Spring 3-14-2016

Ultrasonic Data Transmission and Steganography

Hunter Young
Kennesaw State University

KENNESAW STATE UNIVERSITY

Ultrasonic Data Transmission and Steganography

Honor's Capstone Project

Hunter Young

3/14/2016

Table of Contents

Abstract

This project discusses the feasibility of using ultrasound to transmit data between computer systems, particularly computer systems that have been intentionally cut off from traditional networks for increased security. The goal of this project is to provide a synthesis of the current research that has been done into the use of ultrasonic data transmission, and to conduct a series of tests determining the validity of certain claims made in regards to ultrasonic data transmission within the information security community. All research, experiments, results, and inferences have been discussed in the context of how they relate to the realm of information security. All security concerns discovered during the course of this project have been outlined at the end of this paper, and potential remediation strategies have been suggested.

Collaboration Statement

The experiments and research outlined and discussed within this paper are the product of a multi-semester long collaboration between Alexander Edwards and myself. This collaboration began in the spring semester of 2015, and was explicitly approved by the University Honors Program as well as our supervising professor within the Information Security and Assurance program, Dr. Herb Mattord.

Although the research and experimentation was a cooperative effort, each of our papers will be unique in composition, though similar in content due to a shared pool of results, research, and resources. Any similarities noted between our papers should be attributed to and explained by this collaboration. It is important to note, however, that any and all unquantifiable conclusions drawn from the data obtained and the

phenomena observed may differ greatly between the two of us due to our varying opinions and perspectives. The differences between our interpretations should not be viewed as a conflict or as a lack of adherence to the Scientific Method, but rather as a byproduct of subjunctive variances in our personal experiences, opinions, and viewpoints.

Introduction

Ultrasound is all around us. It surrounds us no matter where we are, or what we are doing. Yet, we as a species are for the most part ignorant of its presence in our daily lives. Much like radio waves, we are unable to sense or perceive ultrasound without the aid of technology. However, unlike radio waves, ultrasound is very rarely used for practical applications, and it is most certainly discussed far less frequently.

Most people have heard of ultrasound at some point in their lives, no pun intended, yet few are conscious of its presence and effects. Ultrasound, for the most part, remains an untapped and unused means of communication. This makes ultrasound the ideal medium for a clandestine or non-traditional data transmission method.

Ultrasonic data transmission uses various techniques and technologies to establish a means of communication through sound waves outside the range of human hearing. Information can then be passed through the air between devices completely undetected by any human beings present in the area.

This capstone project will focus on the applications of ultrasound in regards to data transmission, data exfiltration, and steganography. Over the course of the past year, Alex and I have conducted an enormous amount of research in addition to performing numerous tests, experiments, and proof-of-concept activities. Through our research and our testing, we have learned a tremendous amount about the capabilities and potential applications of ultrasonic data transmission within the realm of Information Security. This paper will serve as a detailed explanation of our findings, as well as a collection of my personal interpretations and opinions.

Initial Theory Summary and Pre-testing

Our initial theory when beginning this project was that the modulation of ultrasonic sound waves provides both an effective and underused means of transmitting data while remaining undetectable by human hearing. This idea was born out of little more than a side comment made during lunch one day during a discussion of radio wave modulation. After the seed of the idea was planted in our minds, we decided to conduct a quick “back-of-napkin” style assessment of the feasibility of transmitting data through the air using ultrasonic sound waves. We setup a tone generator and sound spectrum analyzer on our respective phones and began testing various frequencies from various distances. Once we realized that ultrasound could be generated with the average smartphone, and subsequently discovered that an average smartphone was also capable of receiving ultrasound using the built-in microphone, we knew we had an idea that just might go somewhere.

How this paper is organized

This paper is organized into two primary sections: the Overview, Research, and Discussion section and the Experimentation, Results, and Inferences section. The former section presents the reader with the preliminary research done before conducting any sort of experimentation, while the latter section explains the methodology and results of the experiments performed during the course of the capstone project. The Overview, Research, and Discussion section also includes brief explanations and summarizations of the technical concepts necessary to understand the underlying conclusions of the project for those who do not possess an extensive technical background.

Overview, Research, and Discussion

Overview of Ultrasound and Potential Applications

Advertising

Up until recently, ultrasound has seen very little practical use in the realm of networking and communication. However, a firm known as SilverPush is trying to change that. (Waddell, 2015) SilverPush is beginning to use ultrasonic signals embedded in television advertisements to track what sort of ad content the user has been viewing, and then display targeted ads on other devices owned by the user. This sort of persistence has been used in website cookies to display targeted advertisements across various domains for years, but the use of ultrasound in this way comes as both a surprise, and a rather large privacy concern.

Ultrasonic data transmission allows worlds that would have otherwise remained separate, such as television and web-browsing, to become heavily integrated with one another. By adding persistent cross-device ad tracking to consumer devices, the sheer enormity of metadata that can be collected from an individual has skyrocketed. The implications of this new application of ultrasound has caused enough concern that the FTC held a workshop to discuss the privacy concerns associated with this technology. (Center for Democracy & Technology, 2015) If the use of ultrasound continues to progress in this direction, the obscurity of ultrasonic data transmission will be shattered. Much like the paranoia associated with RFID credit cards, people will begin to purchase the “anti-ultrasonic data transmission” devices which will inevitably spring up on the market in response to privacy concerns.

Meshnets

One of the more inspiring applications of ultrasonic data transmission is the creation of ultrasonic mesh networks. The concept of a mesh network is a simple one; although one device may only be able to transmit and receive from a short distance, if there are a number of devices present, they can relay messages through one another. In this way, each device functions like an individual chain in a link of communication. Since most all communication devices have some sort of microphone and speaker built-in, ultrasonic mesh networks are quite feasible. (Hanspach & Goetz, 2014)

Although mesh nets are not very useful when point-to-point broadband solutions are so readily available, they provide an excellent tool for scenarios when normal networks are either non-existent or unavailable. For instance, there have been several cases in various countries where cell service was shutdown in areas that active protests were occurring. Protesters then created Bluetooth mesh networks in order to reestablish communication between one another. Ultrasound could also be used as a substitute for, or as an addition to existing Bluetooth mesh networks.

Discrete Paging

Another interesting potential application of ultrasonic data transmission is the possibility of using existing intercom or other PA-like audio broadcasts to discretely page individuals when other conventional networks are unavailable. For instance, imagine a concert where thousands of people have been gathered in one small area, and cell service is sketchy at best. Ultrasonic signals could be mixed into the concert audio as needed to distribute messages to security guards or other stage staff.

Behind the Scenes: the Science of Ultrasonic Audio

Sound Waves

Ultrasound is merely a term used to describe high frequency sound waves. Essentially, ultrasound is the inaudible portion of the sound spectrum. Much like ultraviolet light cannot be seen, ultrasound cannot be experienced directly by humans, yet as with UV light, the effects of ultrasound can often times be felt rather than perceived. However, before ultrasound can be discussed in more depth, it is important to understand how sound works in general.

Sound waves are created by the vibrations of an object. As an object vibrates, it creates slight pressure differences in the medium surrounding the object. These pressure changes create waves that travel through the surrounding medium. In the case of humans, the changes in pressure are then picked up by the eardrum, which are then interpreted by the brain as “sound.” The process by which sound is detected by non-humans is relatively similar.

Microphones rely on small, thin diaphragms that vibrate at the same frequency as the surrounding medium. The diaphragm is surrounded by a coil of wire, which vibrates along with the diaphragm as the pressure differences in the air excite the device. The movement of the coil within a magnetic field created by a permanent magnet generates an electric current that becomes the analog signal suitable for interpretation by electronic devices.

One of the limitations that should become readily apparent is the propagation of sound through various mediums. Although air and water provide a decent medium for

sound waves to travel through, solid objects do not - this is especially true for ultrasound. Take for instance the noise coming from an individual's next door neighbor in an apartment complex. When noise complaints are issued, they are most always caused by the presence of loud, thumping bass notes. The reason for this lies in that fact that sound waves of lower frequencies propagate better due to the relative ease with which they are able to incite vibrations in the objects adjacent to the transmitting medium. Conversely, higher frequencies experience far greater difficulty in inciting vibrations in other objects. This means that ultrasound is easily stopped by the presence of walls or other large objects or obstacles in the surrounding area.

Modulation

Modulation is the process of adding data to a given carrier wave. This process can be applied to radio waves, sound, and even light. The different types of modulation will be discussed in the following Behind the Scenes section, though the basic premise will be explained here. Data can be added to a given carrier wave by varying frequency, amplitude, phase, pulse, and polarization. These variables can be used individually or in combination to add data to a carrier signal. For instance, one could vary the amplitude of a wave at a given frequency to signify 1s and 0s in a digital transmission. Conversely, one could keep amplitude constant and vary frequency to symbolize 1s and 0s.

Human Hearing

The range of human hearing is roughly between 20 and 20,000 hertz. Ultrasound is often said to begin above 20,000 Hz, though technically it is defined as inaudible sound outside the range of human hearing, which can vary greatly depending on age and health. As people get older, they tend to lose their ability to hear higher frequencies.

(Smith) This means that ultrasound is less detectable by individuals who might recognize its presence. Although an individual might not be able to hear high frequencies, they can often discern a certain “feeling” or pressure in their ears. This sort of sensation is felt right at the edge of their own range of hearing.

Background Noise (Environments)

Ultrasound is incredibly susceptible to background noise and interference from many different sources. Fans, wind, and electronics are but a few of the common, but frequent sources of spurious ultrasonic emissions. This poses a particular problem when trying to use ultrasound around computers since computers themselves generate so much ultrasound due to the number of small fans present in their construction. (Jiang, 2014) Furthermore, HVAC systems generate large ultrasonic emissions from the movement of air through a building. All of these factors degrade the fidelity of ultrasonic transmission signals.

Behind the Scenes: Computers and Communication

Equipment

Most all electronic devices that are capable of playing or recording sound are capable of transmitting and receiving ultrasound – even small devices such as cellphones can excel at this. Although one might think special equipment is necessary to receive or transmit ultrasound reliability, this could not be farther from the truth. The small diaphragms present within the speakers and microphones of devices such as cellphones, laptops, and tablets are perfectly suited for transmitting and receiving data over ultrasound since the minimum size of the vibrating diaphragm is inversely related to the frequency used.

Modulation Types

As mentioned in the previous section, modulation is the process of adding data to a given carrier wave. Some of the most common forms of modulation used within the realm of radio communication are Frequency Shift Keying (FSK), Phase Shift Keying (PSK), Quadrature Amplitude Modulation (QAM), and Binary Phase Shift Keying (BPSK). There are several other forms of modulation, such as Amplitude Shift Keying (ASK) that are much less frequently used and are not within the scope of this project, but it is important to be aware of their existence.

One of the recurring themes within each of these forms of modulation is the concept of “shift keying.” The process of shift keying is essentially the process of mapping a given variable change to a change in symbol. In FSK transmissions, at least two frequencies are used to represent the binary values of 0 and 1. For instance, a

transmission at 135 hz might represent a value of 0, and a transmission of 136 hz might represent a value of 1. (Multi-Tone FSK for Ultrasonic Communication, 2015) The speed at which these frequencies are changed, or modulated, is referred to as baud rate. The baud rate of a signal represents the amount of symbol changes per second the signal is carrying.

It is important to note that baud rate is not always equal to data rate, or bit rate. The two concepts are often confused, and it is certainly understandable as to why they are. In the scenario outlined above, there are two frequencies representing 0s and 1s, respectively. Every time the frequency changes, the symbol changes, and therefore the bit value changes. Consequently, the bit rate is the same as baud rate. However, if multiple symbols are made available, then the amount of bits per symbol change may be increased. Consider the table below.

Frequency	Symbol (bit value)
x + 0 hz	00
x + 1 hz	01
x + 2 hz	10
x + 3 hz	11

In the example above, there are four distinct frequencies mapped to four distinct binary values (symbols). This specific combination represents a variant of FSK known

as 4FSK. For every change in symbol, two bits of data are transmitted. By adding additional signal mappings, the baud rate has been reduced by a factor of two for the same bit rate. This concept of increasing the number of bits per symbol is embodied in more advanced forms of modulation, such as QAM and BPSK/QPSK. In these forms of modulation, the amount of bandwidth is reduced for a given bitrate due to the ability to transmit a greater number of bits per symbol. This results in an increased spectral efficiency, though not without a price. (Frenzel, 2012)

The more complex and efficient a mode of modulation is, the greater the impact of noise and interference on the signal. As noise increases, the fidelity and reliability of the received signal declines. Less efficient forms of modulation, such as FSK, are less susceptible to interference and noise. Although the forms of modulation discussed above primarily relate to radio waves and transmissions, these forms of modulation are also applicable to sound and light.

Networking (Communication)

Networking is a broad concept that reaches far beyond the scope of this project, but it is integrally important to ultrasonic data transmission. Networking is generally broken down into several layers. The OSI model, being one of the most well recognized models, provides a standard framework for discussing the various components that make the networking of connected devices possible. Ultrasonic data transmission is part of the first layer of the OSI model, the physical link layer. Much like other methods of physically linking networks, such as wire, radio, and fiber-optics, ultrasonic transmissions provide the backbone that supports all of the higher layers necessary to facilitate addressable communication between devices.

Since ultrasound provides a low-bandwidth transfer medium subject to noise and interference, the networking layers built on top of ultrasound must be lean, minimalistic, and ideally self-correcting - current technology does not allow for ultrasound to be used in any other manner. Although full TCP/IP-based connections are possible over ultrasound, these are rarely a good idea. In fact, light-weight transport protocols such as MQTT would prove to be much better suited to ultrasound than the robust protocols commonly seen in 802.11 and 802.3-based networks. At the very minimum, stateless and connectionless protocols such as UDP should be used when interfacing directly with existing computer networks.

File Embedding, audio compression, and sampling

In the previous sections, ultrasound has been discussed more like a subset of the radio spectrum rather than part of the sound spectrum. One of the beauties of ultrasound is that it can be treated as both a radio wave and a sound wave at the same time, and have the techniques of each applied to it. For instance, ultrasound can be embedded in audio files simply by combining the raw WAV files of the normal audio and the ultrasonic audio together. Data can be modulated into a given ultrasonic signal before it is combined with another audio file, essentially hiding data in an inaudible portion of the resulting audio file.

Although ultrasound can be embedded in raw wav files, modulated ultrasound cannot be reliably embedded in compressed audio such as MP3 audio. This is because compression technologies like MP3, Ogg Vorbis, and AAC remove frequencies that humans are unable to hear, ultrasound being first among them. Therefore, embedding ultrasound is only possible in analog and PCM-sampled digital formats such as WAV

files. By using PCM, or Pulse Code Modulation, analog waveforms can be transformed into digital formats in a way that the digital representation of the analog waveform is essentially identical. This process is known as sampling, and is similar to how curved lines are represented on screens that only possess square pixels. By increasing the density of square pixels on a screen, curved lines begin to smooth out once the pixel density reaches a certain threshold. Sample rate is the counterpart of pixel density in regards to audio. As sample rate increases, the curves of the waveform begin to smooth out and become more liken to a true analog waveform.

Security Concepts

Security in General

As society becomes increasingly dependent on various information systems, the ability to secure these systems and the data present within them becomes increasingly important. Security revolves around the ability to maintain the confidentiality, integrity, and availability of data and information. In order to effectively achieve these goals, security professionals must focus on blocking potential threats from exploiting vulnerabilities at as many levels as possible. Consequently, security professionals are beginning to adopt the principle of Defense in Depth, where each portion of an information system is hardened to reduce the likelihood of an attack succeeding if one or more safeguards fail.

“Air gaps”

One of the most prevalent ideas in information security is that isolating a system increases the security of that system, which for the most part is essentially true. If a computer or network of computers are placed in a secure area where physical access is tightly control, and there is no link to the outside world or the Internet, those computers or networks are considered to be highly secured. Areas that demand exceptional security measures such as critical infrastructure systems frequently employ these types of setups. The industry has coined the term “air gapped” to describe high security environments such as these. The term comes from the fact that these high security systems are physically separated from the open Internet and consequently the outside world - a literal gap of air. Organizations that employ these environments place enormous value on the security of their systems, and go to great lengths to ensure that these systems remain air gapped.

During my time spent at the Pentagon, I was able to see a number of the safeguards used in air gapped environments first hand. One of the most interesting safeguards in place at the Pentagon is the existence of a Faraday cage built into the building itself. Faraday cages are essentially containers that prevent radio waves from passing through. These containers are created by embedding mesh netting of various gauges within the walls of the building itself. These Faraday cages prevent wireless signals from escaping the building, and thus ensure that the only communications to and from the building go through authorized channels. Additionally, the Pentagon also utilizes special glass in all of the windows in the outside ring, or E-ring. The glass is designed to prevent light from escaping outside of the building as well as eliminate

surface vibrations in order to prevent laser listening devices. In addition, the exterior glass is almost a foot thick to withstand extreme forces such as gunfire and explosions.

Safeguards like those present in the Pentagon help ensure that systems can remain truly air gapped, however ultrasound is most likely rarely considered when designing high security systems in organizations outside of the Department of Defense. Often times simply “cutting the cord” to a system is considered to be sufficient to create an effective air gap; soon this sort of mentality will no longer be a viable defense strategy. As attackers become increasingly clever in the ways they are able to pivot between systems, security professionals must be increasingly mindful of the unconventional methods an attacker may choose to use.

Encryption & Steganography

Within the realm of information security, confidentiality is a vital concept to the protection of data. Encryption hides data from entities that are unauthorized to view it by making it mathematically impossible, or at least incredibly difficult, for an unauthorized entity to decrypt the encrypted data. Steganography on the other hand aims to maintain the confidentiality of data by hiding it rather than securing it. Perhaps the best analogy between the two concepts would be locking valuables in an uncrackable safe versus hiding them in plain sight.

Steganography has been used for thousands of years to disguise messages within other objects and messages to hide information from prying eyes and mindful ears. Since the concept of ultrasonic data transmission is, at its core, an endeavor in clandestine communication, steganography is a much more appropriate tool than

encryption when using ultrasound to transmit data and establish covert communications. By embedding ultrasound in audio recordings, or mixing ultrasonic signals in real-time with live audio such as intercom, PA, or other broadcast sources, a subtle and relatively unnoticeable means of communication can be established so long as no one is specifically looking for it.

Malware

Malware is software specifically created to perform a harmful or undesired action, and it is extremely prevalent in information systems all over the world - both personal and corporate in nature. Malware is a broad category that includes viruses, worms, trojans, spyware, adware, and ransomware. Each of these types of malware are dangerous in their own right. Some types, such as spyware and adware merely cause a nuisance to the end-user and can potentially result in a loss of privacy. However, targeted malware such as the Stuxnet worm can be incredibly dangerous, and can cause hundreds of millions of dollars' worth of damage.

Ultrasound provides little benefit to innocuous types of malware that are purely interested in information gathering. However for targeted malware, ultrasound provides an avenue of communication that is unmonitored and unaffected by any sort of firewall, network intrusion detection device, or intrusion prevention devices. This makes ultrasound a valuable tool for highly-advanced and highly-specific malware designed for a single purpose in mind.

Data Exfiltration

Data exfiltration is a huge concern in the realm of information security. Corporations stand to lose an enormous amount of money if their intellectual property is stolen. Therefore, governments and corporations go to great measures to ensure that the possibility of data escaping their networks is as low as possible. Modern security appliances such as network intrusion detection and prevent systems have helped reduce the probability of an attack succeeding; however these technologies are not setup to monitor ultrasonic frequencies.

One of ultrasound's greatest strengths is its ability to go where other types of signals cannot go using pre-existing hardware. This makes ultrasound the perfect candidate for undetected data exfiltration. The major problem with ultrasound is that due to the lossy nature of the medium and the exacerbated effects of noise and interference on ultrasound itself, the amount of data that can be transferred using ultrasonic data transmission is relatively low. As it currently stands, ultrasound is incapable of facilitating the transfer of massive quantities of data that are so frequently seen in the world of corporate espionage. Ultrasound remains suitable only for limited data exfiltration and command and control activities.

Reported/Suspected Instances of Use

One of the most interesting and certainly the most sinister reported instances of malware using ultrasonic signals is the case of "badBIOS." Back in 2010, a security researcher named Dragos Ruiu began experiencing strange phenomena in his laboratory. (Goodin, 2013) He began to notice that machines that were infected with malware retained the infection even after installing fresh copies of their operating

systems. After isolating the systems from all possible communication sources, including the power grid, he was forced to conclude that the devices must be communicating using ultrasound. He removed the microphones and speakers from the devices, and suddenly the communication between the devices ceased. Originally, many individuals within the security community believed this to be a clever Halloween hoax - some members of the security community still believe it is a hoax till this day. However, Ruiu has staked his reputation on his claims of the existence of malware capable of propagating ultrasonically from the BIOS. The code responsible for this alleged occurrence has never been observed by anyone else in the wild, and so one is left to wonder what the truth really is. (Grimes, 2013)

Roughly three years after the initial reported discovery of “badBIOS,” a group of security researchers were able to successfully establish ultrasonic communications between air gapped systems. Their findings were published in the Journal of Communication, and lent some credence to the existence of badBIOS, or a rootkit exemplifying similar characteristics as badBIOS. (Hanspach & Goetz, 2014) The researchers were able to borrow technologies used for enabling underwater communication through sound waves. They also went on to emphasize that sophisticated instances of malware could utilize ultrasound to create acoustical mesh networks where each infected device functioned as both a transmitter and receiver, thereby expanding the overall range of the mesh network.

During my time at the GhostRedCTF event at Clemson University in South Carolina, I had the privilege of attending a closed-door presentation discussing how one of the inter-departmental penetration testing teams at General Electric was able to

successfully breach the air gap used to protect the control systems of an undisclosed power plant. Through social engineering, the team was able to successfully upload malicious code containing an ultrasonic listener to an air gapped system. The team was then able to initiate command and control functions by utilizing ultrasonic signals over the intercom system at the power plant. Of course, there were several other flaws in the defense mechanisms in place at the power plant, such as the team being able to gain access to non-air gapped internal systems, but the coup de grace was the ability to maintain control over “isolated” systems through the use of ultrasound.

Experimentation, Results, and Inferences

Hypothesis

The hypothesis below was taken directly from the original capstone proposal.

The modulation of ultrasonic sound waves provides both an effective and underused means of covert data transmission capable of maintaining data confidentiality and integrity. In addition to the innate qualities of inconspicuous propagation possessed by ultrasound, the confidentiality of ultrasonic data transmission can further be increased through use of encryption and/or steganography.

Constraints

Original expectations

When the project was first conceived and presented, Alex and I presented a flow chart with an enormous amount of tests to be formed on an even larger amount of protocols, hardware configurations, and concept variations. After we conducted more research, and began to drill down into the heart of our project, we were forced to ask ourselves what we really wanted to accomplish.

It became readily apparent to us that the scope of our project was still far too broad, and we needed to focus on the core concept behind all of the planned tests and concept variations. Many of the concepts we originally planned to test, such as the interactions between laser microphones and ultrasound, were completely meaningless if we could not firmly establish whether or not ultrasound provided both a suitable and feasible means of communication in addition to having a profound impact within the

realm of information security. Consequently, we decided to focus on determining whether or not ultrasound could bridge divide between air gapped systems effectively and reliably.

Additionally, we decided against writing large quantities of custom code to test very niche scenarios. Instead, we elected to synthesize freely available and existing sources of code, softwares, and commonly available hardware components. The reason for this is because we decided that writing custom code for specific scenarios was a deviation from the core of the project, and quite frankly our time constraints did not allow for it.

Methods and Materials

Hardware

Alex and I used several different devices during our tests: three laptops, and two cell phones. Specifically, we used a Dell Latitude 2100 primarily for transmitting purposes, a Dell XPS 13 9340 for receiving purposes, and an Early 2011 MacBook Pro 13 for both transmitting and receiving transmissions. Both of the Dell systems were running variants of Ubuntu, while the MacBook was dual-booted between OSX 10.9 and Backtrack 5. This provided an incredibly robust environment that was able to leverage the open source libraries available on *NIX platforms.

In regards to cell phones, we used our respective daily-use phones: a OnePlus One and a Motorola RAZR HD XT926M.The cell phones were primarily used as spectrum analyzers and tone generators. All preliminary testing was done using these devices, and provided a suitable baseline for beginning data transmission tests.

One of the reasons we decided to use stock hardware rather than custom-built transmitting hardware was because we believed this was more within the spirit of the project, and represented the closest thing to a real-world scenario we could create. We could have easily purchased ultrasonic horn speakers off of Amazon for a relatively small sum, and connected them to a suitable amplifier, but this would not have allowed for two-way transmission similar to the real-world since one device would be severely overpowered compared to the other. We could have also introduced microphones with higher sensitivities to ultrasonic frequencies into the mix, but again this would have deviated from the core interest of the project.

Software

In regards to software, Alex and I used two pieces of software extensively during our testing: GNU Radio and minimodem. GNU Radio is an open source project used primarily for rapidly prototyping software defined radio receivers. We used GNU radio for the extensive modulation and demodulation libraries it includes by default. After configuring the ASLA drivers on our devices, we were able to use our microphones and speakers as audio sinks for the raw modulation to be piped directly into. Minimodem is a program created by Kamal Mostafa that allows a user to create custom FSK signals using almost any combination of frequency, baud rate, and framing protocol. (Mostafa, 2016) This program was indispensable in conducting our tests and analysis since it allowed for rapid testing of new theories and ideas.

Testing Narrative

After the initial pretesting for the project, our first real tests began with creating a TCP link over ultrasound between two separate laptops. In order to accomplish this, we

utilized the prototyping functionality in GNU Radio. This portion of the project was heavily inspired by the efforts of Anfractuosity. (Anfractuosity) The GNU Radio flow for transmitting was as follows; for receiving the flow was reversed.

TCP Source -> Packet Encoder -> Modulation -> Carrier wave filter -> Audio output

In the experiments conducted by Anfractuosity, 23kHz was used as a carrier wave frequency. We had very limited success with this carrier frequency using FSK once the laptops were moved more a few inches from one another, and so we decided to lower the frequency in large increments until we began to see a noticeable difference in signal strength and propagation. In this portion of our tests, we found frequencies between 17kHz and 19kHz worked best for our devices, and resulted in a distance of around 6-8 feet reliably inside of a heavily crowded room in the Burruss building on campus.

Due to our success in the first test, we decided to pursue FSK in more depth. We had begun to acquire budding suspicions that neither PSK nor QAM modulation would function better than FSK for several reasons. First, ultrasound is an incredibly lossy and unstable medium. PSK and QAM are much more delicate than FSK, especially QAM. Since FSK had such difficulty even with a high amount of resampling, we decided not to bother testing PSK. In the testing conducted by Anfractuosity, they noted that they experienced very limited success with PSK. Our backgrounds in ham radio supported the theory that PSK and QAM as forms of modulation would be unsuitable for this project based on the performance seen with FSK.

After determining that FSK should be explored in more depth, we discovered the minimodem program created by Kamal Mostafa. (Mostafa, 2016) This program allowed us to begin a more formalized method of testing to determine the best frequency, baud rate, and framing protocol suited to ultrasonic data transmission. We selected four different locations in which to conduct standardized testing: a quiet average room, a crowded public space, outdoors nearby a heavily trafficked road, and an active server room. We felt that each one of these spaces represented an environment that ultrasonic data transmission might take place: an office, a public gathering, an outdoor event, and an air gapped server room.

Once we had selected several locations, we began searching for the optimal general parameters for ultrasonic data transmission in all of these locations. We tested frequencies between 17 kHz and 20 kHz since we noticed a sharp fall-off in signal quality and signal strength when transmitting over 20 kHz. We believe this was due to hardware limitations in the form of integrated low-pass filters that prevent the speaker/microphone from wasting energy to generate tones outside of the range of human hearing. However, this did not impair the ability of our transmissions to go unnoticed by human beings. In fact, no one showed any sign that they were hearing any sort of unnatural sounds in any of the locations we tested at.

In addition to varying frequency, we experimented with different baud rates and framing protocols. We originally began testing with the Baudot character map, which was highly successful. However, the issue with the Baudot character map is that it does not allow for the transmission of lowercase characters because it only has 5 bits available to describe a single character. Since we knew we would eventually pipe the

raw output from minimodem into a system shell, we needed case sensitive transmissions. Consequently, we switched to the ASCII character map, which uses 8 bits per character. However, due to the increased amount of symbols required to transmit a single ASCII character, we began to see errors in our communication. We reduced baud rate in response since reducing baud rate should theoretically increase fidelity at the cost of transmission speed. However, decreasing the baud rate increases the probability of spurious emissions of interference affecting the transmitted signal. We ended up settling on a baud rate of 45, which coincidentally happens to be the exact baud rate used in the Radio TeleType standard (RTTY). Historically, RTTY has been used by ham radio enthusiasts all over the world to transmit text across low-bandwidth connections, so that lent some credence to our choice of baud rate.

After we had determined several semi-optimal variables, we used minimodem to set up a connection at 18.6 kHz with a 100Hz offset between the space frequency and the upper mark frequency using a baud rate of 45 and an ASCII character map. This was relatively successful, but we eventually fine-tuned the results using the confidence variable within minimodem. The following command was used to configure minimodem:

minimodem -S 18600 -M 18700 45 --ascii -c 2.5

The -c flag represents the confidence variable, which is an arbitrary number that essentially functions as a squelch control. We tried several values to ensure that we could truncate most interference without running the risk of ignoring valid signals that were merely weak.

With a successful connection now established, we began piping minimodem directly into the system shell with the *minimodem -S 18600 -M 18700 45 --ascii -c 2.5 -q | sh* command. This allowed us to run commands on the remote system as if we were sitting directly in front of it. We used the *cat /etc/passwd* command to display the list of users on the remote device. We could have used any command, but we chose this command arbitrarily simply to demonstrate that commands could be executed successfully.

Alex and I moved on to working on steganography after establishing a working command and control connection over ultrasound. Alex had already verified through his own experimentation that MP3 compression destroys ultrasonic signals embedded in audio files, so we knew would have to use raw WAV files to have any hope of hiding data within an audio file ultrasonically.

We used minimodem to pipe a clean signal of the *cat /etc/passwd* command to a WAV file, and then subsequently spliced that file into an arbitrary audio file. This initial test failed to embed any sort of ultrasonic data since the arbitrary audio file was not scrubbed of random ultrasonic noise beforehand. After clipping all frequencies over 16 kHz in the arbitrary audio file using Audacity, we were able to experience varying degrees of success in demodulating ultrasonic data out of the resulting audio file.

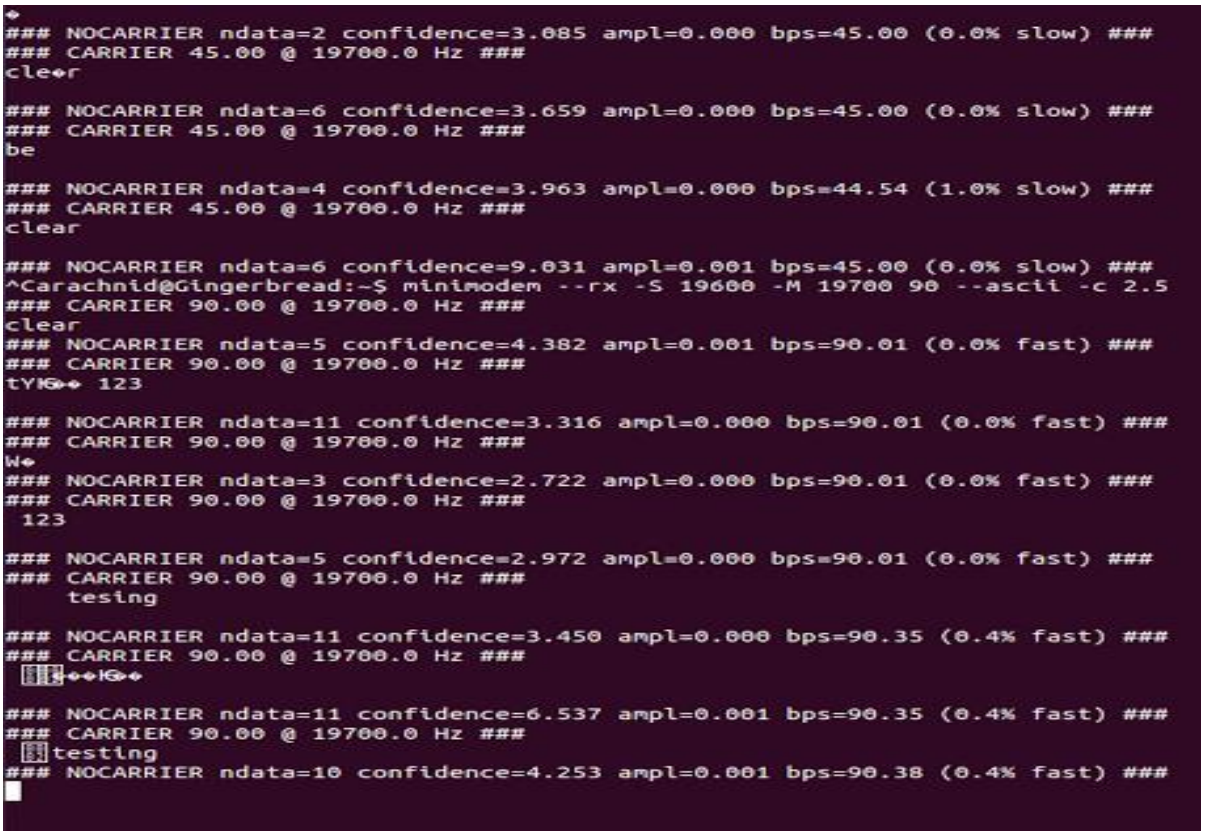
Results

We saw the best results when using FSK modulation, a carrier frequency of 18.6kHz, a mark frequency of 18.7kz, an ASCII character map, and a baud rate of 45. Frequencies below this number can be felt by some human beings, though not

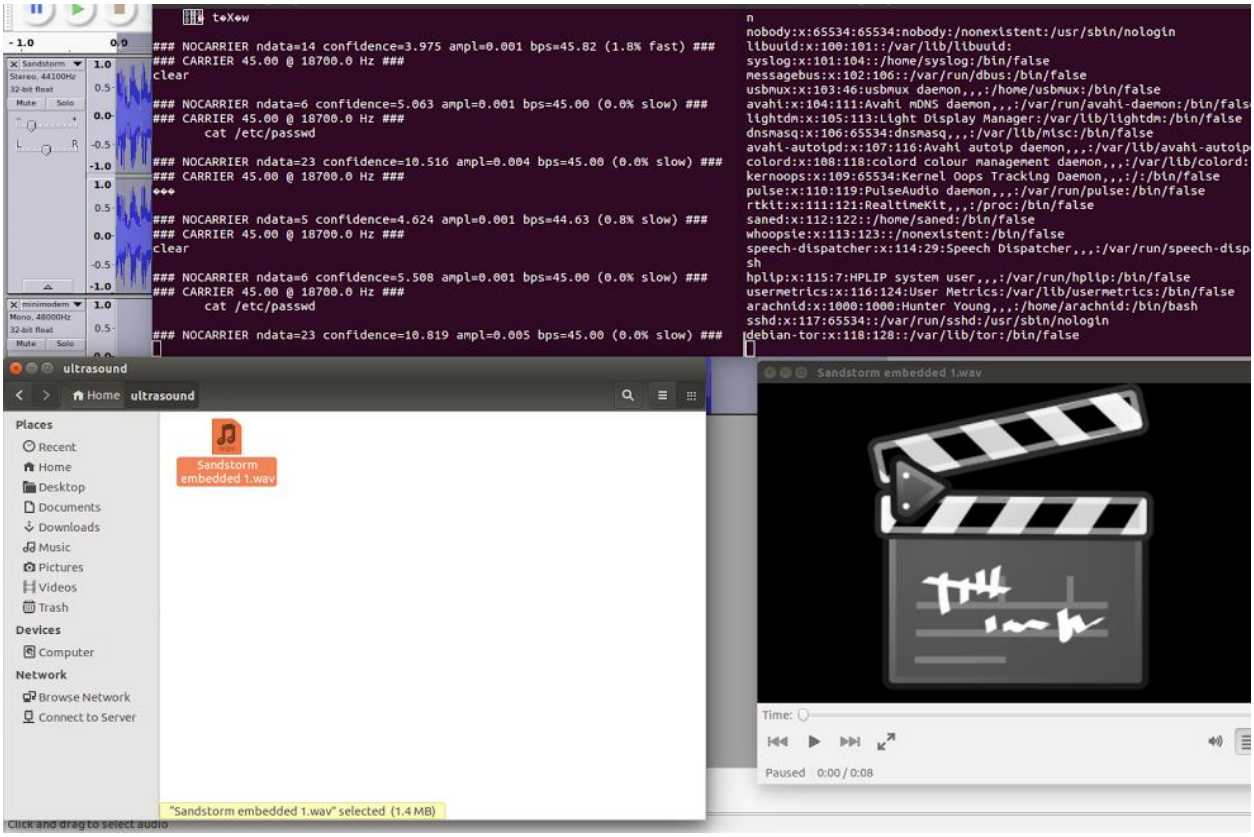
necessarily heard. However, frequencies we tested above this number began to become less reliable. This is most likely due the limitations of our specific hardware. Other devices might behave slightly differently, but 18-19kHz should be usable by nearly all devices. The average distance with which ultrasound could be transmitted and received reliably in all measured environments was approximately 7-9 feet indoors, and 6-8 feet outdoors when using stock hardware.

Our results were not determined using quantitative measurements, but rather on a case-by-case basis regarding binary feasibility. If we considered the behavior we were seeing to be feasible and usable in the real world, it received a “pass” and we continued refining our results based upon that. The parameters outlined above represent the final culmination of that methodology.

The screenshot below shows the debug output from the minimodem for baud rates of 45 and 90 at 19.6kHz. The effect of increasing baud rate can be seen in the additional gibberish introduced in the text transmissions. Transmissions at 45 baud produce clear, error free results, however transmissions at 90 baud produce undesired characters.

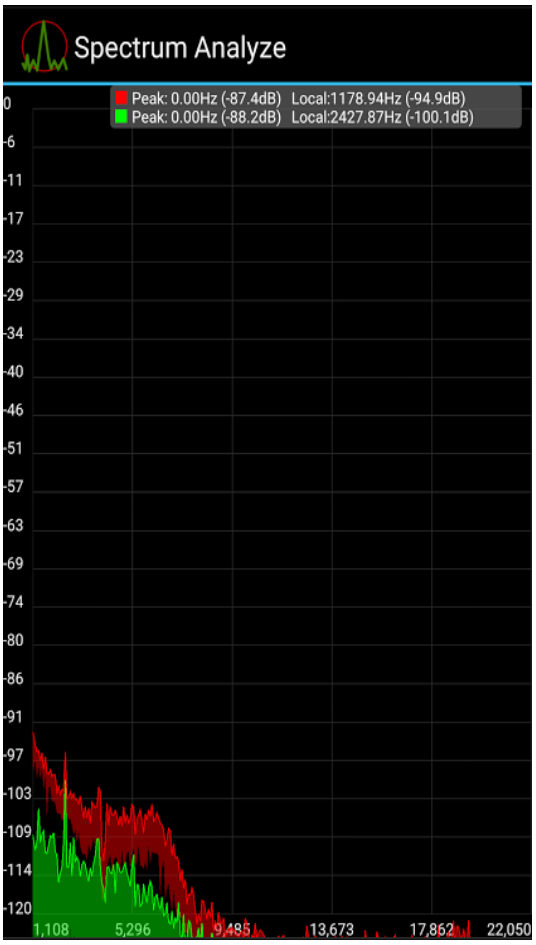


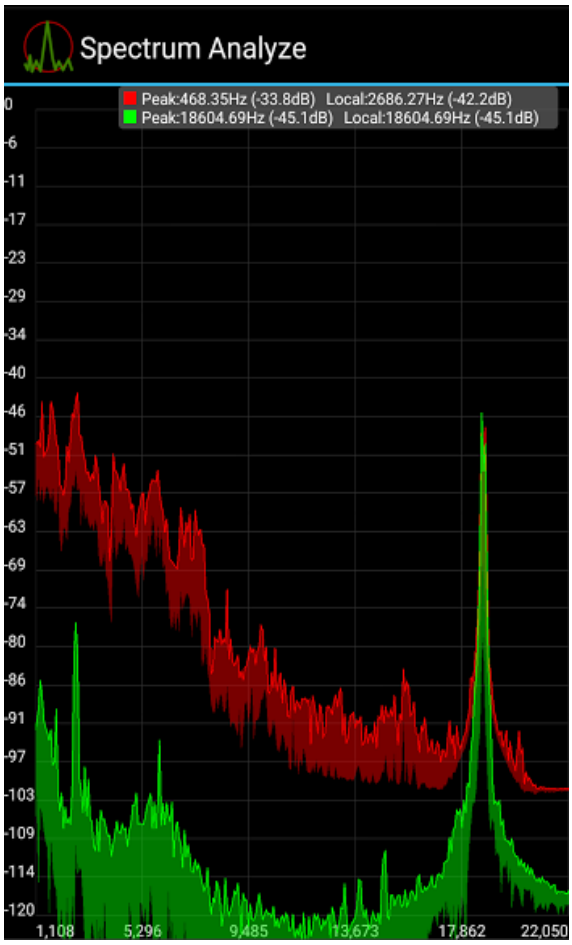
The following screenshot shows the results of our successful steganography test. The window at the top left of the screen shows the debug output of the receiving minimodem instance, while the screen on the top right shows the result of the command embedded ultrasonically in the recording of the arbitrary audio file, Sandstorm by Darude. The window at the bottom right of the screen shows the computer's media player playing the audio file over the computer's speakers; the ultrasonic signals are then being picked up by the computer's microphone. The setup could have just as easily been split up over two computers.



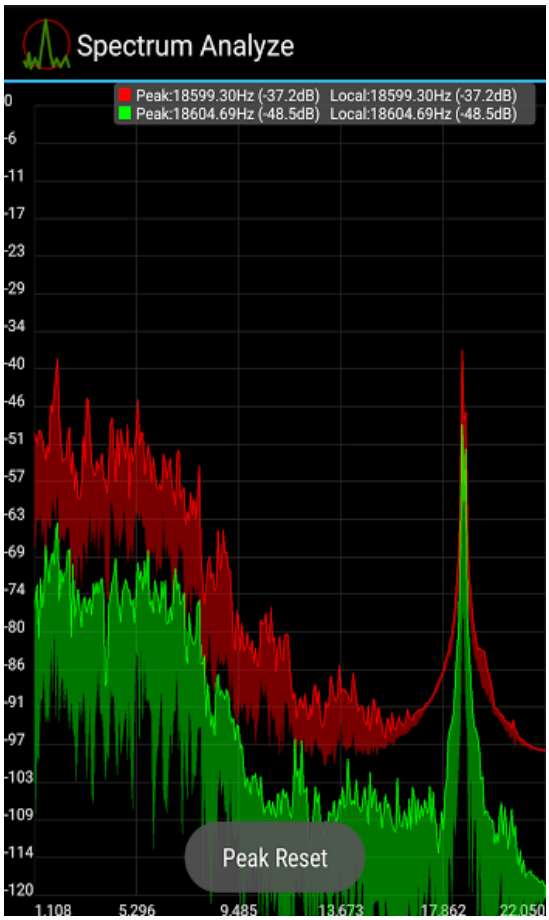
All of the following graphs were created by using the Spectrum Analyzer on the OnePlus One device. The optimally determined frequency stated above was used in all of tests represented in the graphs to ensure that the environmental effects of the various locations could be accurately accessed. The X axis represents frequency, and the Y axis represents signal strength in decibels. It is important to note that a change of -3dB is equivalent to the strength of the signal being cut in half. Values in green represent the sound levels at the time the graph was recorded, whereas values in red represent the peak values. The values in red should be disregarded since they are often created by simply punching a button on the device.

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

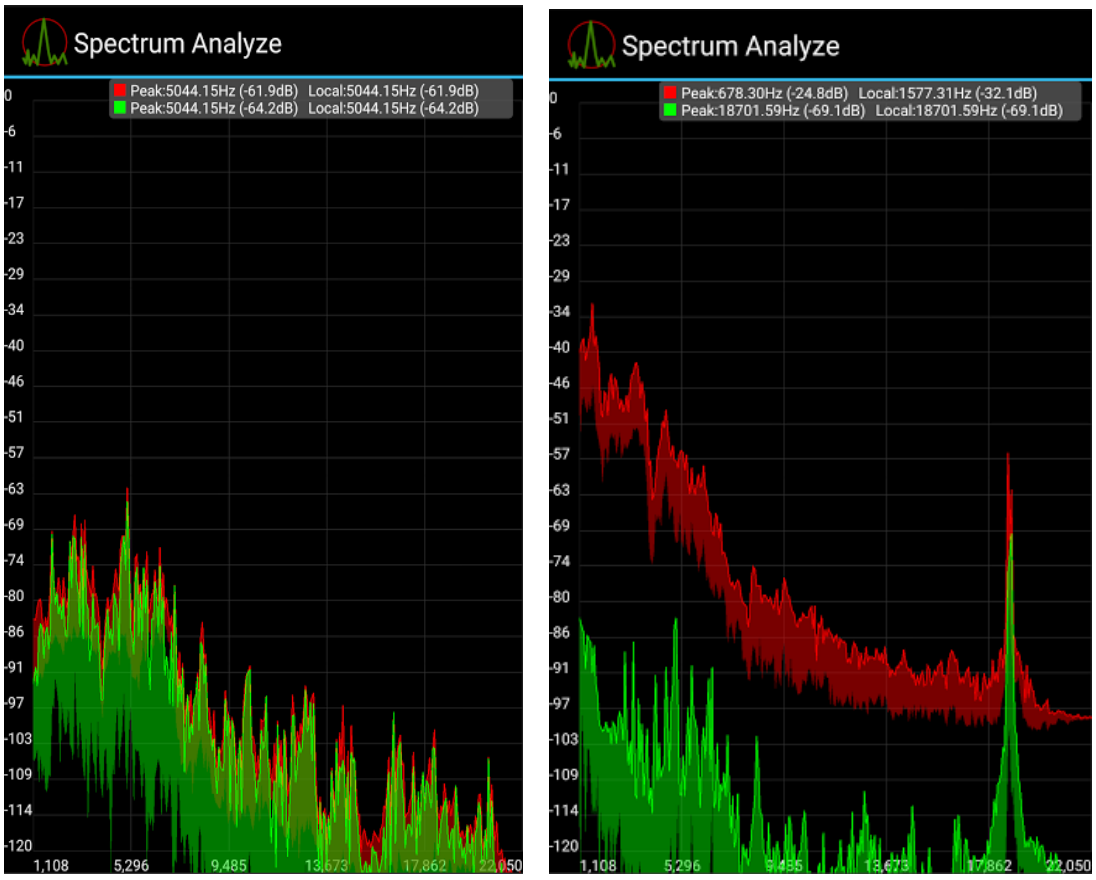




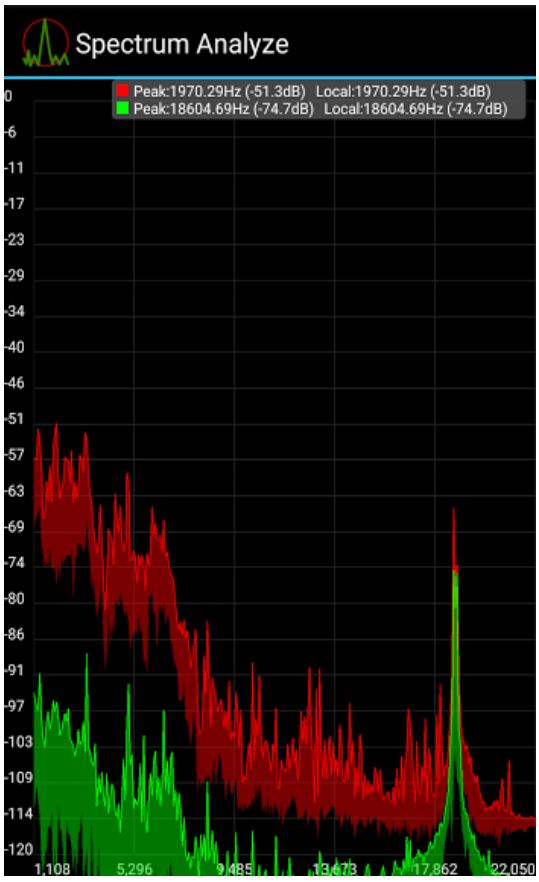
Dorm + Ultrasonic Signal + Music



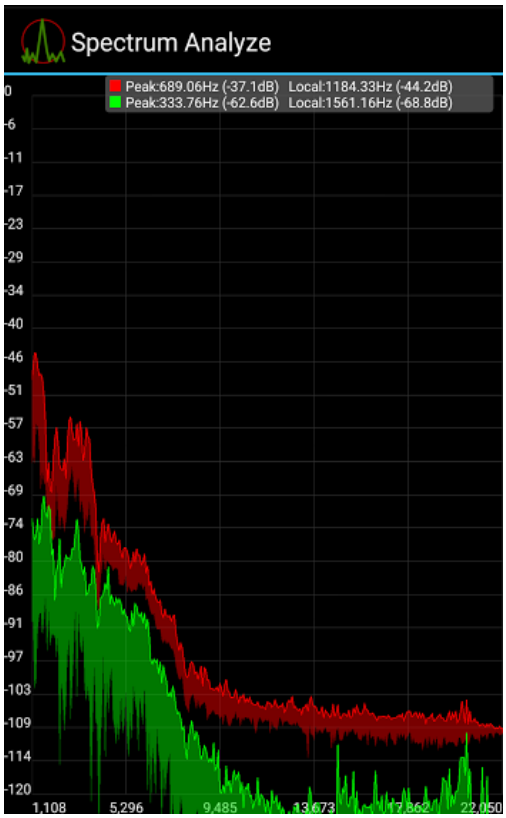
Outdoor Noise Floor (LEFT) and Outdoor + Ultrasonic Signal (RIGHT)

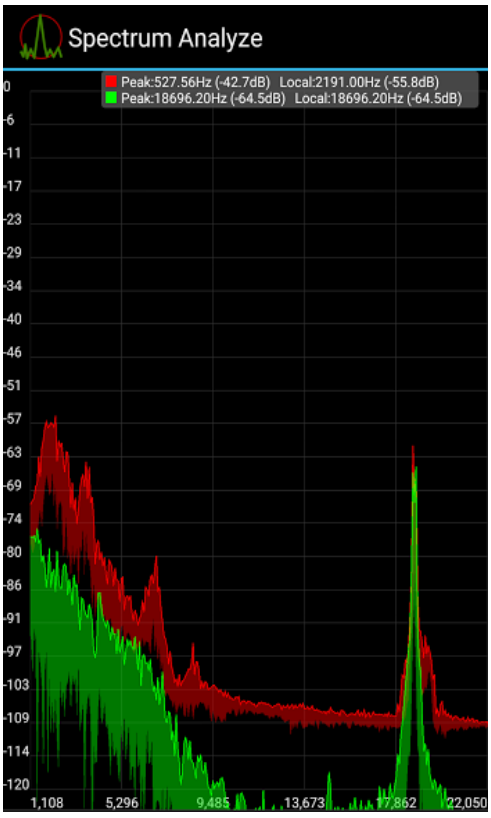


Outdoor + Ultrasonic Signal + Music

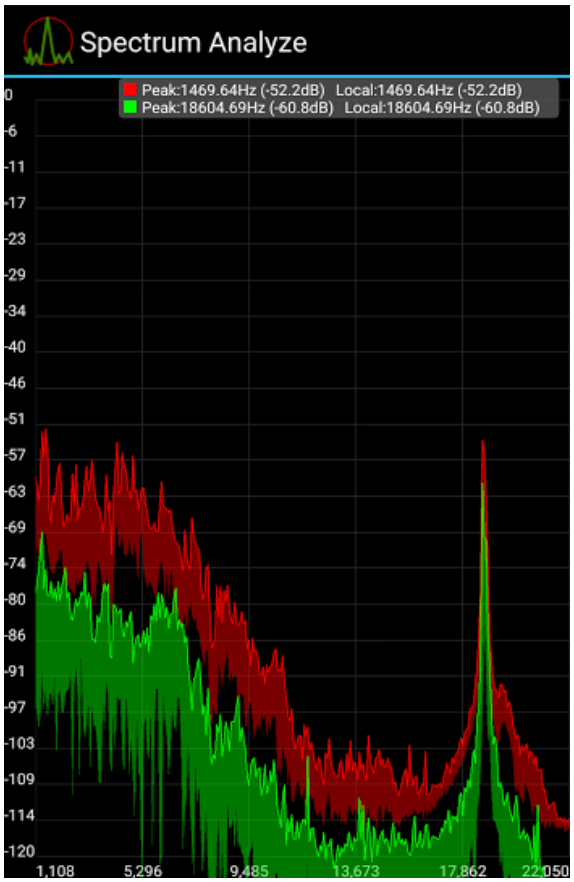


Server Room Noise Floor (LEFT) and Server Room + Ultrasonic Signal (RIGHT)

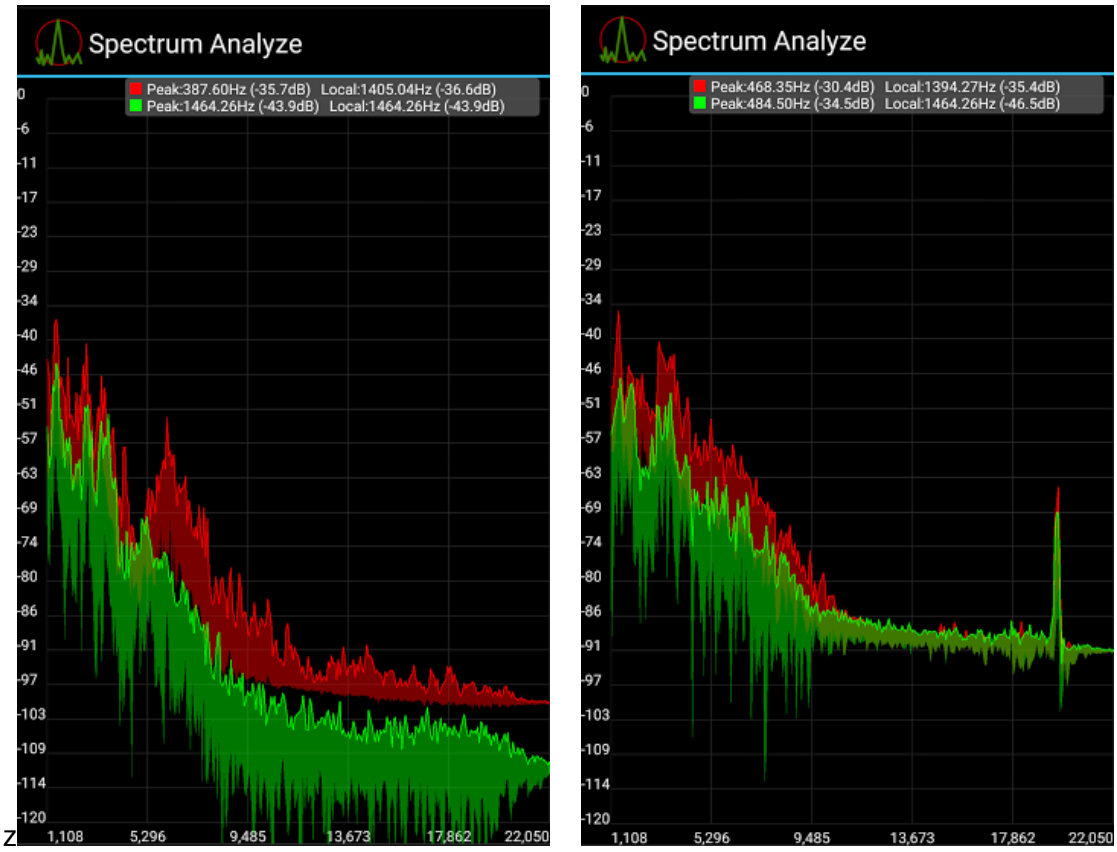




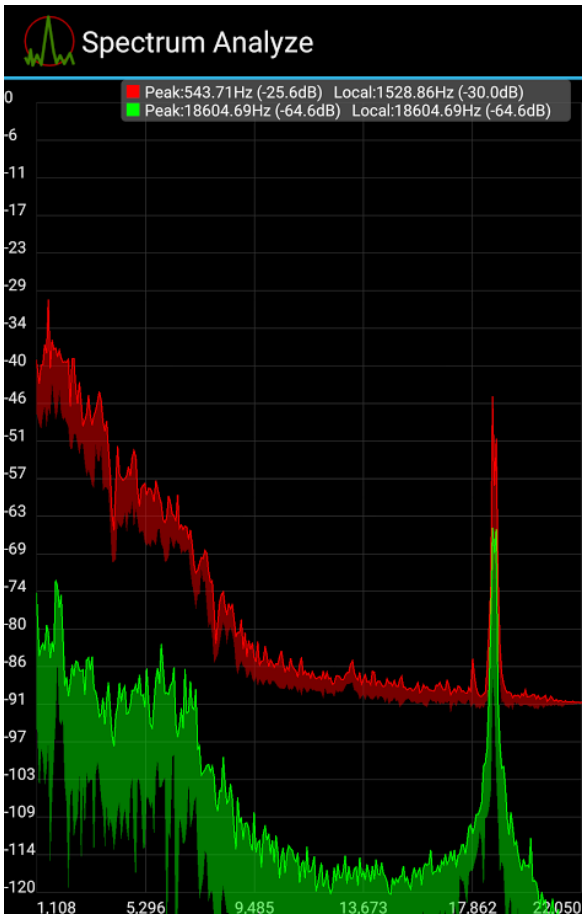
Server Room + Ultrasonic Signal + Music



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



Commons + Ultrasonic Signal + Music



Conclusions

Ultrasonic data transmission is indeed possible, and can be used to transfer data with both confidentiality and integrity. Ultrasonic data steganography is also possible and can be used to achieve the same end goals as ultrasonic data transmission through different means. Additionally, both of these concepts have relevance and a potentially profound impact on the realm of information security.

Through the use of ultrasonic data transmission, it is possible to bridge the divide created between air gapped systems, thus creating a threat to the confidentiality, integrity, and availability of the data contained on the air gapped systems.

Physical Limits

Although both ultrasonic data transmission and steganography are possible, they are not without their limits. Based on our testing, ultrasound does not propagate well past 6-9 feet when using stock hardware that has not been specifically designed to work with ultrasound. Even if better hardware was introduced in an effort to increase this distance, the physical limitations of high frequency transmissions still apply. It takes much more energy for a high frequency wave to propagate as far as a low frequency wave - the laws of physics cannot be changed.

Furthermore, ultrasound will not propagate through solid objects unless the source is placed directly on the solid object itself. Walls and other large obstacles represent near impenetrable boundaries for ultrasound in this portion of the spectrum.

Technological Limits

Despite the fact that ultrasound is capable of bridging the divide between air gapped systems as a communications protocol it still requires a listener to be setup on the air gapped system. The only way to get the listening on the air gapped system is through physical means at that point. So in essence, ultrasonic data transmission only allows an attacker to maintain persistence in an air gapped system, not obtain access to it. Assuming the physical security of the system is maintained, the likelihood of ultrasonic data transmission being useful is slim.

In regards to ultrasonic data steganography, file compression is a death sentence for the embedded ultrasonic data. If ultrasound is intended to be hidden in an audio file, the audio file must remain in a raw, PCM-sampled format. Common compression technologies such as MP3, Ogg Vorbis, and AAC will remove any and all traces of ultrasonic signals in a given recording.

Security Considerations and Recommendations

In order to prevent attackers from utilizing ultrasound to compromise air gapped systems, effective security considerations must be made and appropriate safeguards put in place.

Removal of microphone and speaker

The simplest and surest way to prevent ultrasound from being used to establish a link to air gapped systems is to remove the hardware that makes the transmission of ultrasound possible. If the microphone and speaker are removed from a system, there is no way for it to utilize ultrasonic data transmission. If no reason exists for having the

microphone or speaker, this is the best course of prevention. Essentially, this is the concept of least privilege being applied to hardware instead of user-roles.

Heuristics

Assuming that removing the microphone or speaker is not feasible for some reason, the next best thing would be to provide any sort of anti-virus or HIDPS services running on the air gapped system with the necessary signatures or heuristic algorithms necessary to discover processes passing modulated data to the default sound and recording devices on the system. This sort of safeguard would most likely cause issues with audio editing software as well as potentially some drivers. However, an application whitelist would solve those issues. Considering the system would already be air gapped, it stands to reason that a software whitelist is already in place; therefore a new whitelist would not have to be established.

Extrapolations

Now knowing that ultrasonic data transmission is a viable concept, there are several potential next steps to undertake. The following concepts could become an expansion on this work, and become full-fledged projects in their own right.

Laser Microphones and Ultrasound

Laser microphones are actually incredibly simple. They project a laser beam onto a window, and a camera measures the movement in the reflection of the laser beam. When the laser is projected onto a glass window, the sound in the room causes the glass to vibrate, and the laser to be reflected at slightly different angles. It is unknown whether or not ultrasound possesses the ability to vibrate the types of glass commonly

used in windows. In order for ultrasound to excite measurable vibrations in the glass, it would require a much stronger ultrasonic speaker than is present in stock devices.

Power line Signal Modulators and Ultrasound

Power line adapters are not new. In fact, modulation over power lines is possible for both analog and digital signals. Although many high security systems use filters to ensure that power lines cannot carry modulated data, they may be able to be bypassed by signals modulated ultrasonically. Again, this is unknown and would need to be tested.

Wall Transducers and Infrasound

On the complete opposite end of the spectrum exists the concept of infrasound, or sounds so low that humans are unable to hear them. These sounds are essentially nothing but vibrations that can be felt rather than heard, and they exist below 20 Hz. Since low frequencies propagate so well through solid objects, special bass transducers could potentially be used to exfiltrate data from a building using the same modulation techniques applied in this project to ultrasonic signals.

References

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

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

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

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

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