Near Field Communication (NFC) and the use of Radio Frequency Identification (RFID) in Libraries. – Some information for librarians.

Radio Frequency Identification (RFID) is now widely used in libraries for a whole range of activities from self-issue and return, security, stock management, sortation and more.

Members of the public increasingly use smartphones for a wide range of activities and these two technologies, smartphones and RFID now meet in libraries where smartphones with NFC (Near Field Communication) use the same radio frequency as RFID.

So now is a good time to consider the possible impact of smartphones (and tablets) on library systems using RFID.

What are the possible negative implications of this joining of technologies that library managers should be aware of, and what steps might mitigate any potential threat? This document seeks to answer these questions.

RFID, Smartphones and NFC

The term "RFID" covers a wide range of products, devices and frequencies and many UK libraries use it for stock tags operating at the standard frequency, 13.56MHz. This frequency is now also used by smartphones and tablets equipped with NFC (Near Field Communication).

NFC is an extremely low-power, close-contact/contactless, type of RFID technology, designed primarily for use in vicinity-based RFID applications where information needs to be transferred wirelessly and often securely. Examples of NFC applications include payment (e.g. Google Wallet and PayPass by MasterCard) and mobile-to-mobile (cell phone) interactions.

Many smartphones are now supplied with NFC technology on board. A list of the devices that currently support this technology is maintained at http://en.wikipedia.org/wiki/List_of_NFC-enabled_mobile_devices

Librarians interested in finding out more about RFID standards should look at the resources available on the BIC website at: http://www.bic.org.uk/e4libraries/11/RFID-/

Threats and risks

There are three main ways in which library RFID tags are at risk from NFC – digital vandalism, theft and data locking.

Digital Vandalism

The most direct and most probable threat comes from digital vandalism. Data on tags is simply overwritten with random (or even structured) input generated by an NFC-equipped device.

The most likely consequence of such an act would be to render the item unrecognisable to the RFID application, the Library Management System or both.

In a 'worst case' scenario a perpetrator with knowledge of the standards used by libraries – or with the motivation to decipher the meaning of non-standard data – could selectively alter data elements to deliberately disrupt the systems' item recognition algorithms.

Because of the way in which RFID systems handle security (see below) there is however no guarantee (for the perpetrator) that they will reprogram the correct data bits that would allow it to pass security gates. A random act of mischief is more likely to lead to some inconvenience rather than theft.

The most probable consequence of digital vandalism would be the temporary unavailability of a compromised item to library systems. Depending on circumstances the item could be recovered by either re-writing the correct data, or by replacing the tag altogether.

It would take some considerable time to vandalise a large number of library items and it would involve the repetitive removal of items from shelves, the close proximity of the NFC-enabled device on each item and it is likely that library staff would notice this activity once alerted to the possibility.

Theft

The most common form of RFID security in use in the UK uses a method called AFI (application family identifier) to determine if an item may leave the library or not.

The AFI is a set of values that are modified to allow an item to pass through security checks. Anyone wishing to steal an item therefore needs to know the correct values to set in order for the security system not to react. Anyone intent on stealing items would have to do some research before attempting theft. They would then have to write to the tag via an NFC enabled device. This would require quite technical knowledge of the data structure on the tag and the location of the AFI field.

It should be noted that certain RFID chips have the ability to password protect the AFI section of tag memory, however this feature is not standard or supported by standard commands and should be considered proprietary to NXP semiconductors, there are also implications for the Library of how any secure key is managed. (Should a library lose or forget their key details, then their systems supplier would generally not be able to recover this information for them)

Unwanted data locking

Blocks of data on RFID tags can be locked, and while it may be desirable for a library to lock elements that are constant, locking other more transient data elements could affect the tag's usability. For example the ISIL code (identifying the owning library) may change during an item's lifetime. If this were to be locked it could not subsequently be changed.

There is a possibility that data blocks on RFID tags could be locked. This would require an NFC device and a sophisticated knowledge of the deployed RFID standards and the data model on the tag.

Understanding and mitigating the risk

Whilst all of the preceding threats are possible with currently available NFC enabled hardware, they are not easily carried out:

1. The read range of NFC devices is intentionally small, so in order to read or write data on an RFID tag an item would have to be removed from the shelf so that the reader can be placed close enough to the tag to carry out the operation.

2. The amount of effort required to maliciously manipulate data on a library RFID tag is probably much greater than other easier ways of disrupting library systems or damaging books. For example RFID tags could be damaged or removed by hand more quickly and by more people than any perceived Smartphone threat.

Whilst it is possible to lock data on the tag to prevent malicious alteration, the downsides of this option should be considered very carefully. Once a tag is locked, memory blocks cannot be written to again. Another small point is that it is not individual data elements that can be locked - only the memory blocks in which they reside. Therefore when locking data an encoding application needs to ensure locked elements are in individual blocks - thus using more memory. This may not be a problem of itself but it could prevent more data being added in future should tag memory be used up.

BIC cannot give legal advice on this matter but there may be sufficient protection in existing law to act as a deterrent. For example It is possible that vandalism or malicious damage to RFID tags would be viewed as a violation of the Criminal Damage Act (1971) and may also be covered by the Computer Misuse Act (1990).

Although there is a danger of alerting users to the opportunity (and even the technical challenge) of this activity, libraries might consider posting notices invoking these laws.

It should be noted that none of the major systems, currently supplied in the UK RFID market, store confidential or sensitive information about library users on item tags. There is therefore no obvious risk of infringing privacy or human rights legislation.

What should I do now?

This information sheet has been prepared by Book Industry Communication (BIC). The advice it offers is of necessity generic. It is worth pointing out that NFC poses only a potential threat. It is also true that the damage to RFID tags is very likely to be limited due to some of the factors described above. This problem is therefore seen as low risk and BIC's advice is not to panic but to understand the issues and the potential threat.

This advice was drawn up in consultation with the UK's leading RFID suppliers and has been ratified by BIC's Library Committee – which maintains a watching brief on the development of technology in this area. In the future it may be that suppliers will develop new RFID-based solutions which will enable library users to read tags and reserve books or access additional information or other media e.g. video.

Libraries may wish to take some specific action such as:

1. Inform staff of the potential threats described in this document
2. Decide on action to be taken when a tag does not read correctly (libraries will already encounter occasional tag read failure.) Tags should be re-programmed or replaced,
3. Tag failure rates could be monitored and any increase investigated
4. Library book losses from theft could also be monitored and any increase investigated
5. Notices could be placed around the library warning that library books are protected by RFID and that library users should not interfere with tags, gates etc,

BIC would generally not advise any action that reduces the value of RFID investment and opportunities for interoperability, so encrypting or locking tags is not recommended.

If you are still uncertain as to the implications of NFC for your library we urge you to talk to BIC and of course to your supplier – who will be familiar with your installation, and therefore your options.

NFC should not be viewed with too much trepidation. It is likely to bring far more benefits than concerns to future library operations.