Wireless Defender Lab Report 2019

Factors Influencing Wi-Fi Signal Speed and Attenuation

Patrick Ziemke
Pomperaug Regional High School
Academy of Digital Arts and Sciences

Table of Contents

Abstract

The purpose of the first experiment was to understand how a 5 GHz radio frequency (RF) signal, more specifically a wireless fidelity (Wi-Fi) signal, is affected after passing through various materials that are well-known for their RF signal dampening qualities. This lab consists of two different experiments. The first experiment aims to find the material(s) that block RF signals most effectively, and the second experiment test which orientation of the material is most effective at blocking RF signals. In both experiments, I collected data on two main variables: network speed, and network strength. This series of experiments was automated using various programs, which have been built using the language Python, of which some used for data collection and information gathering, and some used for data analysis and visualization. Using a directional wireless antenna, the signal coverage, direction, and amplitude can all be easily controlled. I will be using the data that I collect to refine the development of a working prototype "shield" that effectively blocks Wi-Fi signals from potential cybercriminals.

Introduction

Wi-Fi network security has been left on the backburner of the field of cybersecurity since the implementation of WPA2 encryption security. This protocol made it more difficult to crack Wi-Fi passcodes by encrypting a shared key between the client and host, and the client can only connect if the encrypted key matches that of the host. Advancements in password cracking, however, have lead to faster methods of gaining unauthorized access to wireless networks, despite the increased security. Popular programs such as Aircrack-ng, inSSIDer, and Airjack have allowed cybercriminals to crack a business's Wi-Fi password in order to gain access to valuable information, without gaining physical access to the inside of the business.

Wireless Defender seeks to put an end to this problem by blocking Wi-Fi signals from leaving the walls of a small or medium business, the most targeted group in cybercrime. Utilizing radio frequency (RF) blocking technology, we can put an end to cybercriminals hijacking a business's network, and restore peace of mind to business owners/management.

In order to build our shield, we need to conduct testing on the ways that a Wi-Fi signal is affected by various types of materials and orientations. In each of our experiments, we will be collecting data on three (3) different variables including network strength (dBm), ping speed (ms), and percentage of packets lost (%). Based on the data gathered from these experiments, I will develop the most efficient product in preventing RF signals from passing through the exterior walls of a business. I hypothesize that the copper sheet metal with RF dampening fabric will be best to use as the core material of the shield, because of it's known frequency-blocking characteristics.

Variables

Independent Variable

Experiment 1: Core Material (Metal) Used

Experiment 2: Orientation of Core Material

Dependent Variable

Percentage of Packets Lost (%), Ping Speed (ms), Network Strength (dBm)

Control Variables

Python (Networking) Constants

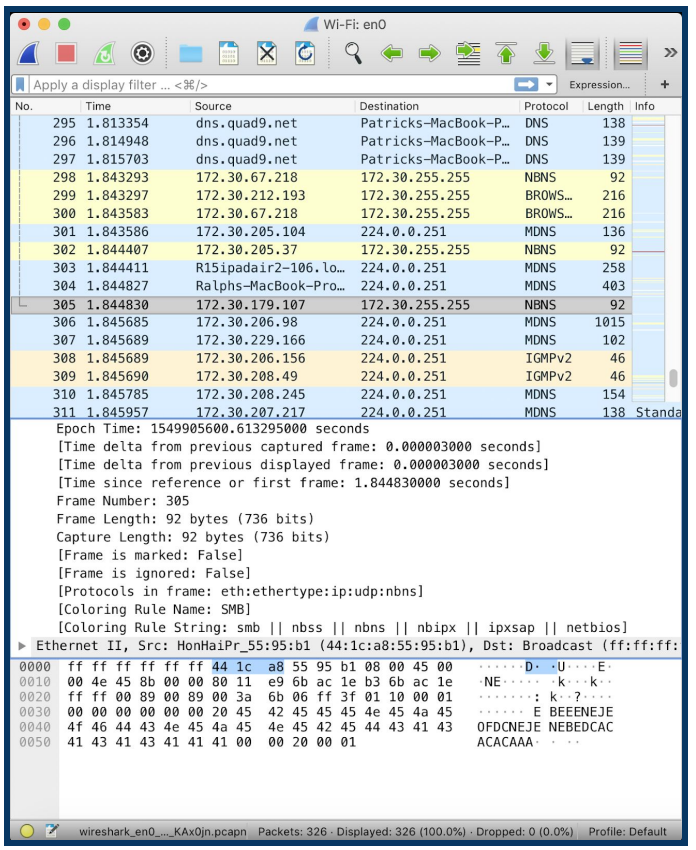
```
type = SOCK_STREAM
protocol = 0
hostname = "192.168.1.1"
port = 80
```

Material List

- Netgear AC 1000 Dual Band Wi-Fi Router
- APA-M25 Dual Band Directional Antenna Panel

- 12 in. x 24 in. Aluminum Sheet
- 12 in. x 24 in. Expanded Steel Sheet
- 12 in. x 24 in. Copper Sheet
- TitanRF Faraday Fabric

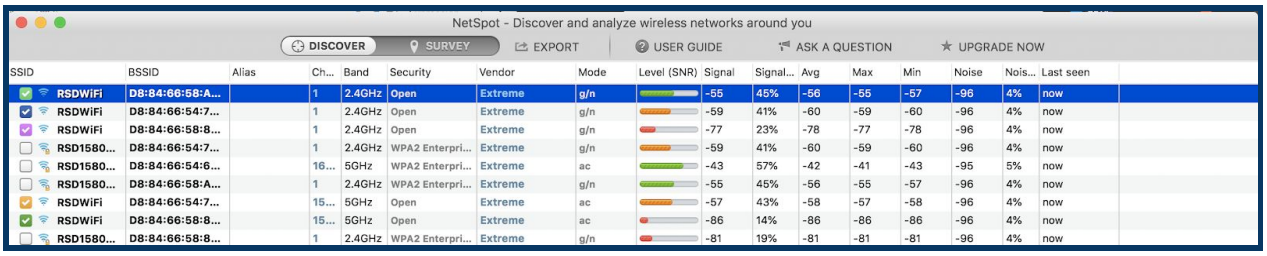
Figure 1 - Wireshark UI



Software

- Wireshark (packet interception and analysis) (see fig. 1)
- NetSpot (network strength/interference) (see fig. 2)

Figure 2 - NetSpot UI



Code

Host Communication (Python)

```
import socket

s = socket.socket()         # Create a socket object
host = socket.gethostname()
port = 80
s.bind((host, port))        # Bind to the port

s.listen(5)
while True:
      c, addr = s.accept()     # Establish client connection
            print 'Got connection from', addr
            c.send(addr + ' is up')
            c.close()

Output:
"""
Got connection from 192.168.1.1
192.168.1.1 is up
"""
```

Ping Data Code (Python)

```
from platform   import system as system_name  # Returns the OS name
from subprocess import call   as system_call  # Executes shell
command
import os

#User Input
targetIP = raw_input("Enter the Target IP Address: ")
count = raw_input("Enter the Number of Iterations: ")
packets = raw_input("Enter the Number of Packets Sent: ")

x = 1
for x in range(0 , int(count)): #repeats (count) number of times

    response = os.system("ping -c " + packets +" " + targetIP)
    if response == 0:
        print(targetIP + ' is up')
    else:
        print(targetIP + ' is down')

x += 1
totalIterations = int(packets)*int(count)
print("Total iterations: " + totalIterations)
```

Program output on following page

Output:

```
"""
Enter the Target IP Address: 172.30.195.117
Enter the Number of Iterations: 1
Enter the Number of Packets Sent: 5
PING 172.30.195.117 (172.30.195.117): 56 data bytes
64 bytes from 172.30.195.117: icmp_seq=0 ttl=64 time=0.086 ms
64 bytes from 172.30.195.117: icmp_seq=1 ttl=64 time=0.100 ms
64 bytes from 172.30.195.117: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 172.30.195.117: icmp_seq=3 ttl=64 time=0.105 ms
64 bytes from 172.30.195.117: icmp_seq=4 ttl=64 time=0.111 ms

--- 172.30.195.117 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.078/0.096/0.111/0.012 ms
172.30.195.117 is up
Total iterations: 5
"""
```

Data (CSV file) Parser - Python

```
import sys
import csv

filepath = input("Enter path of CSV file:")

starBullet = "\033[1;36;40m [\033[1;37;40m*\033[1;36;40m]
\033[1;37;40m"

# initialize titles and materials
fields = []
materials = []

# reading csv file
with open(filepath, 'r') as csvfile:
    # create csv reader object
    csvreader = csv.reader(csvfile)
    fields = csvreader.__next__()

    # extract each data row one by one
    for row in csvreader:
        materials.append(row)

    print("Total number of materials: %s" % (csvreader.line_num))

print("Field names are: " + ', '.join(field for field in fields))
print('\n')
print(starBullet + '     Data Output     ' + starBullet + '\n')
for row in materials[:(csvreader.line_num)]:
    # parsing each column of a row
    for col in row:
        print("%10s" % col),
    print('\n\n')


# initializing rows as variable materials
```

```
control = materials[0]

controlMin = ((float(control[1]) + float(control[4]) +
float(control[7])) / 3)
controlAvg = ((float(control[2]) + float(control[5]) +
float(control[8])) / 3)
controlMax = ((float(control[3]) + float(control[6]) +
float(control[9])) / 3)
# set corresponding variables to integers for each row

for row in materials[0:]:
    materialName = row[0]

    # find the mean of all trial averages
    minAverage = ((float(row[1]) + float(row[4]) + float(row[7])) /
3)
    avgAverage = ((float(row[2]) + float(row[5]) + float(row[8])) /
3)
    maxAverage = ((float(row[3]) + float(row[6]) + float(row[9])) /
3)

    print("\n\nminAverage: %s  avgAverage: %s  maxAverage: %s" %
(minAverage, avgAverage, maxAverage))
```

Procedure(s)

Overview

I will be conducting experiments on two (2) different factors that could affect the shield's efficiency in mitigating Wi-Fi and other RF signals from passing through walls. I will be testing which core metal is most efficient and the orientation of the shield. In the first experiment regarding the core metal, I will test three (3) different metals including copper, corrugated steel, and aluminum sheet metal. I will also test the effectivity of covering the metal in RF blocking fabric. In the second experiment, using the best core

metal from the preliminary experiment, I will be testing which of the three (3) orientations I have chosen will be best to further block the signals.

Procedure for Setting Up Control

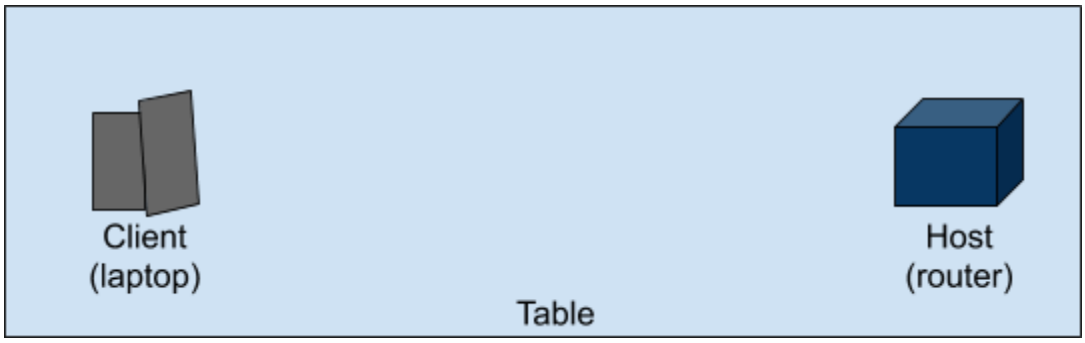
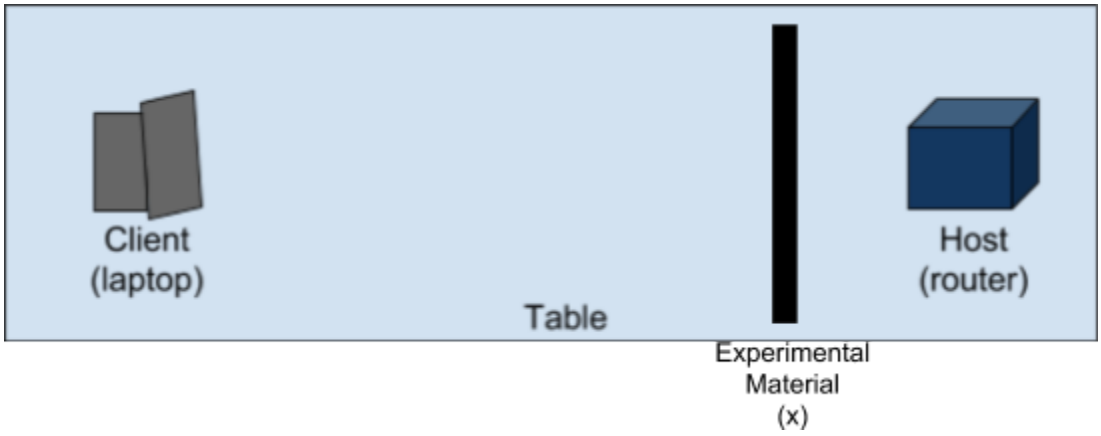


Figure 3

Procedure for Setting Up Core Material and Position Experiments



Procedure for Ping Test & Packet Loss Test

1.) Download the code above, and save it as pingdata.py
2.) Using a computer running OS X, open Terminal.
3.) Using the command cd, navigate to the directory where the file is located.

4.) Type into the Terminal **`python3 pingdata.py`** and press Enter.

```
Enter the Target IP Address: 224.0.0.251
Enter the Number of Iterations: 1
Enter the Number of Packets Sent: 10
PING 224.0.0.251 (224.0.0.251): 56 data bytes
64 bytes from 172.30.213.47: icmp_seq=0 ttl=64 time=0.146 ms
64 bytes from 172.30.213.47: icmp_seq=1 ttl=64 time=0.110 ms
64 bytes from 172.30.213.47: icmp_seq=2 ttl=64 time=0.074 ms
64 bytes from 172.30.213.47: icmp_seq=3 ttl=64 time=0.084 ms
64 bytes from 172.30.213.47: icmp_seq=4 ttl=64 time=0.062 ms
64 bytes from 172.30.213.47: icmp_seq=5 ttl=64 time=0.158 ms
64 bytes from 172.30.213.47: icmp_seq=6 ttl=64 time=0.131 ms
64 bytes from 172.30.213.47: icmp_seq=7 ttl=64 time=0.069 ms
64 bytes from 172.30.213.47: icmp_seq=8 ttl=64 time=0.080 ms
64 bytes from 172.30.213.47: icmp_seq=9 ttl=64 time=0.096 ms

--- 224.0.0.251 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.062/0.101/0.158/0.032 ms
224.0.0.251 is up
```

5.) Follow the instructions on startup by inputting answers to the questions such as target IP address, number of iterations of experiment (trials), and number of packets to send to the server.

Figure 4

6.) When the experiment is done, you should see the statistics at the bottom of the terminal, which houses the information on packet loss, as well as the minimum, average, and maximum times that a packet was sent and returned. It also provides the standard deviation of data.

Below is a diagram (fig. 5) of what is actually happening between the user (client) and server (host) while conducting this test. This depicts the IPX (Internet Packet eXchange) protocol:

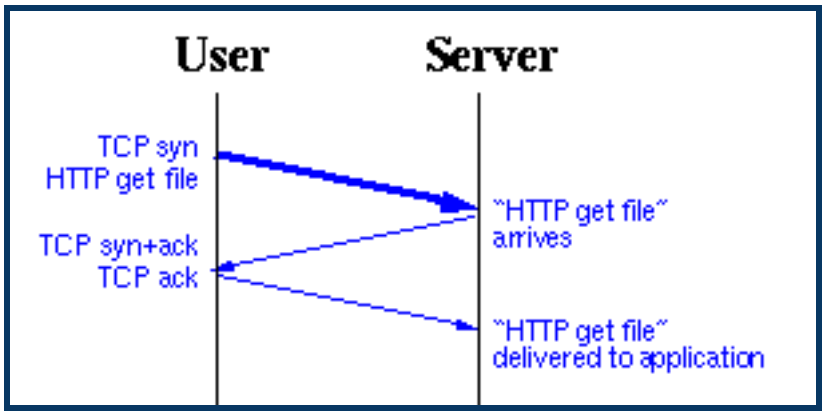


Figure 5

Procedure for Network Strength Test

1.) Using the application, NetSpot, ensure that you are on the "Discover" page, and make sure that your Wi-Fi connection is enabled. You do not need to be connected to the network in order for this program to work.
2.) On the bottom of the page, select "10 seconds" as the scan interval. This will record the data the most often.
3.) Find the connection that you are testing, usually towards the top of the list, and double click on the connection to bring up the individual network information.
4.) On the pop-up menu, select the "Tabular Data" tab, and record the data for signal strength and network noise for 20 seconds, and record in a data table.

Data Collection & Analysis

Control Experiment: No Interference With Signal

Wireless Signal Strength - CONTROL

TRIAL	MIN	AVG	MAX	NOISE (AVG)
1	-37	-38	-40	-96

Ping Test (50 Packets Sent) - CONTROL

Trial 1			Trial 2			Trial 3		
MIN (ms)	AVG (ms)	MAX (ms)	MIN (ms)	AVG (ms)	MAX (ms)	MIN (ms)	AVG (ms)	MAX (ms)
1.107	2.875	7.671	0.889	2.642	5.309	2.113	3.463	12.610
Std. Dev	0.982			0.874			1.632	

Packet Loss (50 Packets Sent) - CONTROL

Trial 1	Trial 2	Trial 3	Average
0	1	0	0.0067% loss

Core Material Experiment

Wireless Signal Strength - Core Material

Material	MIN (dBm)	AVG (dBm)	MAX (dBm)	Noise (dBm)
Copper Sheet	-42	-43	-48	-96
Aluminum Sheet	-43	-44	-45	-96
Perforated Steel Sheet	-38	-39	-41	-96
Copper Sheet w/ RF Fabric	-43	-45	-47	-96
Aluminum Sheet w/ RF Fabric	-48	-50	-53	-96
Perforated Steel Sheet w/ RF Fabric	-40	-45	-44	-96

Ping Test (50 Packets Sent) - Core Material

Material	Trial 1			Trial 2			Trial 3		
	MIN (ms)	AVG (ms)	MAX (ms)	MIN (ms)	AVG (ms)	MAX (ms)	MIN (ms)	AVG (ms)	MAX (ms)
Copper Sheet	1.117	2.921	9.456	1.481	3.985	39.909	1.375	3.090	3.883
Aluminum	1.11	2.788	4.134	1.307	2.990	6.108	1.188	2.684	5.056

Sheet	5								
Steel Sheet	1.341	3.218	4.215	1.083	2.798	5.499	1.378	3.159	4.291
Copper Sheet w/ RF Fabric	1.116	4.576	84.406	1.776	3.333	11.343	1.313	3.351	13.165
Aluminum Sheet w/ RF Fabric	0.960	3.088	23.546	1.197	2.869	4.112	1.169	3.032	4.589
Steel Sheet w/ RF Fabric	1.127	2.900	4.534	1.281	3.220	13.616	0.987	2.639	3.605

Packet Loss (50 Packets Sent) - Core Material

Trial 1	Trial 2	Trial 3	Average
0	1	0	0.0067% loss

Shield Orientation Experiment

Material	MIN (dBm)	AVG (dBm)	MAX (dBm)	Noise (dBm)
Copper Sheet	-42	-43	-48	-96
Aluminum Sheet	-43	-44	-45	-96
Perforated Steel Sheet	-38	-39	-41	-96
Copper Sheet w/ RF Fabric	-43	-45	-47	-96
Aluminum Sheet w/ RF Fabric	-48	-50	-53	-96
Perforated Steel Sheet w/ RF Fabri c	-40	-45	-44	-96

Ping Test (50 Packets Sent) - Core Material

Material	Trial 1			Trial 2			Trial 3		
	MIN (ms)	AVG (ms)	MAX (ms)	MIN (ms)	AVG (ms)	MAX (ms)	MIN (ms)	AVG (ms)	MAX (ms)
Copper Sheet	1.117	2.921	9.456	1.481	3.985	39.909	1.375	3.090	3.883
Aluminum Sheet	1.115	2.788	4.134	1.307	2.990	6.108	1.188	2.684	5.056
Steel Sheet	1.34	3.218	4.215	1.083	2.798	5.499	1.378	3.159	4.291

	1								
Copper Sheet w/ RF Fabric	1.116	4.576	84.406	1.776	3.333	11.343	1.313	3.351	13.165
Aluminum Sheet w/ RF Fabric	0.960	3.088	23.546	1.197	2.869	4.112	1.169	3.032	4.589
Steel Sheet w/ RF Fabric	1.127	2.900	4.534	1.281	3.220	13.616	0.987	2.639	3.605

Packet Loss (50 Packets Sent) - Core Material

Trial 1	Trial 2	Trial 3	Average
0	1	0	0.0067% loss

Conclusion

My initial hypothesis was that the copper sheet metal with RF shielding fabric would prove to be the best use for my RF blocking shield. While this is mostly correct, I actually found that the copper metal worked best for reducing network strength (signal attenuation), I also found that the aluminum metal also worked best for reducing network speed.

I collected and analyzed my data through various Python scripts. I chose to use Python because it is very powerful for automation of data collection. The first python script I developed was to automate the process of pinging the router, or sending packets through the router. This script was able to conduct 3 trials of 50 packets each in a single terminal command. The second Python script I developed took the data I collected from the first script as a .CSV file (comma separated values), and compare the data from the independent variable, to the control data, and found the percent difference.

The data that I have collected is very valuable to the development and refinement of my RF-blocking shield technology, but also my understanding of radio frequency behavior as a whole. Because I concluded that copper and aluminum sheet metal work in unison to reduce network speed and signal strength/attenuation, I will be using both of these metals as the core of my RF-blocking shield. I also found that encasing the sheet metal in RF-shielding fabric significantly reduces both of these factors as well.

Wireless Defender Co.

Research Outline 2019

Patrick Ziemke
Pomperaug Regional High School

Academy of Digital Arts and Sciences

I. Background:

A. Radio Waves:

- The entire series of a wave, before it repeats itself, is called a cycle.
- Radio wave is generated by a transmitter and then detected by a receiver.

1. Wi-Fi: uses radio signals to transmit information from your Wi-Fi enabled devices and the internet, allowing the device to receive the information from the web the same way that a radio or mobile phone receives sound.

- Wireless: Internet data can be transmitted through a LAN, hardwired connection, or wirelessly using Wi-Fi.

i. Wireless Signal Strength: The easiest and most consistent way to express signal strength is in *dBm,* which stands for decibels relative to a milliwatt.
dBm = Decibels in relation to a milliwatt (-30 to -100)

ii. Requirements and Variables: Strength for optimal/desired performance is based on factors including:

- Background noise in environment
- Amount of clients on network
- Desired data rates
- Applications used on network

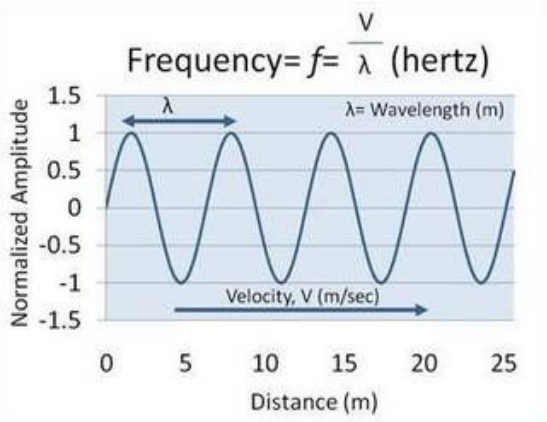
iii. Ideal Strength: For low-throughput tasks (sending emails, browsing web, etc.), -70 dBm is a good signal strength. For higher throughput requests like video streaming, -67 dBm is better, and some engineers recommend -65 dBm if you are planning on using mobile phones or other devices.

- Signal Strengths (and Functionality):

Signal Strength	TL;DR		Required For
-30 *dBm*	Amazing	Max achievable signal strength. Client can only be a few feet from the AP to	N/A

		achieve this. Not typical or desired in real world.	
-67 *dBm*	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/ VoWiFi, streaming video
-70 *dBm*	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 *dBm*	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 *dBm*	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

- Frequency:



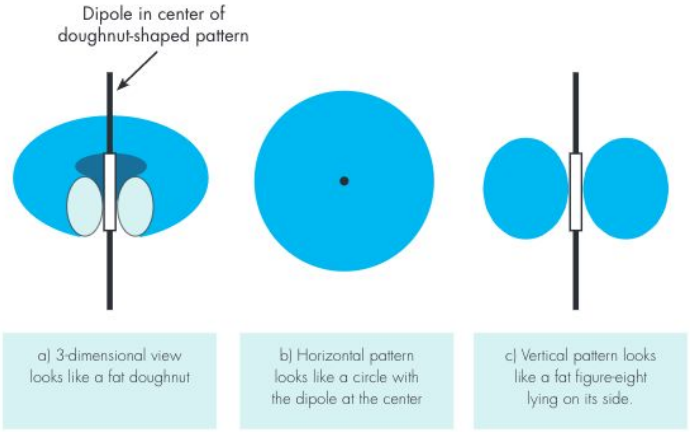
- Frequency is measured in hertz (hZ) referring to number of cycles in a cycle.
- 1 thousand hertz = kilohertz (KHz)
- 1 million hertz = millihertz (MHz)
- 1 billion hertz = 1 gigahertz (GHz)
- Radio spectrum is considered to be 3 KHz to 300 GHz.

B. Wireless Antennae: An antenna is a transducer that converts radio Frequencies (RF) fields into alternating current or vise versa. Antennas play an important role in the operation of all radio equipment.

1. Dipole antenna: The simplest type of radio antenna, consisting of a conductive wire rod that is ½ the length of the maximum wavelength the antenna can generate. This wire rod is split in the middle, and the two sections are separated by an insulator. Each rod is

connected to a coaxial cable at the end closest to the middle of the antenna.

- Omnidirectional signal (sends signal in all directions)
- The resonance of a thin linear conductor occurs at a frequency whose free-space wavelength is twice the wire's length.
- Conductor is ½ wavelength long
- Coverage Pattern:

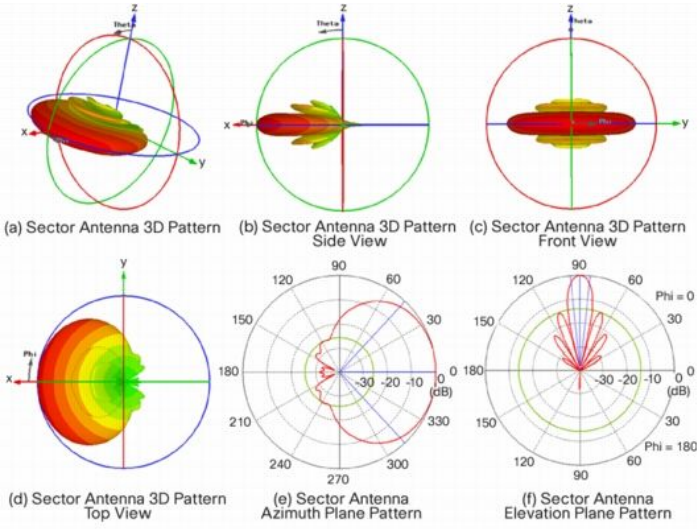


- Benefits:
  - i. Receives balanced signals (from a variety of frequencies)
  - ii. Sorts out problems caused by conflicting signals without losing reception quality
- Drawbacks:
  - i. Pole placement can interfere with reception quality
  - ii. Not much control over signal coverage

2. Directional Antenna:
   - Send/receive data from the are which you point the antenna

2. Directional Antenna (cont.):

- Signal Coverage:



C. Data Transmission: the process of sending digital or analog data over a communication medium to one or more computing, network, communication or electronic devices.

1. Client: The receiving end of a service or the requester of a service in a client/server system.
2. Access Point: a networking hardware device that allows a Wi-Fi device to connect to a wired network.
3. Node: A connection point that can receive, create, store or send data along distributed network routes (data spread over more than one computer.
    - Point-to-Point: Directly links single mainframe data server to workstation on the same network
    - Point-to-Multipoint: Links single mainframe data server to multiple workstations on the same network
    - Multipoint-to-Multipoint: Links multiple mainframe data servers to multiple workstations on the same network

II. Problem:

A. Cybercriminals: individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

B. Cyber Attacks:

The most common types of cyber attacks include:

- **Denial-of-Service (DoS) & Distributed Denial of Service (DDoS)**
    - A malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target with a flood of Internet traffic.
- **Man-in-the-Middle (MitM) Attack**
    - An attack where the cybercriminal secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. All data flow passes through the attacker, and once they secure the middle spot, they can launch an eavesdropping attack to collect all of the data. This is the most popular attack on Wi-Fi networks, especially when paired with an eavesdropping attack.
- **Phishing**
    - Phishing is the fraudulent attempt to obtain confidential/sensitive information such as usernames, passwords, and credit card details by disguising itself as a trustworthy entity.
- **Drive-By Attack**
    - Drive-By Download Attacks is a technique used by cyber criminals to silently install malware on victimized computers. This attack is committed by installing potentially harmful software code on a website, that automatically downloads on a victim's computer.
- **Password Attack**
    - Password attacks use various methods of cryptography to decrypt password hashes (SHA256) stored in databases or Wi-Fi networks.
- **SQL Injection Attacks**
    - SQL Injection is a code injection technique, used to attack data-driven applications, in which SQL statements are inserted into an entry field (on a website, for example) for execution (to dump the SQL database contents to the attacker).

- **Eavesdropping Attack**
    - Also known as Sniffing or Snooping, this attack is an incursion where someone tries to steal confidential information that computers, smartphones, or other devices transmit over a network (especially Wi-Fi networks).
- Exploits:
    - Malicious payloads are the parts of cyber attacks which cause harm. Malicious payloads can sit dormant on a computer or network for seconds or even months before they are triggered. Other payloads can be script injection into a computer network to reveal confidential information.
- Payloads:
    - The payload is what causes the exploit to run. If an exploit is a piece of code written to take advantage of a particular vulnerability, the payload is the piece of code to be executed through said exploit. This being said, viruses with more powerful payloads, such as Wi-Fi Eavesdropping/Sniffing, tend to be more harmful.
- Profit:
    - Cyber crime is a very high-paying job, but obviously comes with a high risk. According to the Bromium Report on how much cybercriminals make from performing cyber attacks, high earners make up to $2 million per year. Mid-level criminals make up to $900,000, and entry-level criminals make up to $42,000.

C. Small Business Risk:

1. Why SMB is Large Risk:

- 58% of cyber attacks are against small businesses
- 60% of companies go out of business within 6 months of a cyber attack.
- Low Quality Passwords
- No Cybersecurity/Network Administration Staff
- Small businesses are most at risk because the staff is typically prone to falling for social engineering attacks due to a general lack

of cybersecurity training, and releasing confidential information, by accident. Many small business employees also tend to not use the most secure passwords, and even using the same password for all of their services. Finally, small businesses are most at risk for cyber attacks because 93% of small businesses have no dedicated Cybersecurity/Network Administration staff.

2. Social Engineering:

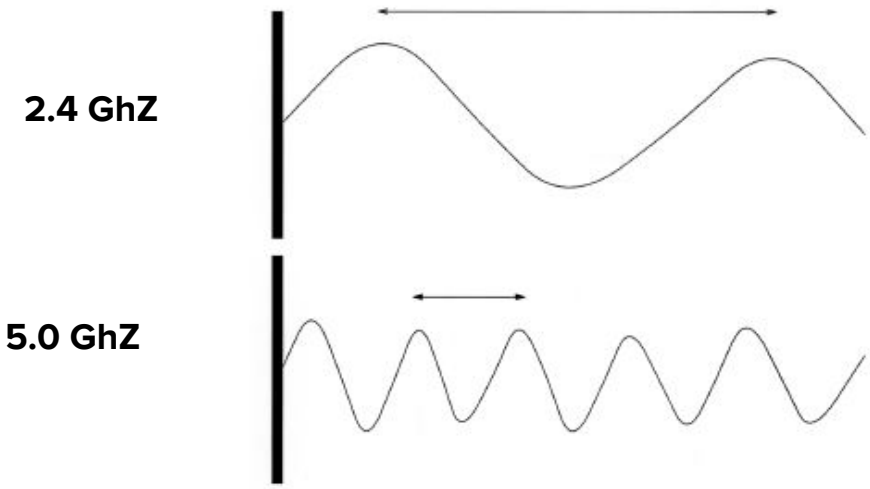
- Social engineering is the art of manipulating people, like employees of a business, to give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick you into giving them your passwords, bank information, or access your computer to secretly install malicious software.

3. Employee Training:

- Employee cybersecurity awareness training can be very beneficial to protect against social engineering attacks. This training aims to equip your employees with the knowledge and skills they need to protect themselves and your business from cybercriminals and their malicious attacks. This being said, it is highly recommended that any employee with access to a work-related computer or mobile device should undergo cybersecurity awareness training.

D. 2.4 GhZ vs. 5 GhZ Wi-Fi:

- 2.4 GhZ signals are lower frequency, so they have much longer wavelengths. This makes 2.4 GhZ the ideal frequency for standard dual-band routers if your device is far away from the router.
- 5.0 GhZ signals are much higher frequency, so they have much shorter wavelengths. This provides a fast signal if you are close in proximity to the router, but you may have signal droppage if your device is far away from the router.



D. Network Security:

- Current cybersecurity solutions and services include:
  - User/endpoint threat protection (including AI)
  - Antivirus software
- Most small business owners cannot afford to hire a cybersecurity consultant, and must wait for an attack to happen.

.

III. Solution

A. Radio Frequency Engineering

a. Radio Frequency (RF) engineering is a subset or electrical/electronic engineering involving the application of transmission line, waveguide, antenna and electromagnetic field principles. As RF signals travel through the air, they can move and behave in a wide range of behaviors including:

- Absorption
- Reflection
- Scattering
- Refraction
- Diffraction
- Loss
- Free-space path loss
- Multipath
- Attenuation
- Gain

b. RF engineering explores the many factors that affect RF signals, and designs & implements technologies in order to accomplish their goal.

B. RF- Shielding Fabric

a.

Radio Frequency-shielding fabric is a material similar to cloth fabric, except it is made out of a conductive material, mainly thin strands of metal that are microscopically woven together. This conductive enclosure is used to block electrostatic fields and radio frequency signals by creating a "Farraday cage" around the enclosed area.

C. Object Interference

a. Because wireless (RF signals) travel through the atmosphere, they are very susceptible to different types of interference than standard wired networks. Interference weakens wireless signals and therefore is an important consideration when working with wireless networking. Physical objects such as trees, masonry, buildings, and other physical structures are some of the most common sources of physical interference. The density of the materials used in a building's construction determines the number of walls the RF signal can pass through, and still maintain adequate coverage.

Wireless Defender Co.

Formal Business Plan

Patrick Ziemke, Owner and CEO
April 29, 2019

Table of Contents

1. Executive Summary

1.1 Product

Security has become one of the leading research areas in the technology field, however, Wi-Fi security has been left on the backburner after the encryption protocol, Wi-Fi Protected Access (WPA2), became somewhat of a standard in the industry. Cybercriminals are able to connect to the network of a small to medium-sized business from outside and take control of the victim's network, without even being inside the building. What if that didn't happen anymore?

Wireless Defender seeks to solve this problem by blocking RF waves (including WiFi signals) from exiting the workplace. A mono-directional wireless antenna combined with a physical shield on the router stops these signals from leaving the walls of the building, protecting the network from cybercriminals who may be trying to connect to the wireless router.

As all buildings have different shapes and interior layouts, the shield must be bent according to the shape of the building. The physical shield on the router will be able to bend to the user's liking in order to block the signals most effectively. I will conduct experimentation on the best material to use for the shield, as well as how shaping the shield differently affects the results. This project has been validated through resources and experimentation.

1.2 Customers

The company's target market consists of small business owners who are serious about protecting their business from cybercriminals. Cybersecurity is one of the most detrimental, and unfortunately, overlooked problems faced by small business owners. According to the 2018 Verizon Data Breach Investigations Report, 58% of cyber attack victims are small businesses. These cyber attacks can be so damaging to a small business because the cost alone of "cleaning up" after a data breach is considerable. Around 60% of small businesses that are cyber attacked must suspend operations, and are unable to reopen, due to bankruptcy. The lost revenue due to downtime, the money spent to remediate the business, and the damage to the business' reputation are why cyber attacks on small businesses are so damaging.

1.3 What Drives Us

Wireless Defender’s solution to this problem is a mono-directional antenna for your business's router, and a Radio Frequency (RF) shielding panel to block any remaining signal. By using RF engineering technology, not only can you optimize your business for Wi-Fi coverage, but you can limit what areas are covered. We have conducted many experiments, and used the data and research to refine the shield. Our patent-pending shielding material, along with a revolutionary RF-shielding fabric, will block any and all extraneous signals. Wireless Defender Co. is committed to providing small businesses with a highly-secure and low maintenance security system to keep their private data in their hands.

2. Company Description

2.1 Mission Statement

Wireless Defender Co. reduces the vulnerability of small business network systems by implementing combined cyber-security and cyber-defense systems that neutralize advanced wireless threats, thereby improving security for all businesses.

2.2 Legal Structure

Our business structure is a sole proprietorship (SP) that is unincorporated and run by a sole individual, Patrick Ziemke, (there are no partners) with no distinction between the business and its owner. As a sole proprietor, Mr. Ziemke is entitled to all of the business's debts, losses and liabilities. This business structure as it is fairly simple to form. Sole proprietorships only require a permit/license and registration with the local government.

Some advantages of this business structure are that these businesses are relatively unencumbered by government regulations, mitigating the risk of facing legal technicalities. Sole proprietorships can also report any tax through income, and do not need to file a separate 'Business' tax plan. One disadvantage of this structure is that sole proprietors are personally liable for all business losses and debts, because there is no legal distinction between the company owner and the business.

3. Market Research

3.1 Industry

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks. This is part of the much broader field of cybersecurity and information technology security which serves to protect computer systems from theft or damage to their hardware, software, or electronic data, as well as from disruption or misdirection of the services they provide.

3.2 Customers

Wireless Defender Co.'s target consumers are the owners of small to medium-sized businesses in the United States. Broadband and information technology are powerful factors in small businesses, reaching new markets and increasing productivity and efficiency. However, with the rise of cyber attacks in the United States, and the fact that 58% of cyber attack victims are the owners of small businesses, owners need a simple cybersecurity strategy to protect their business, their customers, and their data from growing cyber threats. The Internet allows businesses of all sizes and from any location to reach new and larger markets and provides opportunities to work more efficiently by using computer-based tools. Every business that uses the Internet is responsible for creating a culture of security that will enhance business and consumer confidence.

3.3 Competitors

Cybersecurity is a very popular and growing field at the moment, and Wi-Fi security has become a focus in information technology security. However, the competition for Wi-Fi network security only extends as far as companies providing software solutions to small business cybersecurity. These include firewall appliances, Virtual Private Network (VPN) and proxy services, and anti-virus computer protection. There are currently no hardware products on the market today that serves as a solution to Wi-Fi security for small businesses. The most prominent of companies in the wireless network security market include:

- Cisco Systems, Inc. (U.S.)
- Assa Abloy (Sweden)
- Bosch Security Systems, Inc. (Germany)
- Honeywell International, Inc. (U.S.)
- Fluke Corporation (U.S.)
- Symantec (U.S.)

- ADT Corporation (U.S.)
- Brocade Comms. Systems, Inc. (U.S.)
- Fortinet (U.S.)

3.4 Competitive Advantage

Wireless Defender Co. holds a competitive advantage over other cybersecurity companies as we are the only company providing a no-maintenance, responsive, hardware solution to network security. We have done a lot of research and experimentation into the field of cybersecurity and radio frequency engineering, and with the support of the small business community, together, we can take the first step towards eliminating cyber criminals from targeting your business.

3.5 Regulations

3.5.1 S.B. 949

Status: June 30, 2015; Public Act No. 15-142

Relates to data security and agency effectiveness; relates to contractor compliance with breach of confidential information procedures, a data-security program for the protection of confidential information and a report of any breach; requires the Office of Policy and Management to furnish financial accounting statements; requires any owner or licensee of computerized data to provide identity theft protection or mitigation services to victims; requires an inoperable feature on sales of smartphones.

3.5.2 H.B. 6317

Status: June 23, 2015; Special Act No. 15-13

Concerns a study of cybersecurity; requires the Department of Administrative Services, in consultation with the Department of Emergency Services and Public Protection, to conduct a study examining cybersecurity issues facing the state; relates to recommendations to promote and coordinate communication between government entities, law enforcement, institutions of higher education, the private sector and the public to improve cybersecurity preparedness.

4. Product/Service Line

4.1 Product or Service

One way to mitigate the risks associated with cyber attacks on small businesses is to control the coverage area of the Wi-Fi signal. Cybercriminals unable to access a signal from a business are unable to carry out their malicious attack. It would make the hacker's work a lot more difficult, as they would need to gain physical access to the inside of the building. By removing any Wi-Fi coverage from the outside of the building, this will deter the attacker to leave your business and move onto their next target.

Wireless Defender's solution to this problem is a mono-directional antenna for the small business's router, and a Radio Frequency shielding panel to block any remaining signal. By using RF engineering technology, not only can you optimize your business for Wi-Fi coverage, but you can limit what areas are covered. We have conducted many experiments, in which we have taken the data, and used the research to refine the shield. Our patent-pending shielding material, along with a revolutionary RF-shielding fabric, will block all extraneous signals.

4.2 Pricing Structure

Wireless Defender uses a bundle pricing structure, packaging products and services together at a discount to sell in bulk and create a more affordable single offering. Some positive effects of using this pricing structure is that it is a much simpler way of selling and delivering multiple products or services. However, a negative outcome of this structure is that it reduces the consumer's freedom of choice in what exact products or services they're buying.

We chose to sell different Wi-Fi security packages at three relative and differing price points. The *Bronze Package* features only our proprietary RF-blocking shield and Wi-Fi router. The *Gold Package* features our proprietary RF-blocking shield, Wi-Fi router, and professional installation and coverage survey. Finally, the *Platinum Package* features the RF-blocking shield, Wi-Fi router, professional installation and coverage survey, and our CyberDefense network monitoring software.

Pricing model available on following page.

Bronze Package ($229.99)	Gold Package ($259.99)	Platinum Package ($259.99 + $10/mo.)
- RF-blocking shield - Wi-Fi router	- RF-blocking shield - Wi-Fi router - Professional installation - Signal Coverage Survey	- RF-blocking shield - Wi-Fi router - Professional installation - Signal Coverage Survey - Network monitoring software

4.3 Product/Service Life Cycle

Wireless Defender Co. is still in the growth phase. After working diligently to test and refine our product, we are beginning to grow into a functioning business, and begin making sales. We expect to be in the expansion stage by the end of 2019, once all of our assets are in order, and once the company achieves an expected level of success.

4.4 Research & Development

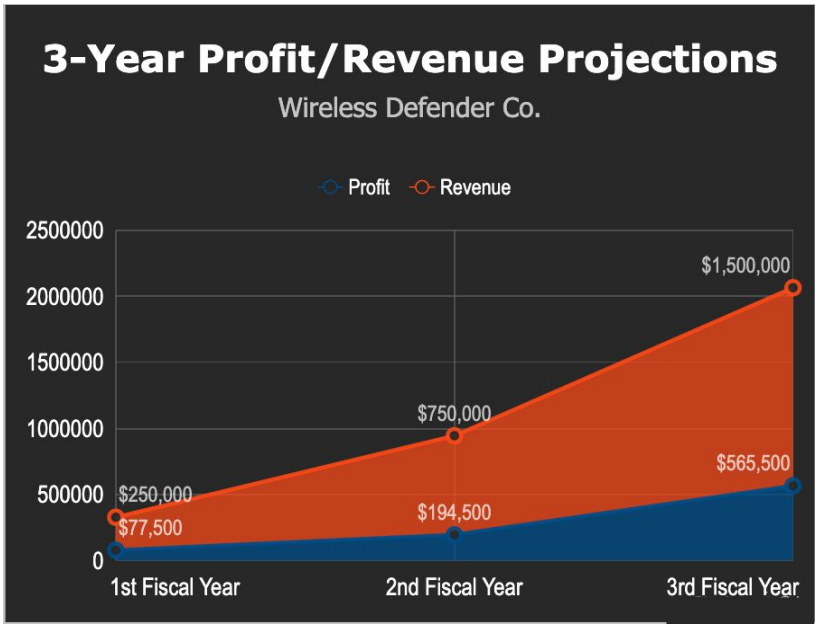
In order to develop and refine the radio frequency blocking capabilities of our proprietary RF-blocking shield, We conducted two different experiments. The purpose of the first experiment was to understand how a 5 GHz radio frequency (RF) signal, more specifically a wireless fidelity (Wi-Fi) signal, is affected after passing through various materials that are well-known for their RF signal dampening qualities. This lab consists of two different experiments. The first experiment aimed to find the material(s) that block RF signals most effectively, and the second experiment test which orientation of the material is most effective at blocking RF signals. In both experiments, we collected data on two main variables: network speed and signal attenuation. This series of experiments was automated using various programs, which have been built using the language Python, of which some used for data collection and information gathering, and some used for data analysis and visualization. Using a directional wireless antenna, the signal coverage, direction, and amplitude can all be easily controlled. We used the data that I collect to refine the development of a working prototype “shield” that effectively blocks Wi-Fi signals from potential cybercriminals.

6. Financial Projections

6.1 Profit & Loss

	Fiscal Year 1	Fiscal Year 2	Fiscal Year 3
Sales	$250,000	$750,000	$1,500,000
Cost/Goods Sold	$199,291	$597,872	$1,195,743
Gross Profit	**$50,709**	**$152,128**	**$304,257**

6.2 3-Year Profit/Revenue Projections



6.3 Profit Margins

	Fiscal Year 1	Fiscal Year 2	Fiscal Year 3
Net Profit (before taxes)	$50,709.00	$152,128.00	$304,257.00
Income Taxes	$6,744.29	$20,233.02	$40,466.18
Net Profit (after tax)	**$43,964.71**	**$131,894.98**	**$263,790.82**

6.4 Break Even Analysis

Product	Bronze Pkg	Gold Pkg	Platinum Pkg
Price per Unit	$229.99	$259.99	$259.99
Variable Cost per Unit	$152.79	$152.79	$152.79
Contribution Margin (CM) per Unit	$77.20	$107.20	> $107.20
x Sales Mix Percentage	40%	10%	50%
Average CM per Unit	$30.88	$10.72	$53.60
Sum: Average CM per Unit		**$92.50**	

Fixed Costs: $10,000.00

	Product 1	Product 2	Product 3	Total
Break-Even Number of Units to Sell	**50**	**11**	**56**	**117**
Product Sales in $	$11,499.50	$2,859.89	$14,559.44	
Sum: Break-Even Sales in $		**$28,918.83**		

6.5 Financial Assumptions

6.5.1 Assumptions for Profit & Loss Projections

We expect to experience an exponential growth rate in gross profit and revenue starting from the first fiscal year. We estimate that in the first year alone, we will sell 1,087 units, with a total net profit of $43,964.71 (see chart 6.3, Profit Margins). We believe with strategic marketing and shifting our focus onto the main problem of small business cybersecurity, we can upsell our initial predictions.

6.5.2 Assumptions for Operating Expenses Projections

Any time a company is started, many unseen or unexpected expenses arise as the company grows and develops. We expect when the company grows to the sales margins of the late-2nd to early-3rd fiscal year, We will have to expand into a larger operational

facility in order to manufacture, process, and ship orders. Other expenses may include fees from advertising agencies handling marketing campaigns, income taxes, and shipping fees.

6.6 Start-Up Funds

This company will be funded through crowdsourcing, on the platform Kickstarter. This is a popular platform to raise money for startup technology companies, as they specialize in creative projects with a robust reward level feature. For example, if a person were to donate $5, they would get a mention on our website. If they were to donate $50, they would get a custom directional Wi-Fi antenna for their router. If they donated $200, they would receive our full *Bronze Package*. Additional rewards are available on the campaign page. With a platform of over 15 million supporters who have raised over $3 billion since the site's inception, this would be a good place to not only raise awareness of the product, but will also generate enough sales to break even before the product is launched.

With crowdfunding through Kickstarter, there are platform fees involved in your fundraising campaign. A 5.0% platform fee and a payment fee of 3.0% + $0.20 will reduce profit margins, however I only hope to raise enough to meet my $29,000.00 break-even goal. Once I have gained Kickstarter's approval on the fundraising of my company, I expect to meet this goal in just four months.

Wireless Defender

Annotated Bibliography 2018

Patrick Ziemke
Wireless Defender Co.
Pomperaug Regional High School
Academy of Digital Arts and Sciences

- Bulk, Frank. "The ABCs Of WPA2 Wi-Fi Security." *Network Computing*, 2 Feb. 2006, p. 65. *Computer Database*, http://link.galegroup.com/apps/doc/A141716150/CDB?u=s2153&sid=CDB&xid=c91ee222. Accessed 29 Nov. 2018.

This article dives deep into the world of network security protocols, outlining the differences/improvements of WPA to WPA2 security, identifies protocols ranging from AES (Advanced Encryption Standard) to PSK, PTK, and PMK protocols. The name of the article is referring to the abbreviations of all of the network security protocols. The author explains the core fundamental designs of each protocol, and then extends into some complications when retrieving server information through each protocol.

This source seems to be very reliable, because it is an excerpt from a scientific journal publications called *Network Computing,* by Frank Bulk. The author is well known in the computer networking field, and has continued to speak at cyber security events. This article shows no signs of bias, and makes reasonable claims while providing sufficient supporting evidence.

I will be using this article as a reference throughout the entirety of my project, because the protocols can become confusing after a while, and can be easily mixed up. This article ensures that I have the right knowledge and sufficient understanding of the way that the protocols can affect different services being completed by the network.

- Empey, Charlotte. “Cybercriminals and the Risk to Small Business.” *AVG Now*, Avast Software, 28 May 2018, now.avg.com/cybercriminals-and-the-risks-to-small-business.

The author of this article begins by describing what cyber criminals are, and what exactly they do. The article gave me a lot of insight on how cyber criminals operate, and why they tend to target small to medium sized businesses the most. At the end of the article, the author gave some tips for protecting yourself and your business from cyber criminal attacks.

This article gave me a lot of background information about the problem with cybercriminals and why they target small and medium businesses. The author of this information comes from a cybersecurity company attempting to market their products to small and medium sized businesses as well, so the information is a little biased in order to make sales.

This article is very useful to me as I learned a lot more about the major problem that exists with small-medium businesses’ network protection, and how cyber criminals can actually steal company information. The author also included images a

- "Firewall offers network security for small/medium businesses." *Product News Network*, 14 Feb. 2008. *Computer Database*, http://link.galegroup.com/apps/doc/A174746571/CDB?u=s2153&sid=CDB&xid=3d33c881. Accessed 29 Nov. 2018.

This article dives deep into a cybersecurity product (software) that is already on the market, that is aimed at making a small business's network more secure. The way I will be using this source is to see how other cybersecurity companies have sold their product in the past. Their product is vastly different to Wireless Defender, however, as it is a software monitoring program.

I think that this is a somewhat biased article, because the purpose for this is to sell a product. The author is affiliated with the product, so immediately it raises some red flags about the article's credibility. However, the information is not meant to misinform the reader, but more to persuade them to buy their cyber security product.

This article is important for me because it gives me an idea on how others sell their cyber security products, especially for small to medium sized businesses. I will use this as a reference for some of the sales and marketing tactics that I use to advertise and sell my product to customers and investors.

- Mansfield, Matt. "Cyber Security Statistics: Numbers Small Businesses Need to Know." *Small Business Trends*, Name Cheap, 24 Oct. 2018, smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html.

This article provides some facts and statistics for small businesses in terms of their network security and risk factors for data breaches. This article gave me some starting points in terms of my own personal market research. These statistics reveal what type of information is commonly stolen from these businesses including employee records, intellectual information, payroll records, etc.

Most of the information seems to come from a survey of the owners of small to medium sized businesses. However, the author never explicitly discloses the source of the information and statistics, so it makes me question it's credibility. However, the data collected does not seem unreasonable.

This article provides me a lot of information on the current problem that business owners are facing. Statistics on how many businesses are targeted, what information is stolen, as well as information on how the cyber criminal obtained the data, are all recorded and visually represented in the article through graphs.

- "New York City Embraces Cyber Security for Public WiFi." *Wi-Fi Wireless LAN*, Mar. 2018, p. 1+. *Computer Database*, http://link.galegroup.com/apps/doc/A534958019/CDB?u=s2153&sid=CDB&xid=e39cd017. Accessed 29 Nov. 2018.

This article discusses the new cybersecurity protocols being implemented in New York City to allow more secure connections to ve made on public hotspots. Security protocol

"Quad9" will be used in addition to the WPA2 and IEEE 802.11 protocols that are currently standard in all public access points. I will be using this source as a reference to how governments manage 48cybersecurity, as well as understanding what network security protocols are already in place.

This article is extremely reliable, as it is from an accredited organization, the Information Gatekeepers, and was published only 9 months ago. The goal of the article was to inform the audience of new policies requiring public hotspots use the new Quad9 protocol, which is the most recent cyber security advancement.

I will be using this article as a guide as to how a security protocol works, as well as how the government addresses cyber security issues. Although this is not the first time that a new protocol was made standard through congressional action, it is surely the most recent, and has proved to be effective in New York City.

- Westover, Brian. "Where to Place Your Router for the Best Wi-Fi Signal." *Laptop*, Laptop Mag / Purch, 8 Feb. 2018, www.laptopmag.com/articles/place-router-best-wi-fi-signal.

This article highlights the different ways that the position of your wireless router can affect signal coverage and signal strength. This information will be important during the research and experimentation phase of my project, as one of the main concerns with my

product is wireless coverage, so this article will give me pointers to control the range of the wireless signal.

This article was written by a technology website that profits from paid promotions of other products. This shows that the information provided may not be completely accurate, however this article never specifically mentions any product or brand names. The purpose of this article was to give the audience some tips to get the best signal coverage possible.

I will probably use this article when I am figuring out the best way to orient my prototype along with the router position. These two variables are some of the most important factors in my project, and I need to calculate the best position for the prototype to output the desired signal coverage.