Kennesaw State University
DigitalCommons@Kennesaw State University

Honors College Capstones and Theses

Honors College

Spring 3-14-2016

Ultrasonic Data Steganography

Alexander Orosz Edwards
Kennesaw State University

Ultrasonic Data Steganography

March 14th, 2016

Alex Edwards

HON 4499

Contents

Forward

Abstract

What started off as a question on the possibly of data transmission via sound above the level of human hearing evolved into a project exploring the possibility of ultrasonic data infiltration and exfiltration in an information security context. It is well known that sound can be used to transmit data as this can be seen in many old technologies, most notably and simply DTMF tones for phone networks. But what if the sound used to transmit signals was in in the ultrasonic range? It would go generally unnoticed to anyone not looking for it with tools such as a spectrum analyzer. This could provide an unnoticed means of transmitting overhead data without the use of radio signals or physical connections, or, more clandestinely, a means to inject or retrieve data virtually undetected for espionage, control, or other malicious activity. As expected, there would obviously be issues with signal quality as the open air is heavy with environmental interference, but in specific cases as seen in the following research, a discrete sonic means of data transmission may not only be practical, but necessary for the task at hand.

This project is an exploration of the practicality of ultrasonic data transmission between computers. It will include research into the topic in general from scientific, technological, and security perspectives. There will be inclusions from other research projects as well as practical applications already in existence. Interestingly, there are already some suspected, but unconfirmed planned systems as well security incidents using this technology. Finally, a short series of semi-formal (in a scientific sense) experiments conducted to provide firsthand accounts and results of the ultrasonic data transmission concept.

Joint Project Statement

This project was a joint effort between myself, Alex Edwards, and Hunter Young. We are both seniors in Kennesaw State University's Bachelor of Information Security and Assurance program. This became a mutual idea with collaborative research occurring on a regular basis. With academic approval, we moved forward with the formal project. Out of many reasons, the need for pooling of resources and ideas provided the necessity for a joint project. The experiments we conducted often needed multiple computers and at least two people across a distance.

While most of our data and sources of research will be identical, these reports are individual efforts with the last step of collaboration being a shared dump of experiment results and ideas about the subject. Hunter and I have similar experience with information security and information technology in general with myself having amateur radio and more professional IT experience and Hunter having more experience in music and acoustics. This provides a unique opportunity to produce two conclusions, each of a slightly different perspective and background, from similar data. There will be intentionally concurrent sections, and correlations beyond experimentation and joint research could be considered a blind consensus between Hunter and I.

Initial Theory

While the concept of ultrasonic data transmission can cover a wide range of practical uses, steganography is of pinnacle interest to those in the information security field. By nature, transmitting anything by ultrasound can be considered steganography as the data is publicly "in the air" but is hidden by anyone not looking for it. Further, because the ultrasound would be a significantly higher frequency than most noise or music, it may be able to better pierce through interference and could be played with music or imbedded into music files.

For cyber security, the ability to discretely remove data or carry a malicious payload in the form of sound presents many opportunities and threats. This theory is amplified by the fact that, while network cables can be unplugged and WiFi radios turned off, most modern computers, especially consumer laptops and phones, have built in microphones and speakers that can be utilized maliciously to compromise or control those compromised systems.

As initial research was conducted, keeping other ideas in mind, “Can this be used to deploy or control malware and how hard is it to stop that?” became the most pressing theoretical question regarding cyber security practicality. What we found reported on the internet and what we were able to accomplish in our experiments proved interesting.

Executive Summary

This report will start with a basic explanation of the science behind sound in a physical sense, and then the practice of modulating waves to carry information. Human hearing’s limits and the limitations imposed by the properties of ultrasound itself will be discussed. Technology, including both audio equipment and audio software will be discussed also. Finally, information security in general, as well as networking, steganography, and data infiltration/exfiltration will be covered. These first three major sections will provide a background for our investigations. This report assumes a basic grasp of these concepts already. Some terms will be explained inline where relevant to the topic at hand.

As expected, there were very few sources to comment on as ultrasonic data transmission and steganography, at least in the use case presented here. However, a potential security and commercial incidence were discovered as well as several short reports discussing specific tests in depth. The first case from Fraunhofer FKIE, was the closest match to our own theory and investigations.

While the tests were narrowed down from earlier plans to meet realistic and in-scope goals, the overall creation of a proof of concept was successful and yielded useful results toward practical conclusions in close concurrence to our research, but also with some interesting variances. Finally, after conclusions are presented, keeping with the theme of practicality, a discussion is included covering suggestions for applications, scenarios, and security controls.

Acoustics

Sound Waves

As many already know, sound is transmitted by the movement of areas of matter that have been compressed or decompressed relative to the rest pressure of a physical medium. These periods of compression travel through a medium from the source in a spherical pattern (assuming no obstacles are present) from the source in the form of a wave. These waves may be absorbed by surfaced and converted into other forms of kinetic energy. Also they may be refracted upon the transition between mediums or reflected back toward the source or in perpendicular direction entirely. These concepts are important to the physical characteristics placing features and restrains on the ability of sound to transmit data.

Along with light, sound is one of our oldest methods of communication principally in the form of speech and also with signals as with sirens or beeps and to deliver entertainment in the form of music. In addition to analog modes, sound is also able to represent digital data in a primitive form. Different frequencies and patters are used to convey messages.

Mode and Modulation

On a more complicated level, as with electromagnetic energy, both types of waves can carry more complicated signals via different modes such as AM and FM. While sound signals, like speech and music, are analog and arbitrary in regard to mode, digital information usually requires a uniform mode. This is often more apparent in electromagnetic waves in the light and radio spectrum. There a multitude of modes in use from the simple constant wave (CW) used for Morse code to amplitude modulation (AM) and frequency modulation (FM) used for analog music and voice. Other, more complex modes are usually combinations of theses simpler modes and alternate between them in a pattern. Slower, but higher fidelity digital modes like phase shift keying (PSK) and frequency shift keying (PSK) are often used for long distance communication while faster, but more fragile, forms of modulation like quadrature amplitude modulation (QAM) used by digital cable TV and WiFi. For our tests, we stuck to one mode, FSK. Justification for this will be provided in later sections. FSK changes the frequency of a wave between two predetermined frequencies, a mark and space frequency, to represent ones and zeroes. As you will see later, the speed that data travels over these methods is measured in baud, or the number of symbols changes per second.

Human Hearing

When these soundwaves reach a human, they travel down the ear canal, impact the eardrum where the kinetic energy absorbed causes the eardrum to vibrate and the connected bones to vibrate. These bones vibrate liquid in the inner ear, which in turn vibrates small fibers attached to nerves. Human hearing range, frequency wise, is roughly 20Hz to 20kHz with many factors contributing to the shrinking of this range, most notably age and occupational damage (Smith). In our tests, we noticed that approximately 17.5kHz was the upper limit of human hearing among ourselves and other college students with the upper range causing a sense of irritation more than an actual perception of sound.

This provides two main reinforcements to why steganography can be achieved by transmitting data sonically above the range of human hearing. While a human would have a hard time interpreting a spontaneous unexpected audible signal, any strange unexplained sounds, especially those emanating from electronic devices would be cause for curiosity and investigation. Also, because humans generate sound intentionally on a regular basis for other humans to hear, ultrasonic signals would be in frequencies above the range of human hearing and therefore would not be interfered with and could be combined with these noises for concealment as you will see in one of our proofs of concept.

Limitations

The same background sounds (environmental noise, music, speech) that can be used to provide distraction, concealment, or a means of steganography might also be a source of destructive interference that can threaten the fidelity of a data signal. Practically, the farther away two sounds are in frequency (including their harmonics) the less interference. Technically, there can be constructive and destructive interference. With destructive interference, the high pressure zones of two or more soundwaves are at opposite alternating or unsynchronized times, canceling out net changes and pressure and reducing the volume of each sound. While humans might not produce ultrasonic interface, machines might, especially electrical components in the devices that would be transmitting and receiving signals.

Aside from background noise, the propagation ability of ultrasound may be diminished compared to lower frequency noise. Many factors in the medium of travel as well as objects in the path of the sound could affect ultrasound differently than sounds in the human hearing range. This could be a research study in itself, but this investigation is mostly concerned with the practical ramification. We performed out tests in different environments because of this. We did find that ultrasound, at the same volume from the same device, did not diffract outside of a doorway as well as other sounds did thus demonstrated the ability for ultrasonic signals to by physically contained to a room.

Technology

Equipment and Hardware

Because we are testing ultrasonic data transmission and steganography in an information security context with computers and mobile devices in particular, it is important to confine the scope of tests and research to the microphones and speakers already installed on the devices. Almost all modern computers and mobile devices, save for a few desktops and higher end specific purpose machines, are sold with audio devices.

Microphones have diaphragms that vibrate when sound waves are absorbed much like eardrums. Speakers work in reverse by vibrating the diaphragm to produce sound waves in the air. Design varies by type of microphone or speaker, but in general they consist of a magnet and a coil of wire with one or the other moving. Receiving sound produces fluctuations in the electrical current in the coil and the wires attached, producing an electrical representation of a sound wave. To create sound, the process is reversed by feeding a fluctuating current into the speaker and moving the diaphragm. From out tests, we have discovered that these devices have no problem generating and detecting ultrasonic signals under 20kHz.

Audio Sampling and Compression (Digital/Analog)

When analog sound is converted to electricity by a microphone, it travels to some kind of digital to analog converter most often referred to as a “sound card” in computer. The electronic representation of sound is digitized by taking measurements of the amplitude at regular intervals in a process called “sampling.” The reverse of this process creates sound from a speaker. The number of measurements per second is referred to as the “sampling rate” and is typically 44.1kHz as the default for consumer electronics. “Bit depth” is the number of digital bits used to represent each sample, with 16bit being the consumer standard (Production Bytes, 2012). Both of these are proportional to the fidelity of an audio signal and together make up the "bit rate" of an audio signal.

When considering the ability to store ultrasonic data in audio files, especially discretely, digital audio has limits beyond the capability of hardware. MP3 is the most common format for storing audio. It is a "lossy" format meaning that to create a smaller file, the audio is "compressed" by removing data. The actual compression algorithm is complex, but has two factors that impede its ability to carry data electronically. Typically, MP3s have a much lower bit rate than "raw" formats like WAV. Also, MP3 was also designed to save space by removing audio, such as ultrasound, that is considered to not be relevantly perceivable to humans (MP3, 2016). One of our very first tests (separate from our main experiments) consisted of trying to interpret an ultrasonic data signal after it was converted to MP3 and played. The signal was almost completely destroyed.

Information Security Concepts

Information Security

For this project, the primary information security concern will be cyber security. This covers both the devices themselves and any information on them at risk. To protect the confidentiality and integrity of information assets, many technical and procedural security controls have been developed over the years to protect these electronic devices including firewalls, malware scanners, access control infrastructures, and encryption. Many of the typical vectors of attack have some kind of preventative or mitigating control.

Networking

Network security falls under the realm of cyber security, and since the beginning of the internet age, the use of networking to share information between electronic devices locally and across the world is ubiquitous and constant. These networking mediums are potential vectors for remote attackers wishing to compromise a system to gain control, acquire confidential information on it, or otherwise damage the information or the device itself. These devices are networked via some type of connection usually Ethernet, WiFi, Cellular using any number of protocols and infrastructures. We have long had the capability to encrypt our communication channels, filter unwanted connections and content, authenticate the integrity of the received and sent information, to isolate and control access to networks, or completely block the flow of information by turning the networking hardware off.

While these attack vectors have security controls, the possibility of network data flow via the audio equipment on the device widens the potential attack surface into uncontrolled and unsecured territory. Turning off networking equipment, unplugging cables, and even removing wireless LAN hardware to ensure that that there is no unauthorized data infiltration or exfiltration is known as an “air gap.” The physical network isolation that an air gap provides may be overcome by the fact that audio equipment would almost never be considered as a means of digital data transmission and that sound uses the air itself as a physical medium to transmit signals.

Steganography

The most common way to prevent unauthorized access to information on a network or computer is encryption. With encryption, information is scrambled into a virtually unreadable code that requires a key to decrypt the ciphertext. However, another, more basic method, steganography, is also used, more often maliciously. Instead of rendering data unreadable, steganography hides data among seemly normal traffic or noise. This prevents reading of the data as it is intended to go unnoticed, unlike encryption. This is often seen in the cyber security world when malware files have seemingly harmless names or in the more novelty practice of hiding one file within another file of a different type for example.

While anti-malware can often prevent or mitigate the use of steganography to hide malicious files by scanning everything for matches to signatures of know malware or by heuristic analysis of the behavior of potential malware, many technical security controls are not designed to handle the obscurity of ultrasonic data stenography.

Ultrasonic signals are stenographic in nature because they are above the range of human hearing and can be hidden in innocent sounding audio files without degradation to fidelity. A seemingly harmless listener program can sit on system for years and not be detected because the malicious instructions or data to be infiltrated are not stored in the program, but are received or transmitted in the air in real time during execution.

Data Infiltration and Exfiltration

Data can mean many things; here, the concern is mostly sensitive information such as credit card numbers, trade secrets, or intelligence adding in further compromise of a system and also data as commands or instructions such as scripts, codes, and prompts. Covert retrieval of or leakage of this sensitive data from an otherwise secure system is exfiltration. The placement of data for the purposes of planting a file or delivery of malicious code on a similarly assumed secure system is infiltration. Recently stated in the preceding sections, infiltration of a payload with an ultrasonic signal via an assumed secure system's audio equipment is of particular concern and will be references again in a few later sections.

Occurrences In The Wild

Reported Incidents

There are multiple internet articles, some skeptical, about a security researcher's investigation of a BIOS (basically the firmware of a motherboard) based rootkit, dubbed "badBIOS," that seems to be communicating between infected systems via ultrasound. The malware is reported to persist on the computers firmware across BIOS flashes and operating system reinstalls and preventing the booting from removable media like CDs and flash drives. The malware is reported to initially infect via USB, make a large number of minor configuration changes, and exchange data between infected computers. Data packet flow was detected between two air gapped infected computer despite being unplugged from power and having all networking hardware removed. The packet flow stopped after the audio hardware was removed (Goodin, 2013). This is assumed to be a hoax by some, as other researchers believe the ultrasonic signals to be artifacts from other sources and the fact the original reporter, Dragos Ruiu, does not provide much evidence of his ongoing investigation (Grimes, 2013).

The Center for Democracy and Technology recently submitted a report to the Federal Trade Commission regarding the privacy concerns over cross device tracking technology. Among these include a company called SilverPush's use of ultrasonic beacons to synchronize and analyze advertisement content allowing better targeting of marketing across media.. When a user accesses a website or watches a commercial from a SilverPush enabled advertiser, an ultrasonic beacon is played. SilverPush enabled apps on phones and tablets listen for this beacon and report the correlations between television choices, app usage, time, and location depending on the beacon. They have stated that distance is a major limiting factor of this technology. It is not known if these beacons are digital data or analog markers (Center for Democracy & Technology, 2015), (Bansal, 2015).

Others' Research

This is a bleeding-edge concept, so research into it, especially in an information security context, is extremely limited. However, some scholars and security researches have touched on this concept. Many possible sources of information just seemed to point back to these same articles offering no new information, usually, it was the study below.

Michael Hanspach and Michael Goetz, two researchers at Fraunhofer FKIE, produced a paper stating that they were able to use a proprietary network stack (set of software and protocols) intended for sonic communication in another project to create an ultrasonic meshnet between laptops with a 20 bit per second speed at a distance of up to 19.7m. They were successfully able to have a keylogger transmit recorded keystrokes across a meshnet of computers and collect the keystrokes of the primary victim computer on remote system (Hanspach & Goetz, 2014). This confirms the validity of the concern that ultrasonic data transmission between systems is a security threat.

Other researchers at University of Oklahoma were able to achieve ultrasonic data transmission via FSK with a bit rate of up to 800 bits per second. However, their experiment was slightly different. They were testing the feasibility of transmitting data across solid metal mediums that would otherwise block radio signals. They used ultrasonic transducers (similar to speakers) to transmit data along steel beams (Multi-Tone FSK for Ultrasonic Communication, 2015). This is an interesting concept because high security organizations do employ controls that prevent radio signals from propagating into or out of the building. However, it does not employ stock hardware that normal consumer electronics would use.

Wentao Jiang published an article at University College Cork, Ireland providing a few possible theoretical uses for ultrasonic data transmission. Most of his scenarios were for applications where data had to be transmitted, but where radio transmission would be harmful or dangerous to people or other equipment, but also suggested the possibility that it could be used to make a more secure wireless network as ultrasound is more easily contained to a room than radio waves (Jiang, 2014).

A developer named Katee wrote a fledgling chat program called “Quietnet” that sends ASCII symbols to other computers at around 19kHz and is intended as a way to discretely chat locally without exposing the text to interception by a packet sniffer. The developer states that Minimodem and GNU Radio, software we use for our tests, are much better than her software though (Katee, 2014).

Testing

Hypothesis

Building on the Initial Theory section, it was important to reduce our testing ideas to fit our constraints. Our tests, and therefore our hypothesis, had to be broken into stages. Overall, based on the research and our knowledge of the underlying science, successful creation a proof of concept seemed achievable. The inability to compress ultrasound; ability to transmit ultrasonic data over a distance; the ability to receive, demodulate and parse that data; and the ability to use music as a means of delivery and steganography was hypothesized and tested in those stages. Hunter's hypothesis and following interpretations of results might differ from mine in his analysis.

Constraints

When first planning out the project, Hunter and I assumed a massive array of tests with many variables. However, as we did research on the nature of the project, we determined that certain environmental factors, software availabilities, time constraints, pre-testing, and practical application narrowed down the necessity and ability to experiment with the multitude of independent variables originally designed. Part of this investigation was learning which tests were not feasible. If they were difficult and impractical for us to test, developers and hackers would likely avoid them also. Most importantly, we incorporated a lot of publicly available freeware that not only existentially reinforced our arguments, but also allowed us to move forward to an easily reproducible, practical proof of concept.

While our first test used an ultrasonic radio developed with GNU Radio, later tests utilized software called Minimodem, an audio modem built for Linux by Kamal Mostafa that utilizes FSK (Mostafa, 2016). This imposed a few very relevant constraints on our test aside from the fact that it was the best available means for our test. FSK is a digital mode that strikes a reasonable balance between the slow, high fidelity modes like CW, and the fast, dynamic, but complex and fragile modes like QAM. Also, we can eliminate temporal modes such as PSK. The creator of the GNU Radio method we used for initial tinkering reinforces this determination as he also claims FSK is superior to PSK in his tests (Anfractuosity). Regarding time, taking more time to transmit a signal can provide for higher fidelity in theory, but the longer time also allows more time to collect interference. These factors are seriously dependent on the mode and environmental noise, though. Most importantly, in regards to practicality, Minimodem is open source, meaning the source code is public. An attacker building malware using this technology would most likely try to incorporate and augment already proven code into their programming rather that tediously "reinventing the wheel" for the same functionality. This allowed us to reasonably eliminate another independent variable.

Because of the availability of testing software like Minimodem and GNU Radio on the Linux platform, most of our transmission tests were confined to Linux only. While it is important to consider other operating systems like Windows, especially when discussing malware, utilizing the concepts presented here on other systems is a matter of programming or "porting" software to those platforms in some way. This is a software development issue and is not within the scope of our tests. While some differences may be introduced by drivers and other audio processing software, the hardware can be considered a constant.

As stated before, the use of stock hardware is important when considered from an information security perspective. We are testing the ability to use ultrasound for data transmission discretely; therefore, all testing device hardware was unmodified. It was acceptable to use both cell phones and laptops as both are in common use as computing devices and containers of information assets. Another hardware affected independent variable we eliminated was loudness, as the amplitude capability varies among the different hardware and volume may be increased up until the point of audio distortion providing a theoretical boost to range, but that concept is not very relevant to our investigation. Four our tests, we used the maximum system volume on each device. This provides a pseudo constant, as the hardware on each device is different.

Testing Narrative

Before trying our main proof concept, we conducted two informal experiments to test our ability to move forward with the main experiment. Using, GNU radio, an open source visual tool to construct software defined radios in Linux, and using the radio setup developed by Anfractuosity on Hunter's laptop, he was able to transmit text via ultrasound (Anfractuosity). While we did not test the ability to receive and interpret the transmission back into text, we did test the ability to receive the signal on another device (verified by spectrum analyzer on a phone) across a crowded room in the Burruss building. Interestingly, the physical containment concept from previous sections was reinforced as the signal was not detected outside of the doorway. While we assumed MP3 compression would destroy an ultrasonic signal, I still tested that as well. Using the open source audio editing software Audacity, I tested the integrity of an ultrasound slow scan television signal after conversion to MP3 so that I could better visualize the effect of compression on it. The signal was reduced to mostly static.

We began Minimodem tests with two laptops, both running Ubuntu Linux, a modern Dell Ultrabook (XPS 9340) as the receiver and an older Dell netbook (Latitude 2100) as the transmitter. We conducted these tests in the common area of a dorm. At first, we were testing with the Badout character set that is traditionally used for Radio Teletype (RTTY). It provides greater speed due to its simplicity, but we realized a fundamental problem in that it was case insensitive when many device operating system commands and data formats are case sensitive, we soon witched to ASCII. We began testing different frequencies between 17kHz and 20kHz in .1kHz intervals and testing their ability to transmit data. As stated before, while slowing down the transmission rate, or baud, would, in initial theory, provide higher fidelity; it also allows more exposure to interference. We experimented with a few baud rates, but decided to stick with 45 baud as it produced the best results over multiple tests. Coincidently, 45 baud is also the most common speed for amateur radio teletype (Radioteletype, 2016). We encountered sporadic problems when the laptop microphones and speakers were not pointed at each other, so we began testing sending text between the devices with their fronts facing each other, for the greatest stability in results, and moved them farther apart each test to get a maximum distance that we were reliably able to transmit text without error. We determined the best overall transmission parameters were 45 baud ASCII with a space frequency of 18.6kHz and a mark frequency of 18.7kHz. This will be explained more in the next section. To start the transmitter at the command line, *minimodem --tx -S 18600 -M 18700 45 --ascii* was entered and text messages were sent afterwards by typing and pressing enter at the command line (receiving command will be demonstrated in the next paragraph).

Our selection of text to transfer between the laptops was arbitrary, but after we were able to determine the best workable parameters, we needed to test the ability to control the computer with ultrasonic commands. Therefore we chose the command *cat etc/passwd*, which returns the user accounts of the system. To receive the ultrasonic commands and pipe them to the command shell for execution the command *minimodem --rx -S 18600 -M 18700 45 --ascii -c 2.5 -q | sh* was used to start the listener on the Ultrabook. There are two new flags in this command. "*-c"* represents the "confidence threshold" or the minimum signal quality the program will accept. Basically, it acts as the squelch, but was not well documented beyond what we could ascertain. 2.5 was high enough to reject most interference, but not reject the intended transmission. The "*-q"* flag removes metadata or debug output about the received signal so only the command is passed to the command shell.

Finally, we needed to test the ability to use steganography. We chose Sandstorm by Darude as the innocuous carrier of the previous ultrasonic audio payload and the test of the resistance to interference when using the music to hide the signal. We knew from earlier tests that MP3 compression damages the ultrasonic signals, so, we combined the audio in Audacity by having it record the speaker output of the signal with the buffer spacing, imported the Sandstorm MP3, and exported it to a raw .WAV file for our tests. We tested the ability to send commands to a discretely listening computer and also took spectrograph images of the signal in different environments.

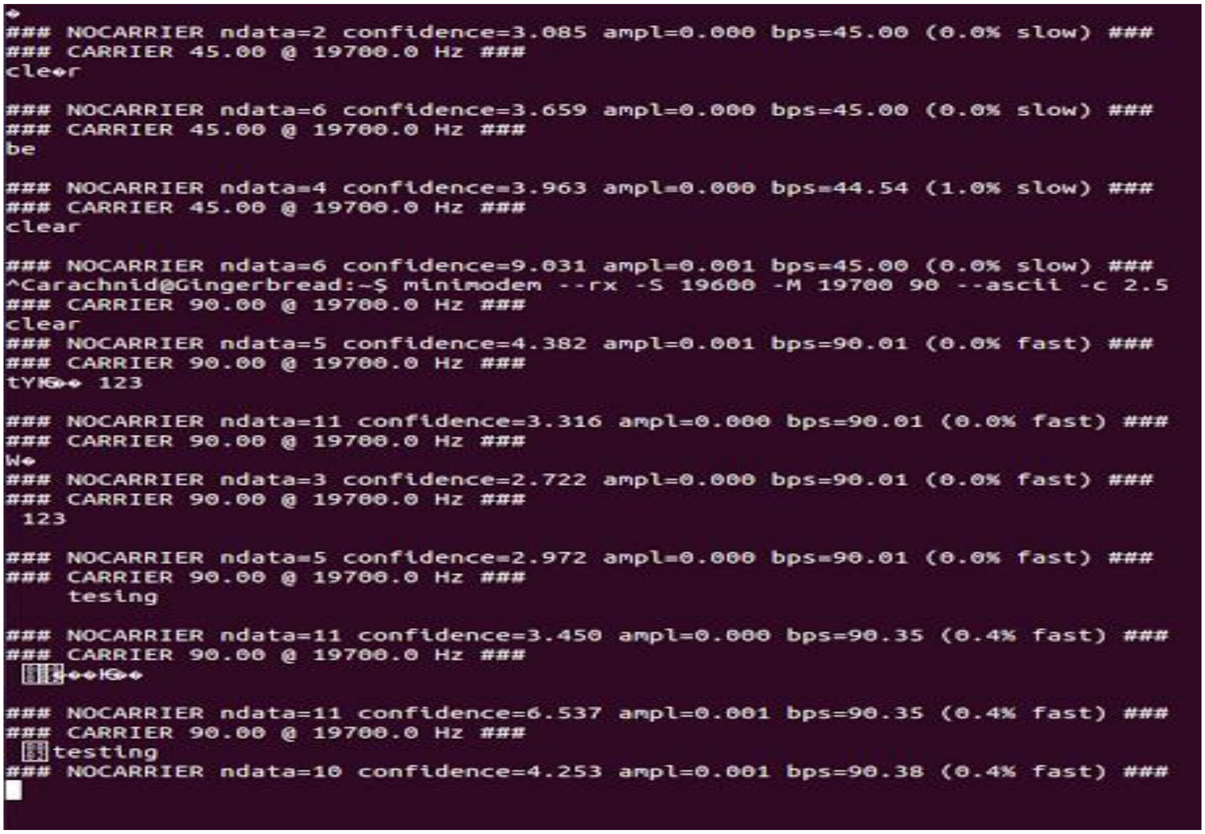
After this, we wanted to collect some data about different environments beyond or initial proof of concept and provide some acoustical context about those environments while allowing visualization of their effect on the noise profile. To do this, we took the audio file from our previous test and the ultrasonic transmission without the music, and played them on my phone (Motorola XT926M) while collecting spectrograph images with a Spectrum Analyzer app on Hunter's phone (OnePlus One). We took a screenshot of the background noise, playing of the ultrasonic signal, and then the signal and music combined in the dorm where our initial tests were conducted, outside of the dorm with traffic going by, a server room, and the KSU Commons. We also repeated our previous tests with the laptops. The last two, a server room and a crowded area represent two environments where ultrasonic steganography usage or attacks might occur. The results are in the next section.

Results and Examples

Most of our tests were conducted with ‘yes’ or ‘no’ possible conclusions until the final environmental tests with the spectrum analyzer. This project is approached from an information security perspective rather than a scientific one. Empirical data is not as important as the practical ability to produce a functioning proof of concept. Also, an abundance of empirical data is not as relevant to the overall question at had as, when dealing with acoustics, there are too many independent variables imposed by the changing environmental factors and the materials used with testing. However, the evidence presented here should provide a glimpse into the real-world possibility of using ultrasonic transmission for data stenography.

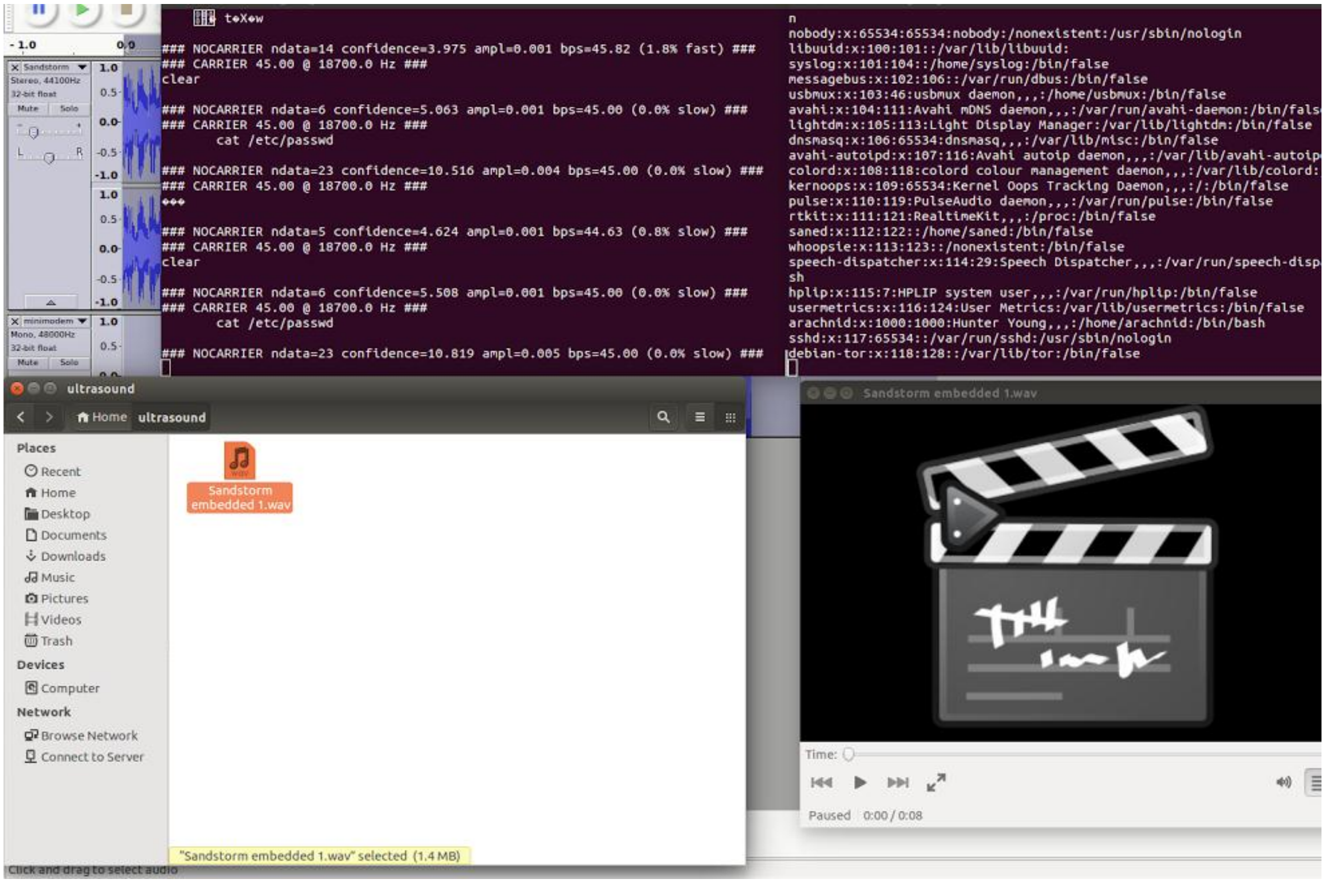
From our tests in the dorm common area it was determined that the best transmission parameters using Minimodem, when considering the relevance to cyber security, was using the ASCII character set at 45 baud, FSK with a space frequency of 18.6kHz and mark frequency of 18.7kHz. With the two laptops facing, were able to receive transmissions without error at a distance of up to 8 feet. These tests were repeated outside of the dorm by a busy road, in server room, and in the crowded KSU Commons. The observable difference was that the usable distance shrank to 6 feet outside and in the server room.

The following is an image of the receiving laptop trying to read a signal at 19.7kHz was one of our tests trying to pinpoint a good frequency. Notice the errors in receiving when the signal is closer to the observed ~20kHz usable limit when trying to receive. This displays the output of the Minimodem listener on the command line.



```
�
### NOCARRIER ndata=2 confidence=3.085 ampl=0.000 bps=45.00 (0.0% slow) ###
### CARRIER 45.00 @ 19700.0 Hz ###
cle�r

### NOCARRIER ndata=6 confidence=3.659 ampl=0.000 bps=45.00 (0.0% slow) ###
### CARRIER 45.00 @ 19700.0 Hz ###
be

### NOCARRIER ndata=4 confidence=3.963 ampl=0.000 bps=44.54 (1.0% slow) ###
### CARRIER 45.00 @ 19700.0 Hz ###
clear

### NOCARRIER ndata=6 confidence=9.031 ampl=0.001 bps=45.00 (0.0% slow) ###
^Carachnid@Gingerbread:~$ minimodem --rx -S 19600 -M 19700 90 --ascii -c 2.5
### CARRIER 90.00 @ 19700.0 Hz ###
clear
### NOCARRIER ndata=5 confidence=4.382 ampl=0.001 bps=90.01 (0.0% fast) ###
### CARRIER 90.00 @ 19700.0 Hz ###
tY��� 123

### NOCARRIER ndata=11 confidence=3.316 ampl=0.000 bps=90.01 (0.0% fast) ###
### CARRIER 90.00 @ 19700.0 Hz ###
W�
### NOCARRIER ndata=3 confidence=2.722 ampl=0.000 bps=90.01 (0.0% fast) ###
### CARRIER 90.00 @ 19700.0 Hz ###
 123

### NOCARRIER ndata=5 confidence=2.972 ampl=0.000 bps=90.01 (0.0% fast) ###
### CARRIER 90.00 @ 19700.0 Hz ###
    tesing

### NOCARRIER ndata=11 confidence=3.450 ampl=0.000 bps=90.35 (0.4% fast) ###
### CARRIER 90.00 @ 19700.0 Hz ###
 ▯▯������

### NOCARRIER ndata=11 confidence=6.537 ampl=0.001 bps=90.35 (0.4% fast) ###
### CARRIER 90.00 @ 19700.0 Hz ###
 ▯testing
### NOCARRIER ndata=10 confidence=4.253 ampl=0.001 bps=90.38 (0.4% fast) ###
█
```

Below is a screenshot of the actual testing of steganography of the *cat etc/passwd* command with music. In the background is the Audacity window, where the sounds where combined into a .WAV file, with the stereo waveform of Sandstorm showing. In the left command shell window, multiple commands for clearing the command shell to the right and testing adding buffer spaces to command can be seen in the Minimodem listener output. In the right shell window, the ultrasonic command has been piped to the shell thus directing the operating system to parse the *etc/passwd* file showing the user accounts. For this test, we transmitted from Hunter’s laptop’s speakers to his laptop’s microphones, from my laptop’s speakers to his laptop’s microphone, and from my phone to his laptop’s speakers. All tests were successful.

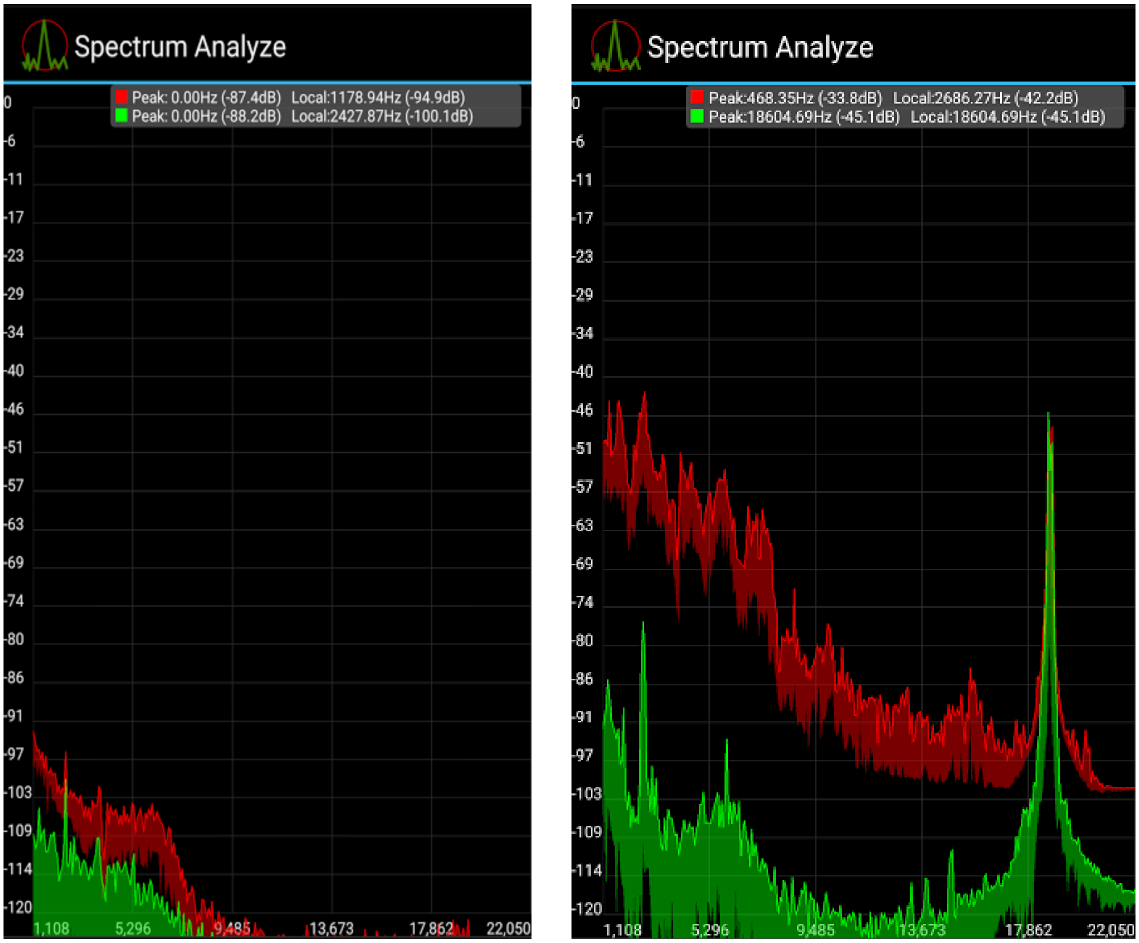


```
   t◆X◆w
### NOCARRIER ndata=14 confidence=3.975 ampl=0.001 bps=45.82 (1.8% fast) ###
### CARRIER 45.00 @ 18700.0 Hz ###
clear

### NOCARRIER ndata=6 confidence=5.063 ampl=0.001 bps=45.00 (0.0% slow) ###
### CARRIER 45.00 @ 18700.0 Hz ###
    cat /etc/passwd

### NOCARRIER ndata=23 confidence=10.516 ampl=0.004 bps=45.00 (0.0% slow) ###
### CARRIER 45.00 @ 18700.0 Hz ###
◆◆◆

### NOCARRIER ndata=5 confidence=4.624 ampl=0.001 bps=44.63 (0.8% slow) ###
### CARRIER 45.00 @ 18700.0 Hz ###
clear

### NOCARRIER ndata=6 confidence=5.508 ampl=0.001 bps=45.00 (0.0% slow) ###
### CARRIER 45.00 @ 18700.0 Hz ###
    cat /etc/passwd

### NOCARRIER ndata=23 confidence=10.819 ampl=0.005 bps=45.00 (0.0% slow) ###
```

```
n
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
usbmux:x:103:46:usbmux daemon,,,:/home/usbmux:/bin/false
avahi:x:104:111:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/fals
lightdm:x:105:113:Light Display Manager:/var/lib/lightdm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:107:116:Avahi autoip daemon,,,:/var/lib/avahi-autoip
colord:x:108:118:colord colour management daemon,,,:/var/lib/colord:
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:121:RealtimeKit,,,:/proc:/bin/false
saned:x:112:122::/home/saned:/bin/false
whoopsie:x:113:123::/nonexistent:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-disp
sh
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
usermetrics:x:116:124:User Metrics:/var/lib/usermetrics:/bin/false
arachnid:x:1000:1000:Hunter Young,,,:/home/arachnid:/bin/bash
sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
debian-tor:x:118:128::/var/lib/tor:/bin/false
```

The following images are the spectrograph tests discussed at the end of the Testing Narrative section. Observe the listed peak value of approximately 18.6kHz and the two pronged appearance of the peak showing the separation of the space and mark frequency. To the left of the ultrasonic signal, environmental noise and music can be seen in the spectrograph. For this spectrograph, the X axis is frequency in Hz and the Y axis is decibels. Ignore the red values.

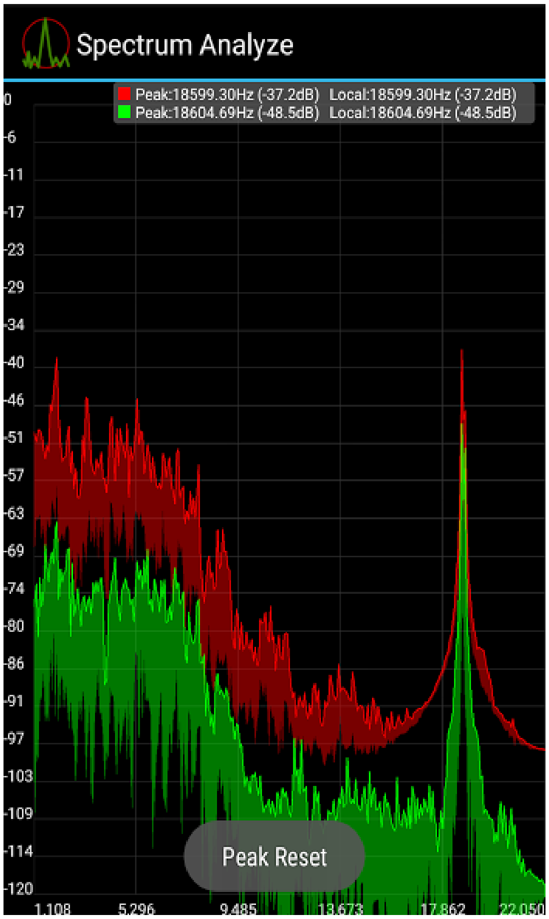
Dorm Noise Floor (LEFT) and Dorm + Ultrasonic Signal (RIGHT)



🟥 Peak: 0.00Hz (-87.4dB) Local:1178.94Hz (-94.9dB)
🟩 Peak: 0.00Hz (-88.2dB) Local:2427.87Hz (-100.1dB)

🟥 Peak:468.35Hz (-33.8dB) Local:2686.27Hz (-42.2dB)
🟩 Peak:18604.69Hz (-45.1dB) Local:18604.69Hz (-45.1dB)

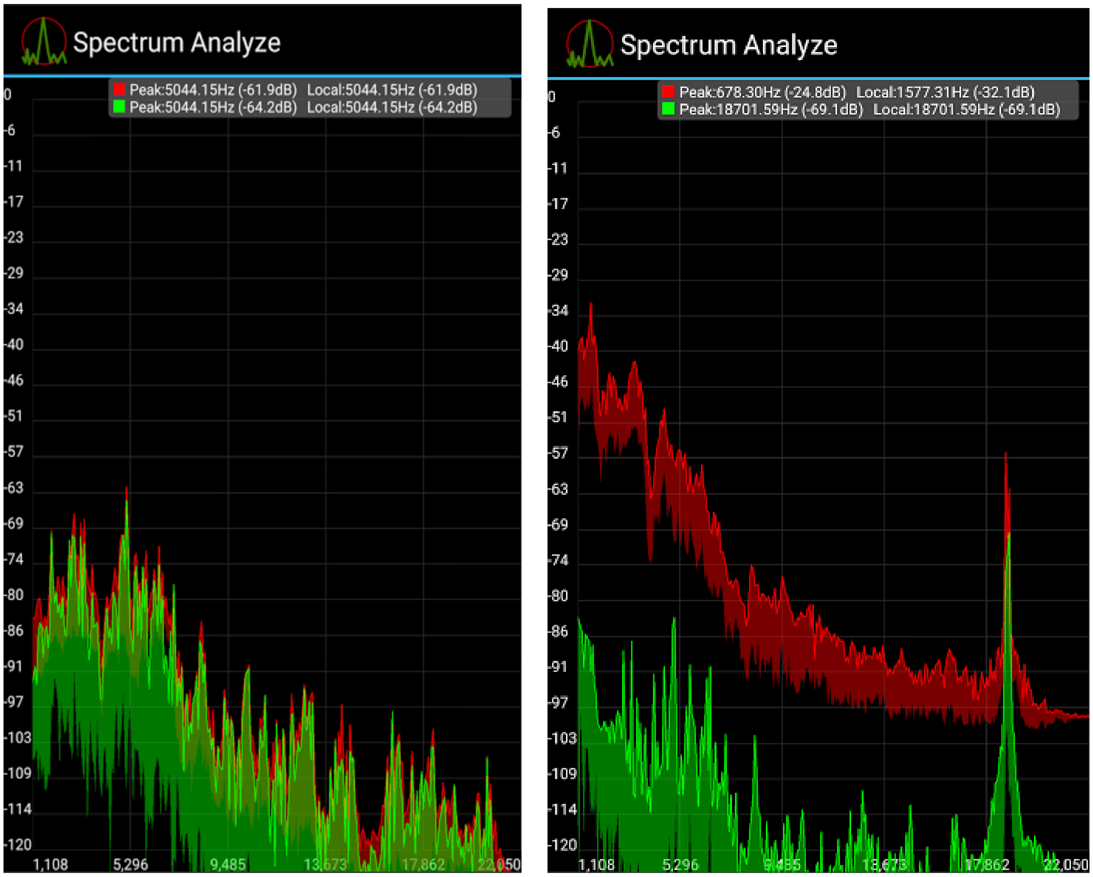
Dorm + Ultrasonic Signal + Music



🟥 Peak:18599.30Hz (-37.2dB) Local:18599.30Hz (-37.2dB)

🟩 Peak:18604.69Hz (-48.5dB) Local:18604.69Hz (-48.5dB)

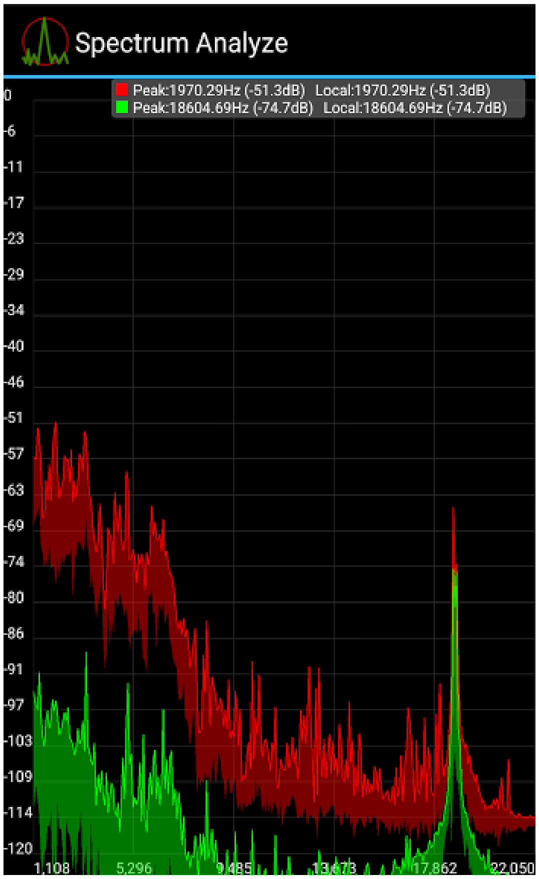
Outdoor Noise Floor (LEFT) and Outdoor + Ultrasonic Signal (RIGHT)



🟥 Peak:5044.15Hz (-61.9dB) Local:5044.15Hz (-61.9dB)
🟩 Peak:5044.15Hz (-64.2dB) Local:5044.15Hz (-64.2dB)

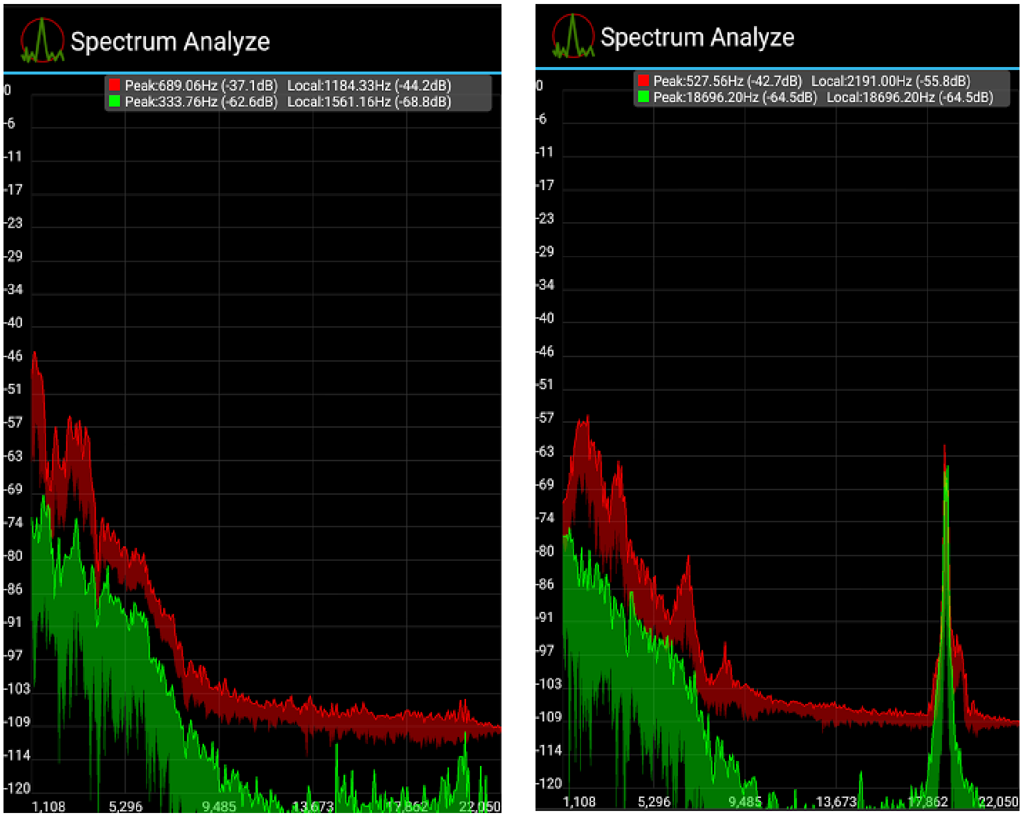
🟥 Peak:678.30Hz (-24.8dB) Local:1577.31Hz (-32.1dB)
🟩 Peak:18701.59Hz (-69.1dB) Local:18701.59Hz (-69.1dB)

Outdoor + Ultrasonic Signal + Music



🟥 Peak:1970.29Hz (-51.3dB) Local:1970.29Hz (-51.3dB)
🟩 Peak:18604.69Hz (-74.7dB) Local:18604.69Hz (-74.7dB)

Server Room Noise Floor (LEFT) and Server Room + Ultrasonic Signal (RIGHT)



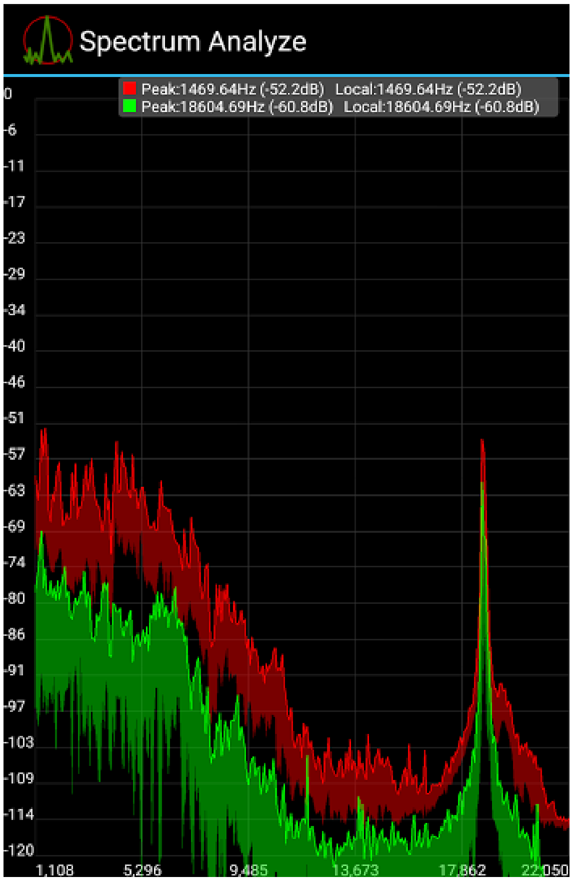
Spectrum Analyze

🟥 Peak:689.06Hz (-37.1dB) Local:1184.33Hz (-44.2dB)
🟩 Peak:333.76Hz (-62.6dB) Local:1561.16Hz (-68.8dB)

Spectrum Analyze

🟥 Peak:527.56Hz (-42.7dB) Local:2191.00Hz (-55.8dB)
🟩 Peak:18696.20Hz (-64.5dB) Local:18696.20Hz (-64.5dB)

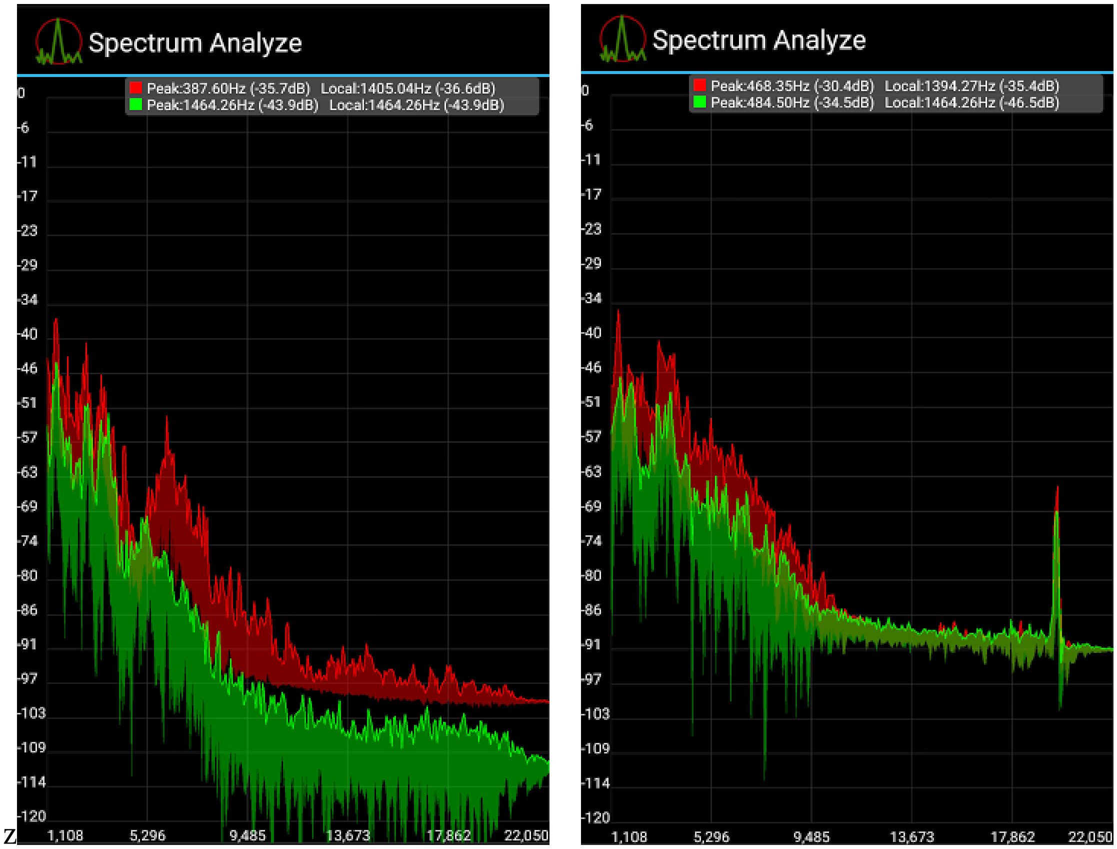
Server Room + Ultrasonic Signal + Music



Spectrum Analyze

🟥 Peak:1469.64Hz (-52.2dB) Local:1469.64Hz (-52.2dB)
🟩 Peak:18604.69Hz (-60.8dB) Local:18604.69Hz (-60.8dB)

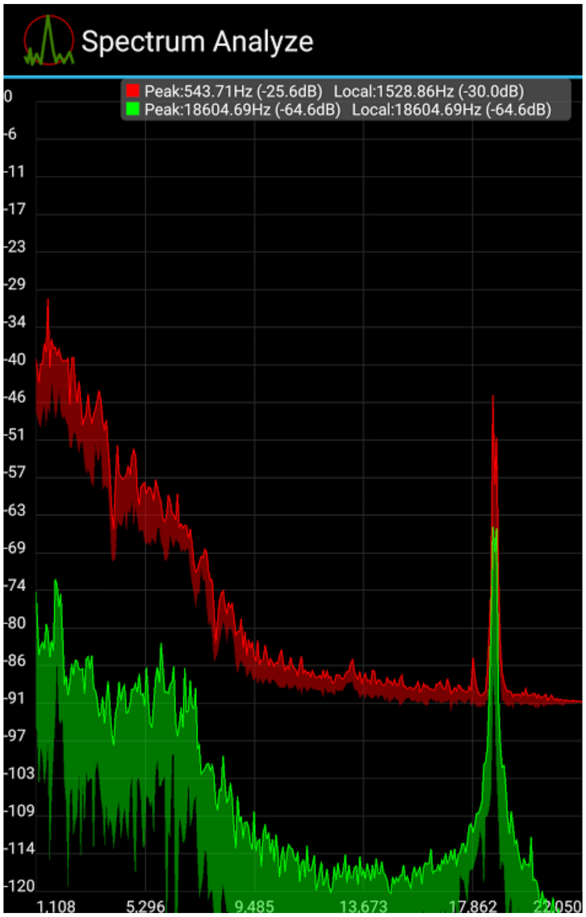
Commons Noise Floor (LEFT) and Commons + Ultrasonic Signal (RIGHT)



🟥 Peak:387.60Hz (-35.7dB) Local:1405.04Hz (-36.6dB)
🟩 Peak:1464.26Hz (-43.9dB) Local:1464.26Hz (-43.9dB)

🟥 Peak:468.35Hz (-30.4dB) Local:1394.27Hz (-35.4dB)
🟩 Peak:484.50Hz (-34.5dB) Local:1464.26Hz (-46.5dB)

Commons + Ultrasonic Signal + Music



Interpretations

The frequencies we chose within 18kHz can be considered arbitrary due to a multitude of environmental factors effecting out tests, but we did have important practical conclusions. Lower frequencies, like those in the 17kHz range may be easier to produce by stock device hardware, but they are slightly within audible range and also closer in frequency to interference produced by humans. Higher frequencies, like those above 19kHz are not handled well by device hardware and often leads to distortion, chirping, and buzzing in speakers resulting in severe loss of fidelity. Most hardware can handle up to 20kHz transmission before the signal is unusable; however, we do not know how drivers and other audio software effects this. Ultrasonic frequencies sometimes produce a loud pop when they first are transmitted on certain hardware, most likely due to an electrical surge in the speaker. It may be necessary to place buffer characters that can accept interference for the pop before the payload of a transmission. Placing spaces as a buffer before the *cat etc/passwd* command remedied this problem as spaces do not affect the parsing of the command by the command shell. While we could have experimented with baud rate further, the usable baud rate was roughly a function of distance + environmental factors + character set. There may be some benefit from choosing a baud rate divisible bits per character (which is 8 for ASCII), but this wasn't tested.

As stated, data was receivable up to 8 feet at maximum hardware volume in the dorm and Commons with the observable difference being that distance shrank to 6 feet outside and in the server room. My project partner, Hunter Young, might differ on these measurements as "usable distance" is subjective. The range can be extended with random losses to fidelity. We believe this is due to mechanical noise from cars and server fans, but also air temperature and movement from these factors might also have an effect. From our earlier tests we determined that while obstacles in the way of a transmission, like people and servers, may not affect the ability to receive a signal, the geometry of a room can. Reception of signals, at least on a spectrograph, in their entirety is virtually impossible outside of a room unless directly in a doorway. Receiving transmissions were extremely difficult when the speakers and microphones were not facing. This may also be affected by the position of the hardware in the device. Therefore, the ultrasonic signals are negligibly affected by obstacles, but are unable to reflect and diffract well. Meshnetting as described in earlier sections might overcome this limit.

Practical Conclusions

From these tests and with reinforcement by a few other researchers, it can be concluded that, while the concept and technology are in their infancy, the ability to transmit data ultrasonically between common consumer computers with their stock hardware is not only feasible but constitutes a form of steganography relevant to the study of information security. However, due to the fragility and low speed of the transmission, the amount of data practically transferable is strictly limited reducing the "data" transferable to simple strings of characters rather than entire information assets. Also, multiple sources along in our research have shown distance to be a major limiting factor. This means that it may not be practical for infiltration other than simple commands for mobile device management and targeting for malware or exfiltration of confidential material beyond keylogging or passwords. This does not mean corporations and governments capable of devoting massive resources cannot improve on this concept technologically.

Practical Applications

Suggestions

When utilizing this concept and developing software for it, during selection of transmission parameters and use case of the software, it is imperative to consider the environment where the software is intended to be used. This may not always be possible, so reproduction and expansion of our tests may be prudent for long term development. The tests performed for this project may be some use; the need for buffer characters to mitigate speaker pop is a good example. In fact, this may mean that any applications of it must be very specifically targeted. This may limit the malware feasibility of ultrasonic data transmission to specific, contained attacks mostly likely as a cyber warfare weapon between nation-states against particular facilities.

As observed, while it can provide data steganography, the concept of ultrasonic data transmission is extremely fragile. However, while it may greatly slow down the transmission time, it may be possible to ensure fidelity without longer exposure to interference through the use of repetition and checking. The same transmission can be repeated several times and software could be written to compare the transmissions, and select the characters that were interpreted most often at each matching point in time across the matching signals to derive a “correct” string. An XOR checksum or a word or character count may also be transmitted at the end of each message for error correction. Longer checksums may be susceptible to inference themselves. If two way transmission is intended, error correction can be further aided by asking the recipient device for an “ok,”, “repeat,” or “verify” reply.

Substitution commands and simpler character sets, like baudot, may be used to reduce signal complexity and transmission time. For example, to instruct software to complete a task, a two character symbol may be transmitted, in a shorter amount of time than an actual full command recognized by a host system, to software that already has the command stored and is listening for the execution prompt. There are caveats to this, though. Baudot, for example, is case insensitive and may have issues with interpretation by operating systems with case sensitive file systems. Using symbols requires the functional payload to already be stored on a on the receiving system in the listening software. This makes the listener less discrete and susceptible to heuristic detection if it is malware.

If exploration into this concept advances to the point where robust protocols can be used, similar or identical to traditional computer networking protocols, the ability to send robust data packets may be possible with enough error checking. Two of the earlier sources were able to develop crude means of transmitting datagrams rather than the raw ASCII text that we were testing with. While also relevant to information security and computer networking, we did not test encryption due to the observed fragility of the data transmission. It is concluded that if encryption is used, it should be done at the character level, not the binary level to preserve data fidelity. Errors at the bit level errors could render entire messages unreadable.

Possible Theoretical Scenarios

The Fraunhofer FKIE study, while using a proprietary protocol stack, demonstrated the concept of ultrasonic data transmission utilizing a meshnet that enhanced its usefulness (Hanspach & Goetz, 2014). The BadBIOS scenario, whether a hoax or not, presented the idea of discrete malware collaboration outside of the conventional network vectors thus potentially allowing the formation of local botnets of airgapped systems (Goodin, 2013). If malware can be propagated to multiple systems in a close proximity, such as with the infected USB drive suggested in BadBIOS, their effect could be amplified. As discussed earlier, the ability to have malware on hosts avoid detection by being only a listener could act an information security time bomb. If the listening malware is distributed densely enough, command payloads, in the form of ultrasonic digital signals could “arm” the malware by many means including, but not limited to shared music, videos, a passerby’s phone, or playing over an intercom. Also the attack could be designed where only one host had to receive an audio payload, and, using stock microphones, and speakers could transmit commands to all other listening hosts.

Also building on an idea from the Fraunhofer FKIE study, very small scale data exfiltration can be an achieved, such as with the keylogger example. While transmitting keystrokes discretely and acoustically may not provide much benefit over traditional keyloggers, it could be used as a means of exfiltration when all traditional data connections are severed (Hanspach & Goetz, 2014). There is also a well-known surveillance tactic using lasers to eavesdrop on distant conversation. Laser light is pointed at a surface that will vibrate as it absorbs local sound waves and the changes in the reflected beam are processed into sound from far way. Perhaps this technology could be adapted to function with digital ultrasound. If a target organization was to restrict network access by policy or by advanced security controls such as metal shielding to contain radio waves from WiFi. An infected system or systems could transmit data ultrasonically and vibrate a window, for example, and keystrokes can be received from a laser microphone far outside the security perimeter.

Powerline Ethernet, a means of modulating the electrical current in a building with special wall warts to send network traffic, is a common consumer solution. There are also powerline audio adapters to eliminate the need to run new cabling for sound as well. While the use of powerline network adapters is common, powerline audio is less so and therefore might appear to be ordinary electrical noise if it were used discretely in a building. If the technology can carry ultrasound, it might be a means of overcoming the physical barriers that prevent the propagation of ultrasound and even the physical barriers of a security perimeter given that the carrying electrical lines cross that barrier.

There are also less malicious and also less security relevant usage scenarios for discrete ultrasonic data transmission. Mobile Device Management could utilize the technology for offline communication between peer devices or for the detection of nearby devices. The natural physical containment of ultrasound could allow better control of local peer to peer networks. Also, as demonstrated by SilverPush, it may be used to support and analyze marketing among device users.

Security Controls

There are obvious security controls, such is including all known ultrasonic communication software (like the software referenced in this project) in anti-malware definitions and having heurist analysis detect any software that functions similarly. This is impractical as it may require repetitive whitelisting of drivers and other audio software. The Fraunhofer FKIE study proposes and idea of an intrusion detection system (IDS) sensitive to ultrasonic attacks. They suggest analysis of audio input and output and any modulations present in the audio to detect signals that might carry data (Hanspach & Goetz, 2014). My project partner and I suggest another, cruder countermeasure: jamming. While it is a federal crime in the US to jam WiFi, Bluetooth, and other radio bands, sound, especially inaudible sound, is virtually unregulated. A quick search on Amazon.com reveals that tweeters, speakers designed for high pitched sounds, in the many hundreds of watts are inexpensive (Pyramid TW36 7-Inch x 3-Inch 400 Watts Wide

Dispersion Horn Tweeter). This would allow the cheap creation of large ultrasonic deadzones, should attacks via ultrasonic data steganography become a significant threat. The only caveat with jamming in this range is potential irritation to animals and people with acute hearing.

References

Anfractuosity. (n.d.). *Ultrasound data transmission via a laptop*. Retrieved from anfractuosity.com: https://www.anfractuosity.com/projects/ultrasound-via-a-laptop/

Bansal, S. (2015, April 16). *New ways to count viewers*. Retrieved from Livemint: http://www.livemint.com/Opinion/3QXskshem9l6fcbfAkqmUO/New-ways-to-count-viewers.html

Center for Democracy & Technology. (2015, October 2016). *Re: Comments for November 2015 Workshop on Cross-Device Tracking*. Retrieved from cdt.org: https://cdt.org/files/2015/11/10.16.15-CDT-Cross-Device-Comments.pdf

Goodin, D. (2013, October 2013). *Meet "badBIOS," the mysterious Mac and PC malware that jumps airgaps*. Retrieved from arstechnica: http://arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/

Grimes, R. (2013, November 12). *4 reasons BadBIOS isn't real*. Retrieved from InfoWorld: http://www.infoworld.com/article/2609622/security/4-reasons-badbios-isn-t-real.html?page=1

Hanspach, M., & Goetz, M. (2014, June 4). *On Covert Acoustical Mesh Networks in Air*. Retrieved from http://arxiv.org: http://arxiv.org/pdf/1406.1213v1.pdf

Jiang, W. (2014). *"Sound of silence": a secure indoor wireless ultrasonic communication system*. Retrieved from The Boolean: Snapshots of Doctoral Research at University College Cork : http://publish.ucc.ie/boolean/2014/00/jiang/09/en

Katee. (2014, July 10). *quietnet*. Retrieved from GitHub: https://github.com/Katee/quietnet

Mostafa, K. (2016). *Minimodem*. Retrieved from whence.com: http://www.whence.com/minimodem/

MP3. (2016, February 24). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/MP3

Multi-Tone FSK for Ultrasonic Communication. (2015, March 25). Retrieved from cs.ou.edu: http://www.cs.ou.edu/~antonio/pubs/conf059.pdf

Production Bytes. (2012, June 8). *Digital Audio 101 - Bit Depth, Sampling Rate, Interpolation*. Retrieved from Youtube: https://www.youtube.com/watch?v=W2-FP7twy8s

Pyramid TW36 7-Inch x 3-Inch 400 Watts Wide Dispersion Horn Tweeter. (n.d.). Retrieved from Amazon: http://www.amazon.com/Pyramid-TW36-7-Inch-Dispersion-Tweeter/dp/B000XDTNL6

Radioteletype. (2016, January 21). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Radioteletype

Smith, S. (n.d.). *Chapter 22 - Audio Processing / Human Hearing*. Retrieved from dspguide.com: http://www.dspguide.com/ch22/1.htm