RFID & Privacy within Libraries

Myths, Misconceptions and the Future

ALIA Conference - Perth WA, September 2006
Discussion outline

- Introduction to RFID privacy issues
- Current RFID Standards within libraries
- Threats involving the privacy of the borrower
- Threats involving the library’s collections
- Vulnerabilities, myths & subjective assessment
- Possible risk mitigation steps
Discussion outline

- Introduction to RFID privacy issues
- Current RFID Standards within libraries
- Threats involving the privacy of the borrower
- Threats involving the library’s collections
- Vulnerabilities, myths & subjective assessment
- Possible risk mitigation steps
RFID Data Security & Privacy

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

Threats involving the library's collections
- Theft of library assets
- Digital vandalism
Discussion outline

- Introduction to RFID privacy issues
- **Current RFID Standards within libraries**
- Threats involving the privacy of the borrower
- Threats involving the library’s collections
- Vulnerabilities, myths & subjective assessment
- Possible risk mitigation steps
RFID standards in libraries

Library
Database

- Staff loans
- Self Serve loans
- Collection management
- Security gates

ISO 15693
ISO 18000-3

RFID tag

Air
Discussion outline

- Introduction to RFID privacy issues
- Current RFID Standards within libraries
- Threats involving the privacy of the borrower
- Threats involving the library’s collections
- Vulnerabilities, myths & subjective assessment
- Possible risk mitigation steps
Threats to borrower privacy

Tracking - determining a unique tag identifier

- Discovering the barcode:
  - Allows possible cross referencing to library database
  - Reading profiles can be generated
  - Material-type to person-type matches
  - Person tracking (ubiquitous network scenario)
  - Personalised marketing (ubiquitous network scenario)
Threats to borrower privacy

Tracking - determining a unique tag identifier

**Discovering the tag’s unique ID:**
- Allows tracking through multiple item observations
- Allows correlated book-person observations
- Material-type to person-type matches
- Person tracking (ubiquitous network scenario)
Threats to borrower privacy

Hotlisting

- Checking transactions against lists of suspects:
  - Allows matching at any point with covert readers
  - Screening at airport check in, etc
  - Library ID not necessarily required
  - FBI has already demonstrated an interest - e.g. Almanacs
Threats to borrower privacy

Profiling

- Material types matched with borrower demographic:
  - Association of specific groups with known items
  - Association of specific groups with particular libraries
Discussion outline

- Introduction to RFID privacy issues
- Current RFID Standards within libraries
- Threats involving the privacy of the borrower
- Threats involving the library’s collections
- Vulnerabilities, myths & subjective assessment
- Possible risk mitigation steps
Threats to library collections

Theft of library assets

- Security bits changed - items not detected
- Tag identities swapped
- Tag identities cloned
Threats to library collections

Digital vandalism

- Tag data overwritten
- Swapping tag information
- Security bit memory locked - denial of service
- Self replicating tag viruses
Introduction to RFID privacy issues
Current RFID Standards within libraries
Threats involving the privacy of the borrower
Threats involving the library’s collections
Vulnerabilities, myths & subjective assessment
Possible risk mitigation steps
Vulnerabilities of RFID technology

Discovering the item’s ID number (barcode)

- No **Read** password in ISO 15693 or 18000-3 mode 1
  - The item ID may not be encrypted
- No reader authentication process in current standards
  - Tag will respond to appropriate command from any reader
Discovering the Tag’s ID (manufacturer’s number)

- No *Inventory* password in ISO 15693 or 18000-3 mode 1
  - The library tag will offer its 64 bit ID if asked
- The tag’s ID may leak during collision avoidance process
  - Multiple *mask queries* reveal the Tag’s unique ID
  - Coded at a very low level - privacy unachievable
Vulnerabilities of RFID technology

Matching numbers with titles

- Library’s database may be hacked
- Adversary may scan specific books while on shelf
- Tracking can be accomplished with any identifier
RFID Myths & Misunderstandings

RFID operating range is all about reader power

ISO 15693 / ISO 18000-3 tags are inductively coupled

- Employ load modulation for signaling
- Operate ONLY in the nearfield of the antenna
- Nearfield = \( \omega / 2\pi \)
- 13.56Mhz wavelength is 22.1 metres
- \( 2 \times \pi = 6.3 \)
- \( 22.1 / 6.3 = 3.5 \) metres absolute maximum range
RFID Myths & Misunderstandings

Eavesdropping is possible from great distances

An inductively coupled tag’s signal is very weak

- Approximately 100,000 times weaker than the reader signal
- In theory radio waves propagate infinitely
- In reality the tag’s signal is soon swamped by noise
Conclusions

ISO 15693 / 18000-3 Mode 1 is not a secure platform

- No reader authentication
- Poor password protection
- Unique tag ID leaked during collision avoidance
- Security bit denial of service attacks possible
Conclusions

ISO 18000-3 Mode 2 has security potential

- Has potentially private collision avoidance scheme
- Better password protection
- Would still require an anonymous ID scheme
- May require better password management
Subjective security assessment

Who are the adversaries & what are their objectives?

Government agencies (CIA, FBI, ASIO, Police etc)
- Using library RFID to track the movements of suspects
- Using library RFID to profile individuals
- Using library RFID to track reading patterns of suspects

Level of protection

<table>
<thead>
<tr>
<th></th>
<th>Subjective threat assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Standards</td>
<td>Some threats possible -</td>
</tr>
<tr>
<td></td>
<td>Uncommon</td>
</tr>
<tr>
<td>Future Standards</td>
<td></td>
</tr>
</tbody>
</table>
Subjective security assessment

Who are the adversaries & what are their objectives?

Covert commercial operations

- Want to gain competitive advantage
- Using library RFID to profile customers

<table>
<thead>
<tr>
<th>Level of protection</th>
<th>Subjective threat assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Standards</td>
<td>Possible - Unlikely</td>
</tr>
<tr>
<td>Future Standards</td>
<td></td>
</tr>
</tbody>
</table>

Subjective threat assessment

Possible - Unlikely
Subjective security assessment

Who are the adversaries & what are their objectives?

Terrorist organisations

- Using library RFID to track targets

<table>
<thead>
<tr>
<th>Level of protection</th>
<th>Subjective threat assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Standards</td>
<td>Possible - Unlikely</td>
</tr>
<tr>
<td>Future Standards</td>
<td></td>
</tr>
</tbody>
</table>
Subjective security assessment

Who are the adversaries & what are their objectives?

Malicious independent vandals / thieves

- Want to steal library items
- Want to create technical mayhem

**Level of protection**

<table>
<thead>
<tr>
<th>Current Standards</th>
<th>Subjective threat assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inevitable - Uncommon</td>
</tr>
</tbody>
</table>

**Future Standards**

- 😊
Discussion outline

- Introduction to RFID privacy issues
- Current RFID Standards within libraries
- Threats involving the privacy of the borrower
- Threats involving the library’s collections
- Vulnerabilities, myths & subjective assessment
- Possible risk mitigation steps
What can be done

Limit the data on the tag to the library ID only

- Limits the functionality offered by storing other data
- If the library database is compromised - privacy is affected
- Does not stop tracking & hotlisting scenarios

Encourage vendors to develop a secure ISO based model

- Consider ISO 18000-3 Mode 2 tags and readers
- Develop anonymous ID schemes (Ohkubo et al)
- Enhance password protection (Molnar et al)
- Develop strong authentication protocols
- Consider dynamic data profiles
RFID & Privacy within Libraries

Myths, Misconceptions and the Future

To obtain a copy of the handouts from this presentation visit www.sybis.com.au