REPORT

On

RFID SECURITY

Submitted to
Professor Richard Sinn

College of Engineering
CmpE-296T - Software Security Technologies
San Jose State University

By
Sankate Sharma
Sangbeom Ryu

This report gives an overview of the RFID technology. It starts from answering the basic question of "What is RFID", and then gives an overview of RFID implementation. This report covers the working of RFID, most common uses of RFID and key considerations in those implementations. It describes the security perspective of current state of this technology and the future prospects of this technology.

Table of Contents

1. Introduction

This report gives an overview of the RFID technology. It starts from answering the basic question of "What is RFID", and then gives an overview of RFID implementation. Overview section covers the working of RFID, most common uses of RFID and key considerations in those implementations. It briefly describes different types of the RFID tags. It also describes the current state of this technology and the future prospects of this technology.

Second section of this report covers the various applications of RFID and discusses potential problems with these uses.

Third section of the report covers the Privacy and Security issues related to RFID technology.

The report concludes with describing proposed solutions for the RFID privacy and security issues.

2. RFID Implementation

Overview

RFID stands for Radio Frequency Identification, RFID describes any system of identification where an electronic device that uses radio frequency or magnetic field variations to communicate is attached to an item. The two most common components of an RFID system are the tag, which is the identification device attached to the item we are tracking, and the reader, which is a device that can recognize the presence of RFID tags and read the information stored on them. The reader can then inform another system about the presence of the tagged items. The system with which the reader communicates usually runs software that stands between readers and applications. This software is called RFID middleware. An RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader.

Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a radio frequency signal and can also be used for other

specialized functions. The second is an antenna for receiving and transmitting the signal. A technology called chip-less RFID allows for discrete identification of tags without an integrated circuit, thereby allowing tags to be printed directly onto assets at lower cost than traditional tags.

Today, a significant thrust in RFID use is in enterprise supply chain management, improving the efficiency of inventory tracking and management. However, it still needs to be seen that the current growth and adoption in enterprise supply chain market is sustainable or not. A fair cost-sharing mechanism, business process improvements and justified returns from RFID technology investments are the key ingredients to achieve long-term and sustainable RFID technology adoption. Figure 1-1 shows how the pieces fit together.

Source: RFID Essentials *by* Himanshu Bhatt*;* Bill Glover *Publisher:* O'Reilly*Pub Date:* January 2006

Figure 1-1. Spreadsheet of CDDiscs and days

RFID (Radio-Frequency Identification) is a technology for automated identification of objects and people. RFID may be viewed as a means of explicitly labeling objects to facilitate their “perception” by computing devices. An RFID device – frequently just called an RFID tag – is a small microchip designed for wireless data transmission. It is generally attached to an antenna in a package that resembles an ordinary adhesive sticker. The microchip itself can be as small as a grain of sand, some 0.4mm2. An RFID tag transmits data over the air in response to interrogation by an RFID reader.

In academic and print media RFID has been the center of attraction in the past few years. One important reason for this is the effort of large organizations, such as Wal-Mart, Procter and Gamble, and the United States Department of Defense, to deploy RFID as a tool for automated oversight of their supply chains. This is because of dropping tag costs and vigorous RFID standardization, RFID is gaining

widespread use. RFID will enter the home and the supermarket aisle when the prices of readers and tags become low enough and when the information infrastructure to use and maintain the new technology is in place. Some of these applications may seem far-fetched, but they are things we know we can do with a bit of engineering. RFID promises a lot of great engineering solutions that we can't even imagine at this stage of adoption.

RFID Tags

RFID tags come in three general varieties: *passive*, *active*, or *semi-passive* (also known as *battery-assisted*). Passive tags require no internal power source, thus being pure passive devices (they are only active when a reader is nearby to power them), whereas semi-passive and active tags require a power source, usually a small battery. To communicate, tags respond to queries generating signals that must not create interference with the readers, as arriving signals can be very weak and must be told apart. Besides backscattering, load modulation techniques can be used to manipulate the reader's field. Typically, backscatter is used in the far field, whereas load modulation applies in the near field, within a few wavelengths from the reader.

Passive

Passive RFID tags have no internal power supply. The minute electrical current is induced in the antenna by the incoming radio frequency signal; it provides just enough power for the CMOS integrated circuit in the tag to power up and transmits a response. Most passive tags signal by backscattering the carrier wave from the reader. This means that the antenna has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not necessarily just an ID number; the tag chip can contain non-volatile, possibly writable EEPROM for storing data.

Active

Unlike passive RFID tags, active RFID tags have their own internal power source, which is used to power the integrated circuits and broadcast the signal to the reader. Active tags are typically much more reliable (i.e. fewer errors) than passive tags due to the ability for active tags to conduct a

"session" with a reader. Active tags, due to their onboard power supply, also transmit at higher power levels than passive tags, allowing them to be more effective in "RF challenged" environments like water (including humans/cattle, which are mostly water), metal (shipping containers, vehicles), or at longer distances, generating strong responses from weak requests (as opposed to passive tags, which work the other way around). In turn, they are generally bigger and more expensive to manufacture, and their potential shelf life is much shorter.

Semi-passive

Semi-passive tags are similar to active tags in that they have their own power source, but the battery only powers the microchip and does not broadcast a signal. The RF energy is reflected back to the reader like a passive tag. An alternative use for the battery is to store energy from the reader to emit a response in the future, usually by means of backscattering.

The battery-assisted receive circuitry of semi-passive tags lead to greater sensitivity than passive tags, typically 100 times more. The enhanced sensitivity can be leveraged as increased range (by a factor 10) and/or as enhanced read reliability (by one standard deviation).

3. Applications of RFID

RFID today and tomorrow

We already use RFID tags routinely. Examples include:

• Proximity cards, that is, the contactless cards used for building access.

• Automated toll-payment transponders – the small plaques mounted in automobile windshields. (These are usually semi-passive.)

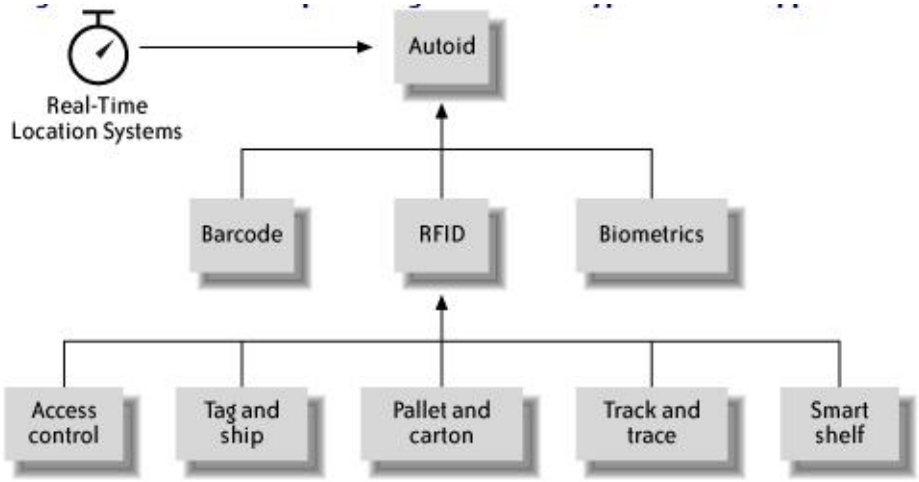
• The ignition keys of many millions of automobiles, which include RFID tags as a theft-deterrent.

• Payment tokens: In the United States, the SpeedPass token for petrol station payments is an example. Contact-less credit-cards, like American Express ExpressPay and the Mastercard PayPass use RFID.

Certain broad types of RFID applications characterize whole approaches to this technology and are different enough in considerations and implementation. The tree in Figure 1-2 [*source: RFID Essentials by Himanshu Bhatt; Bill Glover Publisher: O'ReillyPub Date: January 2006*] shows RFID's relationship to other identity systems, as well as the relationships between different types of RFID. The term "autoid," short for automatic ID, describes any automated system for attaching an identity to an item. Real-Time Location Systems (RTLSs) are automated systems for tracking the location of an item. These five categories are inclusive enough to provide at least some sense of the issues and considerations involved in typical RFID applications. The future will bring even more varied applications, but they will raise many of the same concerns as the applications in these categories.

Source: RFID Essentials *by* Himanshu Bhatt*;* Bill Glover *Publisher:* O'Reilly*Pub Date:* January 2006

Figure1-2: Applications of RFID



Access Control

Access control applications are RFID systems used to selectively grant access to certain areas—for example, RFID tags attached to an automobile or held in a person's hand as a card, key chain, or wristband may allow access to a road, building, or secure area. Key Considerations are: *Anti-counterfeiting* [Counterfeit tags must be recognized and attempts to use or manufacture them

discouraged.] ,*Tailgating* [Tailgating occurs when an unauthorized person or vehicle enters just behind an authorized person or vehicle before the gate or door can close.], *Emergency access* [In an emergency, the access control system must allow emergency personnel or vehicles access to secured locations. It must also allow nonemergency personnel to evacuate without getting in the way of the emergency response team.]

Tag and Ship

Tag and ship applications are minimal RFID systems that allow a user to associate an RFID tag with an item, apply the physical tag to the item, and then verify that the tag operates properly while attached to the item. In some cases, these systems even use pre-encoded tags to further reduce cost. Primary considerations for this type of application are: *Cost* [
Because the drivers for this sort of application typically comply with a mandate, keeping cost low is the primary concern of the end user.], *Isolation* [Tag and ship systems are in some cases the first automated system to be deployed at a given location. The support and maintenance infrastructure needed for such systems, and even the floor space they take up at the dock or shipping area, often aren't readily available.] , *Tag failure* [Manufacturing defect rates are still high for the smart labels used in this type of application.] ,*Impact on processes* [Because this type of application is typically implemented in response to an external mandate rather than a perceived internal need, the application's impact on the throughput of what may be a finely tuned manual process can be an important issue.]

Pallet and Carton Tracking

One of the most commonly mentioned forms of RFID, pallet and carton tracking, essentially puts a "license plate" on a shipping unit made up of one or more individual items. Primary considerations for this type of application are: *Pallet or carton integrity* [Pallet and carton tracking can be ineffective if there is a possibility that the pallet or carton may be broken down and reconstituted. In this case, the counts or manifest may become invalid.] , *Pallet orientation* [Pallets have six sides. Given that the bottom is typically inaccessible, we still have five choices when deciding where to attach the tag. Because most dock doors are roll-ups, placing a reader overhead can be difficult, so few

implementations tag the top of the pallet.] , *Interfering contents* [A tag on a box of metal cans can be difficult for a reader to distinguish.]

Track and Trace

One of the earliest uses of RFID was to track dairy cattle. Now, companion animals and livestock of all types are routinely tagged with inject able glass capsules or button ear tags. These tags are used to identify lost pets and to sort, care for, and track the history of livestock. In recent years, RFID has also been increasingly used to track produce and pharmaceuticals. Information from livestock, produce, or pharmaceutical tracking can be critical in the event of a public health threat. Primary considerations for this type of application are: *Information sharing [*One of the key requirements when merging information is coordinated identification. In any track and trace system, each identity must be unique across all producers and for as long a period as the information must be maintained.], *Role- and instance-based access control* [Sharing information includes pooling information with competitors. Track and trace systems must have a provision for role- and instance-based control over access to information.]

Smart Shelf

A smart shelf system is a set of shelves or some other container (such as a refrigerator), that constantly keeps track of the individual items it contains. If an item is removed or added, the shelf immediately updates the inventory. By tying the identity of an item to its attributes, such as expiration date or lot number, a system using smart shelves can immediately locate all expired products and products from a certain lot. Primary considerations for this type of application are: *Item-level inventory support* [Resolving inconsistencies between existing applications and a system that handles individual inventory.] ,*Physics and hardware* [Developing a reliable smart shelf system from readers, antennas, and standard shelving is a difficult task due to the complexity of choosing components, placing antennas, and modeling the possible side effects.] , *Handling spurious reads* [A reader may sometimes fail to recognize a tag. This can be due to interference or absorption of the RF signal.]

4. Privacy and security issues

Privacy

RFID raises two main privacy concerns for users: *clandestine tracking* and *inventorying*. RFID tags respond to reader interrogation without alerting their owners or bearers. Thus, where read range permits, clandestine scanning of tags is a plausible threat. As discussed above, most RFID tags emit unique identifiers, even tags that protect data with cryptographic algorithms (as we discuss below). In consequence, a person carrying an RFID tag effectively broadcasts a fixed serial number to nearby readers, providing a ready vehicle for clandestine physical tracking. Such tracking is possible even if a fixed tag serial number is random and carries no intrinsic data. The threat to privacy grows when a tag serial number is combined with personal information. For example, when a consumer makes a purchase with a credit card, a shop can establish a link between her identity and the serial numbers of the tags on her person. Marketers can then identify and profile the consumer using networks of RFID readers – both inside shops and without. The problem of clandestine tracking is not unique to RFID, of course. It affects many other wireless devices, such as Bluetooth-enabled ones.

The main concern of privacy are Tracking and Sniffing**:**

Tracking

RFID technology facilitates clandestine monitoring of individuals' whereabouts and actions. RFID readers placed in strategic locations (such as doorways) can record RFID tags' unique responses, which can then be persistently associated with a person's identity. RFID tags without unique identifiers can also facilitate tracking by forming constellations, recurring groups of tags that are associated with an individual. RFID technology also enables monitoring entire groups of people.

Identity Theft

Privacy advocates caution that the information contained in RFID chip could easily be stolen, so that storing anything private in it would be to risk identity theft. As the human-implantable microchip only contains a unique 16-digit electronic identifier, the unique number is used only for such purposes as accessing personal medical information in a password-protected database or assessing whether

somebody has authority to enter into a high-security area.

Security

RFID technology has following potential security risks.

Denial of service

RFID systems only work when RFID tags and back-end databases are available. Thieves can exploit this to steal RFID-tagged items by removing tags from the items completely or by putting them in a foillined booster bag that blocks RFID readers' query signals and temporarily deactivates the items.

Sniffing

RFID tags are indiscriminate—they're designed to be readable by any compliant reader. Unfortunately, this lets unauthorized readers scan tagged items without the knowledge of the bearer, often from great distances. People can also collect RFID data by eavesdropping on the wireless RFID channel. Unrestricted access to tag data can have serious implications; collected tag data might reveal information such as medical predispositions or unusual personal inclinations, which could cause denial of insurance coverage or employment for an individual.

Spoofing.

Attackers can mimic authentic RFID tags by writing appropriately formatted data on blank RFID tags. For example, thieves could retag items in a supermarket identifying them as similar,
but cheaper, products.

Replay attacks.

Relay devices can intercept and retransmit RFID queries, which offenders can use to abuse various RFID applications. England's new RFID-enabled license plates, e-Plates, are one example of a modern RFID system that's susceptible to attack by a relay device. The active e-Plate tags contain an encrypted ID code that is stored in the UK Ministry of Transport's vehicle database. An attacker can record the encrypted identifier when another car's license plate is scanned and replay it later (perhaps to avoid paying the Congestion Charge when driving into central London).

Data Accessibility

Anyone possessing a VeriChip reader can read the human-implantable RFID microchip; the data is

unencrypted, and VeriChip does not have the functionality to authorize only certain people to read it. Being a passive RFID microchip containing only a unique 16-digit identifier it can be read by a VeriChip reader held up closely to the location of the inserted chip. This concern can be partially mitigated by using such a chip without implanting it, as by inserting it into the wristband of a watch, which can then be removed at will.

5. Security and privacy solutions

Cryptography

Cryptography can be applied to RFID to provide security and privacy. The problem of applying cryptography to RFID tags is that computation is required for encryption and decryption. This is a problem of low-cost RFID tags because it cannot run standard functions of cryptography [1]. Even symmetric key encryption cannot be executed in low-cost RFID. The research of Juels [2] suggests minimalist cryptography so that cryptography can be applied to low-cost RFID tags. Public key-based Basic Access Control for electronic passport is one of the first examples, which is deployed using RFID authentication. Figure 1-3 shows biometric electronic passport with RFID chip embedded.

Source: Check on travel document counterfeit, Adi Tedjasaputra, eGov

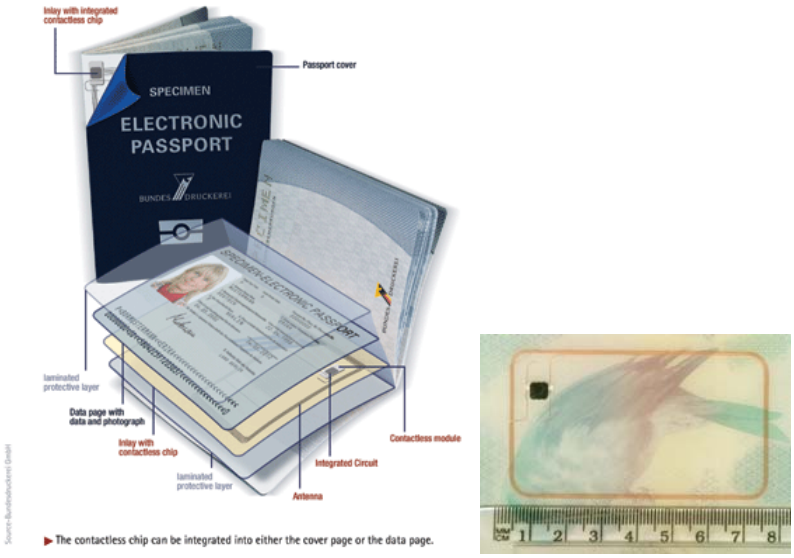


Figure 1-3 Biometric (Electronic) Passport Using RFID Chip

Skimming

By using an embedded metallic element in the passports, it provides RF signal blocking. The RF blocking material covers the passport so that it only can be physically opened when it should be read.

Eavesdropping

Basic Access Control (BAC) minimizes the chance of skimming and eavesdropping. Initial interaction should be necessary between the RFID chip in the passport and the control reader which contain protocols that are for the secure communication channel. Figure 1-4 shows Basic Access Control.

source: A Security Review of the Biometric Passport, Bart Jacobs & Ronny Wichers Schreur, Radbound University Nijmegen

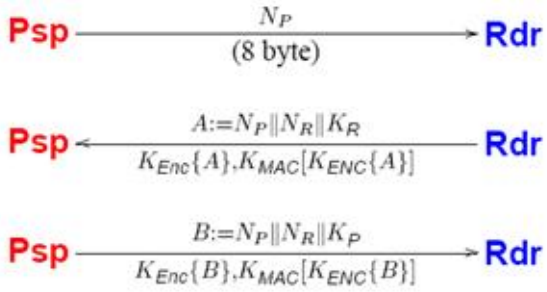


Figure 1-4 Basic Access Control

Once authentication is done successfully, the data from passport will be issued. If not, the passport declines the access of data content.

Tracking

Unique Identifier (UID) is still possible to be tracked even though BAC is used. The solution of tracking is using a random UID (RUID). Embedded random number generator (RNG) generates a RUID.

Cloning

RFID chip can be copied, so it can be used for another electronic passport. By comparing the chip data and the data on electronic passports data page, it is possible to diminish of cloning. Using Public Key Infrastructure (PKI) is one of the ways to prevent cloning. PKI can be applied to the travel document, so that comparing the data between the chip and travel document. If the data is stored by authority, the data is not changed.

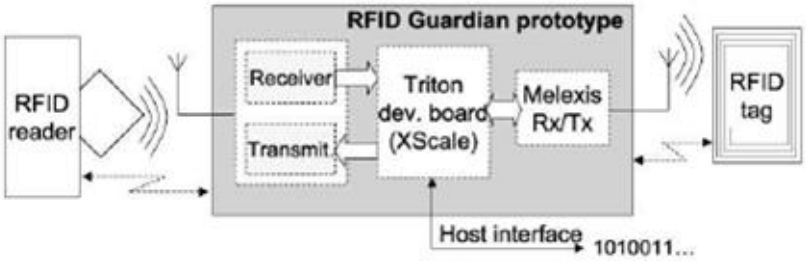
Detection and evasion

Detection

It is possible to detect RFID which is not authorized to be activated by using a gadget [4]. RFID Detektor (http://www.heise.de/ct/04/09/132/) is one of the examples. It can detect spied RFID device, and alarm silently to the owner.

Evasion

There is a device, RFID Guardian that can decode RFID scans. Customers also can avoid RFID scan by blocking it. Figure 1-5 illustrates RFID Guardian HW architecture.



Source: A platform for RFID Security and Privacy Administration [105]

Figure 1-5 RFID Guardian HW Architecture

Temporary deactivation

There is another way to protect personal privacy. By making RFID tags deactivate, privacy can be protected. One of the ways to deactivate is using Faraday cage which can block out external electrical fields. EPCglobal tags make enables to deactivate tags forever by using password-protected deactivate function [4, 5]. The tags which have temporary deactivation functions can be found in more expensive RFID tags.

Addressing RFID privacy

Government legislations and guidelines are very important to address the privacy issues. Government

has to enforce that illegal tracking and intrusion of privacy using RFID is prohibited under law. The law / guidelines enforce following

- The right of the consumer to know what items possess RFID tags
- The right to remove or deactivate the RFID tag once a product is purchased
- The right to products and services even if a consumer chooses not to use RFID tags
- The right to know where, when, and why an RFID tag is being read
- The right to know what information is being stored inside an RFID tag

6. Conclusion

RFID technology is growing rapidly and widely. Already RFID environment is implemented everywhere. In the contrary in convenient of RFID, there are threats compromising security and privacy. The more RFID is used in daily life and provide important personal information, the bigger security and privacy issues are increased. Currently many researches related about RFID security and privacy are being progressed. In order to protect personal information and provide safe RFID environment, the more researches about RFID privacy and security should be done.

7. Appendix

Information sources

[1] RFID Security and Privacy: A Research Survey, Ari Juels, RSA Laboratories, 28 September 2005

[2] Minimalist Cryptography for Low-Cost RFID Tags, Ari Juels, RSA Laboratories

[3] The U.S. Electronic Passport Frequently Asked Questions,

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

[4] The Evolution of RFID Security, Melanle R. Rleback, Bruno Crispo, Andrew S. Tanenbaum, Pervasive computing, Jan-Mar 2006

[5] M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman, A.S. Tanenbaum. "A Platform for RFID Security and Privacy Administration" 20th USENIX/SAGE Large Installation System Administration conference (LISA 2006), Washington DC, December 2006. *Best Paper Award*

[6] EPCglobal Tag Class Structure,
http://www.epcglobalinc.org/standards/TagClassDefinitions_1_0-whitepaper-20071101.pdf

[7] RFID Essentials by Himanshu Bhatt; Bill Glover Publisher: O'ReillyPub Date: January 2006