An Investigation of Infrasonic Audio Steganography

Dustin Watson

For CNA 473

**Introduction:**

“Can Infrasonic sounds be used in Steganography?” was an open question left the work of Edwards and Young (Young, 2016) in the work in which both wrote separate papers on a shard project regarding ultrasonic data steganography in the spring of 2016. Their work showed that ultrasonic sound quickly attenuates and is unable to transmit data over open air beyond six feet. I tested hypnosis is that it is possible and show the findings.

I review following:

* What makes a good covert channel, is infrasonic AFSK is a good covert channel?
* How hard it is for people without much training to build this type of covert channel?
* What does this sound like in open air; is it noticeable for someone to try to find it and cut the connection?
* How does background noise impact the signal?

**Abstract:**

I show that data transmission via air is possible, but with extremely limited data rates given the nature of the AFSK method. A greater physical distance than ultrasonic waves is possible with infrasonic sound, however with several limitations. Tests with other students in various environments show that the connection can be stable up to 20 feet using consumer grade hardware costing less than $70. 4 students confirmed that they were able to detect (hear or feel) the sounds from a distance of 20 feet. Baud rates must be below 100 bps and, in some cases, below 10 bps to be stable data transmission. Data rates at this speed would only allow a very simple command and control interface. Other challenges include standard microphone not picking up frequencies below 30 Hz. Even with the use of a masking sound file at higher frequencies where not enough to overcome the perception of the pressure from the air waves. A surprising and interesting note was directionally of the soundwaves given the hardware that was used; Carrier waves where only acquired when in line of sight of the subwoofer speaker. A combination of speaker and microphone create this directionally.

Keywords:

* Minimodem
  + Open source software project created by Kamal Mostafa that encodes and decodes data into sound using FSK at any specified baud rate using various framing protocols.
  + Website: http://www.whence.com/minimodem/
* FSK
  + Frequency-shift keying
  + A method of encoding data on a carrier frequency by modulating it between one of two discrete values. Binary FSK is used in this project, or only two frequency values are used.
* AFSK
  + Audio FSK
  + Transition of data using audio waves using FSK
* Baud
  + A measurement of the number of symbols per second that are transmitted.
* Mark
  + In Binary AFSK it represents a binary one
* Space
  + In Binary ASK it represents a binary zero
* Infrasonic:
  + Sounds near or below normal human hearing range. They still may be felt.
* Attenuates:
  + Attenuation is the reduction of signal strength. High frequency waves tend to attenuate faster than lower frequencies.
* Frequency response
  + The range of frequencies a speaker or microphone is able to recreate or detect.

**Methods:**

Hardware:

* Dell 3025 laptop
* Samsung Galaxy 6 Edge
* Altec Lansing 251 5.1 sound system (using only the center speaker and subwoofer)
* Audio-Technica ATR3350 lavalier microphone

Software:

* Windows 10 Home
* Ubuntu 16.04 installed in VirtualBox
* VuritalBox 5.2.6
* Spectral Analyzer (Android App)
* Audacity
* Minimodem
* Online Frequency Tone Generator (<http://www.szynalski.com/tone-generator/>)

What is required to transmit data via any wave:

Shannon–Hartley theorem, that was covered as a part of our program states C = B log2(1 + S/N)

Also, Nyquist rate is a maximum amount of data that can be transmitted given a bandwidth, Frequency of signals <= 2B, B is bandwidth.

Given this information, and low frequency sound only slow bit rates will work. The bitrate has to ½ or less the difference of the High frequency (Mark) and the lower frequency (Space).

Testing Hardware:

The first method was to test frequency response of the laptops built in speakers. I used an Online Frequency Tone Generator. These speakers failed to product any sound that was below 40 Hz. Using Spectral Analyzer showed that no production at or below 40 Hz.

Minimodem and Audacity is in the repos for Ubuntu, meaning recreating the work of Edwards and Young took only a few mins. After installing the software, and learning the command line switches for Minimodem, and some trial and error, the first encode wave file had been created.

A bash script was created to aid in testing the various range of tones at or near infrasonic sound in AFSK. (Appendix: create\_all\_tones.sh) Playing these files on the Dell laptop only produces a small buzzing sound as the speakers do not support any tones in infrasonic sounds. The build in microphone is also not setup to support low frequency sounds. This led to using the microphone and subwoofer listed to get lower response rates.

VirtualBox 5.2.8 has a known issue that that keeps it from taking input as a guest OS on windows 10 hosts. (Ticket 17597) By downgrading to 5.2.6 this issue was resolved.

Initial tests had shown that the first few bytes of data would go missing in air while the Minimodem would try to establish a carrier. I used a common method in steganography, continual, to insure transitions. When tested, this method worked well. Even if one or two bytes is unreadable the receiving and can make a good guess at the message. This is very basic forward error correction.

Edwards and Young work used a copywritten song as a cover file. I was not able to use this file. I found a copywrite free song, “Stars and Strips for Ever”. This would provide as a cover for the data transmission. To ensure that none of the cover file would interfere with the transition, a high-pass filter was run to remove the lower frequencies from the cover sound file. An encoded data file with the message was merged into the wave file.

Testing in a Noise Home:

The weather didn’t permit testing outside as this spring was unusually snowy. My home is filed with people talking and/or playing at any given point, and 3 to 4 different broadcasts of TV shows. In addition to the normally audible sounds, my house is forced air with a fan that might make sounds near the frequencies used to transit sound. Spectrum Analyzer was used before and during transmit of data for a comparison of sound near the microphone receiver. With this transmission, the bandwidth range was 50 to 100 Hz. This was found to be a very stable transmission at 8 baud no matter what the sounds in the area. The signal carried in open air for a range of 10 feet. The bass tones where noticeable even with the cover file (See appendix for spectrum in lower frequencies)

Testing in a Server Room:

The second location testing took place was in Headey Hall 213. It has many computers and switches with fans that when testing the where found to provide a peak of -56 dB at 60 Hertz. Enough possible background noise to interfere with transmission of the data. I was not expecting there to be as much noise as there was in this room until I tested it.

Frequency Perception Testing:

5 students in the lab (myself including) of various ages most under 30. hearing ability decreases as people age (Age-related hearing loss - Presbyacusis, n.d.)

First, the online tone generator (Szynalski, n.d.) was used to test the hearing of the students in the Lab. This was done without the benefit of the external speakers. Since this has been tested already with the spectrum analyzer, it was known that the laptop speakers can’t put out tones around 40 Hertz. Each student was able to pick up all the tones from 40-200 in open air at a range of about 6 feet from the laptop.

By playing sounds ranging wave files created from create\_all\_tones.sh allowed the students in the lab to rate their ability to hear or feel the encoded message. These sounds where generated by the subwoofer and central speaker from the 251-speaker listed in the hardware listing. Noticeability was directly proportional to the volume level of the speakers. All the students reported being able to hear or feel the transmission. This makes open air transmission of data poor in terms of steganography.

Range of infrasonic Transmission in the Lab:

The range of a stable carrier at 8 baud and 50Hz Mark, 100Hz Space was greater than 15 feet. It was very directional. The directionality was not expected until initial tests where done with sound transfer in open air was conducted. It was directional enough to require line of sight with the subwoofer’s hole opening.

**Results:**

Is Infrasonic open-air transmission of data viable method of Stenography?

Microphones are the limiting factor. The microphones on smartphones appear to be of higher quality than very cheap condenser microphones found in laptops and common microphones. It also could be that the lavalier is by design meant to not pick up background sounds and has a directional cone of responsiveness. This could also explain why it was so directional. The use of another microphone that is more omnidirectional may have had different results.

Another limiting factor is the reduced bit rate. Since ranges must be between 1 and 20-60 Hz (given the amount of other background noise) this limits max bandwidth to ½ of 59 or about 27 baud. All the tests done where within 8 to 16 baud. Anything more than 8 tended to be unstable. 8 baud is only good for short messages in a command and control situation. This was without repeating the message to create some type of forward error correction. The channel is just to narrow too get much data though. It could however, be used as a relay to start another faster channel or as an unexpected out of band channel.

Would the added lower frequencies prompt someone to investigate and/or brake the channel?

Other students didn’t ask me to outright stop, however, from my own experience working with the low frequency tones this creates it can cause ears to become painful or start to ring after a several minutes. Without a very loud cover sound, it can cause ears to buzz and/or ring. I believe that a person who is authorized and knows what an air gapped trusted computer base should sound like might investigate the tones.

Some of these downsides however, are possible positives if the file is transferred by more conventional means like a flash drive. If the message is very short, it could be encoded and merged with a sound file using a program like audacity in a similar fashion. Then by using Minimodem directly, a perfect copy of the data can be extracted. Low bit rates make these files very large.

What makes a good covert channel, is infrasonic AFSK is a good covert channel?

Overall, AFSK is not a good covert channel. Unless there is a very specialized case for it (longer range or the possibility of penetration of concrete or other barriers) the challenge in setting up a connection comes from microphones limitations in detecting these tones. AFSK based in file steganography creates very large files because of the very low bit rate.

How hard it is for people without much training to build this type of covert channel?

Anyone with an understanding of how to use a command line and install software on Ubuntu could create this type of channel. Its easy to start creating a channel.

Does background noise impact the signal?

One surprising highlight is that background noise didn’t seam to impact the transmission of data that much. The encoding method was bell 202, which may include some error correction.

**Conclusions:**

AFSK can be used to for data transfer when less than 100 bits per second is acceptable. Infrasonic AFSK data transfer is only useful were other types of sound waves will not work for the environment and could be used for creating a one-way command and control system. Higher frequency sound waves can transmit more data per second and are less detectable with a subwoofer.

Detection of steganography in in air audio requires training staff to be alert and investigate any sounds that sound similar to tones or beeps. Any tech who has access to a server room or air gapped system should be trained to always listen then look for any beeping or tones and then report the incident. Most of the things they find doing this will be an attempt to hide a secret communication channel and will be normal faults or failures. Techs need to be open to the idea that this is possible so they know what to look for when working in sensitive areas. They also to be aware of anything that might look like or could operate as a microphone including speakers (Vaas, 2016).

Prevention of this attack also requires following all access control methods. Setting up this type of side band requires access, time, and planning. Any items which are not needed in an air gap like load speakers should be removed as to no allow for a way to transmit signals across the air gap. Over air audio signals require an authorized user to act as a vector to install software, most likely from a USB drive. Proper hardening and monitoring of data transfer over USB ports or disabling USB on critical systems could also hinder this attack. Auditing of the device that are overlooked such as load speakers that might cross physical perimeters may also prevent this covert channel.

# Works Cited

*Age-related hearing loss - Presbyacusis*. (n.d.). Retrieved from Hear-it: https://www.hear-it.org/Age-related-hearing-loss

Szynalski, T. P. (n.d.). *Online Tone Generator*. Retrieved from Online Tone Generator: http://www.szynalski.com/tone-generator/

Vaas, L. (2016, 11 24). *How your speakers could be turned into eavesdropping microphones*. Retrieved from Naked Security: https://nakedsecurity.sophos.com/2016/11/24/how-your-speakers-could-be-turned-into-eavesdropping-microphones/

Young, H. (2016). Ultrasonic Data Transmission and Steganography. *Honors College Capstones and Theses*, 6.

**Appendix**

**Create\_all\_tones.sh:**

#!/bin/bash

for i in `seq 10 10 100`;

do

hivalue=$(expr $i \\* 2)

baud=8

echo Mark $i Space $hivalue baud 8

cat ~/Desktop/hiddenmessage.txt|minimodem --tx $baud -S $i -M $hivalue -f infrasonic-b-8-s-$i-m-$hivalue.wav;

done

**hiddenmessage.txt:**

Hidden Message

Hidden Message

Hidden Message

Hidden Message

Hidden Message

Hidden Message

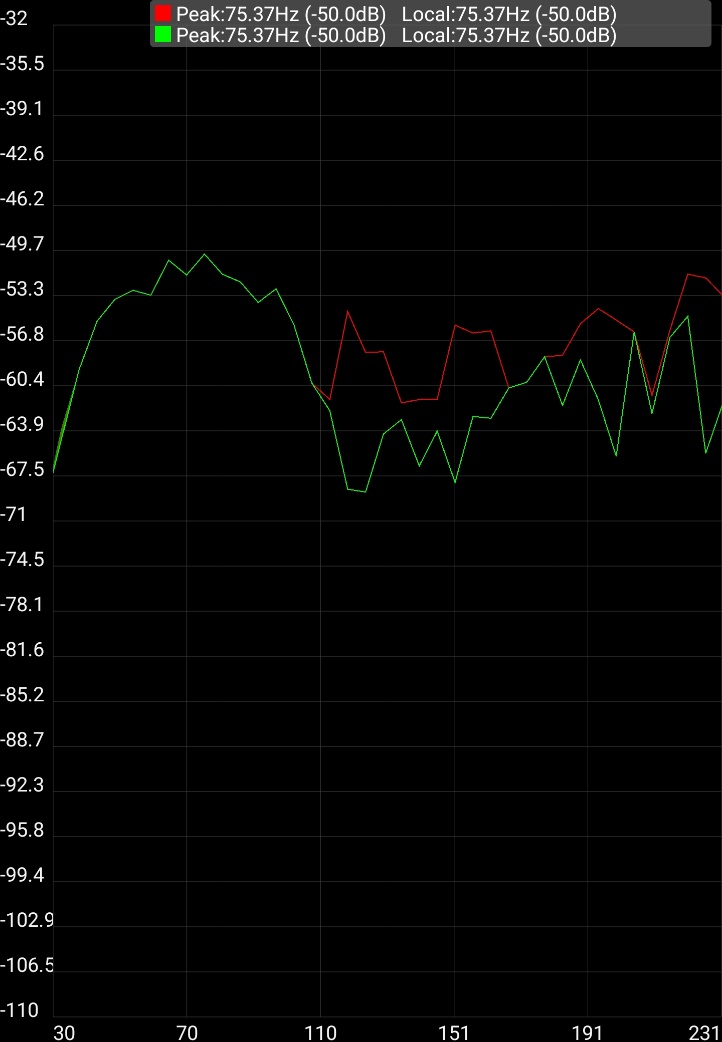
Hidden Message

Hidden Message

Hidden Message



Noise house: background sounds on the left, Transmitting on the right. Numbers at the bottom are in Hertz.



Headley Hall 213 Computer Lab: Background Noise on the left. Transmit on the right.