

RFID SECURITY

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Introduction.....	3
An Introduction to RFID.....	3
How does RFID work?	4
II. Adoption of RFID.....	5
Business Trends	5
Government Use	6
III. Security and Privacy Issues	7
Tag Data.....	7
RFID Reader Integrity.....	9
Personal Privacy.....	10
IV. RFID Security Trends	11
V. Approachs for Tackling Security and Privacy Issues.....	12
Solutions For Tag Data Protection.....	12
Solutions For RFID Reader Integrity	13
Solutions For Personal Privacy.....	14
VI. Conclusion	17

SUMMARY

The deployment and use of Radio Frequency Identification (RFID) technology is growing rapidly across many different industries. Developers apply the technology not only in traditional applications such as asset or inventory tracking, but also in security services such as electronic passports and RFID-embedded credit cards. However, RFID technology also raises a number of concerns regarding privacy, security and law enforcement¹.

In this paper, the basic concepts behind RFID technology are introduced, and the associated security issues and threats in using RFID technology, along with possible measures on how to tackle them, are discussed. The objective is to deliver a greater understanding of the security related aspects of this technology.

¹ <http://www.eecs.harvard.edu/cs199r/bd-rfid/lawEnforcement.pdf>

I. INTRODUCTION

AN INTRODUCTION TO RFID

Radio Frequency Identification (RFID) technology is a non-contact, automatic identification technology that uses radio signals to identify, track, sort and detect a variety of objects including people, vehicles, goods and assets without the need for direct contact (as found in magnetic stripe technology) or line of sight contact (as found in bar code technology). RFID technology can track the movements of objects through a network of radio-enabled scanning devices over a distance of several metres.

A device called an RFID tag (or simply a tag) is a key component of the technology. An RFID tag usually has at least two components:

1. an integrated circuit for modulating and demodulating radio signals and performing other functions;
2. an antenna for receiving and transmitting the signal.

An RFID tag can perform a limited amount of processing and has small amount of storage. RFID tags are sometimes considered to be enhanced “electronic barcodes”².

RFID tags that do not have any integrated circuit are called chipless RFID tags (also known as RF fibres). These tags use “*fibres or materials that reflect a portion of the reader's signal back and the unique return signal can be used as an identifier*”³.

² http://www.eurosmart.com/Update/07-10/Eurosmart_White_paper_on_RFID_Oct07.pdf

HOW DOES RFID WORK?

Systems that make use of RFID technology are typically composed of three key elements:

1. An RFID tag, or transponder, that carries object-identifying data.
2. An RFID tag reader, or transceiver, that reads and writes tag data.
3. A back-end database, that stores records associated with tag contents.

Each tag contains a unique identity code. An RFID reader emits a low-level radio frequency magnetic field that energises the tag. The tag responds to the reader's query and announces its presence via radio waves, transmitting its unique identification data. This data is decoded by the reader and passed to the local application system via middleware. The middleware acts as an interface between the reader and the RFID application system. The system will then search and match the identity code with the information stored in the host database or backend system. In this way, accessibility or authorisation for further processing can be granted or refused, depending on results received by the reader and processed by the database.

³ <http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=28>

II. ADOPTION OF RFID

Commercial applications of RFID can be found today in supply chain management, automated payment systems, airline baggage management, and so on. According to RFIDupdate.com, one of the catalysts for the RFID industry has been mandates issued by Wal-Mart and the US Department of Defense (DOD) for their suppliers to adopt RFID technology⁴. Although the market has not grown quickly or as large as originally expected, these two mandates continue to be important drivers in development of the industry.

BUSINESS TRENDS

In June 2003, the world's largest retailer, Wal-Mart, sent out a request to its top 100 suppliers to "*put RFID tags on all cases and pallets of consumer goods shipped to a limited number of Wal-Mart distribution centers and stores*" by 2005⁵. While the deployment of the RFID project continued, Wal-Mart indicated in 2006 that "*out-of-stock items carrying RFID tags could be replenished three times faster than they were before the project began*"⁶.

⁴ <http://www.rfidupdate.com/articles/index.php?id=1264>

⁵ http://www.symbol.com/assets/files/Supplier_Compliance_with_the_DOD_RFID_Mandate.pdf

⁶ <http://www.computerworld.com/mobiletopics/mobile/story/0,10801,109418,00.html>

However, not all companies have found RFID technology that helpful. A number of smaller Wal-Mart suppliers have had trouble justifying the investment in implementing RFID in their supply chain⁷ in order to meet Wal-Mart's expectations.

GOVERNMENT USE

Similar to Wal-Mart, the US Department of Defense (DOD) began a policy in July 2004, requesting vendors supplying goods directly or indirectly to the DOD integrate RFID into their shipping procedures⁸. This mandate triggered a number of DOD suppliers to test RFID, or run pilot projects in order to comply with the new requirements.

Another adoption of RFID technology has been by governments, with the electronic passport project. In a number of countries, traditional paper passports are gradually being replaced with passports embedded with a small integrated circuit. Biometric information, such as face recognition, fingerprints or iris scans are stored in the electronic passport. The electronic passport project was initiated by the US, requesting all countries participating in the Visa Waiver Program issue passports with integrated circuits. The main objectives are for automated identity verification, and for greater border protection and security⁹.

⁷ <http://www.rfidgazette.org/walmart/index.html>

⁸ http://www.symbol.com/assets/files/Supplier_Compliance_with_the_DOD_RFID_Mandate.pdf

⁹ http://travel.state.gov/passport/eppt/eppt_2788.html

III. SECURITY AND PRIVACY ISSUES

With the adoption of RFID technology, a variety of security and privacy risks need to be addressed by both organisations and individuals:

TAG DATA

RFID tags are considered “dumb” devices, in that they can only listen and respond, no matter who sends the request signal. This brings up risks of unauthorised access and modification of tag data. In other words, unprotected tags may be vulnerable to eavesdropping, traffic analysis, spoofing or denial of service attacks. We will look at each of these in turn:

Eavesdropping (or Skimming)

Radio signals transmitted from the tag, and the reader, can be detected several metres away by other radio receivers. It is possible therefore for an unauthorised user to gain access to the data contained in RFID tags if legitimate transmissions are not properly protected. Any person who has their own RFID reader may interrogate tags lacking adequate access controls, and eavesdrop on tag contents.

Researchers in the US has demonstrated a skimming attack on an RFID credit card, through which credit card information, such as the cardholder's name and account information, could be skimmed if not properly encrypted¹⁰.

Traffic Analysis

Even if tag data is protected, it is possible to use traffic analysis tools to track predictable tag responses over time. Correlating and analysing the data could build a picture of movement, social interactions and financial transactions. Abuse of the traffic analysis would have a direct impact on privacy.

Spoofing

Based on the data collected from eavesdropping or traffic analysis, it is possible to perform tag spoofing. For instance, a software package known as "RFDump",¹¹ that runs on a notebook computer or personal digital assistant, allows a user to perform reading or writing tasks on most standard smart tags if they are not properly protected. The software permits intruders to overwrite existing RFID tag data with spoof data. By spoofing valid tags, the intruder could fool an RFID system, and change the identity of tags to gain an unauthorised or undetected advantage. One example is trying to save money by buying expensive goods that have had their RFID price tags spoofed to display cheaper prices.

¹⁰ http://www.nytimes.com/2006/10/23/business/23card.html?pagewanted=1&_r=1

¹¹ http://freshmeat.net/projects/rfdump/?branch_id=61265&release_id=264928

By combining the two capabilities of eavesdropping and spoofing, a replay attack is possible where an attacker can “*query a tag, receive the information it sends, and retransmit this information at a later time*”¹².

Denial of Service Attack

The problems surrounding security and trust are greatly increased when large volumes of internal RFID data are shared among business partners. A denial of service attack on RFID infrastructure could happen if a large batch of tags has been corrupted. For example, an attacker can use the “kill” command, implemented in RFID tags, to make the tags permanently inoperative if they gain password access to the tags. In addition, an attacker could use an illegal high power radio frequency (RF) transmitter in an attempt to jam frequencies used by the RFID system, bringing the whole system to a halt¹³.

RFID READER INTEGRITY

In some cases, RFID readers are installed in locations without adequate physical protection. Unauthorised intruders may set up hidden readers of a similar nature nearby to gain access to the information being transmitted by the readers, or even compromise the readers themselves, thus affecting their integrity. Unauthorised readers may also compromise privacy by accessing tags without adequate access controls.

¹² http://blogs.sun.com/ks/entry/rfid_technology_security_concerns

¹³ http://www.eurosmart.com/Update/07-10/Eurosmart_White_paper_on_RFID_Oct07.pdf

As a result, information collected by readers and passed to the RFID application may have already been tampered with, changed or stolen by unauthorised persons. An RFID reader can also be a target for viruses. In 2006, researchers demonstrated that an RFID virus was possible. A proof-of-concept self-replicating RFID virus was written to demonstrate that a virus could use RFID tags to compromise backend RFID middleware systems via an SQL injection attack¹⁴.

PERSONAL PRIVACY

As RFID is increasingly being used in the retailing and manufacturing sectors, the widespread item-level RFID tagging of products such as clothing and electronics raises public concerns regarding personal privacy. People are concerned about how their data is being used, whether they are subject to more direct marketing, or whether they can be physically tracked by RFID chips. If personal identities can be linked to a unique RFID tag, individuals could be profiled and tracked without their knowledge or consent.

For instance, washing clothes tagged with RFID does not remove the chips, since they are specially designed to withstand years of wear and tear. It is possible that everything an individual buys and owns is identified, numbered and tracked, even when the individual leaves the store, as far as products are embedded with RFID tags. RFID readers can detect the presence of these RFID tags wherever they are close enough to receive a signal.

¹⁴ <http://www.rfidvirus.org/>

IV. RFID SECURITY TRENDS

Since RFID remains an emerging technology, the development of industry standards for protecting information stored on RFID chips is still being explored and strengthened. Research into the development and adaptation of efficient hardware for cryptographic functions, symmetric encryption, message authentication codes and random number generators will improve RFID security. In addition, advances in RFID circuit design and manufacturing technology can also lower development costs releasing more resources in tags that can be used for other functions, such as allocating power consumption towards security features.

Today, certain public key technologies are also being studied and in some cases deployed by RFID vendors. This helps improve confidentiality, user authentication and privacy of RFID tags and associated applications. RFID vendors are also conducting research into integrity and confidentiality issues around RFID reader infrastructure. Data can now be stored on a token using dynamic re-keying, where specific readers can rewrite a token's credentials/signature, and verify the token's identity. However, the cost and performance issues around using public key technologies in RFID applications have stalled its use for critical security applications.

V. APPROACHS FOR TACKLING SECURITY AND PRIVACY ISSUES

There are a variety of solutions for tackling the security and privacy issues surrounding RFID. They can be categorised into the following areas:

1. Tag Data Protection
2. Reader Integrity
3. Personal Privacy

SOLUTIONS FOR TAG DATA PROTECTION

Password Protection on Tag Memory

Passwords can be used to protect tag data, preventing tags from being read without the original owner's permission. But if the passwords for all the tags are identical, then the data becomes virtually public. However, if each tag is going to have a different or unique password, there may be millions of passwords that need to be recorded, meaning the reader would have to access the database and perform a lot of comparisons for each reading attempt.

Physical Locking of Tag Memory

The tag manufacturer locks information such as a unique identifier into tag before the tag is released into an open environment. In other words, the chip is read-only and is embedded with information during the manufacturing process. This provides proof of origin.

The limitation of this method is that no rewriting of data can be done on the tag chip. Additional memory would be required for storing modifiable or extra information and an algorithm would be needed for finding the latest tag data. This would result in higher memory cost and a larger size memory.

Authentication of the “Author” in Tag Memory

The author or owner of the tag encrypts the tag data with his own private key (i.e. digitally signs the tag) and writes the encrypted data into tag memory along with the author’s name, a reference to his public key and the algorithm used in non-encrypted form. When the reader wants to verify the authenticity of information, it retrieves the author’s name and other non-encrypted information from the tag to verify that the data has been actually written by the original author as claimed. However, if the RFID reader needs to update the tag with new data, a key management system is required in order to manage the private key.

SOLUTIONS FOR RFID READER INTEGRITY

Reader Protection

Readers can reject tag replies with anomalies in response times or signal power levels which don't match the physical properties of tags. If passive tags are used, this can be a way to prevent spoofing attempts.

Readers can also use random frequencies with tags designed to follow a frequency dictated by the reader. Readers can change frequencies randomly so that unauthorised users cannot easily detect and eavesdrop on traffic.

On top of this, data transmitted between the reader and the RFID application server could require verification of the reader's identity. Authentication mechanisms can be implemented between the reader and the backend application to ensure that information is passed to the valid processor.

Read Detectors

RFID environments can be equipped with special devices to detect unauthorized read attempts or transmissions on tag frequencies. These read detectors may be used to detect unauthorized read/update attempts on tags, if they are used together with specially designed tags that can transmit signals over a reserved frequencies, indicating any attempts to kill or modify tags.

SOLUTIONS FOR PERSONAL PRIVACY

Kill Tag

By executing a special “kill” command on a tagged product, the RFID tag will be “killed” and can never be re-activated. This “kill” command may disconnect the antenna or short-circuit a fuse. This ensures that the tag cannot be detected any further, and thus protects the privacy of the individual who possesses the product.

However, there may be instances where tags should not be “killed”. A store may wish for example to re-detect the tags on defective products returned by customers. Also, smart-cards embedded with RFID chips for access control will need to be activated continuously.

Faraday Cage

An RFID tag can be shielded with a container made of metal mesh or foil, known as a “Faraday Cage”. This foil-lined container can block radio signals of certain frequencies and thus protect tagged products from being detected. However, this approach might not work in some situations. For example, it is difficult to wrap foil-lined containers around tags used in clothing for pets and people.

Active Jamming

Active jamming of RF signals refers to the use of a device that actively broadcasts radio signals in order to disrupt the operation of any nearby RFID readers. This physical means of shielding may disrupt nearby RFID systems.

However, the use of such a device may be illegal, depending on the broadcasting power of the device and government regulations in force. There is a risk of severe disruption to all nearby RFID systems if the jamming power is too strong.

“RSA” Selective Blocker Tag

A blocker tag is a passive RFID device that uses a sophisticated algorithm to simulate many ordinary RFID tags simultaneously. It provides an endless series of responses to RFID readers through the use of two antennas to reflect back two bits simultaneously, thereby preventing other tags from being read, performing a kind of passive jamming.

However, this approach gives individuals a lot of control. In addition, a blocker tag may be used maliciously to circumvent RFID reader protocols by simulating multiple tag identifiers.

Logical “Hash-lock”

When a tag is locked, it is given a value (or meta-ID) that is a hash value of the corresponding key or PIN. The tag will refuse to reveal its ID until it can be unlocked by presenting the value of the key or PIN value. For example, tags may be locked at check out time in a supermarket and then unlocked by the individual using a given meta-ID and PIN after returning home. These meta-ID and PINs may be read optically by individuals, and be printed on the interior of the package or on the payment bill after purchasing, rather than transmitted by radio.

The limitation of this approach is that individuals need to manage the lock/unlock features and the associated PINs for a whole collection of tags and purchases, and need to keep track of which objects carrying which RFID tags. This approach also incurs additional cost as it involves a cryptographic operation on tags.

VI. CONCLUSION

While the use of RFID technology is increasing across a range of different industries, the associated security and privacy issues need to be carefully addressed. Because RFID tags come in different flavours, there is no overall, generic RFID security solution. Some low-cost passive and basic tags cannot execute standard cryptographic operations like encryption, strong pseudorandom number generation, and hashing. Some tags cost more than basic RFID tags, and can perform symmetric-key cryptographic operations. Organisations wishing to use RFID technology need to therefore evaluate the cost and security implications as well as understand the limitations of different RFID technologies and solutions.