The Little Seal Bug

Optical Sound Recovery from Lightweight Reflective Objects

By: Dr. Ben Nassi, Raz Swissa, Dr. Boris Zadov

Researchers

Ben Nassi

Raz Swissa

Prof. Yuval Elovici

Dr. Boris Zadov

Ben-Gurion University of the Negev

Agenda

- Background
- Threat Model
- Analysis
- Recovering Speech
- Evaluation
- Takeaways
- Q&A

The Great Seal Bug

What do you know regarding the picture presented on the right side of the slide?

The Great Seal Bug

What do you know regarding the picture presented on the right side of the slide?

- It is a picture of an eagle.
- It was given as a gift to the United States Ambassador to the Soviet Union from the Soviet Union in 1945.

The Great Seal Bug

What do you know regarding the picture presented on the right side of the slide?

- It contained a concealed passive device, which is considered a predecessor of radio frequency identification (RFID) technology which was used for eavesdropping.
- It was the first covert listening device that utilized passive techniques.
- It took the Americans six years to determine its real purpose.

The Great Seal Bug

What do you know regarding the picture presented on the right side of the slide?

- It contained a concealed passive device, which is considered a predecessor of radio frequency identification (RFID) technology which was used for eavesdropping.
- It was the first covert listening device that utilized passive techniques.

It was named “The Great Seal Bug” or “The Thing”

The Great Seal Bug

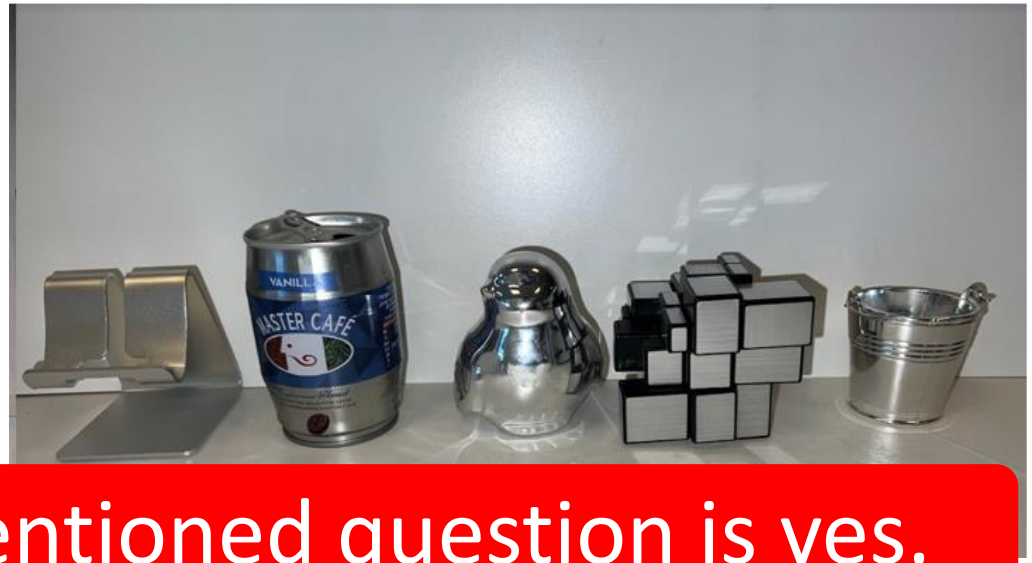
Can eavesdropper's exploit **passive, unaltered, shiny lightweight** objects as optical implants for the purpose of speech eavesdropping?

- A silver empty beverage can
- A silver smartphone stand
- SWAG, souvenirs and desktop ornaments

The Great Seal Bug

Can eavesdropper's exploit **passive, unaltered, shiny lightweight** objects as optical implants for the purpose of speech eavesdropping?

- A silver empty beverage can
- A silver smartphone stand
- SWAG, souvenired and desktop ornaments



The short answer to the abovementioned question is yes.

Throughout this talk we will show you how..

The Great Seal Bug

Can eavesdropper's exploit **passive, unaltered, shiny lightweight** objects as optical implants for the purpose of speech eavesdropping?

- A silver empty beverage can
- A silver smartphone stand
- SWAG, souvenired and desktop ornaments

We name these lightweight shiny object “Little Seal Bugs”

The Great Seal Bug

Can eavesdropper's exploit **passive, unaltered, shiny lightweight** objects as optical implants for the purpose of speech eavesdropping?

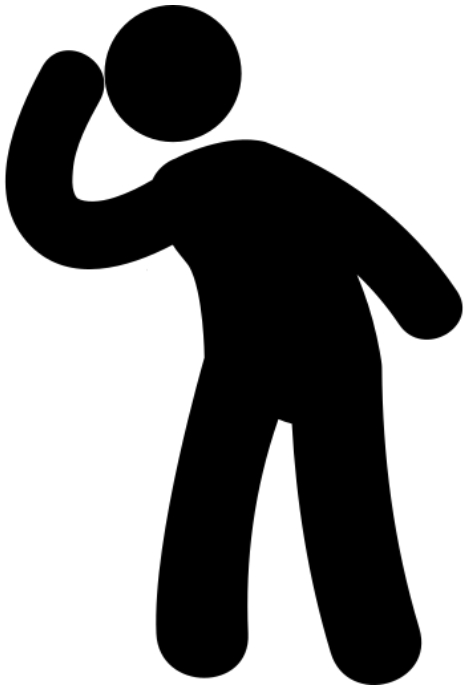
- A silver empty beverage can
- A silver smartphone stand
- SWAG, souvenired and desktop ornaments

Let’s review the needed background before we will dive into understanding the nature of the attack

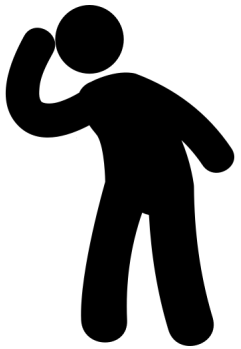
Background

Eavesdropping

The act of secretly recovering sound from a target/victim without his/her consent (Wikipedia).



Eavesdropping

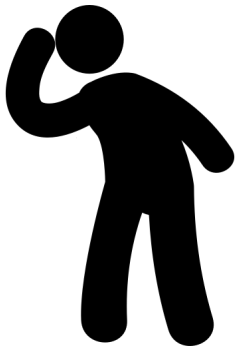


Sound eavesdropping can be applied as:

TEMPEST attacks

- Methods that rely on leakage from devices (e.g., EMR, power measurements).
- Require to obtain data using a dedicated sensor and exploit the correlation between sound processed by the device (e.g., speakers, headphones, microphone) and the device's leakage to recover the sound.
- Limited at recovering speech from virtual meetings.

Eavesdropping



Sound eavesdropping can be applied as:

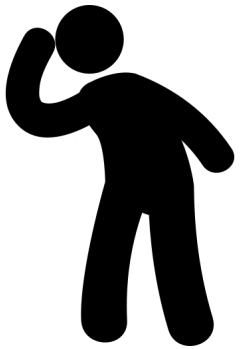
TEMPEST attacks

- Methods that rely on leakage from devices (e.g., EMR, power measurements).
- Require to obtain data using a dedicated sensor and exploit the correlation between sound processed by the device (e.g., speakers, headphones, microphone) and the device's leakage to recover the sound.
- Limited at recovering speech from virtual meetings.

Side Channel attacks

- Methods that exploit lightweight object as vibrating diaphragms (e.g., a bag od chips, a hanging light bulb).
- Require to obtain data using a dedicated sensor and exploit the correlation between the movement of the lightweight object to the sound near object
- Can be used to recover physical conversations.

Eavesdropping



Sound eavesdropping can be applied as:

TEMPEST attacks

- Methods that rely on leakage from devices (e.g., EMR, power measurements).
- Require to obtain data using a dedicated sensor and exploit the correlation between sound processed by the device (e.g., speakers, headphones, microphone) and the device's leakage to recover the sound.
- Limited at recovering speech from virtual meetings.

Side Channel attacks

- Methods that exploit lightweight object as vibrating diaphragms (e.g., a bag od chips, a hanging light bulb).
- Require to obtain data using a dedicated sensor and exploit the correlation between the movement of the lightweight object to the sound near object
- Can be used to recover physical conversations.

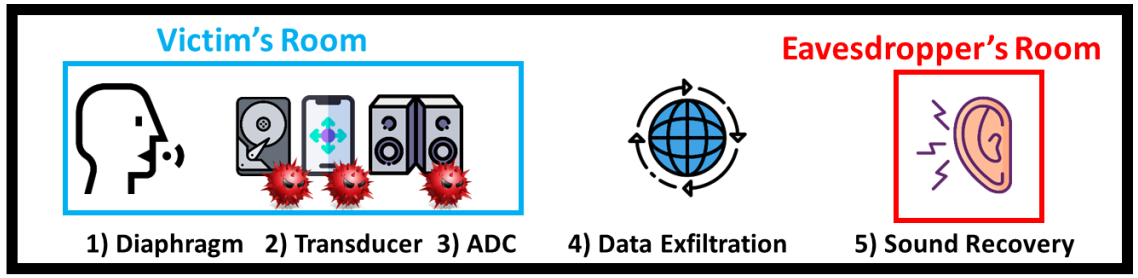
The Little Seal Bug Attack is a side-channel attack that exploits lightweight objects as diaphragms.

Related Work

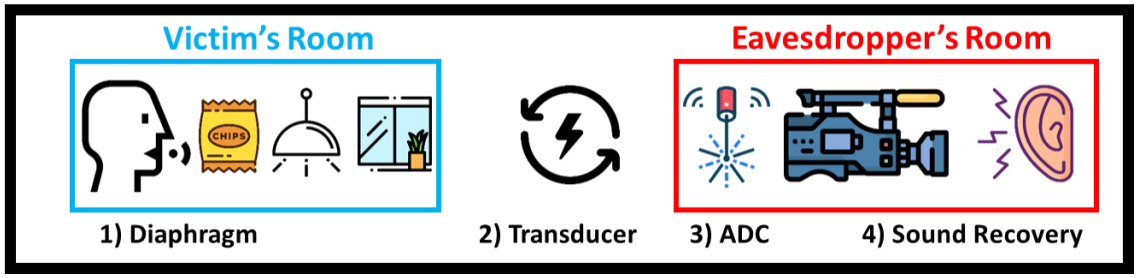
Eavesdropping Related Research

- In recent years, the scientific community has suggested various ways to recover sound.
- There are two categories of methods:

Internal Methods

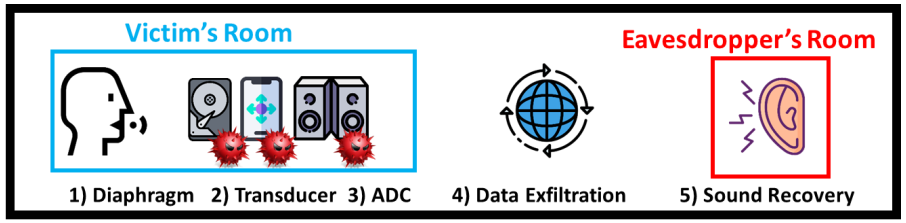


External Methods



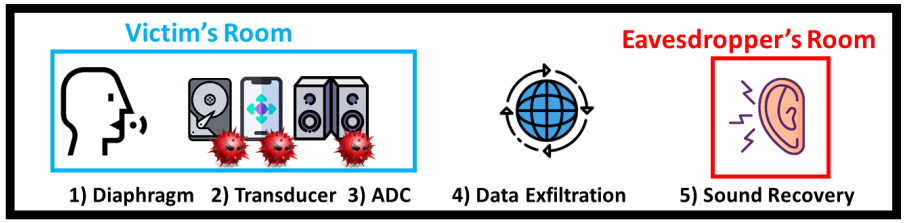
Internal Methods

- Methods that rely on data obtained by a device located in proximity to a victim



Internal Methods

- Methods that rely on data obtained by a device located in proximity to a victim



Motion Sensors

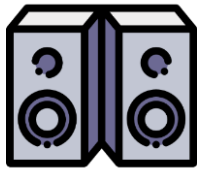
Gyroscope [1]

Accelerometer [2-4]

Output Devices

Speakers [5]

Vibration Motor [6]

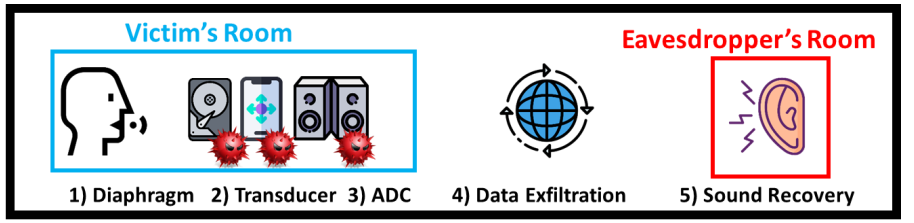


Misc.

Hard Drive [7]

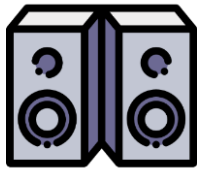
Internal Methods

- Methods that rely on data obtained by a device located in proximity to a victim



Motion Sensors
Gyroscope [1]
Accelerometer [2-4]

Output Devices
Speakers [5]
Vibration Motor [6]



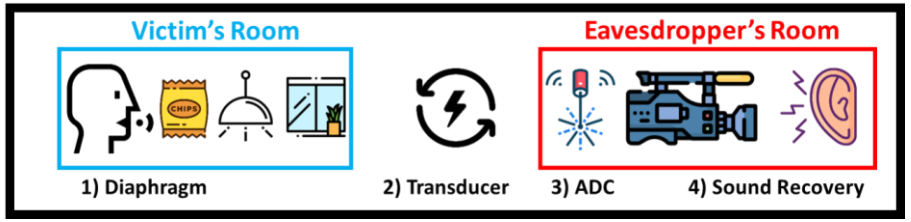
Misc.
Hard Drive [7]

From the eavesdropper's perspective, these methods

- Are **permission-less** - applications that implement these methods do not require any permissions to obtain data from the devices
- Require the attacker to **place a malware compromised device near a victim** to obtain and exfiltrate data

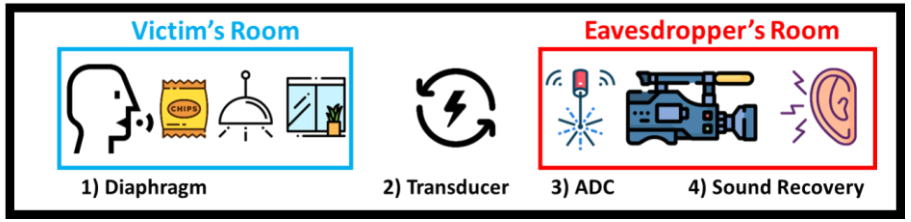
External Methods

- Methods that rely on data obtained by a device that is not located near a victim



External Methods

- Methods that rely on data obtained by a device that is not located near a victim



Laser Microphone [8]

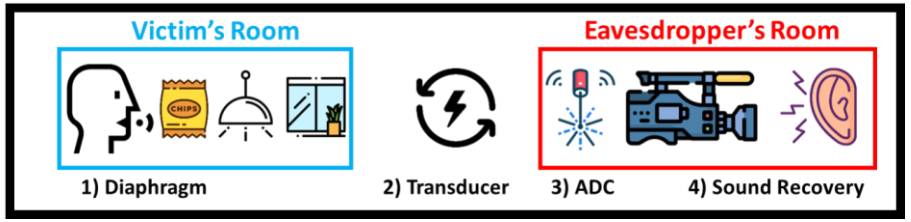
Uses a laser transceiver to recover sound by directing a laser beam at an object and analyzing the object's response to sound.

From the eavesdropper's perspective, this method

- Is **external** - does not require placing a malware compromised device near the victim
- Can be applied in **real-time**
- Is **active** - the laser beam can be detected by victims/organizations by using an optical sensor

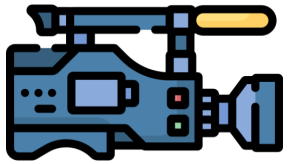
External Methods

- Methods that rely on data obtained by a device that is not located near a victim



Visual Microphone [9]

Uses a high-frequency video camera (~2000 FPS) to recover sound by analyzing the object's (e.g., a bag of chips) response to sound.

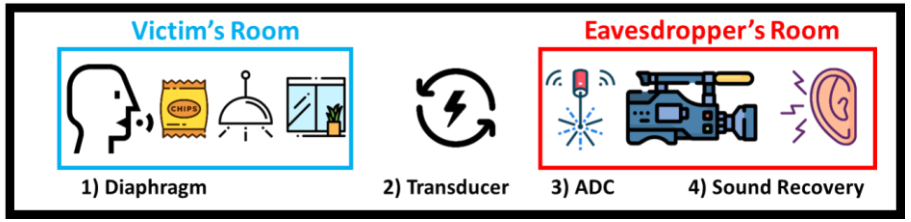


From the eavesdropper's perspective, this method

- Is **external** - does not require placing a malware compromised device near the victim
- Is **passive** - making its detection very difficult for victims/organizations
- Cannot be applied in **real-time** - requires heavy computational resources (it takes a few hours to reconstruct a few seconds of sound)

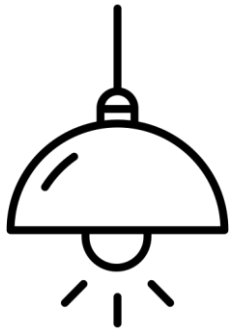
External Methods

- Methods that rely on data obtained by a device that is not located near a victim



Lamphone

Uses a photodiode to recover sound by analyzing a light bulb's response to sound.



From the eavesdropper's perspective, this method

- Is **external** - does not require placing a malware compromised device near the victim
- Is **passive** - making its detection very difficult for victims/organizations
- Can be applied in **real-time** – fast and easy to recover speech after obtaining the data
- Require **uncommon object** in the victim's room- not every conference or meeting room contain the bulbs that work with the threat model

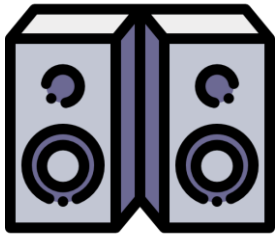
Summary of Related Work

Internal Methods

External Methods

Motion Sensors

Output Devices

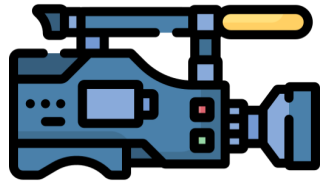


Misc.

Laser Microphone

Lamphone

Visual Microphone

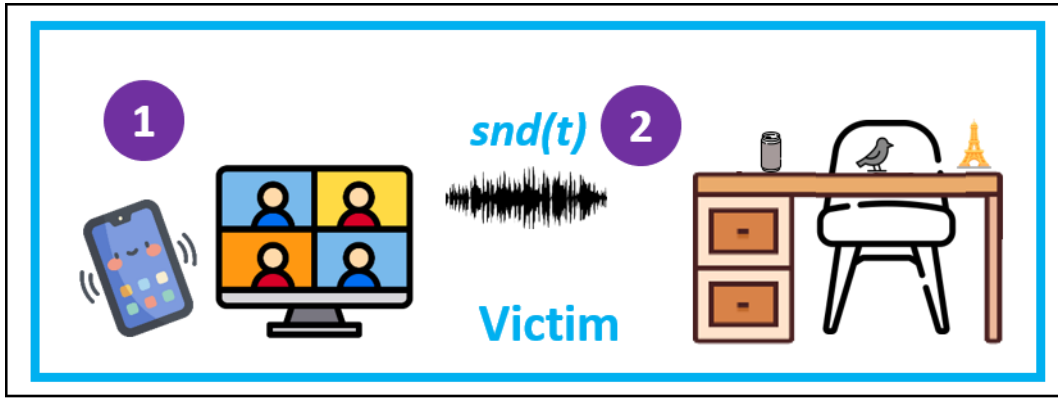


From the eavesdropper's perspective, each method is limited by one of the following:

- **Relies on a remotely controlled device** - eavesdroppers must compromise a device with a malware
- **Active** - which makes it easier for the victim to detect the use of the method
- **Cannot be applied in real-time** - because it requires heavy computational resources
- **Relies on an uncommon object in the victim's room**

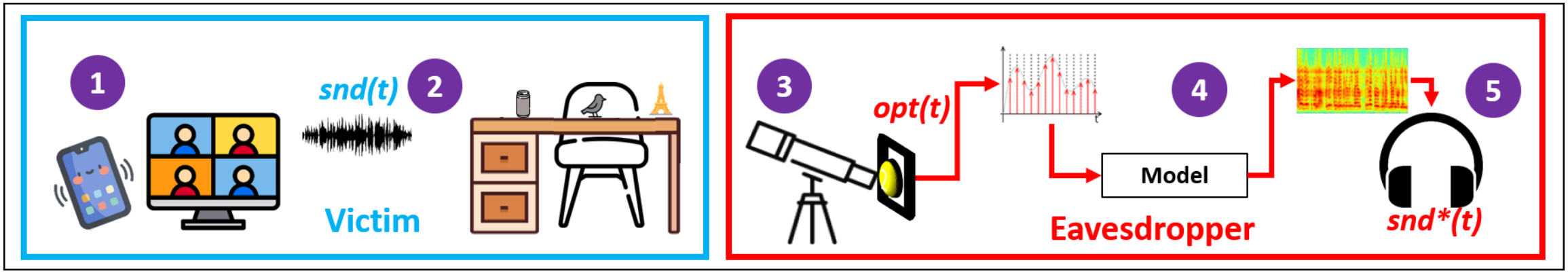
Threat Model

The Little Seal Bug Attacks



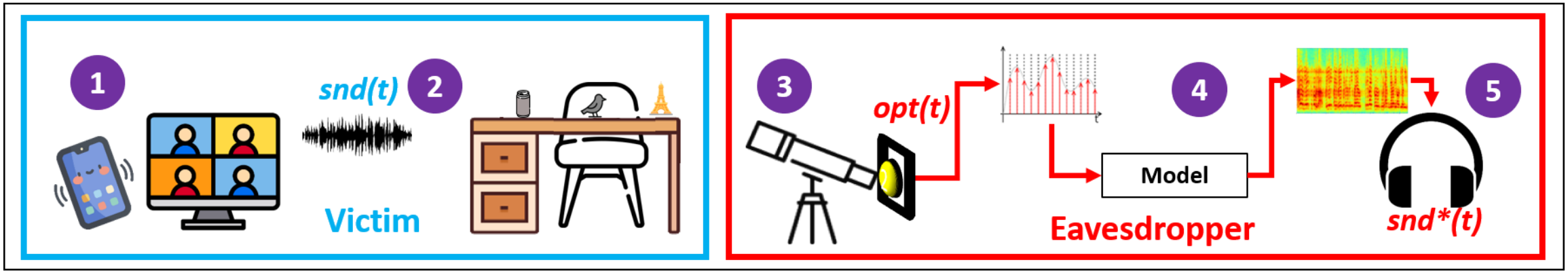
1. We assume that a victim makes the call/attends the meeting from an office/room that contains a little seal bug, in the form of a lightweight shiny object.
2. The sound $snd(t)$ from the victim's conversation creates fluctuations on the surface of a lightweight reflective object (e.g., an empty iced coffee can, desk ornaments) placed on a desk.

The Little Seal Bug Attacks



3. The eavesdropper directs a photodiode at the lightweight shiny object via a telescope.
4. The optical signal $opt(t)$ is sampled from the photodiode via an ADC.
5. An algorithm is used to recover the acoustic signal $snd*(t)$.

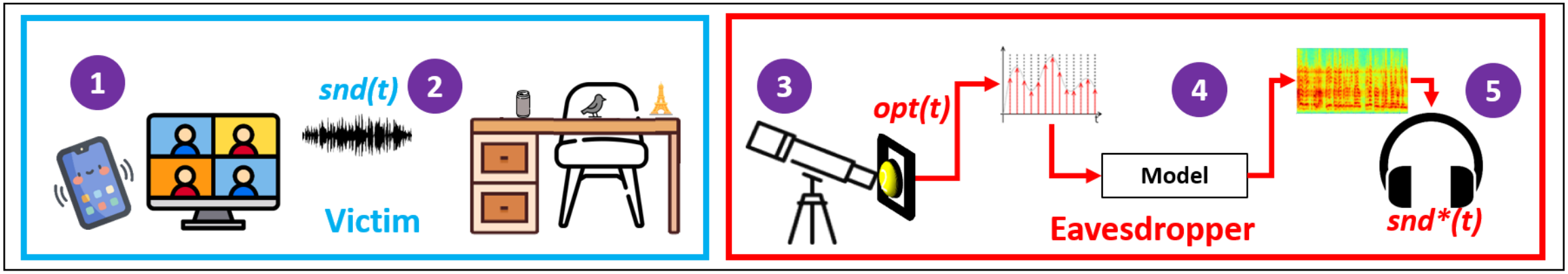
The Little Seal Bug Attacks



From an eavesdropper's perspective, The Little Seal Bug's threat model is

- **External**
- **Passive**
- Can be applied in **real-time**.
- Based on more commonly used objects (e.g., a smartphone stand, an empty beverage can, desktop ornaments, etc).

The Little Seal Bug Attacks



From an eavesdropper's perspective, The Little Seal Bug's threat model is

- **External**
- **Passive**

Let's analyze the physical phenomenon associated with The Little Seal Bug Attack.

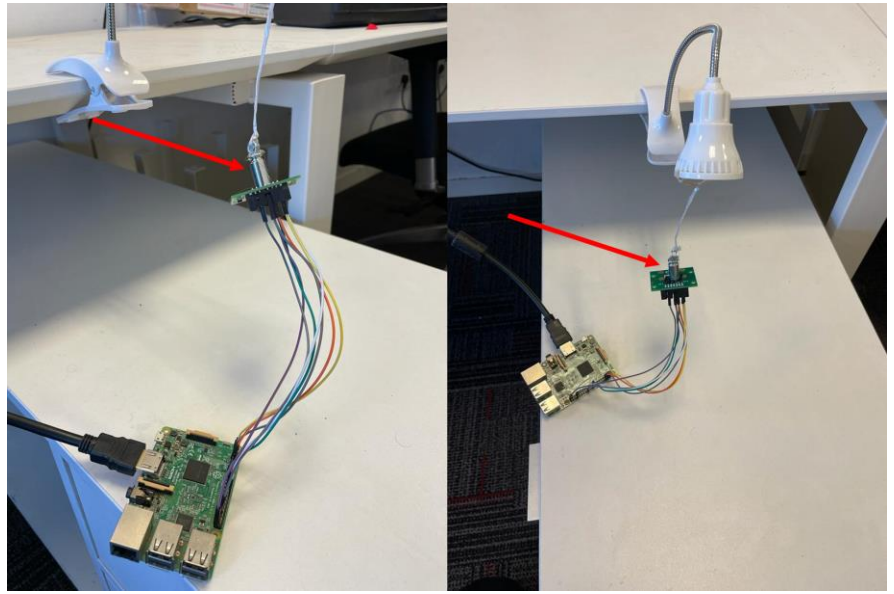
beverage can, desktop ornaments, etc).

Analysis

Measuring reflective object's Vibrations

Experiment

- We took a shiny weight (50 grams)
- We connected the weight to a gyroscope that was connected to Raspberry Pi 3.
- We played a frequency scan (200-1500 Hz) from speakers placed 10 cm from the weight (at 75 dB).

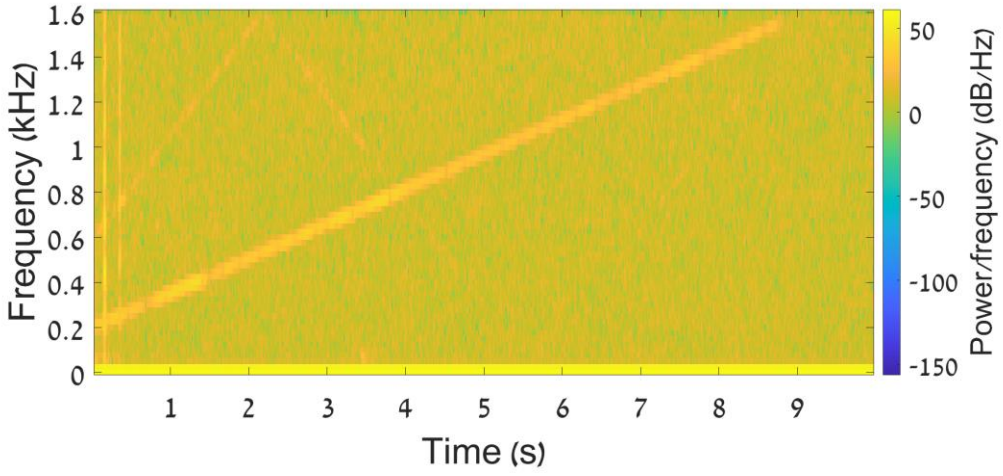


Measuring reflective object's Vibrations

Results

The figure presents a spectrogram extracted from the measurements obtained by the gyroscope.

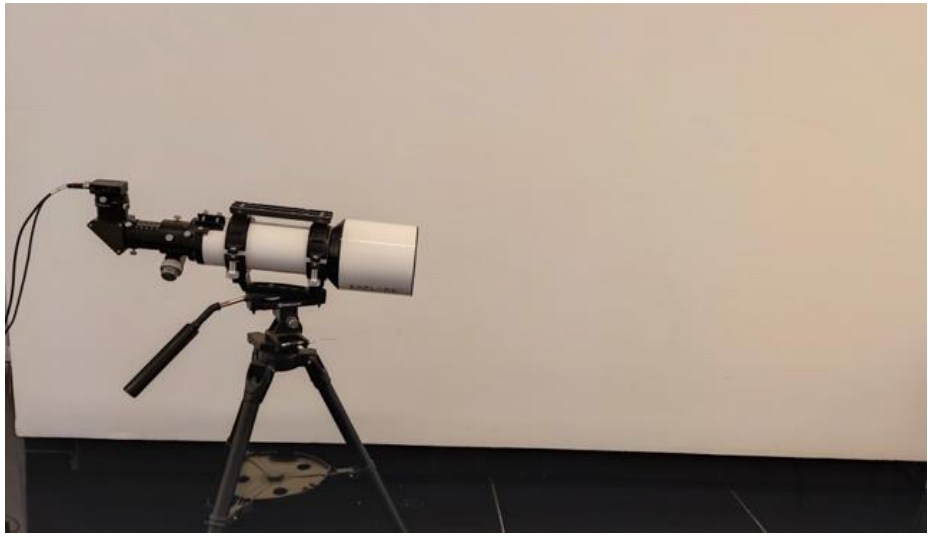
As can be seen from the spectrogram, the weight vibrates based on the nearby sound.



Analyzing light reflected from the object

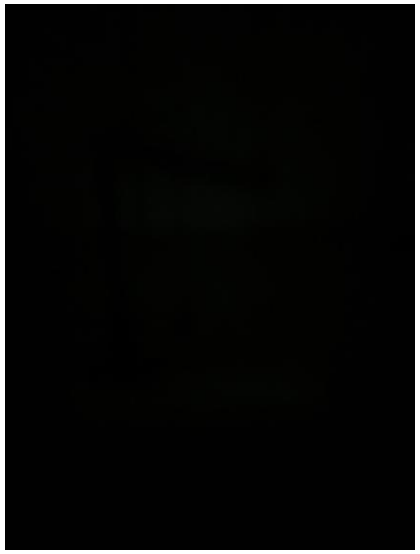
Experiment

- We directed a telescope at the weight.
- We mounted a photodiode (the Thorlabs PDA100A2) to the telescope and used ADC to sample it.
- We played an audio file of a frequency scan (100-2000 Hz) via speakers which were placed **10 cm** from the weight (**at 75 dB**).
- We obtained the optical signal via the photodiode when the (1) lights in the room were on, (2) weight was covered with black tape, and (3) the lights in the room were off.



Lights in the room were on

Weight is covered with black tape

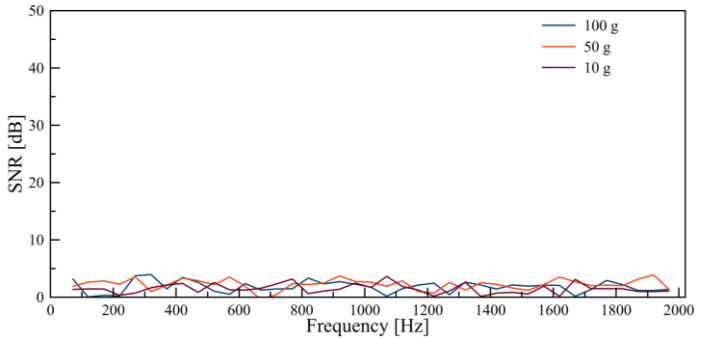


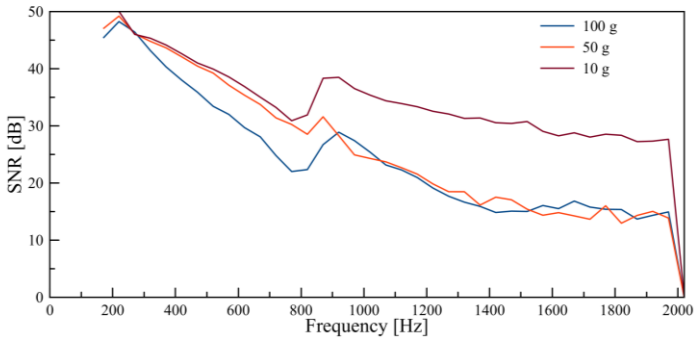
Lights in the room were off

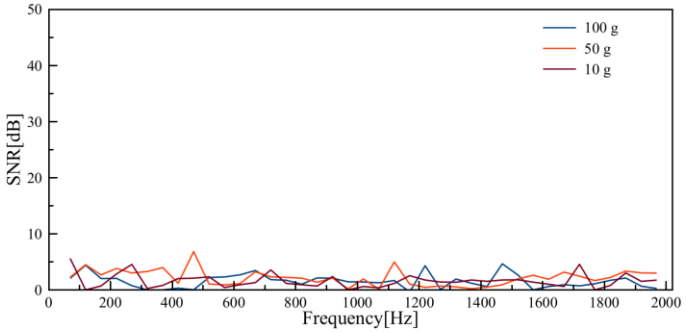
Analyzing light reflected from the object

Results

We calculated the SNR obtained from the optical measurements







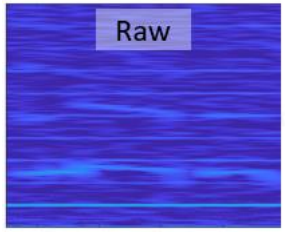
The sound that was played near the weight can be recovered only when the lights are on and the weight reflects light (does not covered in black tape)

A risk of speech recovery to a subject exists only if lights are on and a nearby object reflects light. If one of these conditions is not satisfied, sound cannot be recovered.

Isolating the sound from the optical signal

Isolating the sound from the optical signal

We recover speech using the following steps:

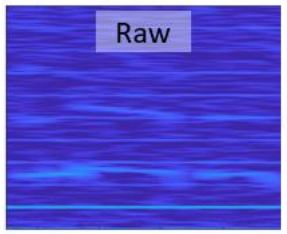


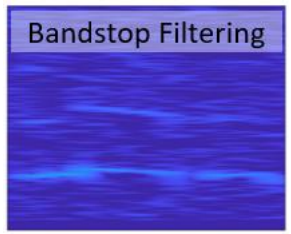
Isolating the sound from the optical signal

We recover speech using the following steps:

- **Filtering Side Effects**

The optical signal consists of side effects that are not the result of the sound played, e.g., the harmonics of 100 Hz (200 Hz, 300 Hz, etc.).
We filter these frequencies using bandstop filters.



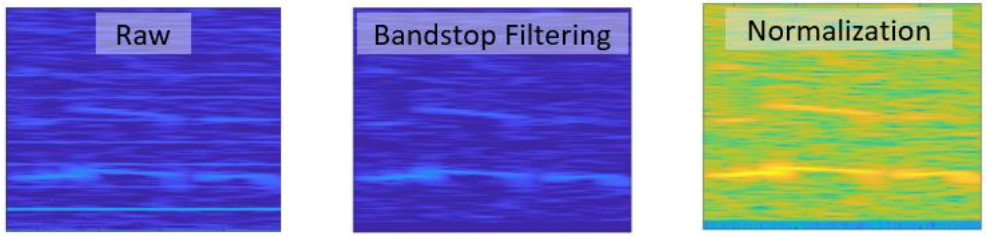


Isolating the sound from the optical signal

We recover speech using the following steps:

- Filtering Side Effects
- **Normalizing**

We enhance the speech signal by normalizing the values of $opt\ (t)$ to the range of [-1,1].

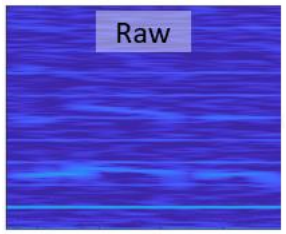


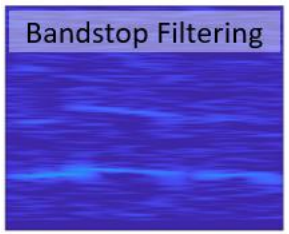
Isolating the sound from the optical signal

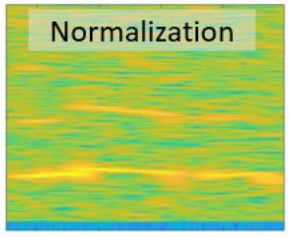
We recover speech using the following steps:

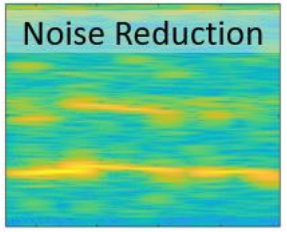
- Filtering Side Effects
- Normalizing
- **Noise Reduction**

  We reduce the noise by applying spectral subtraction, an adaptive technique used to denoise single-channel speech without any prior knowledge/assumptions on the measurements' distribution







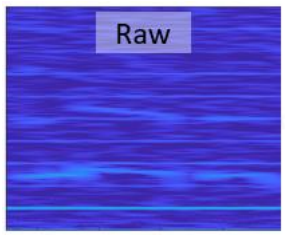


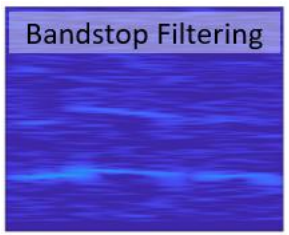
Isolating the sound from the optical signal

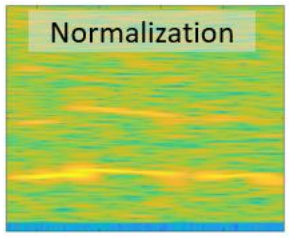
We recover speech using the following steps:

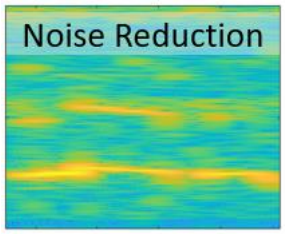
- Filtering Side Effects
- Normalizing
- Noise Reduction
- **Equalizer**

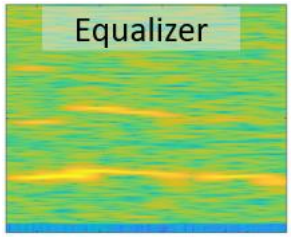
We use an equalizer to amplify the response of weak frequencies.











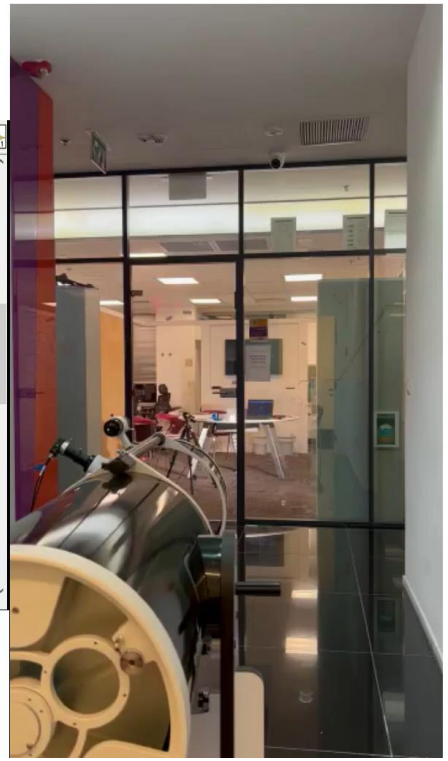
Evaluation in a Real Setup

Experimental Setup

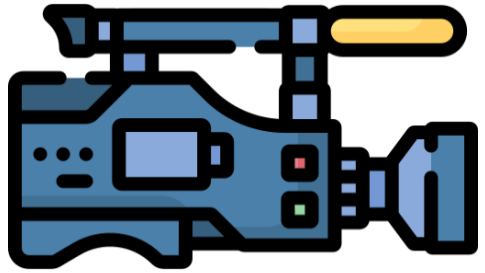
Real Time Demonstration

We played two sine waves (280 Hz and 380 Hz) from the speakers.
One sine wave at each time.

Real Time Demonstration



Comparison to Visual Microphone



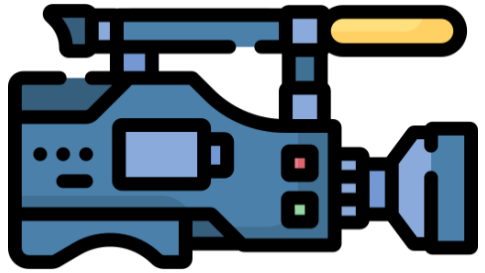
We evaluated The Little Seal Bug Attack under the same experimental setup of Visual Microphone.

Quick reminder:

Visual microphone was presented in 2014 by a group from MIT.

They demonstrated speech recovery by analyzing the vibrations of a bag of chips using a high-frequency video camera (2200 FPS).

Comparison to Visual Microphone

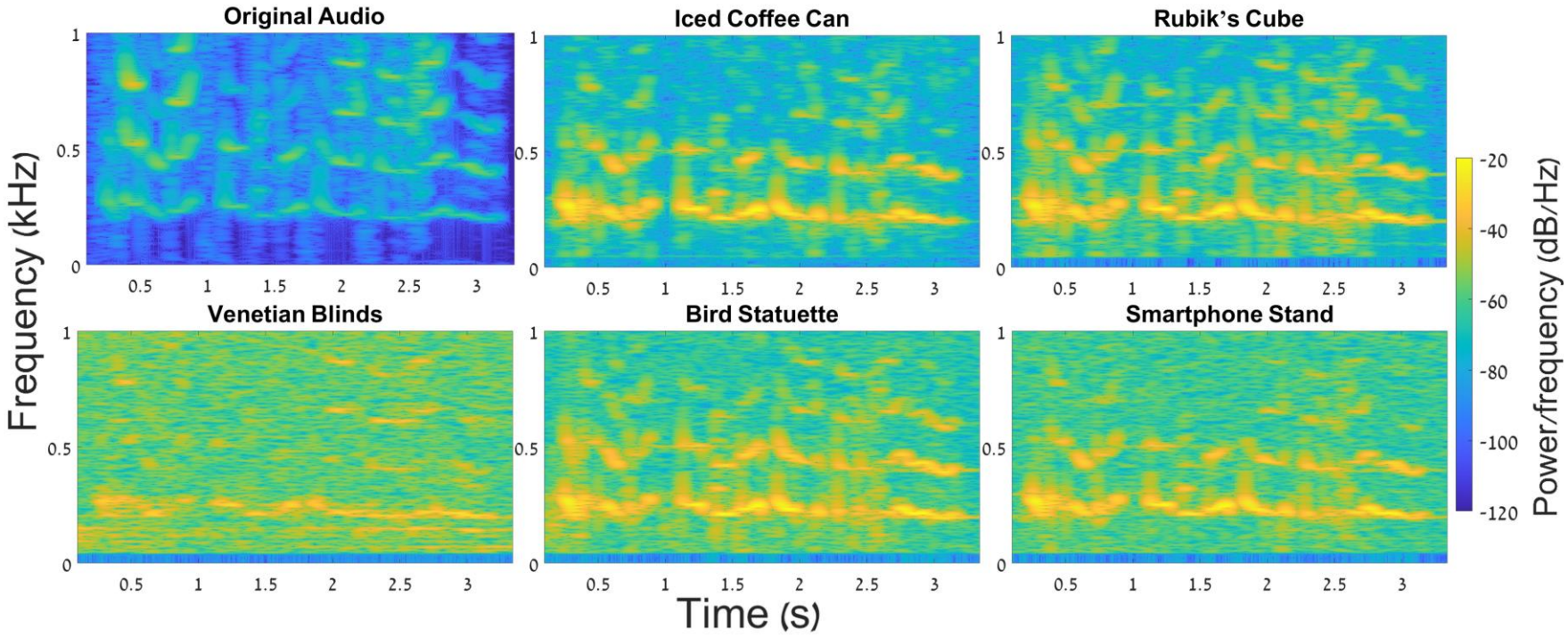


We replicated the experimental setup used in the visual microphone study as follows:

- We placed the speakers on a dedicated stand **5 cm from various shiny objects**.
- We played the same **six sentences** from the TIMIT repository recovered by the visual microphone.
- The volume level the speakers played at **95dB** (very high).
- We placed the eavesdropping equipment **2.5 meters** from the lightweight reflective object.

Comparison to Visual Microphone

The spectrogram of the original sentence and the recovered sentence "She had your dark suit in greasy wash water all year" from various objects



And now we will proceed to listen to the recordings of the recovered sound

mccs0, sa1: “She had your dark suit in greasy wash water all year”

Original

mccs0, sa1: “She had your dark suit in greasy wash water all year”

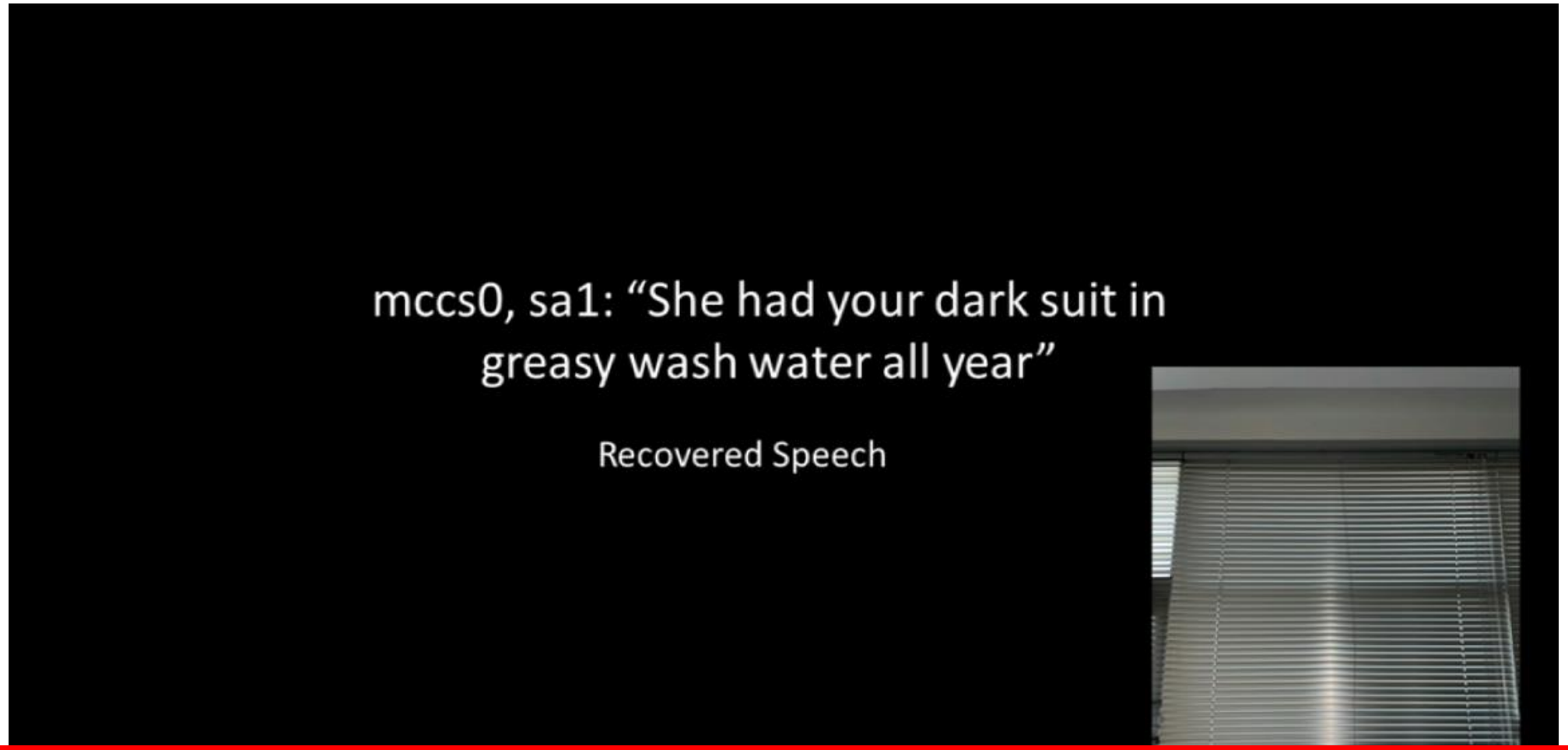
Recovered Speech

The next sentence was recovered from Venetian Blinds.

mccs0, sa1: “She had your dark suit in greasy wash water all year”

Recovered Speech

Venetian blinds, a piece of equipment that is intended to increase a subject’s privacy, can be exploited to eavesdrop on the subject.



Interestingly, the Little Seal Bug Attack is capable of recovering speech in real-time at the same quality as Visual Microphone.

Comparison to Lamphone

We evaluated The Little Seal Bug Attack under the same experimental setup as Lamphone.

<u>Quick reminder</u>:

Lamphone was presented in 2020 by our group at BlackHat USA.

We demonstrated speech recovery by analyzing the vibrations of a hanging light bulb using a photodiode

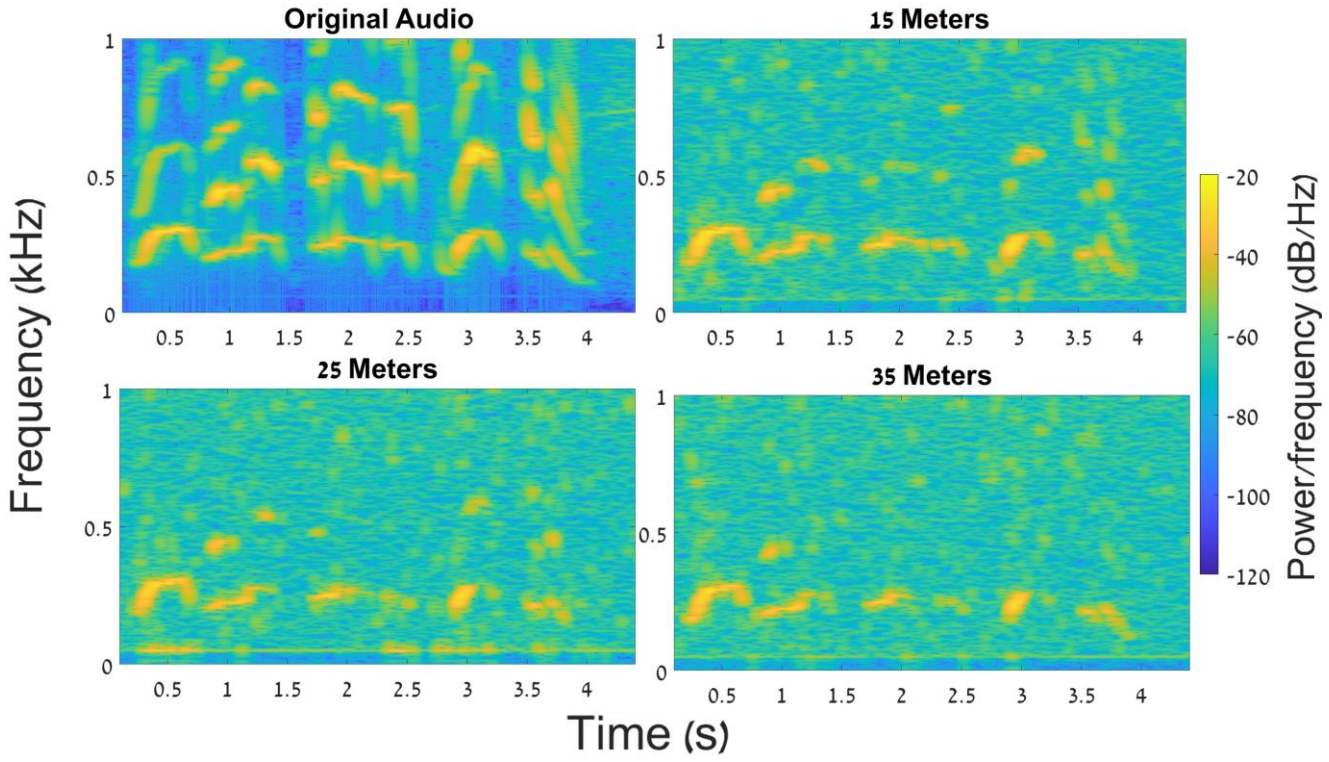
Comparison to Lamphone

We replicated the experimental setup used in the Lamphone study as follows:

- We placed the eavesdropping equipment at **various distances (15,25,35 meters)** from three objects used in this experiment.
- The speakers were placed **at a distance of 25 cm** from the reflective objects.
- We played a statement made by former President Donald Trump via the speakers at the **volume level of a virtual meeting (75dB)**.

Comparison to Lamphone

The spectrogram of the original statement and the recovered statement from the Rubik's cube from various distances:



And now we will proceed to listen to the recordings of the recovered sound

We will make America great again

Original

Takeaways

Takeaway 1: Many shiny lightweight objects can serve as optical implants that can be exploited by eavesdroppers to recover sound.

Takeaways

The area of optical speech eavesdropping has advanced significantly in the last seven years:

- Visual Microphone (high-frequency video camera)– 2014
- Lamphone (photodiode) – 2020
- LidarPhone (LiDAR)– 2021
- The Little Seal Bug (photodiode)– 2020

Takeaway 2: We expect that more optical eavesdropping methods that rely on optical sensors will be demonstrated in the next few years.

Takeaways

Fact 1: Photodetectors are integrated into most smartphones nowadays.

Fact 2: Smartphone manufacturers continue to increase the smartphone sampling rate (in some Android devices, the system supports a sampling rate of 500 Hz).

Fact 3: Obtaining data from the photodetector does not require a user's permission.

Takeaway 3: We might see an implementation of a new type of malware and compromised applications for speech eavesdropping via a smartphone's light sensor in the near future.

Thank you for attending this talk!

Questions?

www.nassiben.com/little-seal-bug