Lab01- Demodulation

In this lab, we will look for transmissions that are hidden or obfuscated and see a very simplified method of triangulating the physical location of a transmission.

Note: for this lab, since it requires audio, you can't use the IA Lab. The lab's web interface does not allow the routing of audio, so you'll need a mechanism to run things locally.

History: The Thing

The Thing, or so it was called at the time, was a listening device installed in a carving of the Great Seal of the United States. It was gifted to the US ambassador to the Soviet Union after WWII. It was mounted in the *Spaso House*, which served at times as both the residency and offices of the US Embassy in Mosco.
It was discovered largely by accident—radio operators noticed the voices of ambassadors on frequencies adjacent to other normal transmissions. You can find more info about The Thing here: https://www.cryptomuseum.com/covert/bugs/thing/index.htm

Part I: Scavenger Hunt

A secret signal is being broadcast in the 850-950 MHz range in our cybersecurity lab. This is being broadcast on an ISM band—one open to be used without a license. We have Software Defined Radios available to be used over the internet (since you likely don't want to travel to campus to complete this lab).

Instructions

Find the hidden signal that is being broadcast within the range.

1. Connect to one of the remote radios listed below using SDR#.
2. Scan through the signals, the signal uses a narrow bandwidth
3. Listen to the audio through your speakers, you'll find a few different transmissions. If at first you think you're getting trolled by the Russians, you're close, but the trolling isn't the secret message itself.
4. Take a screenshot of discovering the signal. What is the signal saying (audio)?

Connection Information:

When you are done, please reset the radio back to 100MHz before disconnecting!!
SDR IP Address for use in SDR#: sdr://138.247.12.20:5555
When you are done, please reset the radio back to 100MHz before disconnecting!!

Background Info

To give everyone access to the RF environment we have on campus, I have setup a Spy-Server, which is a remote connection for a Software Defined Radio. You can read all about them as well as find instructions for connecting your Client PC here: https://www.rtl-sdr.com/rtl-sdr-tutorial-setting-up-and-using-the-spyserver-remote-streaming-server-with-an-rtl-sdr/

Eight software defined radios are available running on a batch of VMs behind a load balancer. The load balancer (HAproxy) will only allow one session per radio, so if you try to connect and it fails, it means that all 8 radios are in use. Since there are only ~15 students, you're probably safe to wait a bit and reconnect. Also, please play nice, reset the radio to 100MHz and disconnect from the radio as soon as you're done.

Part II: Triangulation

We know the basics for the relationship between received power, distance, and antenna gains. Given this information, we should be able to determine a mobile device's rough location. In our scenario, we're assuming we have free space propagation and that in our mystical world, all antennas' gains are 1. Given the information below, determine the approximate location of the mobile device. Make sure to show/explain/demonstrate how you determined the location, and show what you've found on some sort of a map. How you choose to render the map is up to you.

$$P_r = \frac{G_r \ G_t \ P_t}{\left(\frac{4\pi d}{\lambda}\right)^2}$$

Free Space Propagation

- Base Station 1:
  - Location: 44.012320,-97.109509
  - Power Transmitted: 200 watts
  - Power Received: 17.3512367 watts
  - Transmitter Gain: 10
  - Receiver Gain: 25
  - Frequency: 450 kHz
- Base Station 2:
  - Location: 44.013371,-97.289582
  - Power Transmitted: 200 watts
  - Power Received: 0.99757704 watts
  - Transmitter Gain: 10
  - Receiver Gain: 25
  - Frequency: 450 kHz
- Base Station 3:
  - Location: 44.119244,-97.215958
  - Power Transmitted: 200 watts
  - Power Received: 0.9337055 watts
  - Transmitter Gain: 10
  - Receiver Gain: 25
  - Frequency: 450 kHz

Tips:

- Remember, you know how to determine how far a transmission should go, use that formula with a bit of algebra
- Our transmitters radiate signal in a circle.
- Plot the location of the tower then simply draw a circle around each transmitter.
- When you find a spot where all three transmissions overlap, you'll know where the device is

- If you're lost as to how to plot the circles, Google "google maps plot circles" and check out some of the results, the tools exist!

What to Submit

Submit a screenshots of your SDR# interface showing the signal you've detected along with the secret message in addition to your findings for where our secret device is transmitting from. Submit these as a PDF to D2L & answer the following questions based on the top secret data you've recovered:

- Part I: Hidden Signal
  - What is the secret message?
  - Include a screenshot showing that you've found it in SDR#
- Part II: Where are you?
  - Where is our transmitter at? Take a screenshot from a mapping tool showing that you've found the rough location.
  - Show your math!

DAKOTA STATE UNIVERSITY © Kyle Cronin CSC441 Cyber Ops IT