Global Information Assurance Certification Paper

Is Radio Frequency Identification (RFID) Secure Enough?

GSEC Practical Assignment

Version 1.4c

Stephanie D. Lyon

November 15, 2004

Abstract/Summary

Radio Frequency Identification (RFID) technology is a very hot topic. While it is not a new technology, in the past five years it has gained tremendous momentum driven largely by its use in supply chain tracking. Additionally, it is a rapidly evolving technology. Historically its common use has been in the security arena via the ubitquous smart proximity card. Looking forward, the potential exists to use the technology in new ways to support secure application. But is the technology up for the task? The information presented here will demonstrate that like any good security tool, RFID can provide appropriate and effective security when applied within its limitations.

Overview of RFID

It is likely that you have seen the commercial where a man is walking through a grocery store. He appears to be stealing items – stuffing them into his pockets and under his coat. As he is walking out the door, a security guard calls out to him, "Sir, you forgot your receipt." That commercial is the poster child for RFID technology. Convenience for the consumer, theft protection for the retailer. But as information presented later in this paper will indicate, all the items may not have been registered on that receipt.

Radio Frequency Identification (RFID) is an electronic tagging technology that supports automatic identification of assets. As the name states, it does so by use of radio frequency waves. The main components are a tag (also called a transponder) , an antenna and a reader which powers and communicates with the tag. The tag is basically a silicon chip. In many cases, the tag includes an antenna to enable communication with the reader. The antenna is important in that its size will effect the range, or distance, at which the tag can be read. Tags come in all shape and size. They can be metallic threads embedded in paper, rice grain size for subcutaneous injection in humans and animals, encased in plastic for key fobs, a backing for a human readable shipping label, and business card size for use in smart cards, just to name a few. I was surprised at how long a comprehensive list would be!

Optionally, the tag can contain a battery. The battery power is used by the tag to increase its communication range. A tag that contains a battery is known as an active tag, a tag without a battery is a passive tag. Since the limits are in flux due to changing technology, in general one can state that a passive tag needs to be very close to the reader (centimeters) while an active tag can be as far as 30 feet away. Active tags are more expensive and larger than passive tags. Cost per tag information varied so widely, and published pricing lists is not common, that it is not productive to cite here. At this writing, upwards of .25cents (US) seemed to be widely stated, although certainly volume discounts exist. A tag can also be read-only or read-write.

The reader communicates with a tag via another antenna, which may be either external or built into the reader. The reader generates an electrical field. When the tag passes within this field it is powered up so it can pass information to the reader. The reader can also serve as a conduit to a network processor that correlates the information returned by the tag with some central database.

Since this technology uses radio frequency to communicate, in the United States it is regulated and limited by the Federal Communications Commission (FCC). The regulations permit the use of certain frequency bands. The low frequency ranges (30 to 300 KHz) provide international compatibility since they are available worldwide. "High-frequency devices (3 to 30 MHz) are used most commonly in smart card and smart label applications such as baggage tracking or small product labeling. Very high-frequency devices (300 MHz to 3 GHz) are primarily used in highway toll-collection application. In the United States, systems typically operate at 900 MHz or 2.45 GHz; in Europe, similar systems operate in the 5.8 GHz range." (Shepard, p.61-63)

Historical recounts attribute emergence of modern RFID to work done in the 1970's by various research and commercial entities. The earliest applications were in toll collection and livestock tracking. As material and hardware technology grew more sophisticated and compact, the applications for RFID grew. RFID technology has been widely used in access control smart cards, or proximity cards, "speed-pass" tags for tolls and gas/fuel purchase, and automobile security systems. The most rapidly emerging application is supply-chain management. Other emerging applications include hospital patient identification, anti-fraud protection, and general asset tracking.

Most literature on RFID states that the minimum amount of information a tag will provide is a unique 96-bit number. An organization called EPC Global Inc (www.epcglobalinc.org) in cooperation with the Auto-ID Labs, would like this number to be a globally unique Electronic Product Code (EPC). EPC Global is working with early adopter organizations, specifically in the global supply chain arena, to establish standards that will enable a world-wide supply chain database. A huge incentive towards adoption of RFID as a technology, and the EPC standards is being driven by the US merchandising giant Wal-Marts (2), the German Metro AG chain, and the US Department of Defense. These entities have compliance imposed requirements on some number of their vendors by early 2005.

But, as with any emerging technology the standards are evolving. At this time, it is up to the deploying entity to decide what information, in what form it will store on tags. These decisions will be made based on applications and cost. If I need a million tags, chances are they will be the lowest-cost passive tag, which are encoded with some id number by the tag manufacturer.

Several ISO specifications speak to tags, readers and security (ISO 14443). Security mostly as applies to financial applications.

At least 50%, perhaps higher, of the mainstream press that RFID currently receives is related to personal information privacy concerns. Consumers are concerned about tags imbedded in products they purchase, employees are worried about their movement being tracked, and hospital patients are worried about the protection of their medical records. RFID privacy issues is certainly a topic in its own right, and as such cannot be covered comprehensively in this paper. However, clearly privacy issues speak to a concern for securing sensitive information, and as such cannot be ignored.

Sensing the volume of consumer privacy concerns, several companies are working on various ways to defeat RFID. Currently, RSA Technologies is pushing their proposed "Tag Blocker" technology which would defeat RFID by overwhelming the reader with responses. Theoretically, a blocker tag would respond as all tags. Another company, Tagzapper.com, has developed a handheld unit which would deactivate a tag. Targeted at consumers, at this time, the company has not released details of their product (www.tagzapper.com). It is safe to guess that the intent is to fry the circuits.

Why use RFID as a Security Measure?

There are a number of valid reasons to look into RFID as a security measure. Perhaps one of the most important is that it requires no human intervention. As the tag is moving through its life, it will respond to communications from readers. This happens automatically. And can be inconspicuous so as not to alert or annoy. Both tags and readers can be disguised or hidden. Human intervention or interaction can be a weak link in the security chain. Following a lengthy security procedure can be taxing for people. Even the most security minded person can be tempted to cut corners.

Another important feature of RFID is that it is non-contact. While the tag may have a very short range of operation, it does not require contact with the reader to communicate. The optimistic long range limits vary so widely that it is clear it can only be assessed by physical tests in the application environment. A commonly noted limit is around 30 feet. Under 30 feet still allows for a great amount of coverage. It certainly encompasses the standard doorways, auto toll lane widths and supply chain conveyor belts.

Since the communication does not require line-of-site, less effort needs to be put into object orientation as it goes into the reader field. And the tag can be embedded inside a more convenient use container. For example a car security tag can be easily embedded inside a key shape.

The ability to get a reading quickly, and read multiple tags at once are other security application attributes. Since a typical RFID application would be reading a tag at different points in its movement, being able to identify an item is now missing is important. Even more so when the items are together in some larger packing unit. The detection and notification in real time are invaluable in reducing incident response time, especially in application such as theft detection. This is another area where technology will only improve. Today multiple reads is possible by software collison detection. The vendor deploys an algorithm that detects multiple tag responses, determines which response to accept, and then proceeds to re-query the group until all tag responses have been registered. Vendors are researching ways to build this into the reader hardware to make it possible to have true multiple reads. This would result in even faster read times.

RFID tags are very durable. They can survive years of the washer and dryer. In label form, they remain usable when scratched or dirty. Of course embedding them in a sturdy case increases their durability. In smart card applications, an embedded RFID tag is not susceptible to de-magnetization as magnetic strips are. So there is less chance it will fail in the field. The tag can be damaged by blunt force injury, say a hammer, or by removing the antenna, and microwaves will fry the circuits. Under normal conditions tag life is 10 years or more.

Assessing RFID

Ideally any decision on whether RFID is appropriate for a security application should be based on a Risk Assessment. Looking at the "three bedrock principles" that a secure application would need – confidentiality, integrity, and availability – along with assessment of any threats and vulnerabilities provides the information needed to decide.

SANS Institute publications define a vulnerability as "a weakness in your systems or process that allow a threat to occur." (Cole et al, p.27) What are the vulnerabilities and threats involved in using RFID? Any comprehensive examination would factor in the application and environment where its use will be deployed.

Confidentiality speaks to the level at which the information carried by RFID is protected. The minimum amount of information would be a single identification number, theoretically that number would be globally unique. The ID number is used to map into a larger remote database which contains more extensive information. So confidentiality in the simplest case is enforced by the security of the remote database. Or is it? In the case of a globally unique ID, the number itself, since it is unique, is itself sensitive information because it relates to only one tag. Accumulation of readings for a unique ID taken together could compromise confidentiality.

RFID readers are still fairly expensive which limits the availability, but any one with a reader can scan tags. Plus it will not be long before there are more software utilities like RFDump. "***RFDump*** is a tool to detect RFID-Tags and show their meta information: Tag ID, Tag Type, manufacturer etc. The user data memory of a tag can be displayed and modified using either a Hex or an ASCII editor. In addition, the integrated cookie feature demonstrates how easy it is for a company to abuse RFID technology to spy on their customers." (Grunwald, p.1) While this utility speaks to information privacy issues, it can also be used by an enemy in a military situation or a competitor in a business situation to threaten confidentiality.

A bigger concern may not be that a malicious reader is set out to sniff information, it is that a radio frequency scanner and an antenna could be used from a mile away to intercept data exchange with the reader. Prudence would suggest that encryption of sensitive data is critical. The current cost associated with encryption may be stopping its more widespread use. In particular since many applications are not making encryption a requirement, even when the data may be sensitive as in traveler passports.

While encryption of the data stored on the tag, or encryption of the information stream as it passes between tag and reader are possible, this drives up the cost, significantly in some applications. The minimum tag cost is still somewhere in the .25cent (US) range – this is for the dumb version that merely listens and responds, and does not validate who it is responding to. It is pretty safe to say that current mass tag deployment, especially in the supply chain, is of low cost variety that does not incorporate encryption.

"Many companies, trying to comply with requirements by the DOD, Wal-Mart or other retailers, are taking a "slap-and-ship" attitude about RFID by making minimal investments to meet the requirements, said Reik Read, an analyst at Robert W. Baird & Co." (Gross, p.2) Unfortunately minimal investment implies little or no attention to security. Potentially this is more serious in a DOD application than a retail supply chain. Do we want anyone with a reader to how what military supplies are being shipped from location A to Iraq? Not to minimize the importance of protecting business data, Target may be very interested in how many pallets of shampoo Wal-Mart is getting from Proctor & Gamble every month.

The financial industry is really the leader is deploying secure RFID applications. "Personally identifiable data elements subject to privacy regulations are Triple-DES encrypted on EMV cards. The latest contactless EMV cards are based on the ISO 14443 standard card, which can be read from only within 10 cm. " (Willoughby, p.3) The attention that is paid to security, authentication and encryption by industry vendors such as BULL reenforce the power that regulations can wield. Interestingly, while labeled privacy regulations, to a large extent they also help reduce fraud and theft that can effect the business bottom

line. Creating a duplicate, fraudulant card is more difficult with RFID than it is with magnetic strip cards.

When we look at the integrity of the information the tag provides we want it to be reliable. Again, in the simplest case, the tag will merely provide an ID number. Given a read-only tag with a globally unique number, there is a high degree of integrity. Once we move into the world of read/write tags, or even read-only tags that can be assigned an ID by the deploying entity, the integrity level drops. If the tag can be changed as it moves through its life, then the integrity of the information is related to how trusted the readers that it has encountered are.

The threat to data integrity in a closed, or closely controlled environment is easier to assess. The movement of goods within a warehouse has a high degree of reliability since it is accessed by readers deployed by the warehouse owner. When a pallet of goods is shipped from the warehouse to an overseas location, it will pass through any number of stops at which point it is vulnerable. It may sit for weeks on a shipping dock suseptible to tampering. Of course the real importance of this threat is measured in how important the data is to the business. If this is a pallet of sweatshirts maybe not so important. If this is perishable goods, how long it takes to get from source to distribution is important.

RFID excels when it comes to providing data availability, especially in the simplest case. A tag has no higher purpose than to answer a request for its name, rank and serial number. While there are physical limitations to a tag's ability to answer a request, in the general case they are not compelling enough to prevent an in depth assessment. Items containing liquid or metal are especially hard to chip. Liquids tend to absorb the energy needed to power the chip and metal tends to reflect it. Vendors are constantly working to overcome limitations for specialized applications. For example, the human body often disrupts RFID communications; however, recently RFID vendor VeriChip announced "the world's first implantable radio frequency identification (RFID) microchip for human use, has been cleared by the U.S. Food and Drug Administration (FDA) for medical uses in the United States". (VeriChip.com)

Noise in the target operating frequency needs to be evaluated in the deployment environment to make sure availability is not compromised. It is important to do live on-site testing using the expected target frequency. And to perform this testing over a sufficient span of time to be sure that some periodic event would not create conflicting noise. These are the limitations of the technology that would be investigated by any competent assessment.

There are bigger threats to availability. These are threats which could originate from a malicious source, or from a sloppy technology implementation. The signal could be jammed using energy at the right frequency. The tag could be disabled, or "killed", by error, or by use of a tag zapper technology. Or a reader could be overwhelmed by using a blocker tag to obscure the valid tags. "The

operation of a basic blocker tag is quite simple: It simulates the full set of 2^a possible RFID-tag serial numbers." (Jules et al, p.11) While the blocker tag is being investigated as a privacy tool, its ability to disrupt data availability rises to a critical level if it were used to masked the location of a visitor in a secure facility.

Availability is compromised when the tag is physically damaged or destroyed. A thief would try removing, puncturing, or crushing the tag. The bigger the tag, the bigger is this threat because it is easier to spot.

Data becomes unavailable when the tag is sheilded. Metal containers, certain types of electro-static bags and moisture are known problems. Damp cardboard can interfere with the signal between tags and reader. Some times these problems can be solved by changing the placement of the tag on the item. This assumes the tag was not intentionally sheilded.

Any in-depth assessment requires that the specific needs of the application be taken into consideration. This can be a rather complex process, and is often difficult to generalize even within a specific industry. For example, RFID is being widely deployed in supply chain applications. While there is some set of good business practices, the weight of any threat is ultimately based on what the business can, or will, bear. At this time, it seems that cost is a major factor to consider when looking at security in an RFID system.

Conclusion

RFID is a compelling technology with a rapidly growing list of applications. It is the de facto bar code replacement with mass adoption only a matter of time. One of the factors slowing growth is the cost is still not in the no-brainer range. This delays return on investment in a climate of cautious economic growth. For those driven to adopt RFID, cost containment can mean buying into the low end of the technology where built-in security is non-existent. This can be acceptable in environments where many security tools are deployed, or in closed environments. However, the near term mass deployment of RFID looks to be in response to mandates by large retailers, and large government. And it is safe to guess that your local quickie mart is not going to implement any more than is necessary at this point. Current economics are not facilitating on-board security for any but the regulated applications. This leaves a whole lot of information suseptible to sniffing and tampering.

Any amount of research on RFID will quickly turn up the growing issue of privacy concerns. Keeping these concerns front and center has increased vendor attention towards securing confidentiality of the data carried by RFID. As a pleasant side-effect, this vendor attention will no doubt result in better and cheaper security than may have evolved in a more privacy complacent atmosphere.

Access control cards have a long history of providing security, and the growing use of by the finiancial industry of RFID in smart cards confirms that the technology can assure confidentiality when regulations exist. Without the forced incentive of compliance, the majority of the tags and readers deployed in the short term will not be the higher cost models that employ encryption. To keep costs low, the burden of security will remain at the central data repository. However, RFID can be secured for those willing to make a bigger investment.

For this example, we will suppose that we have a small museum with approximately 100,000 items. The items have values that range from zero to half a million dollars. The genre of the museum is such that the items range in size from inches to 10 feet. They can be made of wide variety of materials including ceramics, fabric, wood, canvas, metal, plastic, and paper. The items already exist so there is no opportunity to embed an RFID tag during the manufacturing process. Further, size, value or material may restrict how a tag may be affixed to an item.

Important threats to a museum include loss or theft of items, and damage to items that may result in decreasing value. Demonstrated inability to secure the location and condition of the item jeopardizes not only the overall value of the museum, but also reduces the confidence of donors who may be interested in lending or gifting items.

Examining RFID as a technology to mitigate risk of these threats in the museum, there are several areas where the technology can be deployed.

Physical access is an important vulnerability. While physical access to public areas must be controlled mainly by security personnel and video monitoring, the public areas are not where the bulk of the items reside. The use of employee smart identification badges, and access control readers to limit access to collection storage areas is a good fit for RFID. Access control is perhaps the most widely used application of RFID. RFID tags in the badges can both authorize access by opening a lock, and log entry into any location, including those that do not require locks. Additionally, visitor badges could contain tags that cannot open a lock, but can help keep track of visitors who are going to be in non-public areas. Especially when one person may be escorting a group of visitors, it is hard to prevent people from wandering. If a visitor wanders into a restricted area, a reader could trigger a notification event like an audible alarm.

Obviously, physical possession of an authorized badge allows one to gain access. But a lost or stolen badge can be shutout very quickly. Plus it still continues to provide tracking information until it is shutout.

Securing the possession of the items is a great vulnerability. Theft is an obvious threat. Misplaced items are a less obvious threat, but it can happen in an environment where an item does not have one right place to be. It may be in

storage, it may be on public display, it may be in a staging area, or it could be under repair. Any museum would have some procedure in place on tracking items. These procedures normally involve human intervention, which can be a weak link in the chain. RFID has the great benefit of removing a lot of the human intervention from item tracking. Strategically placed readers can track tagged items from storage right onto the display floor. Unlike bar codes which require a button to be pressed, RFID can work without disrupting the movement of the item. In the case of a fire or flood when all good procedures might be bypassed, a network of readers could track the items as they are moved to safer locations. Of course if an item is removed from the building, it may only be tracked to the door.

In order to track individual items, an RFID tag must be attached to the item. And preferably the tag is securely attached to the item in a inconspicuous spot. Inconspicuous both to not advertise its presence, and to not interfere with the presentation of the item. If the tag must be removed to display the item, then any benefit is defeated. Current technology supports very small (microns) tags, and they will continue to work in this direction. The tag size is not as problematic as how they will be affixed to an object, an issue that is related to physical materials of the item. One especially problematic material is metal since it causes reflections in radio waves.

The problems caused by metal represent a vulnerability of RFID in the museum example. Not only as it relates to tags being applied to items, but it also interferes with the ability to completely track items. A knowledgeable thief would bring along a metal case.

In the ideal world, all the items in the museum have an RFID tag. Readers are placed in strategic locations to track movement. There are also mobile readers for inventory. Since RFID tags can automatically respond to reader requests without human intervention, I can inventory my 100,000 items by merely walking my storage areas and display areas. Except that most museums use metal storage shelves, racks and cabinets. There are tags that work better in adverse conditions, and vendors are striving to improve the technology. Testing RFID tags and readers in their deployment environment is important so that the optimal components can be used. While inventory is not going to be a walk in the stacks, moving in for closer proximity reads, and opening cabinets and drawers still provides an efficiency improvement over doing bar code scans.

The environment in item storage locations is another area of vulnerability. Light, temperature and humidity must be monitored and controlled. Not only is this the ideal environment to deploy RFID, it can assist in monitoring and alerting. RFID tags placed at various locations within a collections area, and periodically polled by a reader, can trigger alerts for damaging changes in environment. This can be taken to the item level and provides an efficient way for the display environment to be optimized for a group of items.

Bar codes are commonly used by museums to do inventory and asset tracking. RFID can easily handle not only this task, but can be deployed effectively as a security tool.

References

1. Shepard, Steven. RFID: Radio Frequency Identification. McGraw-Hill, NY, August 2004. (NOTE: Interestingly the copyright date in my copy of this book says 2005)

2. RFID Journal News. "Wal-Mart Draws Line in the Sand". RFIDJournal.com. URL: http://www.rfidjournal.com/article/articleview/462/1/1/%20 (June 11, 2003)

4. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. et al. SANS Security Essentials and the CISSP 10 Domains: Defense In-Depth. The SANS Institute, January 2004.

5. Best, Jo. "RFID: The tags that would not die". Silicon.com http://hardware.silicon.com/storage/0,39024649,39120757,00.htm (May 17, 2004)

6. Juels, Ari. Rivest, Ronald. Szydlo, Michael. "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". 2004 White Paper for RSA Laboratories, MA http://www.rsasecurity.com/content_library.asp?type_id=22&region=&id=

7. Grunwald, Lukas. Wolf, Boris. "RFDump". RF-Dump.org http://www.rf-dump.org/about.shtml.

8. Gross, Grant. "Speakers debate RFID benefits, challenges". ComputerWorld http://www.computerworld.com/softwaretopics/erp/story/0,10801,96259,00.html (SEPTEMBER 29, 2004)

9. Willoughby, Mark . "Securing RFID information". Computer World. http://www.computerworld.com/softwaretopics/erp/story/0,10801,96051,00.html (SEPTEMBER 20, 2004)

10. BNTng EMV™ Technical features. Bull Web Site. http://www.bull.com/security/BNTng_EMV-tech.html

11. VeriChip Web Site. News & Events. http://www.4verichip.com/nws_10132004FDA.htm (October 13th 2004)

12. Singel, Ryan. "American Passports to Get Chipped". Wired.com http://www.wired.com/news/privacy/0,1848,65412,00.html. (Oct. 21, 2004)