof of a building opposite with a high-powered RFID reader at their disposal. It is perhaps this particular threat that evokes the greatest outrage from the public as it clearly forms a seemingly indefensible invasion of privacy.

2.1 Overview of threats involving the library's collections

Theft of library material may be achieved in several ways by exploiting the weaknesses in most, but not all, library RFID systems. The very nature of RFID that serves to offer benefits to libraries, that of non-line-of-sight operation, can be exploited by a knowledgeable and well equipped adversary. The majority of systems targeted at the library market employ RFID tag-based security methods. It is technically conceivable that an individual possessing a portable RFID system may covertly alter the state of the tag based security data, thus disarming the security. RFID library systems employing non-tag-based security are, of course, not vulnerable to this specific threat.

The possibility also exists for a borrower to switch or clone tag data once items are removed from the library in the way that, with patience, physical barcodes could be switched. This might allow an individual borrowing two items to report an inexpensive item as being lost (and subsequently paid for) while actually retaining the more expensive one. Of course, armed with the portable RFID system mentioned earlier and an appropriate understanding of the technology, an antagonist could switch tag data before the loan to accomplish a similar objective.

Digital vandalism might take many forms but could include erasing RFID tag memory, locking the security data to prevent a range of items from leaving the library (a type of denial-of-service attack), and overwriting valid tag data with scrambled or malicious data. It has also been demonstrated that a self replicating tag-based virus is possible under certain controlled situations such as within a supermarket distribution centre (Tanenbaum et al, 2006). While it might be arguable that memory capacities within RFID tags currently employed in the library application are insufficient to allow this kind of attack, it would be premature to say that it couldn't be done under any circumstances.

3. Current RFID Standards within the library application space

Two standards dominate the RFID solutions currently available to libraries:

- ISO/IEC 15693
- ISO/IEC 18000-3 Mode 1

For the purposes of a discussion regarding RFID security, these two standards may be considered as identical. In fact ISO/IEC 15693 is a perfect subset of ISO/IEC 18000-3 Mode 1.

Unfortunately, these standards cannot provide the basis for a truly secure RFID architecture. There are several vulnerabilities within these standards to some of the of threats listed previously and several of these are briefly considered.

3.1 Tracking

The key to the tracking threat is the ability to discover a data element on the RFID tag which can then theoretically be used to make multiple observations of the unsuspecting subject. The primary item ID of the library item is an obvious candidate as it is almost always required for the item to circulate. Unfortunately, even if the RFID tag had no library data written to it at all, every tag has a unique manufacturer's number encoded in the system area of the tag's memory which may serve the purpose of a tracking adversary (Molnar and Wagner, 2004). As part of the normal collision avoidance protocol under the two standards mentioned, this manufacturer's ID is "leaked" and could be detected by a covert reader (ibid). This collision avoidance protocol is part of the normal operation under the standards when multiple tags are present in the interrogation field. The manufacturer's number is used by the RFID interrogating device to enable it to address the RFID tags individually and is not encrypted in any way.

In the case of the tracking threat, it doesn't matter what particular data is read from the tag and any tag operating under the standards mentioned will transmit its manufacturer's ID number when asked to do so. Furthermore, the standards do not provide for any sort of reader authentication. From the perspective of the RFID tag, all readers are trusted and so there is no

mechanism within the standard to discriminate between authorised and unauthorised readers. Password protection of the tag data is also weak.

3.2 Hotlisting and profiling

Both of these threats usually assume that some library data external to the RFID tag will be available to the antagonist. In the case of *Hotlisting*, an association needs to be established between the title of the item and the primary item identifier (assuming that the title is not encoded in the RFID tag). There are several ways that this association could be determined. Items of interest to the antagonist may simply be borrowed and the details of the tag data determined. Alternatively, the antagonist might use a portable and covert data collector to scan selected items within the library to establish which tag ID corresponds to which title. As mentioned previously, the tags will reveal at least their manufacturer's ID (and probably more) to any reader that requests it. Finally, if the primary item ID within the tag is the same number as that on the library database (the original barcode number in most cases), then a hacker attack on the library's system would reveal the needed information. Of course it's entirely possible that even with a barcode-based system, a well resourced antagonist could determine which borrowers have specific material on loan by accessing the library's database. The concern with RFID appears to be the covert way in which the material can be detected at specific points (Givens, 2006).

In attempting to *Profile* an individual, the antagonist must also determine something about the nature of the library material carried by the individual under scrutiny. If the primary ID is available, this may indicate which library loaned the material. If libraries have specific ID prefixes or particular number ranges, this data serves to identify the source of the material. If the owning or circulating institution data is available (perhaps encoded in the tag for the purposes of inter-library loan) then the task is greatly simplified.

3.3 Digital vandalism

Once again, the standards do not provide strong protection against the attacks mentioned earlier. The principal vulnerabilities are listed below:

- RFID tags adhering to the standards mentioned previously do not support read passwords or other read-access controls.
- No reader authentication is provided within the standards and so the tags will communicate with any reader, including unauthorised ones.
- If a security bit within the data encoding area is used for item security, the block containing this bit may be locked by an antagonist thus rendering the security inoperable (and preventing the item to which the tag is attached from being circulated by the library).
- As the standards don't include password protection for "write" commands, tag data contained in non-locked blocks may be overwritten by an antagonist with a suitable portable RFID device.

It should be noted that RFID systems with architectures that do not require data to be written to the tag for normal operations and instead use proprietary Write-Once-Read-Many (WORM) tags are protected from many digital vandalism attacks. Some systems that employ proprietary EAS technology for item security may also be immune to security bit denial of service attacks.

4. Evaluation of the threats

What are we to make of all this? Should libraries migrate to RFID technology or should the borrower-privacy and data security issues be significant enough to deter them? Which of these attacks are realistic and which represent a flight of fantasy?

We could perhaps begin by dealing with those attacks that simply could not take place due to the restrictions within the 13.56 MHz RFID technology platform used by libraries. These systems employ passive tags which are inductively coupled to the reader and communicate via load-modulation. This simply means that the tags derive all of their power over the air-interface with the reader and must lie within the near-field of the reader's antenna to operate. Without delving too deeply into the detail involved, the essential point is that, at 13.56 MHz, the maximum operational range of the passive tag is approximately 3.5 metres (Finkenzellar, 2004). This range limit applies regardless of the reader's power and is set by the physics relating to the radio wave's propagation.

So, scanning RFID tagged library materials from helicopters hovering in the sky is simply not possible. Neither is it possible to scan from a rooftop across the street or a van parked on the opposite side of the road. However, it may be entirely possible to scan at a security point or a building doorway with hidden equipment. Scanning may also be possible at other service points (such as retail outlets) where suitable equipment exists.

Any objective discussion of data security should take into account who the antagonist might be and what is the value to this antagonist of that which we seek to protect. These two considerations directly inform the reasons why the local bank chooses to spend significantly more on security systems than perhaps does the local florist.

So who are the antagonists in our case? Who is it that wants to track or profile library users? To wreak vandalism on library collections? Perhaps we could suggest that these antagonists fall into two broad categories which, for want of better terms, we might label the Vandals and the Snoopers.

4.1 The Snoopers

Anecdotal evidence would suggest that most discussion characterises the Snoopers as government agencies (spies or police), organised criminals, or terrorists with perhaps government agencies as the most likely candidates and terrorists the most feared. Also anecdotally there have been reports of government agencies requesting lists of items borrowed by specific

individuals from libraries, thus cementing their position as the most likely antagonists. Each library must weigh the likelihood that such agencies would engage in nefarious activities by means of library technology or whether traditional methods of surveillance would be more practical. The fact that something might be technically possible does not mean that it is necessarily the best method. In the case of terrorists, for example, it is not clear what, beyond a limited ability to detect regular citizens at certain points, is really to be gained by tracking library items. Particularly when we put possible RFID terrorist threats into the broader commercial and community context. The United States of America, for example has recently passed legislation requiring all new car tyres to be uniquely traceable. Major tyre manufacturers plan to use RFID tags in each tyre to comply with the new regulations (Roberti, 2005). Here in Australia, as in other countries, many vehicles including VIP vehicles (toward which terrorists display a preference as targets) carry an RFID tolling device which may be read from a distance and at speed (Allen, 2006). Naturally, privacy advocates will not accept an argument attempting to justify more RFID devices in the community based on existing proliferation. Clearly, each library will need to make a determination of whether borrowers are needlessly imperilled by the migration to RFID.

4.2 The Vandals

In discussions of such matters, often the privacy issue becomes foremost and the issue of possible digital vandalism slips into the background. While both are legitimate data-security issues this is perhaps understandable as the risk to the library's assets may be one that the organisation may choose to accept whereas the risk to the borrower is regarded as one that should remain within the borrower's ability to control. However, high-tech vandalism has a had a long and celebrated career among a certain sector of the population, most often visible through hacking attacks on large organisations and the release of software viruses. Given the fact that RFID reader and antenna technology is freely available and may be purchased on the Internet, it might be considered to be inevitable that an incident will occur at a library somewhere in the world. How often this might happen and how severe the consequences might be is, of course, not possible to say at this early stage. It should not be overlooked however, that the level of technical complexity required for digital RFID vandalism is significantly less that that required to breach complex network security (Molner et al, 2006).

So how to make a subject judgement? Perhaps one conclusion might be that the risk from The Snoopers is very small but will require the most effort to manage in a public-relations context whereas the risk from The Vandals is larger, perhaps even inevitable (ibid) but has largely internal consequences and requires a technical rather than a social effort.

5. Possible steps to mitigate risk

It may be considered infeasible to protect the privacy of library borrowers from the well resourced and determined agencies of their own government – often the prime suspect in the case of RFID security concerns. The following is a list

of possible actions, their implementation to be based on the perceived level of threat:

- Don't use RFID tags for borrower cards – if an RFID borrower card is required, employ specific, purpose-built smart-card technology, not a laminated RFID tag.
- Reduce the amount of data on each RFID tag – putting only the primary item ID on the tag may assist in the customer-relations effort where privacy is expected to be an issue.
- Don't allow bibliographic searches by the public using the barcode – this reduces the likelihood that the item identifier and the title can be linked.
- Ensure that transparency exists with regard to library RFID projects – this serves to help manage expectations and fears within the population of library users. Several high profile cases of covert RFID testing have been exposed in the retail area and have generated much negative publicity for the organisations involved.
- Review security procedures generally – as some of the attacks outlined depend on matching other information with the data on the RFID tag, ensure that the library is secure in all its practices and policies, particularly in the area of information and communications technologies. Consider a specialist audit.
- Lobby vendors for improved security solutions – while not of immediate benefit, much development work could be done to improve the security status of RFID systems based on current standards. These include:
    - Development of anonymous ID systems using randomly generated numbers on issued tags paired with real accession numbers on the library database.
    - Improved authentication of readers.
    - Improved password protection.
    - Solutions based on ISO/IEC 18000-3 Mode 2
- Support research into library specific solutions for current RFID privacy concerns.

6. Conclusion

Current standards do not offer a platform for secure RFID systems and have several vulnerabilities which may permit both theoretical privacy-compromising activities as well as acts of digital vandalism. Current RFID chips are also not capable of handling many high-level encryption tasks due to their low memory capacity and processing power.

Many of the scanning and tracking threats which may or may not be possible on other RFID platforms and which are often publicised in the popular media are not possible with library-standard 13.56 MHz tags. Some of the threats considered involve matching the tag data with other information about the item and so where privacy is likely to be an issue, the tag data should be confined to the primary item ID only. Libraries implementing RFID for item

identification should also review their general security policies at the same time.

Each library needs to make an individual decision regarding the risk / benefits of a migration to RFID and should ensure that the public is aware of the project and that opportunities to address any security concerns that borrowers might have are provided for. The need for education for library staff and borrowers to enable them to accurately asses the real risk factors is ongoing.

Library professional bodies can do much to assist in raising awareness of the issues and perhaps in working toward a code of best practice for RFID enabled libraries, mirroring work that continues in other RFID application areas (Lahiri 2006).

References

Albrecht, K. (2006) *RFID: The Doomsday Scenario*. RFID Applications, Security and Privacy, Addison Wesley, 259-273

Allan, B. (2006) *Texas Instruments – lessons from successful RFID applications.* RFID Applications, Security and Privacy, Addison Wesley, 360-361

Ayre, L.B. (2005) *Wireless tracking in the library: Benefits, Threats, and Responsibilities,* RFID Applications, Security and Privacy, Addison Wesley, 229-243

CNN.Com *FBI urges police to watch for people carrying almanacs*. Retrieved from http://www.cnn.com/2003/US/12/29/fbi.almanacs.ap/

Electronic Frontier Foundation (2005) *Keep RFID's out of Californian Public Libraries!* Retrieved from http://www.eff.org/Privacy/Surveillance/RFID/

Finkenzeller, K., (2004) *RFID Handbook - Fundamentals and applications in contactless smart cards and identification*. Wiley 114

Givens, B (2006) *Activists: Communication with consumers, speaking truth to policy makers.* RFID Applications, Security and Privacy, Addison Wesley, 432

Lahari, S., (2006) *RFID Sourcebook*, IBM Press. 101-111

Mather, K. and Wiebell, H. (2005) *RFID should be restricted by the state.* Information Age December 2005 / January 2006 - Australian Computer Society

Molnar, D. and Wagner, D., (2004) *Privacy and security in library RFID - Issues, practices and architectures* CCS'04 October 25-29 2004 Washington DC, USA

Molner, D. and Stapleton-Gray, R. and Wagner, D. *Killing, Recording and Beyond.* RFID Applications, Security and Privacy, Addison Wesley, 353

O'Connor, MC., (2005) San Francisco Library denied funds for RFID. RFID Journal. Retrieved from http://www.rfidjournal.com/article/articleview/1708/1/1/

Roberti, M (2005) *Auto Industry RFID Standard Proposed* Retrieved from http://www.rfidjournal.com/article/articleview/2043

Tanenbaum, A. and Crispo, B. and Rieback, M. (2006) *Is Your Cat Infected with a Computer Virus?* Retrived from http://www.rfidvirus.org/papers/percom.06.pdf