Project 4

RFID Technology

Caden Johnson

CNA 465

12/10/2020

# Table of Contents

[Table of Contents 2](#_Toc58414521)

[Introduction 3](#_Toc58414522)

[Section 1 3](#_Toc58414523)

[Basic Fundamentals 3](#_Toc58414524)

[Usage 6](#_Toc58414525)

[Vulnerabilities 7](#_Toc58414526)

[Security Measures 9](#_Toc58414527)

[Section 2 10](#_Toc58414528)

[Conclusion 13](#_Toc58414529)

[Bibliography 14](#_Toc58414530)

# Introduction

Over the course of this project, I will be going over the basics and implementation of RFID (radio frequency identification). RFID is a method of identification and tracking using wireless signals. You have probably seen this type of technology used for various purposes throughout your daily life. RFID can be used for almost anything including, but not limited to door locks, package tracking, identification badges, etc. RFID has been used to increase security and accessibility, but also has vulnerabilities similar to any other computer system. I will be going over the basics of RFID technology, where and how it is used, vulnerabilities and security measures associated with it, and finally, implementation of RFID using code and examples.

# Section 1

## Basic Fundamentals

First off, RFID technology consists of many parts. The main components that I would like to go over include the following:

Readers:

* Transmitter
* Receiver
* Microprocessor or computing device/system

Tags:

* Antenna
* Tag/transponder

To be clear, there are two main types of RFID. Passive RFID is the most common type to see in daily life due to the cheaper cost and increased usage. Passive RFID is much cheaper and easier to use for every-day things. In this case, the reader sends out a wireless signal, and the signal will bounce off of the tag and contain the data that is stored on the tag. On the other hand, there is active RFID, where the tag receives the wireless signal, then transmits its own signal back containing the data stored on the tag. The main differences between the two types (besides cost) are that active RFID tags must have a power source and the passive tags do not. This results in much farther accessibility distances for the actives tags. Passive tags most often have shorter ranges, and can typically use different frequencies depending on the requirements.

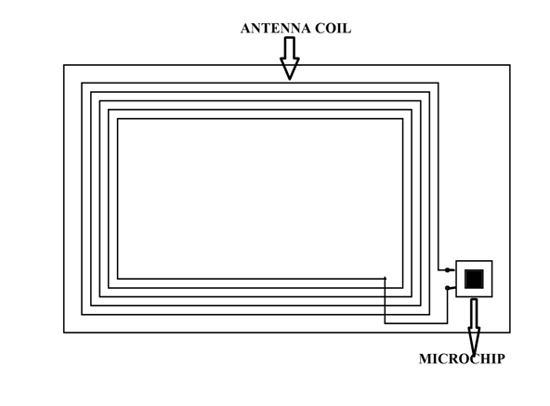
Passive RFID:

* Low Frequency (LF) = 125-134 KHz = around 4 inches
* High Frequency (HF) = 13.56 MHz = around 3 feet
* Ultra-High Frequency (UHF) = 300 MHz-3 GHz = around 30 feet

Active RFID:

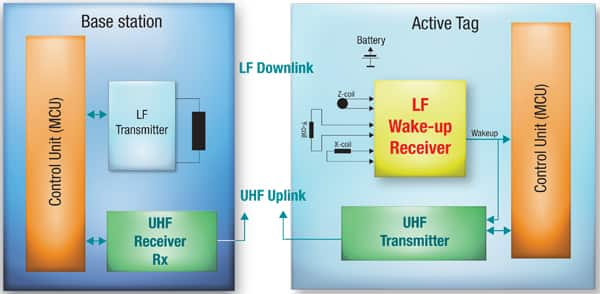
* 433 or 915 MHz = around 300 feet or more

Depending on the requirements of what you are using it for, you may want a RFID tag using a different frequency or maybe even an active RFID tag. However, as the frequency and distance increase, the chance of interference or loss of signal increases. Below, you can see an example of a passive RFID tag:



(RFID Tag, 2018)

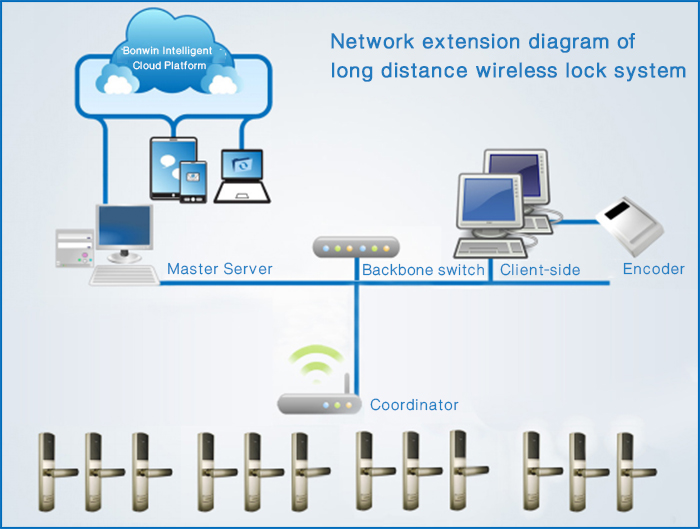
On The other hand, below is an example of an active tag. This example uses a low frequency to “wake up” the tag and an ultra-high frequency to transmit the data:



(Leoncavallo, 2011)

Next up, I would like to go over how the tags work. Like any type of data storage, tags can have many options. These include read-only, read/write, or WORM (write once, read many). Obviously, read write access is not always the most secure option since anyone with the right technology and skills can rewrite the data being stored, but this can also be beneficial in certain circumstances and can help save money if security isn’t as much of an issue. The amount of data able to be stored depends on the type of RFID tag and can range anywhere from only 64 bits to more than 32 KB. The range of readability and the amount of data stored all depends on what kind of tag you use and what you are using it for.

In many RFID systems, such as door locks, badges, etc., the metadata about usage can be transmitted from the reader to a system where it can be stored and/or analyzed. An example of this implemented by hotel door networks can be seen below:

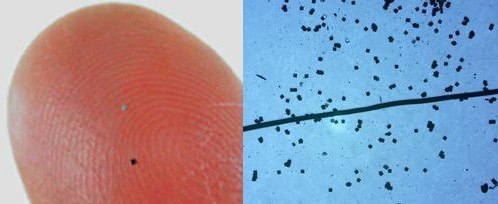


(BONWIN)

## Usage

With the amazing potential that this technology provides, and the ease at which it can be manufactured and sold, it is obvious why it is used so much in our daily lives as well as in various industries. Tags come in all sizes and ranges, and it all depends on what it is being used for. For example, badges, door keys, etc. don’t need much range, but require enough data to represent the user. Furthermore, when used, these systems keep track of usage in order to monitor who goes where and when. This can immensely increase security in a facility if managed correctly.

Secondly, RFID has found its majority of use through tracking packages, shipments, etc. and is being used more and more due to the demand for user accessibility. Smart label tags combine the functions of providing a label, a barcode, and a super thin RFID tag in order to provide multiple methods of accessibility and readability. These usually have an adhesive side and can be attached to anything that you need to track such as packages. In extreme cases, passive RFID tags can be very small. Recently, Hitachi has come out with RFID tags that are so small, they are being called “smart dust”. These tags are .15 x .15 mm, can carry 128 bits, and can be seen in the image below:



(Gingichashvili, 2020)

Active tags, on the other hand, are not used as often and are saved more for high-value tracking. These are often used by the military or even in the industry in order to function as sensors. Since the active tags have a power source, some contain sensors which can collect data on temperature, humidity, location, intrusion, etc. These can then send the requested data to the reader at long distances and the data can then be sent back to the server or database where it can be analyzed and utilized.

## Vulnerabilities

First off, I’d like to say that RFID has many uses in the world of security and has been implemented in many different industries. That being said, there are vulnerabilities similar to any other piece of technology. Attacks or vulnerabilities can come in many forms:

* Impersonation/spoofing
* Unlimited access
* Anonymity
* Data storage attacks

These vulnerabilities are all serious, but the severity mainly depends on the usage of the RFID tag. If a tag is being used for tracking a simple Amazon package, there is not much risk. However, if the tag is being used by the military to track hostiles or retrieve vital sensor data, there is a lot of risk and preventative measures must be taken.

In the case of impersonation or spoofing, this first begins by the attacker either acquiring the data stored on the tag, or by acquiring the details about frequency, encryption, etc. from the reader. The attacker then uses this data to gain access where they shouldn’t. This can be seen in the example below:



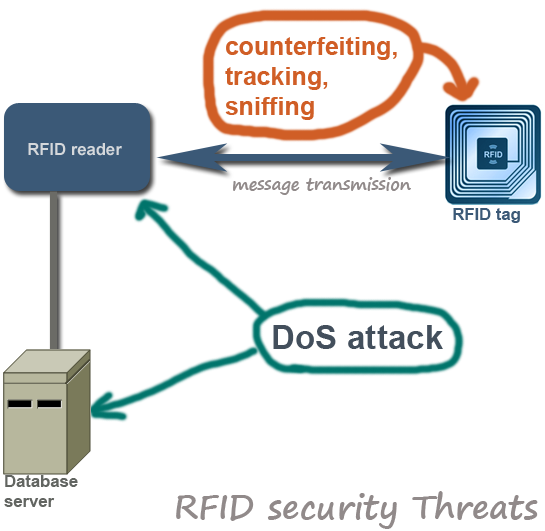
(Nachreiner, 2015)

This image can be seen in the show “Mr. Robot” in a scene where the attacker steals the RFID badge information using a reader/card cloner and then they later use the data to maliciously access a data center. All it takes is casually bumping into someone or getting close enough to them to steal their badge data. Additionally, spoofing can be used to access active tags as well. If configured properly, an attacker can connect to the active tag, pretending to be the lawful user, and maliciously access the data.

Next up is unlimited access. Due to the accessibility of passive tags, anyone with physical access (or withing the readability range) can access the data stored on the tags. There are methods on how to prevent this and I will go over them in the next section.

Anonymity is especially important when it comes to active tags. In sensitive situation where you do not want outside actors to notice your signals (either incoming or outgoing), it can become difficult to transmit data at long distances. Tags and readers can use a wide range of frequency, but hostiles that know what they are doing can scan for this sort of thing. Once sensed, they can find your tag and destroy or manipulate it.

Lastly, there are always attacks that are not related to the tags or readers, but towards the computing systems that either process the data or store the retrieved data. These attacks vary and have been discussed in many of our other courses. This could include a variety of DOS attacks to take down the server or system designated to retrieve the data, malicious intrusion into databases to remove or alter the stored data, or even blocking/jamming signals in order to sniff data being transmitted. An example of this can be seen in the sketch below. Although simplified, it demonstrates how the reader, the connected system, and the tag are all susceptible:



(Wing)

## Security Measures

As with IOD devices, RFID also lacks in security. Specifically, passive tags are very vulnerable due to their accessibility. When implemented in badges or door locks, it is important to make sure that the readability range is only as long as necessary, since theft of tag data can be detrimental to security and very easy to acquire. As we saw in the image earlier, an attacker can easily brush by you and clone your badge or door key in order to spoof their identity or impersonate you. This can grant them access to areas that only you should have access to. Additionally, since passive tags only transmit data by reflecting the signal and are not actually connected, they can be easily stolen. Lastly, the read/write rights are very important and should most often be write protected and set to WORM (write once, read many). It may be alright to reprogram tags in certain instances in order to reduce cost, such as hotels, a lot of problems can occur if attackers start rewriting RFID tags with altered or malicious data.

When it comes to Anonymity, there is not a lot that can be done. However, certain frequencies can be utilized in order to hide from normal scanners. Size also plays a huge roe since a larger device is more likely to be found. Since lower frequencies do not travel as far, using a reader or even a repeater nearby could prove to be beneficial in order to extend the signal and extend the range while keeping the frequency low. Since the active tags have their own power supply and can cover multiple functionalities, encryption of data can prove to be beneficial as well.

Regarding attacks that occur farther down the line such as attacks on servers, workstations, and databases, we have discussed multiple security measures in our various courses that can help. These include firewalls, configured rules, patched systems, etc. Combining all of the security measures that I have discussed can help secure an RFID network and prevent against malicious attacks. However, like I stated, RFID (similar to IOD devices) is very susceptible to attacks and should be managed properly with the recommended safeguards such as cameras, MFA (multi-factor authentication), and backups of data.

# Section 2

Over the course of this section, I will be discussing programming related to RFID technology and how it can be implemented. First off, I would like to share an excerpt from “Java Developer’s Guide” by Alien Technology. They provide code that they use for readers and below, you will see the different classes to controlling the different parts:

*“The library contains five discrete functional groups (Java packages) for controlling various aspects of the reader:*

*• reader - classes for communicating with a reader*

*• tags - classes dealing with RFID tags and EPC data*

*• discovery - classes for discovering the locations of readers connected by RS-232 or Ethernet*

*• notify - classes for listening to "push" notifications and streamed data from readers over the LAN*

*• util – classes for performing bit operations, converting between hex/ASCII/binary strings, XML parsers, serial port management, and for determining the API version.”*

(Alien Technology, 2008, pg. 1-2)

Obviously, the code itself is pretty complicated, and since I have not learned Java yet, I will not be able to implement any of my own code. However, below, you can see an example of code that they used for opening a connection and retrieving a list of the tags:



(Alien Technology, 2008)

As I’ve mentioned, RFID networks can contain many tags, such as in the hotel example, and this code has been used to provide an example of how the system can reach out to the reader and retrieve a list of all of the available tags. This is very valuable in order to manage them and make sure that they are all available and functional. If the reader cannot reach one of the tags, you then know that there is either an error, or that tag is not functional anymore due to damage, failure, or theft.

# Conclusion

In conclusion, RFID technology is a huge advance in accessibility and security. It has many functionalities in society from a simple tracker places on package labels to networks maintain building access. It has many vulnerabilities, but with the right security precautions and preventive measures, it can be a very useful tool in almost any circumstance. New uses are being found every day, and with the advancement in size and range of tags, we will definitely be seeing even mor of RFID technology in the future.

# Bibliography

Nickolas, Christina. “RFID The Basics.” *DigiKey*, Electronic Products, 7 July 2011, www.digikey.com/en/articles/rfid-the-basics.

Arnold, Shannon. “Active vs. Passive RFID: How to Choose the Right Tracking Tech.” *Real Time Networks*, www.realtimenetworks.com/blog/active-vs-passive-rfid-how-to-choose-the-right-tracking-tech-for-your-organization.

“RFID Tag.” *Components101*, 2018, components101.com/sensors/rfid-tag.

Leoncavallo, Ruggero. “Low-Frequency Radio in Active RFID Systems.” *DigiKey*, Convergence Promotions LLC, 3 Mar. 2011, www.digikey.hk/zh/articles/low-frequency-radio-in-active-rfid-systems.

Gingichashvili, Sarah, “Hitachi Develops World's Smallest RFID Chip.” *TFOT*, 27 June 2020, thefutureofthings.com/3221-hitachi-develops-worlds-smallest-rfid-chip/.

BONWIN, “Hotel Wireless Lock,Door RFid Card Lock,Online Lock.” *BONWIN*, www.bonwinlocks.com/wirelesslock.html.

Nachreiner, Corey. “'Mr. Robot' Rewind: Analyzing Human Exploits in a Wild Episode 5.” *GeekWire*, 24 July 2015, www.geekwire.com/2015/mr-robot-rewind-analyzing-human-exploits-in-a-wild-episode-5/.

Alien Technology. *Java Developer's Guide*, Sept. 2008.

Wing. “Top 10 RFID Security Concerns and Threats.” *Securitywing*, securitywing.com/top-10-rfid-security-concerns-threats/.