An Overview of RFID Systems and their Security Implications

By: Caitlin Klein

I. Abstract

RFID has become a ubiquitous piece of technology entrenched in many peoples' daily lives. To name just a few of its uses, RFID has applications in access management, public transportation, identification, and health records. Since its conception there has a been a concern for its security based on its applications (access to high end companies and personal data) and ability to hack. However, in addition to being so widely used, RFID is cheaper to produce and faster to use then other technologies such as "chip and pin" cards. RFID also has wider applications in industries such as retail manufacturing and pharmaceuticals. For these reasons the technology will not be going away any time soon, therefore, it is necessary to ensure its security and integrity. This paper will be an overview of RFID technology with its weaknesses and corresponding defenses, culminating in an assessment of the overall security of a prevalent technology.

II. Introduction

RFID (Radio Frequency Identification) refers to a system that utilizes radio frequency to communicate wirelessly. An RFID system consists of a tag, a reader, middleware software, and a backend database. (Campbell). There are two types of tags: passive tags and active tags. A passive tag consists of an integrated circuit

with a radio transceiver. It is powered by the current that the RFID reader's signal induces in the tag's antennas. The signal from the reader produces enough power for the tag to send one transmission. As the signal is relatively weak, the tag must be close to the reader for the transmission to be read. An active tag also has a radio transceiver, but in addition it has its own power source allowing for the tag to be read at a greater distance than a passive tag (Igoe).

An RFID reader transmits radio frequency energy through one or more antennas to query tags and receive data from them. Middleware software provides three important functions: it connects to the readers, it processes the raw RFID data to be handled by other applications, and it provides an interface to handle readers and capture filtered RFID events (Glover).

RFID tags, readers, and middleware software interact with each other to provide meaningful data to a backend system. The reader sends out radio signals at a distinct frequency and interval through one or more antennas. Any tags within the proximity of the reader detect the frequency with its built-in antenna. The tag's antenna will only pick up certain frequencies based on the size and shape of the antenna. This means that not all readers and tags can communicate with one another. Tags, both passive and active, convert the radio frequency energy sent by the reader into electrical energy by induction from the reader's transmission. This powers the tag's semiconductor chip connected to the antenna which stores the tag's id. The tag relays this id back to the reader by raising and lowering the resistance of the antenna as a way to represent 0 and 1 bits. RFID middleware formats the stream of information obtained from the tags. The reader sends out

transmissions hundreds of times per seconds resulting in a lot of information to parse through. Middleware processes this data and provides a way for applications to receive only useful, relevant information that is essential to their function and to obfuscate the physical infrastructure of the RFID system (Glover).

RFID systems are great tools for tracking objects, merchandise and employees, and can be used to implement systems to control the number of products a retailer stocks and for access control in corporate buildings and in public transportation. However, RFID is transmitted wirelessly creating security risks that must be handled to prevent tag data from being corrupted and to prevent unauthorized access to both information and buildings.

III. To The Community

The use of RFID to easily track objects, from manufacturing to employees, has become integral to contemporary life. Retail stores make use of RFID for the purpose of preventing against theft, streamlining inventory checks, and even keeping track of the demand of products to ensure shelves are stocked and shipment orders placed accordingly.

Businesses use smart cards, implemented with the help of RFID, to handle access management – preventing unauthorized individuals from entering areas where their information could be compromised. Many cities transportation systems rely on smart cards to collect fares and process transfers. RFID technology has emerged in the pharmaceutical industry to combat counterfeit

drugs and to more accurately fill prescriptions. RFID tags are being placed in passports to better protect against counterfeits from being produced.

RFID systems are used in a wide range of industries. In most of them it has become so integral to the process that if RFID technologies were removed from them their efficiencies would drop. Accessing public transportation would take longer. Checking inventories and handling product demands would be much slower.

For these reasons, is it important to make sure that RFID meets the standards of having: confidentiality, only the intended recipient receives the message; integrity, the message received is the correct message and no substitution has been made; and availability, the system should be up and running. If RFID systems will be used for the foreseeable future, then they should be held to high standards of security.

IV. Action Items

RFID technologies are wireless based and because of the small chip size which makes up the tags, its encryption is weak making it is easily susceptible to attacks. Because RFID technology is wireless based, attackers have the advantage of not having to physically access the tags in order to clone them or modify their data (Haines). The attacker can do this by just being in the proximity of the RFID tag. However, most RFID tags, specifically the ones that would be cloned for access to monitored buildings, have a short range so the attacker would have to be fairly close to the individual. Also many buildings with RFID access control systems also have guards to check photo ids upon entering the premise. As in

most cases, the key to insuring that a system runs smoothly is to account for failures and to have contingencies based on them. This way if one method of securing something fails, there are other methods in place to prevent it from being fully compromised.

If an attacker is able to clone an RFID tag in order to access a building, a security guard should be able to spot them before they enter the site. If that fails as well, audit logs should be monitored and can report if a person enters the same are twice without having left, then potentially someone has cloned their access card. Of course, this only works if entrances and exits are closely monitored and if employees do not hold the door open for others. This system can also check if an employee enters at a time where they would not typically do so, say in the middle of the night, then the system can catch this discrepancy and report it.

Another defense against cloning or modifying RFID tags is deploying tags with cryptographic protocols. This prevents them from being easily cloned. When RFID tags do not have any authentication protocols in place then any reader that pings the tag will get that tag's data. Putting in place a way for a tag to know that the reader trying to access its data is authorized to do so, helps prevent against the unauthorized access of data. Authentication protocols help prevent against cloning, but are not always foolproof. RFID chips are small and have very little processing power. Because of this, it is difficult to use robust cryptographic algorithms. This way proven in the case of the MIFARE Classic system, a tag built by NXP Semiconductor. NXP developed their own cryptographic algorithm meant to fit on the chips in the RFID tags. NXP hoped to rely on security through

obscurity and it had worked for many years. However, twelve years after releasing their product a research duo, Henryk Plotz and Karsten Nohl, painstakingly cracked their algorithm (de Koning Gans).

The biggest problem with encrypting RFID tags is cost. Encrypting the data on the tags requires additional storage and processing power increasing the cost of producing the chips which when dealing on a large scale becomes quite expensive. In addition, if chips did have more storage and processing power they would be larger reducing the great benefit of RFID chips – their size. Since using robust, cryptographic algorithms on RFID tags is not feasible, manufacturers create their own challenge-response authentication protocols which could potentially be insecure and has in the past been proven that it can be reverse engineered in the case of MIFARE Classic.

One surefire way to protect against the tampering of RFID tags is to cover them in a layer of foil when they are not in use (Campbell). This acts as barrier and prevents the sending and receiving of radio frequencies. However, this becomes a compliance issue. Individuals need to use the protective cases on their cards and not consider keeping them in the cases when not in use an unnecessary inconvenience. If individuals do not follow this security protocol then it is useless.

Inversely the use of protective cases can be used to steal items that use RFID as an anti-theft device. For stealing multiple items, an attacker could also more efficiently modify the data on the tags associated with the items. Contingent on the retailer's use of RFID tags, an attacker could change the stock number on the tag so it does not appear missing, or modify the price and purchase the product at

a reduced rate (Campbell). With the increase in self-checkout kiosks, it would be harder to detect the fraudulent actions as a clerk is not overseeing the transaction.

V. Conclusion

RFID technology has been of great use since its inception. It has provided an efficient way to track objects wirelessly. Its applications are vast and far-reaching. While there are some concerns for its security risks, it is important to remember what security looked like before the advent of RFID. While RFID tags can be cloned and used to access buildings, these buildings were still susceptible to unauthorized entry before. Before RFID access systems, buildings were monitored by security personnel. However, security personnel are prone to error. They can fall asleep, not be paying attention to their job, be bribed, or be attackers themselves. Currently RFID provided an extra check to help reduce the risk of human errors. And although, RFID can be compromised security personnel are there as another security check. When dealing with security it is important to have contingencies so if one things fails something else will catch it and the whole system will not be compromised.

So while it is important to consider the very real vulnerabilities in technology, the human factor remains another security concern. A business could implement an RFID system where the tags are not susceptible to cloning or corruption, yet attackers could still get unauthorized access. Following a person through an open door as they hold it open. Claiming a card is not working and getting a replacement without going through the proper checks as the person responsible

for replacing cards does not want to create a hassle of going through the proper procedures.

Another important discussion when talking about security and vulnerabilities is risk management. A company is not going to want to spend copious amounts of money on upgrading a system which in the past has worked fine. Sadly even a company in charge of creating a product meant to handle security concerns will try to produce something less secure, but cheaper for both them and their clients. Companies frequently preform a cost benefit analysis in these situations. The greatest security protection in the world could be invented, but if it does not make sense in a business setting then it will not b implemented.

VI. References

Igoe, Tom. Getting Started with RFID. Maker Media, Inc. 2012.

Glover, Bill, and Himanshu Bhatt. RFID Essentials. O'Reilly Media, Inc. 2006.

Campbell, Anita, et al. RFID Security. Syngress, 2006.

Haines, Brad. Seven Deadliest Wireless Technologies Attacks. Syngress. 2010.

de Koning Gans, Gerhard. Outsmarting Smart Cards.