Politecnico di Torino

Cybersecurity for Embedded Systems
01UDNOV

Master's Degree in Computer Engineering

Track 2: DoS attacks on microphones

Project Report

Candidates:
Costabile Digregorio (S318078)
Francesco Gallo (S319989)
Gianmarco Bachiorrini (S309909)

Referee:
Prof. Alessandro Savino

Contents

List of Figures

List of Tables

Abstract

This is the space reserved for the abstract of your report. The abstract is a summary of the report, so it is a good idea to write after all other chapters. The abstract for a thesis at PoliTO must be shorter than 3500 chars, try to be compliant with this rule (no problem for an abstract that is a lot shorter than 3500 chars, since this is not a thesis). Use short sentences, do not use over-complicated words. Try to be as clear as possible, do not make logical leaps in the text. Read your abstract several times and check if there is a logical connection from the beginning to the end. The abstract is supposed to draw the attention of the reader, your goal is to write an abstract that makes the reader wanting to read the entire report. Do not go too far into details; if you want to provide data, do it, but express it in a simple way (e.g., a single percentage in a sentence): do not bore the reader with data that he or she cannot understand yet. Organize the abstract into paragraphs: the paragraphs are always 3 to 5 lines long. In LaTeXsource file, go new line twice to start a new paragraph in the PDF. Do not use to go new line, just press Enter. In the PDF, there will be no gap line, but the text will go new line and a Tab will be inserted. This is the correct way to indent a paragraph, please do not change it. Do not put words in **bold** here: for emphasis, use *italic*. Do not use citations here: they are not allowed in the abstract. Footnotes and links are not allowed as well. DO NOT EVER USE ENGLISH SHORT FORMS (i.e., isn't, aren't, don't, etc.). Take a look at the following links about how to write an Abstract:

- `https://writing.wisc.edu/handbook/assignments/writing-an-abstract-for-your-research-paper/`
- `https://www.anu.edu.au/students/academic-skills/research-writing/journal-article-writing/writing-an-abstract`

Search on Google if you need more info.

CHAPTER 1

Introduction

1.1 Report introduction

In recent years, there has been a rapid proliferation of devices equipped with microphones, such as smartphones, smart speakers, and smartwatches. This has led to a significant decline in user privacy, especially as many of these devices come with an 'always-listening' feature enabled by default. As a result, the security vulnerabilities in microphones have attracted the attention of both attackers and defenders: while the motivations of the former are self-evident, the latter, in an interesting role reversal, can leverage these vulnerabilities to enhance user privacy. In other words, it is possible to execute an attack that disables nearby microphones to preserve the privacy of users who may be unaware of potential eavesdropping.

From the perspective of improving user privacy by exploiting microphones' vulnerabilities, this project investigates Denial of Service (DoS) attacks on microphones, with the goal of understanding the underlying technologies, identifying vulnerabilities, and replicating attacks on real hardware. The project seeks to provide a comprehensive analysis of microphone manufacturing technologies, evaluate the state-of-the-art in attack techniques, and explore the limitations and implications of these attacks. In particular, the project will focus on a specific type of DoS attack, which involves flooding the target microphone with ultrasound waves to prevent it from recording any conversation. Additionally, a fully functioning prototype device capable of executing the attack has been developed. As we navigate through both the sotware and hardware implementations of the project, an analysis of the results will be presented, assessing the strengths and weaknesses of the prototype device.

1.2 Report description

The remainder of the document is organized as follows:

- Chapter 2: This chapter offers a comprehensive overview of the project's theoretical background, detailing the key features of various microphone technologies and examining known attack methods.
- Chapter 3: This chapter provide a general overview of the project's implementation, offering the reader a simple description of the prototype device's components and capabilities.
- Chapter 4: This chapter presents a detailed explanation of the device, covering everything from its initial design to its physical construction and realization.

- Chapter 5: This chapter outlines the results obtained and proposes ideas for potential improvements to the device in future work.
- Chapter 6: This chapter recaps with a high-level summary what has been done in the project.

CHAPTER 2

Background

This section of the report will introduce to the reader the most relevant microphone technologies, highlighting their core features and primary domains of use.
Furthermore, the different types of known DoS attacks on microphones will be reviewed, evaluating the advantages and disadvantages of each. This analysis will justify the selection of the chosen attack method for the project.

2.1 Microphone Technologies

Microphones are critical components in many modern devices, enabling audio capture for communication, recording, and interaction with digital assistants. Since they are used in a wide range of devices, their underlying technology must meet diverse requirements, resulting in both orizontal diversification and vertical improvement over the past century.
While acknowledging the historical significance of early microphone implementations, this report will focus only on the most commonly used models today, as they are most relevant to the development of the project.

2.1.1 Dynamic Microphones

A dynamic microphone is a type of mic that converts sound waves into electrical signals using electromagnetic induction thanks to a special component, the permanent magnet. The permament magnet can either be a metal coil or a 'ribbon transducer': when the sound waves hit the microphone, the magnet will move, resulting in the generation of an electrical signal. This type of microphone is known for its durability, ability to handle loud environments, and tolerance of background noise. Additionally, it does not require external power, making it a versatile option for various situations. Although it may not be as sensitive or well-suited for recording high-frequency sounds, it is ideal for live music events and concerts involving loud sounds.

2.1.2 Condenser Microphones

Often referred to as the 'cousins' of dynamic microphones, condenser microphones generate electrical signals from sound waves through the use of a capacitor. The capacitor consists of two charged metal plates, one of which is movable. When a sound wave strikes the diaphragm (the movable plate), the distance between the plates changes, producing an electrical signal that corresponds to the sound captured. While condenser microphones require an electrical current to charge the plates and are more

sensitive to environmental conditions compared to dynamic microphones, they excel at capturing high-frequency sounds and vocals, delivering crisp, detailed, and high-quality audio. These qualities make condenser microphones ideal for studio recording, as they are best suited for quiet environments and require the external power source.

2.1.3 Electret Condenser Microphones

The electret condenser microphone is a subtype of the standard condenser microphone. The key difference is that, while standard condenser microphones require a power supply to maintain the electrical charge, electret microphones use an electret material to keep the capsule charged. This type of material is one that carries a permanent electrical charge sealed within an insulating film. Since electret microphones don't require an external power source to charge the plates, they tend to be less expensive than standard condenser microphones, making them ideal for use in consumer electronics and mobile devices.

2.1.4 Micro-Electro-Mechanical Systems Microphones

MEMS microphones is another subtype of the standard condenser microphone which shares many characteristics with the electret type one. However, in this case, the transducer is a microscopic component that integrates seamlessly with the microscopic semiconductor-based components in an integrated circuit. This allows for smaller devices, making them suitable for an even wider range of applications, such as smartphones, tablets, laptops, hearing aids, voice biometric, digital voice assistants, and more. Additionally, compared to electret microphones, MEMS microphones can offer superior audio performance, though they tend to be more susceptible to mechanical and electrical noise.

2.2 Microphone Attacks

Having explored the landscape of microphone technologies, it is evident that the ones we encounter most frequently in daily life are Electret microphones, and even more commonly, MEMS microphones. Both technologies share key components, namely the membrane and the capacitor, each of which is vulnerable to specific types of attacks that can effectively prevent microphones from recording conversations intended to remain private.
The membrane can be made to vibrate by flooding the microphone with sound waves, thereby overwriting the sound waves from the conversation and preventing proper recording. Meanwhile, the capacitor can be targeted by altering its electric charge, causing it to produce a distorted or different electrical signal instead of the original one.
The following section will examine known DoS attacks that exploit the vulnerabilities of these two components, evaluating each attack technique in terms of its suitability for the project.

2.2.1 Electromagnetic Pulse Attack

A general EMP attack involves releasing a burst of electromagnetic radiation capable of disrupting or destroying electronic equipment and systems across the target area. It is frequently employed in modern warfare with the goal of causing infrastructural disruption, targeting communication systems, computers, vehicles, and other critical equipment.
When using an EMP to disable microphones, the strategy involves emitting a powerful burst of electromagnetic radiation that overwhelms and potentially damages the electronic components within the microphones. This could result in the microphones failing to generate the intended electrical signals, or even becoming completely non-functional, thus disabling their ability to record or transmit audio.

The severity of the impact would depend on the intensity and proximity of the EMP, potentially leaving affected microphones unusable until they are repaired or replaced.
While theoretically the most effective method on paper, employing an EMP for this project is impractical for several reasons. First and foremost, health concerns must be taken into account, as this type of attack could pose risks to nearby individuals with pacemakers, hearing aids, or other medical devices. Secondly, it would lack control over the range of action and the potential impact on targets. Additionally, testing the prototype device would be extremely difficult, with results that could be highly unpredictable and the testing targets potentially suffering permanent damage. Finally, the need for high power sources makes it unsuitable for embedded devices.

2.2.2 Laser Injection Attack

Luminous attacks on microphones involve using lasers to disrupt or damage their functionality. Lasers emit focused beams of intense light that can interfere with microphones in several ways. First, a powerful laser beam can overload the microphone's optical or electronic sensors, causing them to register false signals. Second, laser light can interfere with the microphone's ability to accurately capture sound waves, potentially distorting or disrupting the audio signal. In extreme cases, particularly with high-powered lasers, the intense heat generated by the beam can physically damage the microphone's components, such as diaphragms, sensors and circuitry. Moreover, luminous attacks can compromise privacy by remotely activating microphones through light-based signals, thereby bypassing traditional security measures.
However, this type of attack does not align with the project's objectives. The limited applicability due to its high specificity, the need for precise targeting making it impractical in general environments, and its high production costs classify the laser injection attack as unsuitable for this project.

2.2.3 Ultrasonic Sound Waves Jamming Attack

Ultrasonic sound waves are those that travel at frequencies above 20 kHz, exceeding the range of human hearing. This type of sound wave can be used to perform jamming attacks on microphones, disrupting their functionality. In particular, they can overwhelm the microphone's sensors, which are typically calibrated to capture frequencies within the audible spectrum. When exposed to ultrasonic sound waves, these sensors may register false signals or become saturated, resulting in inaccurate audio captures and, thereby, distorted or unintelligible audio output.
This attack meets all the requirements to be suitable for the project: it can target nearly any everyday microphone, delivers strong performance, and when properly tuned, becomes extremely difficult—if not impossible—for humans to detect. Moreover, its low implementation cost and non-destructive nature make testing the prototype device much more feasible.

CHAPTER 3

Implementation Overview

This chapter presents the project's objectives, the specific problem it seeks to address, and the challenges encountered during its development. Additionally, it provides a high-level overview of the proposed solution.

3.1 Goal of the project

Nowadays, with the rise of smart devices and the increasing spread of home automation, we are literally surrounded by microphones. All these devices can potentially be used to record sensitive data from our conversations without our consent.

The goal of this project is to create a device capable of (at least partially) deny the aforementioned risk and enhance users' privacy. The desired device should satisfy the following requirements:

- Effectiveness: the device should deliver perceptually high performance within a reasonable operational range.
- Inaudibility to humans: the device should operate without causing any disturbance during conversations and should only interfere with the functionality of microphones when activated.
- Portability: the device should be designed to be easily transportable.
- Ease of use: the device should be intuitive and user-friendly, ensuring that it can be operated by individuals of varying technical expertise.
- Low energy consumption: the device should be designed to operate with minimal energy requirements.
- Affordability: the device should be produced at minimal cost while ensuring all required functionalities are maintained.

If all the requirements are met, the device will offer an effective solution to the problem, enhancing the privacy of individuals who are often concerned about the risk of being recorded.

3.2 Core Concept

The first step is to formalize the problem and identify the most suitable attack vector that meets the previously aforementioned requirements. Following a thorough analysis, as outlined in Background,

the ultrasonic sound wave jamming attack was determined to be the most appropriate option due to its high applicability, (potential) strong performance, and difficulty for humans to detect.

A cost-effective implementation of this attack involves the use of ultrasonic transducers, which are commonly found in low-cost distance sensors as they operate at the required frequencies (above 20kHz), or they can be bought in bundle at almost any online electronic retailer. Consequently, a signal generator is required to produce the appropriate sound wave for the speaker. Finally, a microcontroller is necessary to orchestrate the operation of the device, managing the control logic and interfacing with the signal generator.

3.3 Key Challenges in Implementing the Core Concept

The core concept satisfies certain requirements, such as inaudibility to humans and low cost. However, aspects like portability, effectiveness, and ease of use are not fully achieved by implementing only the core idea. Furthermore, some properties are inherently interconnected. For example, increasing effectiveness may raise overall costs, reducing affordability, while portability is closely tied to low energy consumption, as high energy demands would compromise the device's practicality.

Therefore, careful evaluation and selection of available market components are crucial to ensure all requirements are met.

3.4 Practical Implementation of the Core Concept

Having outlined the core concept, its development requires additional components to ensure full functionality and satisfy the imposed requirements.

To make the signal effective in a real-world scenario, an audio amplifier is necessary, as the generated signal's power must be boosted to a specific level. By utilizing an external power source, the amplifier module interfaces the microcontroller-signal generator subsystem with the speaker.

The external power source has been implemented as a set of batteries to ensure portability and keep costs low. Specifically, the batteries are lithium-based and are connected together to achieve the required voltage and power.

Finally, a remote-controlled switch has been integrated, enabling the end user to power the device on and off via the *Home* application in the iOS environment or through the lightweight MQTT protocol.

3.5 Final Implementation

At this stage, with all functional and non-functional requirements met through the selected components, the final step is to design the device and integrate all elements into a cohesive unit.

The speakers are embedded into a 3D-printed spherical shell with strategically placed openings to house them. This design enables the jamming attack to be performed in nearly a 360-degree radius, maximizing the coverage of the surrounding area.

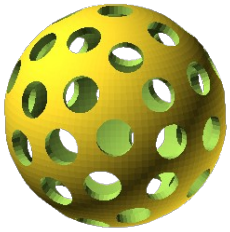
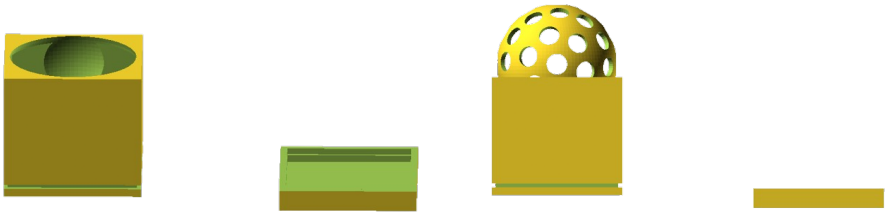


Figure 3.1: 3D-printed spherical shell

The shell is mounted on a base that houses the battery along with all the previously mentioned components, including the microcontroller, audio amplifier module, signal generator, and remote-controlled switch. This base provides an organized and concealed arrangement of the internal components, offering the end user a polished and minimalist appearance while maintaining practicality.



(a) Support base (b) Shell resting on the base

Figure 3.2: Final implementation appearance

CHAPTER 4

Implementation Details

This is where you explain what you have implemented and how you have implemented it. Place here all the details that you consider important, organize the chapter in sections and subsections to explain the development and your workflow.
Given the self-explicative title of the chapter, readers usually skip it. This is ok, because this entire chapter is simply meant to describe the details of your work so that people that are very interested (such as people who have to evaluate your work or people who have to build something more complex starting from what you did) can fully understand what you developed or implemented.
Don't worry about placing too many details in this chapter, the only essential thing is that you keep everything tidy, without mixing too much information (so make use of sections, subsections, lists, etc.). As usual, pictures are helpful.

CHAPTER 5

Results

Device	Range 1	Range 2	Range 3	Range 4
Smartphone				
PC				
Smartwatch				

Table 5.1: Performance Table

5.1 Known Issues

Although this implementation fully satisfies the requirements outlined in the Implementation Overview chapter and achieves respectable performance, the device is still in its prototype phase and is affected by certain issues:

- Physical barriers: physical barriers can partially or completely negate the jamming attack, as it relies on soundwaves, which are affected by physical laws such as absorption, transmission, and diffraction.
- Range: the current implementation performs adequately at X range, but there is still room for notable improvement.
- Rechargeability of batteries: currently, despite the low energy consumption mitigating the impact of this issue, there is no possibility of recharging the batteries.
- Shell prototype design: The spherical shell's speaker holes are slightly inconsistent in size, with some being larger and others smaller, and the two halves of the sphere are held together in a rudimentary manner.

5.2 Future Work

The concept of this project has successfully achieved its predetermined objectives. However, there are several areas where it could be further improved.

Given more time, most of the known issues could be addressed: increasing the power to the speaker could enhance the operational range and effectiveness of the jamming attack, and higher-quality materials could be used to improve the robustness of the spherical shell and base.

Another significant improvement would be the addition of a white-noise generator with a dedicated speaker, introducing two potential operational modes for the device. The 'Stealth mode' would maintain the current jamming attack functionality, while the 'Paranoic mode' would activate the white-noise speaker to generate additional distortion, providing the user with greater assurance that nearby microphones cannot capture sensitive conversations. Additionally, incorporating the ability to adjust the volume of the white noise could help mitigate the issue caused by physical barriers.

CHAPTER 6

Conclusions

This final chapter is used to recap what you did in the project. No detail, just a high-level summary of your project (1 page or a bit less is usually enough, but it depends on the specific project).

Bibliography

[1] Donald E. Knuth (1986) *The TEX Book*, Addison-Wesley Professional.

[2] Leslie Lamport (1994) *LATEX: a document preparation system*, Addison Wesley, Massachusetts, 2nd ed.

APPENDIX A

User Manual

In the user manual you should explain, step-by-step, how to reproduce the demo that you showed in the oral presentation or the results you mentioned in the previous chapters.
If it is necessary to install some toolchain that is already well described in the original documentation (i.e., Espressif's toolchain for ESP32 boards or the SEcube toolchain) just insert a reference to the original documentation (and remember to clearly specify which version of the original documentation must be used). There is no need to copy and paste step-by-step guides that are already well-written and available.
The user manual must explain how to re-create what you did in the project, no matter if it is low-level code (i..e VHDL on SEcube's FPGA), high-level code (i.e., a GUI) or something more heterogeneous (i.e. a bunch of ESP32 or Raspberry Pi communicating among them and interacting with other devices).

APPENDIX B

API

If you developed some source code that is supposed to be used by other software in order to perform some action, it is very likely that you have implemented an API. Use this appendix to describe each function of the API (prototype, parameters, returned values, purpose of the function, etc).