Global Information Assurance Certification Paper

SANS Institute – GIAC Security Essentials Certification (GSEC)

Practical Assignment Version 1.4c, Option 1

RFID Technology: The Risk and Reward

GSEC Practical Assignment

Aaron Legner

February 11, 2005

Table of Contents

Abstract/Summary……3

RFID Background……3

Useful Implementations……4

Security Vulnerabilities……6

Security Solutions/Mitigations……8

Conclusion……10

References……12

Abstract/Summary

The search and collection of consumer data and buying habits, inventory management and shoplifting are three areas that retailers focus on in today's market. One piece of technology that is making all of that easier is RFID Tag technology. Radio Frequency Identification (RFID) is starting to be deployed for use at large retail stores such as Wal-Mart. The concept behind the RFID tags is that it is a very low cost, simple way to track products within a store to combat theft and to store information such as the price of the product or the quantity left in inventory. These tags, which can be as small as a half millimeter, currently cost about $.05 per tag. The size and cost associated with this technology only increase its popularity. There are also other ways that RFID technology can be used as a benefit, which will be explored in this paper. However, one major flaw with RFID Tags is its inherent lack of security. The security vulnerabilities associated with RFID technology can be exploited by both the consumer and the retailer. This paper will also examine how a very useful technology is being misused to the point that the negatives may outweigh the positives; to the extent that until proper security is formed around Radio Frequency Identification it should be used in a limited fashion. RFID tags could be used negatively by retailers using the data to prey on consumers for financial gain, or used by police to constantly monitor civilians, which would violate their right to privacy. These tags can also be used harmfully by hackers who can alter the data on the tags to change a high priced item in a store to a very low priced item and simply walk through the self checkout unnoticed. While there is a lack of security, some solutions are being developed to help lessen some of the concerns. The intent of this paper is to present factual information regarding RFID technology. In turn a reader should feel capable of making informed decisions on the subject of whether or not RFID technology is right for them or their place of business.

RFID Background

The basic concept behind Radio Frequency Identification technology is a small silicon chip that is wrapped in paper or plastic, attached to an antenna. This chip can then communicate wirelessly with a reader. The silicon chip's size can vary but can be as small as a millimeter or as big as a quarter. The storage capacity on these tags is very small allowing only a limited amount of data storage on the chip. RFID technology is somewhat similar to bar code data collection technology. Even though the storage capacity is small, compared to

newer media, RFID tags can hold much more information than the traditional bar code, which can only hold a product or account number. Their functionality consists of listening for a radio query and responding by transmitting their unique ID code. The query that is sent out also contains enough power that most RFID tags don't need batteries, which helps keep the size small and the cost down. Currently RFID tags, made by Alien Technology, can be read up to 15 feet away (McCullagh). However, as time goes on one can imagine that the range will only grow. Even now hackers can create more powerful receivers that don't comply with FCC regulations, which can be read from much further away than 15 feet. According to Lukas Grunwald, Radio Frequency Technology operates globally on different frequencies, the most common using the ISM (Industrial Science Medical) bands (Grunwald).

There are three basic kinds of RFID tags available today, but given the scope of this paper and basic functionality differences, we will combine the differences into two types. The different categories are passive and semi-active/active. Passive tags are the cheapest and the most prevalent today. As described above, passive tags have no batteries and obtain power from the radio frequency field of the reader. Semi-Active and Active chips have a much broader range and greater storage space because they have a built-in on-board power source. Since these tags provide greater functionality and are inherently more complex, they cost considerably more. However, both of these types of tags offer a read-only or a read/write version. The read-only tag can be programmed only once and read multiple times, whereas the read/write version can be read and written to multiple times. While the read-only version may provide some added security, they are not used as much because the lack of reuse costs more money. The read/write style of chip is used more for providing greater versatility to be used multiple times or corrected if a mistake is made.

Useful Implementations

As stated earlier, Radio Frequency Identification Technology can provide benefits to both consumers and retailers. At around $.05 per chip when bought in bulk, with most being smaller than a penny, size and price make them very attractive to retailers. A store could add these tags to its products to track inventory. Every time a consumer bought a TV or a box of laundry detergent a radio frequency could be sent out decrementing the total number in the inventory. In fact, stores like Wal-Mart and Germany's Metro Group are preparing to do just this for advanced supply chain management. The amount of savings this could bring to a store is quite staggering. This technology would provide efficient stock management and reduce instances of items being out of stock. When Lukas Grunwald spoke at the Blackhat briefings in 2004, he stated that many manufacturers and supply chain companies could benefit from the use of RFID technology by allowing for easy integration at the product plant, providing tracking and sorting of boxes and goods as well as just-in-time

production and tracking of the maximum and minimum temperatures for sensitive goods (Grunwald). RFID technology can also help retailers reduce theft, which cost the industry close to $50 billion a year (McCullagh). If a company added these tags to their merchandise and a thief tried to steal it, a signal could be sent out that would sound an alarm and notify the store of a shoplifter. Since the tag is so small and can be hidden easily, most burglars wouldn't even know the tag was attached to the product.

Another useful implementation of RFID technology is adding tags to all library books to make libraries more efficient. RFID tags could provide for a speedier book checkout and return process. No longer would a librarian have to search the entire library for a misplaced book. He or She could simply send out a radio frequency signal and wait for the tag to respond. According to a report written by Alorie Gilbert, "RFID systems are already in place or soon to be installed at more than 300 libraries in the United States and millions of books tagged. There is little doubt that the long-heralded arrival of a huge RFID wave is for real" (Gilbert). In fact, libraries are on the bleeding edge of RFID technology and are further along in the implementation than any other merchant or retailer. Their use of RFID technology could pave the way for a much broader use. They could help work out many of the bugs and security holes so other companies would be more inclined to use the equipment. One reason for the large scale deployment is that library books and other borrowed materials are different, because they are supposed to be returned. Each book is tagged and should not need to be replaced. New tags would only be needed for new books. In the retail world the tag is lost after each sale, so it may not be economical to place a RFID tag that ranges between $.05 and $.25 a piece on each pack of gum if net profit on that item is less than that.

Another use for RFID technology which is slowing rolling out today is that hospitals are placing RFID chips underneath an employee's skin to be used as an authorization biometric. According to an article written by Michael Kanellos, of CNET news.com, "VeriChip sells 11-millimeter RFID tags that get implanted in the fatty tissue below the right tricep. When near one of VeriChip's scanners, the chip wakes up and radios an ID number to the scanner. If the number matches an ID number in a database, a person with the chip under his or her skin can enter a secured room or complete a financial transaction."(Kanellos) The last step to determine whether hospitals can use this technology is the final review by the FDA, which is currently underway. What makes this very interesting is that the FDA is not really questioning the chips from a health standpoint. Instead, they are concentrating on the privacy aspect. If an employee had this implanted to be used at the hospital, the tag would also be active away from the work. The hospital, or even an ordinary person with and RFID reader, could follow this person and track every place he/she were to go. However, this same process can also be used to identify patients when they come into a hospital. If a patient were to come into a hospital unconscious or without a form of identification (e.g. driver's license, social security card) the tag

could be read and would associate the patient to their records. This will allow doctors to immediately know the patient's history and any drug reactions.

Finally, the last benefit to RFID technology we will look at is how Radio Frequency Identification technology is being used to produce highway traffic reports. According to Carol Swedberg, the goal of the Orlando/Orange County Expressway Authority is to implement a system that would "trace the travel time of individual cars as they pass the roadside readers, create an average trip time and then disseminate that information to the public" (Swedberg). Readers or receivers that are positioned about every ½ mile to one mile will track cars passing by and transmit the data to the department of transportation with information like traffic time and flow. The local news and radio stations could then pass this information along to drivers so they could avoid heavy traffic and other travel delays as they make their commutes. However, Florida has implemented a system that takes news and radio out of the equation. They have developed a technique that would send traffic and travel times to message boards that drivers could read and then make their route decision based off that information. The Florida Department of transportation says the information scanned in by the roadside readers is encrypted before it is sent over the wire and the data is eventually destroyed when it is no longer useful (Swedberg).

Security Vulnerabilities/Threats

Now that we have taken a look at the many ways Radio Frequency Identification can be useful, we must now look at the ways it can be hacked or used in a harmful manor. First, we will look at how a retail store or a user of the RFID technology can exploit it in an improper way. One of the biggest risks and fears of RFID technology is that it will be used to collect private data that consumers do not want kept about them. Those opposed to RFID technology like to use the slippery slope argument that someday in the future we will all be tracked by the chip or tag that's been sewn into our clothes or placed on the bag of chips we just bought. Declan McCullagh wrote an article called "RFID Tags: Big Brother in Small Packages" and he paints a pretty scary picture of how RFID tags could be used unlawfully. In his article he writes,

> *"Imagine: The Gap links your sweater's RFID tag with the credit card you used to buy it and recognizes you by name when you return. Grocery stores flash ads on wall-sized screens based on your spending patterns, just like in 'Minority Report.' Police gain a trendy method of constant, cradle-to-grave surveillance. You can imagine nightmare legal scenarios that don't involve the cops. Future divorce cases could involve one party seeking a subpoena for RFID logs to prove that a spouse was in a certain location at a certain time. In all of these scenarios, the ability to remain anonymous is eroded." (McCullagh)*

While that scenario is pretty over-the-top, it does bring some very valid points to light. If a clothing store were to place tags in its clothing to store personal information on it, they could read that article of clothing and immediately know if you are a big spender or not and what types of clothes you have bought in the past. In fact, KSW-Microtec, a German company, has invented washable RFID tags designed to be sewn into clothing. Another thing that McCullagh touches on in his article is the use of RFID tags by private citizens to prove where people were or were not at a certain time. Even though there are currently other ways of doing this today, those methods, such as GPS satellite tracking, require much bigger chips that cannot be hidden as easily and are much more expensive.

The same basic theme keeps coming up when people talk about the possible exploits or abuse by retailers or users of RFID tags for legitimate reasons. Privacy and security are the two biggest issues that people are concerned about when it comes to RFID technology. As stated above, some feel that if Microsoft, for example, were to place RFID chips in all of their MP3 players for purposes of shipment tracking and anti-theft purposes, they may be tempted to use it in a violation of privacy or even the law. The thought is that if someone were to buy a Microsoft MP3 player and carry it around with them while they go on a walk or a trip, Microsoft could track them where ever they go. While this scenario may not be likely, the fact that it is a possibility could prevent companies from being able to use RFID tags on individual products. Another thought is that the police or law enforcement could take advantage of this type of equipment and use it against people. While some think that the police could benefit from the use of RFID tags, others think that it may be taken too far and violate a private citizen's right to privacy.

Now that the ways to exploit RFID technology from a retailer's standpoint have been discussed, we should now examine the ways consumers or end users could take advantage of RFID technology. One of the most common examples used to show how a consumer can manipulate a RFID tag is using some sort of RFID device or receiver that has been hacked or altered to change the price of the targeted product as a way to steal it. For example, someone with impure motives decided they wanted to pay $8 instead of the asking price of $20 for a DVD at the local Best Buy store. To do this they could pull out a personal digital assistant or even a modified cell phone that is outfitted with a RFID reader. They could then go to the sale rack, pick up a discounted DVD, read in the RFID tag on that case and download the information to the PDA or cell phone. Then they could manipulate any data they chose, or not change a thing, and upload the discounted pricing information back on the $20 DVD making it $8. Then when he or she goes to the checkout register they get charged the lower price and the clerk has no idea that anything happened. The picture painted above could be made even easier if the store has automated self checkout counters. This way the hacker could more significantly change the data stored on the tag and walk through the self checkout without ever having to

interact with a human. Some teenage kids trying to play a prank may do the same type of thing but instead of actually walking out with the item they could just swap tags and change the price for fun and sit back and watch while someone gets charged $24.99 for a bottle of soda. While some may think this is funny and others do not see the harm, this type of prank could cost a large retailer hundreds and thousands of dollars by forcing them to close their store and conduct a physical inventory. A different way that pranksters can abuse RFID technology is by creating some sort of jamming device that could overload and destroy all RFID tags within a certain radius. This would be the RFID equivalent to a buffer overrun or overflow attack. Think of the damage someone could cause if they walked into Wal-Mart or Target and just started overloading every tag, with which they came in contact. The cost to fix this type of problem would almost completely outweigh any benefit gained by the use of RFID tags. A different way RFID tags or chips can be bypassed is by shielding the field so that no RFID reader could actually read the tag. In this case a shoplifter would not need an expensive RFID reader or hacking software. All they would need is something as simple as aluminum foil and the RFID anti-theft chip could be avoided.

The scenarios discussed above are not improbable. Many shoplifters steal goods and merchandise today on a regular basis, somehow bypassing electronic security in one form or another. By changing the price stored within the chip a thief can "steal" a product in a very inconspicuous way. If retailers lose almost $50 billion a year on theft, think how much more they will lose when RFID tags become more prevalent. An additional way RFID tags can be used by thieves is to find RFID tags located on the boxes of expensive electronics. A thief could get a high powered RFID reader, that has been modified or hacked, and survey a dumpster or garbage cans outside a house looking for high priced goods. Think of it as a new technological way to dumpster dive. Once the thief got a "hit" on something that could be high priced, they know that expensive goods are around and they could then break into the nearby houses looking for those goods.

The worry and concern over RFID tags being abused and exploited by consumers boils down to manipulating data on the chip or blocking the radio frequency. If the data is changed it could cause confusion and chaos for store owners resulting in loss of business and additional expenses to correct the problem. The other data manipulation scenario is that the data is changed so that a product is at a lower price or an item that had an age limit or restriction is removed. The last exploit concern is to simply block or completely deactivate a RFID tag rendering the chip and functionality useless. All of these are valid concerns and questions because currently the necessary level of security for Radio Frequency Identification does not thoroughly exist. Because the security for this technology is in its infancy and was designed without security in mind, it opens itself up for almost every hacker attack that been exploited. It may be the types of attacks discussed above or the more common computer type attacks

such as a denial of service attack, worm, or a virus.

Security Solutions/Mitigations

Now that we have discussed many possible vulnerabilities and exploits of Radio Frequency Identification we must now look at ways to mitigate the risk associated with using this technology. Since the various security weaknesses in RFID technology have been widely reported on, many security solutions have been developed or at least proposed. Some solutions are focusing on protecting customers and consumers from a violation of privacy while others are centered on safeguarding the retailer or user of RFID tags for business purposes. The Utah House of Representatives passed a Radio Frequency Identification Right to Know Act. Just prior to that, California State Senator Debra Bowen introduced a comparable bill. The bills in Utah and California require that consumers be notified if RFID tags are placed on products and that those tags be "killed," or deactivated, before they leave the store. Taking it even further, the California bill also requires a consumer's consent before personal information can be collected by RFID or sold (Claburn). This shows that states are taking it upon themselves to introduce legislation that will help protect its citizens from being unknowingly and unwillingly tracked or having personal information recorded, stored and possibly even sold. This in no way means that it cannot happen or will not happen, but it greatly reduces the chance and puts some responsibility and pressure on the organizations using RFID tags. Along those same lines, stores and places that have put RFID technology to use could voluntarily post signs or banners stating that they are using RFID tags. This type of disclosure would also coincide with some sort of privacy policy stating that the information collected will not be used without consent and will not be sold. The privacy policy could be very similar to the ones commonly used by credit card and insurance companies. Another type of voluntary act users of RFID technology could employ is the same “killing” or deactivation that is required by law in Utah and California. This process would be very comparable to a register clerk removing the plastic security tag from a pair of jeans at a clothing store. However, in this instance as soon as the product is considered bought or sold, a signal would be sent out that would disengage the RFID tag and prevent it from ever being turned back on.

RSA security has also come up with a few ways that consumers can protect themselves from the risks associated with RFID technology (Protecting, RSA Website). RSA also believes that “killing” RFID tags after the intended use is an appropriate way to protect end users. They have also come up with a RFID tag called the “RSA Blocker Tag”, which is designed to “spam” any reader that attempts to scan tags without the right authorization. According to RSA’s website, “Thanks to their selective nature, blockers do not interfere with the normal operation of RFID systems in retail environments. They prevent unwanted scanning of purchased items, but do not affect the scanning of shop inventories” (Protecting, RSA Website). Therefore, the usefulness of these tags

has not been lost but the protection has been increased greatly. The latest concept that scientists at Intel have been working on to help protect consumer privacy is using distance measurement to determine if a RFID reader is authorized to read the tag. These scientists have discovered that RFID tags may be able to estimate the distance of the reader from the tag by using the signal-to-noise ratio of the transmissions they receive from a reader. Then, with the distance calculated, it could imply that the reader is an appropriate distance away and would therefore trust it (Protecting, RSA Website).

While those security solutions relate to customer privacy, Pete Abell, an RFID consultant at Boston-based EPCGroup has come up with three proposed security solutions that could help alleviate some of the risk associated with using RFID technology. His three recommended solutions are to have devices in stores that could detect outside readers, program the RFID tags to only respond to certain readers, and increase the encryption to a more advanced level (Hesseldahl). RFID readers send out signals to "talk" to RFID tags. Abell's first suggestion is to create a device to scan and search for unauthorized readers sending out signals and alert someone that such activity is going on. This is the same type of concept as a radar detector, detector. This would help prevent people from bringing in such readers or scanners to change and manipulate data. The next solution that Pete talks about is to program the tags to only respond to specific readers. The company using the tags could program all of their tags to only respond to a certain few readers that are owned and maintained by the company. This would prevent hackers from being able to modify the data stored on the chip. Abell's last suggestion is to have more advanced encryption on the RFID tags. Most of the tags used today either have no encryption on them or 8-bit encryption, which, in the eyes of a hacker, is like not having encryption at all. This last idea is a good one but the types of tags that can store sophisticated encryption cost much more than the standard chips. In order for this to be a viable option, the cost will have to come down.

Many scientists have also been trying to develop ways to help prevent RFID tags from eavesdropping and have come up with two main ways to help companies that use RFID technology. The first, offered by researchers at MIT, is called silent-tree walking. The concept slightly modifies the standard reading protocol for RFID tags and eliminates reader broadcast of tag data. The second security solution is being worked on by RSA Laboratories. Their solution changes the appearance of the RFID tag through the use of pseudonyms by carrying multiple identifiers and emitting different identifiers at different times. Therefore, outside transmitters would not be able to read the tags. However, legitimate readers would be capable of reading the different identifiers from one tag (Securing, RSA Website).

Conclusion

Radio Frequency Identification technology can help retail companies, shipping and delivery outfits, libraries and even the medical world. These RFID chips can be embedded into almost anything, including the human body, and are gaining in popularity. The benefits they can provide are countless. From helping prevent theft to being used as a biometric, the usefulness of these tags and technology only seems to be limited by one's imagination. Many future thinkers envision a time where every person and every good has a RFID chip implanted in them. Grocery shopping will be as simple as selecting a good to buy and walking out of the store and being billed for those goods through the use of the RFID. The tags link you and your merchandise back to your credit card. The tags could even aid in the return of products without a receipt because all purchase information is kept in the RFID chip that is still located in the product. RFID chips can even be placed in cars and then used to determine traffic patterns and travel times. However, there is on major flaw with RFID technology that limits many implementations and may cause the full potential never to be realized and that is the inherent lack of security and controls. RFID technology has virtually no security associated with it and thus, has many privacy groups and lawmakers up in arms. The potential for privacy invasions and harmful hacking is alarming. RFID tags can be used to store personal information about people at the time of the purchase of a product like name, credit card number and other goods purchased at the same time. This in itself is not really that shocking or different from what currently happens today with barcode technology, however the big difference is the fact that RFID can still be read and tracked after the purchase. Everyone that has a RFID reader could track everywhere you went if something you were wearing or using had an RFID tag on it. These same people that have the RFID readers could also manipulate or change data stored on the chips to bypass security measures, change prices, or just wreak havoc for the sport of it. Therefore, even though there are many people working to develop security and controls for RFID technology, whether it is from a technological standpoint or legal, as it stands today these chips should not be used when security and privacy are extremely important. In spite of this, RFID technology is an ever growing and evolving science and could one day be used, in a secure fashion with consumer privacy in mind, to benefit a myriad of people.

References

Bruce, Lindsay. RSA introduces RFID blocker technology. (Online) Available <http://www.csoonline.com.au/index.php/id;132384534;fp;4;fpid;3> 27 February 2004.

Claburn, Thomas. Privacy Fears May Slow RFID Progress. (Online) Available <http://informationweek.securitypipeline.com/news/18311264> 8 March 2004.

Gilbert, Alorie. RFID, coming to a library near you. (Online) Available <http://att.com.com/RFID%2C+coming+to+a+library+near+you/2100-1012_3-5411657.html?tag=st.rc.targ_mb> 18 October 2004.

Grunwald, Lukas. Black Hat: Day 1 Briefings. (Online) Available <http://www6.tomshardware.com/business/20040730/black_hat-01.html> 24 July 2004

Grunwald, Lukas. RF-ID and Smart Labels: Myth, Technology and Attacks. (Online) Available <http://www.rf-dump.org/slides.shtml> 24 July 2004.

Hesseldahl, Arik. A Hacker's Guide To RFID. (Online) Available <http://www.forbes.com/business/commerce/2004/07/29/cx_ah_0729rfid.html> 29 July 2004.

Kanellos, Michael. Under-the-skin ID chips move toward U.S. hospitals. (Online) Available <http://att.com.com/Under-the-skin+ID+chips+move+toward+U.S.+hospitals/2100-7337_3-5285815.html?tag=nl> 27 July 2004.

Lemos, Robert. RFID tags become hacker target. (Online) Available <http://att.com.com/RFID+tags+become+hacker+target/2100-1029_3-5287912.html> 28 July 2004.

McCullagh, Declan. RFID tags: Big Brother in small packages. (Online) Available

<http://att.com.com/RFID+tags+Big+Brother+in+small+packages/2010-1069_3-980325.html?tag=nl> 13 January 2003.

Piquepaille, Roland. Innovative Uses of RFID Tags. (Online) Available <http://www.primidi.com/2004/11/20.html> 20 November 2004

Protecting Consumer Privacy. (Online) Available <http://www.rsasecurity.com/rsalabs/node.asp?id=2119> 2004.

Radio tags dress up RFID concept store. (Online) Available <http://att.com.com/Radio+tags+dress+up+RFID+concept+store/2100-1001_3-5269511.html?tag=nl> 14 July 2004.

Saita, Anne. Low-cost way(s) to 'foil' low-tech RFID tags. (Online) Available <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci999990,00.html> 12 August 2004.

Securing RFID Tags From Eavesdropping. (Online) Available <http://www.rsasecurity.com/rsalabs/node.asp?id=2118> 2004.

Swedberg, Claire. RFID Drives Highway Traffic Reports. (Online) Available <http://www.rfidjournal.com/article/articleview/1243/1/1/> 17 November 2004.

Tracking RFID progress. (Online) Available <http://americanprinter.com/prepress/workflows/printing_tracking_rfid_progress/> 1 January 2004.