# Microphone Jamming

Adam Janicki, Chris Rinard, Kyle Sandell

*Massachusetts Institute of Technology*

May 10, 2022

# 1 Abstract

For our final project for 6.857, we implemented and tested a microphone jammer. A microphone jammer is a device or tool that prevents a microphone from accurately recording audio; this is done by emitting ultrasonic waves to interfere with microphone hardware. This ultrasonic wave is around 20 kilohertz in frequency, and barely above the upper edge of human hearing, meaning it can't be heard by humans but is able to disable nearby microphones. We exploit a weakness in consumer grade microphones where ultrasonic waves are amplified down to human hearing range, which effectively covers the conversation audio with nonsensical noises. Although there exist more advanced techniques for jamming microphones (we describe another technique, phase superposition in detail in section 3.2), given the time and budget constraints, we decided that the traditional ultrasonic approach was optimal for this project scale. We built a jammer based on this technique and quantified its effectiveness.

# 2 Introduction

Today, many encryption schemes and systems focus on securing data over a relatively complex medium of communication. Many of these schemes are complex and focus on internet security; TLS, TCP, and RSA all serve as good examples. With this focus on securing modern means of communication, relatively primitive means of breaking security have remained static despite recent advancements in both offensive and defensive technology primitives.

The recent proliferation of cheap microphones, connected devices, and unlimited storage have enabled widespread recording of individuals without their consent or knowledge. This leads to the problem where in-person conversations may not be secure. Potentially malevolent microphones are copious and can include even your own devices, where applications like Google or Siri can passively listen to you even if you are unaware that you are being recorded at the moment. Consider a scenario where Alice tells Bob her Microsoft login so he can play her Xbox. If Alice uses this same password for numerous other websites and this audio was recorded, that would imply that anyone who recorded or found this data would be able to sign-in to countless accounts of Alice's.

In response to the threat, over the years various technologies have emerged that are used for jamming, but many of these are clumsy and indiscriminate with high power consumption, limited portability, and weak security guarantees. Additionally, current device jamming can have unintended consequences, such as jamming non-malicious users, like people with hearing aids, and potential health side effects which can be particularly worrying for children and animals. Given issues with currently available technology, we implemented a basic system and propose more advanced ones to secure conversations.

# 3 Microphone Jamming Techniques

Microphone Jamming technology has two primary design goals: 1) render microphones unable to record accurate data, and 2) not have a substantial effect on the humans around the jammer. Currently, there are two methods of accomplishing this: traditional ultrasonic jamming and ultrasonic phase superposition. We describe each technique below and discuss the benefits and downsides of each.

## 3.1 Traditional Ultrasonic Jamming

In modern microphones, the hardware is optimized to pick up sound waves in the human hearing spectrum. The human hearing spectrum ranges from around 20 Hz to 20 kHz. 20 kHz borders on the line between audible sound and ultrasound. Traditional Ultrasonic Jamming is the technique where a device transmits a powerful ultrasound wave at 2̃1kHz and directs it at a microphone; the microphone becomes saturated by this sound and masks out all underlying noise from the environment [Adi22]. However, this wave must be transmitted at greater power than the audio it is intended to mask. This poses some concerns: in a loud environment an ultrasound wave would have to be transmitted at a even louder volume. Although these waves are inaudible to most people, transmitting them at a high enough power risks damaging people's hearing. Additionally, these waves are audible to certain animals and young children, which causes significant discomfort.

## 3.2 Phase Superposition

A less damaging approach to this problem is to use phase superposition. Originally developed as an offensive technique to trigger voice assistants, phase superposition can be modified to be a strong defensive mechanism [CLT+20]. This approach relies on transmitting two ultrasonic waves at different frequencies, $f_1$ and $f_2$. When these waves arrive at the microphone hardware, nonlinearities cause it to be processed as noise inside the audible spectrum (specifically, there is an artifact from the frequency $f_1 - f_2$). This approach is much safer than the traditional ultrasonic approach because the two waves are significantly above the ranges that would be considered damaging to hearing, and requires less power because it can superimpose random noise on a conversation rather than completely drowning it out.

# 4 Security Considerations

## 4.1 Security Policy

We first lay out definitions for our security policy:
**Host**: the person utilizing the microphone jammer.
**Adversary**: the person attempting to record host without permission.
**Bystanders**: the people audio recording for a legitimate & legal purpose, or not recording at all.
**Goal**: an adversary should not be able to record the host, where bystanders should be unaffected (within reason, someone who is very close to the host may be affected)

## 4.2 Security Goals

Now that we have defined the players in this game, below we define the goals of security for a jamming system. We considered 3 primary goals that the system should prioritize in order to be effective as a defensive device.

1. **Effectiveness**: This refers to the usability of the device, i.e., does it work all the time, part of the time, or none of the time? An ideal system would work all of the time. Realistically, any system will break sometimes; we believe that a system with a mean time to announced failure of 1 month would be suitable for most use cases.

2. **Difficult Decryption**: Decryption refers to taking the audio recording with ultrasonic waves and removing the extra noise to recover the original conversation. For the system to be successful, we have to ensure that an adversary who recorded a jammed conversation cannot remove the ultrasonic noise from the recording, as this would render the device useless.

3. **Directional**: Finally, the last goal is to make the device able to target microphones. As mentioned above, one of the issues with currently available devices is that they can't pick and choose which microphones they disable; they simply disable everything within their range of operation. We'd like the ability to aim the device to protect innocent bystanders involved in the game.

# 5 Implementation

We did not find it plausible to implement a phase superposition jammer within class time constraints given the specialized parts and code required. However, when searching, we found plans for an ultrasonic jammer that required less than $30 in parts that could easily be found around MIT. We felt given the time constraints, it would be more worthwhile to build a simple device so that we could get it working and run tests on it. As such, we built out a first version from this initial schematic [Bur20]. After finishing our initial version of the device, we knew we had to expand on it to improve its range. Our first test, although successful, only worked at a range of mere centimeters. A device held over an inch away would still be able to record without difficulty. Luckily, in order to improve the range of effectiveness of our device, we just need to boost the power provided to the system, which in turn boosts the power of the emitted waves.