The Little Seal Bug: Optical Sound Recovery from Lightweight Reflective Objects

Ben Nassi, Ras Swissa, Yuval Elovici, Boris Zadov
Ben-Gurion University of the Negev
{nassib, razsw, elovici, zadov}@post.bgu.ac.il

***Abstract*—In this paper, we introduce "the little seal bug" attack, an optical side-channel attack which exploits lightweight reflective objects (e.g., an iced coffee can, a smartphone stand, a souvenir) as optical implants for the purpose of recovering the content of a conversation. We show how fluctuations in the air pressure on the surface of a shiny object can be exploited by eavesdroppers to recover speech passively and externally, using equipment not likely to be associated with spying. These air pressure fluctuations, which occur in response to sound, cause the shiny object to vibrate and reflect light which modulates the nearby sound; as a result, seemingly innocuous objects like an empty beverage can, desk ornament, or smartphone stand, which are often placed on desks, can provide the infrastructure required for eavesdroppers to recover the content of a victim's conversation held when the victim is sitting at his/her desk. First, we conduct a series of experiments aimed at learning the characteristics of optical measurements obtained from shiny objects that reflect light, by using a photodiode to analyze the movement of a shiny weight in response to sound. Based on our findings, we propose an optical acoustical transformation (OAT) to recover speech from the optical measurements obtained from light reflected from shiny objects. Finally, we compare the performance of the little seal bug attack to related methods presented in other studies. We show that eavesdroppers located 35 meters away from a victim can use the little seal bug attack to recover speech at the sound level of a virtual meeting with fair intelligibility when the victim is sitting at a desk that contains a reflective object.**

I. Introduction

"The Great Seal Bug" [1], a.k.a., "the Thing," was the first covert listening device that utilized passive techniques to transmit an audio signal for the purpose of speech eavesdropping.[1] It consisted of a passive device that was concealed inside a gift (a picture of an eagle) which was given to the United States Ambassador to the Soviet Union from the Soviet Union in 1945. The concealed passive device, which is considered a predecessor of radio frequency identification (RFID) technology, became an operative listening device when it was activated by the Soviets who "illuminated" it using electromagnetic energy from an external source. Since the device was passive and considered quite innovative at the time (eight decades ago), it took the Americans six years to determine its real purpose as a listening device when it was accidentally found by a British radio operator at the British embassy.

Well-known incidents[2] and various studies [2–11] published over the years have shed light on the practicality of speech eavesdropping. The incidents and studies showed how far motivated entities are willing to go in order to recover the content of speech. Moreover, the incidents proved that compromised devices can be used for eavesdropping via non-acoustic data obtained from: (1) an integrated sensor [2–7, 9–11] (e.g., using a smartphone's motion sensor data, using a robotic vacuum cleaner's LiDAR data) or (2) emanations from the device [8, 10–13] (e.g., electromagnetic radiation (EMR) emitted from a PC's hard disk and earphones and light emitted from speakers). In order to prevent eavesdroppers from recovering the content of conversations from compromised devices, organizations implement policies aimed at preventing employees and guests from using their electronic devices on their premises.

As a result, eavesdroppers have sought new methods for recovering speech that do not rely on a compromised device, and in recent years, several methods have been demonstrated (e.g., (1) the visual microphone [14], (2) Lamphone [15], and the laser microphone [16]). While the studies presenting these methods improved understanding regarding the privacy risks posed by objects located in proximity to potential victims, the proposed methods suffer from at least one of the following disadvantages: (1) some methods are limited to recovering speech at a high volume (+85 dB), which limits their effectiveness at recovering speech from virtual meetings (the sound level of such meetings is typically 75 dB); (2) some methods rely on spying equipment, which limits their use in countries that restrict the sale of this equipment; (3) some methods require an active laser beam to be directed at objects located near the target, a fact that increases the likelihood of detection, and (4) some methods rely on the presence of a hanging light bulb, a form of lighting which is not commonly used in offices today.

In this paper, we present "the little seal bug," an optical eavesdropping method aimed at recovering speech from lightweight shiny objects that reflect light. We show how eavesdroppers can exploit lightweight shiny objects (little seal bugs) that reflect light and serve as optical implants, in order to recover the content of conversations. This is done by analyzing optical data obtained by a photodiode directed at the objects; such objects are often placed on desks for personal use (e.g., a smartphone stand, an iced coffee can) or decoration (e.g., souvenirs). Such lightweight reflective objects

[1] https://en.wikipedia.org/wiki/The_Thing_(listening_device)

[2] https://en.wikipedia.org/wiki/Covert_listening_device

can be exploited by eavesdroppers to recover speech from the minuscule vibrations that occur when sound (air pressure) hits the object's surface. First, we analyze the movement of various shiny objects and show that their vibrations can be captured by a photodiode. Based on our findings, we suggest a sound recovery model that recovers speech from light obtained from reflective objects. Finally, we compare the proposed little seal bug attack to three state-of-the-art methods (visual microphone [14], Lamphone [15], and the hard drive of hearing [8]). We show that the proposed attack can be used to recover the content of a victim's conversation held when the victim is seated at a desk, with fair intelligibility from a distance of 35 meters.

In this paper we make the following contributions: (1) We raise awareness regarding the fact that lightweight shiny objects can be exploited as optical implants for the purpose of recovering speech (hence their name "little seal bugs"). Such objects, which may be purchased by potential victims for personal use/decoration or received as swag at conferences, are often placed on desks. By virtue of their presence on desks, such objects may behave as diaphragms and vibrate in response to conversations (e.g., virtual meetings and phone calls) that take place at the desk. Moreover, when light is reflected from their surface, they modulate the speech of the conversation optically, a fact that can be exploited to recover the content of the conversation using a remote photodiode. (2) We show that the issues associated with speech recovery from light are more serious and widespread than initially thought based on prior research that focused on recovering speech directly from objects/devices that emit light (e.g., a hanging light bulb [15] and the power LED of speakers [13]). We show that eavesdroppers can indirectly convert light to speech from offices that do not contain hanging light bulbs or speakers that leak information from the power LED, by analyzing optical measurements obtained from objects that are not electrical and do not emit any light.

The rest of the paper is structured as follows: In Section II, we review existing methods for eavesdropping. In Section III, we present the threat model. In Section IV, we analyze the response of a shiny weight to sound. We present an optical acoustical transformation (OAT) for recovering sound in Section V, and in Section VI, we evaluate the little seal bug attack's performance on the task of recovering sound. We discuss the limitations of the attack and suggest future work directions in Section VII.

II. Related Work

In this section, we review related work in the area of speech eavesdropping. Speech eavesdropping has been used by clandestine agencies for many years. Before the Internet era, the most popular approach for eavesdropping speech was to conceal a covert listening device in a strategic location by using a supply chain attack. By concealing a bug inside a covert device placed in a victim's office, the eavesdropper could recover the content of the victim's conversations. Many covert listening devices were developed and concealed in mementos or gifts (e.g., pictures) and legitimate devices (e.g., typewriters) placed in embassies and other diplomatic posts for the purpose of diplomatic espionage.[2] An incident demonstrating the enormous effort clandestine agencies are willing to invest in developing and implanting such devices is "the Great Seal Bug" (a.k.a., "the Thing"), which is considered a predecessor of radio frequency identification (RFID) technology and was used by the Soviets as a listening device three decades before it was patented in the US for commercial use [1].

Since the beginning of the Internet of Things (IoT) era, the trend of eavesdropping speech using supply chain attacks has changed to eavesdropping speech using data obtained from a sensor of an Internet-connected device by a compromised application. In order to protect users from speech eavesdropping performed via a compromised application, a permission-based mechanism was integrated into the operating systems of smartphones and PCs which requires the user's authorization/permission to obtain acoustic measurements via the integrated microphone. The integration of this mechanism has limited the ability of a compromised application to obtain acoustic data without the user's consent. This mechanism has prevented various compromised applications that are disguised as legitimate applications (e.g., a flashlight) from obtaining the needed permission to obtain acoustic measurements for their real undeclared purpose of speech eavesdropping.

The permission-based mechanism requires eavesdroppers to apply alternative methods that can bypass the mechanism (i.e., to recover speech without a user's consent), and in recent years, many innovative methods that use non-acoustic data to recover speech from compromised IoT devices have been demonstrated [2–8]. The methods involved: (1) obtaining motion sensor data from a smartphone [2–5], (2) reprogramming a computer's audio port from output to input [6], (3) inverting the process of a smartphone's vibration motor [7], (4) analyzing magnetic data obtained from a PC hard disk head [8], and (5) obtaining optical data from the LiDAR of a robot vacuum cleaner [9]. These methods have demonstrated that various vibrating objects can effectively become diaphragms in response to sound. As a result, various transducers (i.e., sensors which convert the diaphragm's vibrations to measurements) that are co-located with the diaphragms in devices can be exploited by eavesdroppers to convert the vibrations of the device to measurements that reflect the device's vibrations (e.g., a motion sensor of a smartphone) [17]. These methods pose a serious threat to privacy, because non-acoustic data is not commonly associated with speech eavesdropping; as a result, applications/programs that implement such methods do not require a user's permission to obtain this data, and they do not raise any suspicion from the user/operating system regarding their real use (i.e., eavesdropping). However, from an eavesdropper's perspective, the two primary disadvantages of these methods are that (1) they require the eavesdropper to compromise a device (with malware) located near the victim (who serves as the sound source) in order to obtain data and exfiltrate it to the eavesdropper, and (2) many privacy-aware organizations prohibit their employers and guests from using personal devices on the organization's premises.

The need to compromise a device with malware has in-

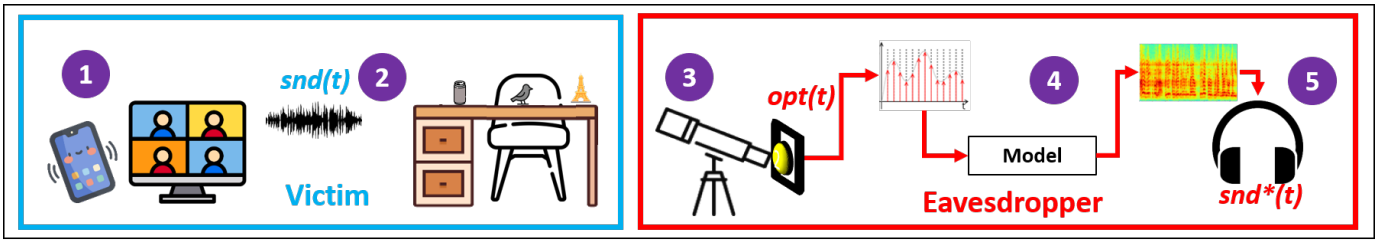

Fig. 1. The little seal bug's threat model: The sound $snd(t)$ from the victim's conversation (1) creates fluctuations on the surface of a lightweight reflective object, e.g., an empty iced coffee can and desktop ornaments (e.g., statuettes of a bird and the Eiffel tower), that is placed on a desk (2). The eavesdropper directs a photodiode at the object via a telescope (3). The optical signal $opt(t)$ is sampled from the photodiode via an ADC (4) and processed, using an algorithm to recover the acoustic signal $snd^*(t)$ (5).

creased eavesdroppers' interest in external methods for speech recovery that do not require obtaining measurements from a compromised device. In external methods, the diaphragm (the vibrating object) is not co-located with the transducer (the sensor which is used to obtain the measurements of the diaphragm which are later converted to acoustic measurements). A few TEMPEST attacks have used novel techniques to recover speech from non-compromised devices by exploiting the correlation between the information delivered/processed by devices and their emanations. Several studies have proposed methods that use a remote universal software radio peripheral (USRP) to recover the content of conversations; the proposed methods exploited: (1) EMR emitted from earphones and speakers [12], and (2) a side effect of VoIP compression algorithms (the variable bitrate) which leaks information regarding the content of the speech via the bitrate of the encrypted traffic [18–20]. In a recent study, the authors were able to recover speech by directing a photodiode at the power LED of speakers to obtain optical measurements and exploiting the correlation between the power consumed by the speakers and intensity of their power LED [13]. These studies demonstrated unique methods that exploit the emanations of a device, to recover the content of virtual meetings, but they cannot be used to recover the content of physical meetings.

Over the years, several side-channel attacks aimed at recovering speech from physical meetings that do not necessitate the use of malware have been introduced [10, 11, 14–16]. Two studies presented external methods that recover sound by exploiting the physical characteristics of Wi-Fi signals sent by a router [10, 11] using a remote USRP. This was done by exploiting the signal strength indication and channel state information (CSI) of the Wi-Fi signals sent by a router that was vibrating according to sound produced by nearby speakers. Other studies [14–16] presented external optical sound recovery methods that rely on data obtained using optical sensors. The laser microphone [16, 16] is a well-known method that recovers sound using a laser transceiver which directs a laser beam through a window into a target room; the laser beam is reflected off an object and returned to the transceiver which then converts the beam to an audio signal. The visual microphone [14] recovers sound by analyzing the vibrations of material inside the victim's room (e.g., a bag of chips, water) using video obtained from a high-speed video camera (2200 FPS) to recover speech. Lamphone [15] uses a remote electro-optical sensor to recover sound by exploiting the vibrations of a hanging light bulb; the vibrations cause a remote electro-optical sensor to capture optical changes which are associated with sound waves produced by nearby speakers. While these methods [14–16] pose a great threat to privacy, from an eavesdropper's perspective, they are limited in one of the following ways: they rely on (1) a very high sound level (over 85 dB, on average) which is beyond the sound level of speech and virtual meetings (e.g., [10, 11, 14]), (2) active sensors that use a laser beam (e.g., [16]), a fact that increases the likelihood of detection (compared to passive sensors), (3) hanging and desktop light bulbs, which are not commonly used in office settings today (e.g., Lamphone [15]), or (4) specialized equipment for spying [16], a fact that may limit their use in countries which limit the sale of such equipment to, e.g., police departments.

III. Threat Model

In this section we describe the threat model and compare it to methods presented in other studies.

Assumptions. We assume a victim (person) that is located in his/her house and seated at a desk exchanging/sharing information in a phone call or virtual meeting. We assume that the 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, which is located up to 50 cm away from the victim, a reasonable distance from an individual seated at a standard desk (the depth of a standard desk is 60 cm). We note that the little seal bug could be an object purchased by the victim for personal use (e.g., a beverage can, a smartphone stand) or received as a gift (e.g., a desk ornament received as swag from a conference). We consider the eavesdropper to be a malicious entity interested in recovering speech from the victim's conversation by performing the little seal bug attack. The eavesdropper could use the recovered information for various malicious purposes, including spying, shaming, blackmailing, or to gather business intelligence. We assume that the eavesdropper is located within 35 meters of the target room. The eavesdropper could be: (1) a person located in a room in an adjacent building (e.g., a nosey neighbor), or (2) a person in a nearby car (e.g., a private detective). We consider this threat to be highly likely in the COVID-19 era due to the increased number of personal and business meetings being held in unsecured home environments.

Components. The little seal bug consists of the following primary components: (1) Telescope - This piece of equipment

is used to focus the field of view on the little seal bug from a distance. (2) Photodiode - This sensor is mounted on the telescope and consists of a semiconductor device that converts light into an electric current. The current is generated when photons are absorbed in the photodiode. Photodiodes are used in many consumer electronic devices (e.g., smoke detectors, medical devices). (3) Sound recovery model - This model receives an optical signal as input and outputs the recovered acoustic signal. The eavesdropper can implement such a model with dedicated hardware (e.g., using capacitors, resistors, etc.). Alternatively, the eavesdropper can use an ADC to sample the photodiode and process the data digitally using a laptop; in this study, we use the digital approach.

The conversation held in the victim's room creates sound $snd(t)$ that results in fluctuations in the air pressure on the surface of the little seal bug (i.e., the shiny object). These fluctuations cause the object to vibrate, resulting in a pattern of displacement over time that the eavesdropper measures with the photodiode, which is directed at the object via the telescope. The analog output of the photodiode is sampled by the ADC to a digital optical signal $opt(t)$. The eavesdropper then processes the optical signal $opt(t)$, using an audio recovery algorithm, to an acoustic signal $snd^*(t)$. Fig. 1 outlines the threat model.

In general, microphones rely on three components (a diaphragm, transducer, and ADC). In the little seal bug attack, the shiny object serves as a diaphragm, which vibrates when sound waves hit its surface. The transducer is the remote photodiode, which is used to convert the vibrations of the lightweight shiny object (the diaphragm) to optical measurements using the emitted light of the target room which is reflected on the surface of the shiny object. An ADC is used to convert the electrical signal to a digital signal (as in standard microphones).

Significance. The significance of the little seal bug attack with respect to methods presented in other studies is that the little seal bug: (1) is an external method that relies on a line of sight between the photodiode and the little seal bug (unlike other methods that require eavesdroppers to compromise a device located in physical proximity of the victim in order to obtain data and exfiltrate it [2, 4–8, 10, 11]), (2) recovers intelligible audio signals, so it is not limited to classifying isolated words that appear in a precompiled dictionary (unlike [2, 4, 5, 10]), and (3) can be used to recover the content of physical and virtual meetings (in contrast to TEMPEST attacks that can only be used to recover the content of virtual conversations [12, 13, 18–20]).

The methods most related to ours are the laser microphone, the visual microphone [14], Lamphone [15], and the Glowworm attack [13], all of which are also passive optical methods for sound recovery. Unlike those methods, the little seal bug attack can recover speech: (1) from reflections of light on objects that are not electronic (as opposed to Lamphone [15] and the Glowworm attack [13] which recover sound from electronic devices that emit light, respectively speakers and light bulbs), (2) from objects which are more commonly placed on desks (e.g., iced coffee can, a smartphone stand) than light bulbs, (3) at a sound level of 75 dB, the average volume of a phone call or virtual meeting (as opposed to the visual microphone [14] and other methods [8, 10, 11, 14] that are limited to recovering speech at higher volumes), (4) using a photodiode, a passive sensor that does not provide any indication regarding its use (as opposed to the laser microphone [16] which relies on a laser transceiver) and is composed of hardware (ADC, photodiode) that is not associated with spying (as opposed to the laser microphone [16]).

IV. Reflective Objects As Microphones

In this section, we describe the series of experiments we performed which were aimed at: (1) explaining why lightweight reflective objects can be used to recover sound, and (2) gaining increased understanding of the characteristics of the optical measurements obtained by a photodiode when shiny objects vibrate in response to sound.

A. The Physical Phenomenon

In this experiment, we measure the vibrations of an object that occur when sound waves hit its surface.

Experimental Setup: We used a wire to attach a shiny weight (50 grams) purchased from Amazon[3] to the upper edge of a stand. We attached a gyroscope [21] to the bottom of the weight and connected the gyroscope to a Raspberry Pi 3. We sampled the gyroscope via the Raspberry Pi at 4000 Hz (see Fig. 2). We created an audio file of a frequency scan (chirp/sweep) from 200-1500 Hz and played the audio file, via speakers which were placed near the weight, at an average volume level of 75 dB.

Results & Conclusions: Fig. 2 presents a spectrogram extracted from the measurements obtained by the gyroscope. As can be seen from the spectrogram, the weight vibrates based on the sound played near the weight.

The experiment described above demonstrates that objects (weights) vibrate in response to nearby sound. In the next experiments, we show that the vibrations of an object can be captured using a photodiode when light is shining on the object.

Experimental Setup: We directed a telescope (with a lens diameter of 25 cm) at the weight. We mounted a photodiode (the Thorlabs PDA100A2 [22]) to the telescope. The voltage was obtained from the photodiode using a 24-bit ADC NI-9234 card [23] and processed in a LabVIEW script that we wrote. We created an audio file that consists of various sine waves (120, 170, 220, ... 1020 Hz) where each sine wave was played for two seconds. We played the audio file, via speakers which were placed near the weight, at an average volume level of 75 dB from a distance of 10 cm. We obtained the optical signal via the photodiode when the lights in the room were on and off, using three different weights: weights of 10, 50, 100 grams.

Results & Conclusions: Fig. 3 presents the signal-to-noise ratio (SNR) obtained from the optical measurements when the lights in the room were on and off. The following insights were

[3] https://www.amazon.com/gp/product/B08SQ2WTNY/ref=ppx_yo_dt_b_asin_title_o00_s00?ie=UTF8&psc=1

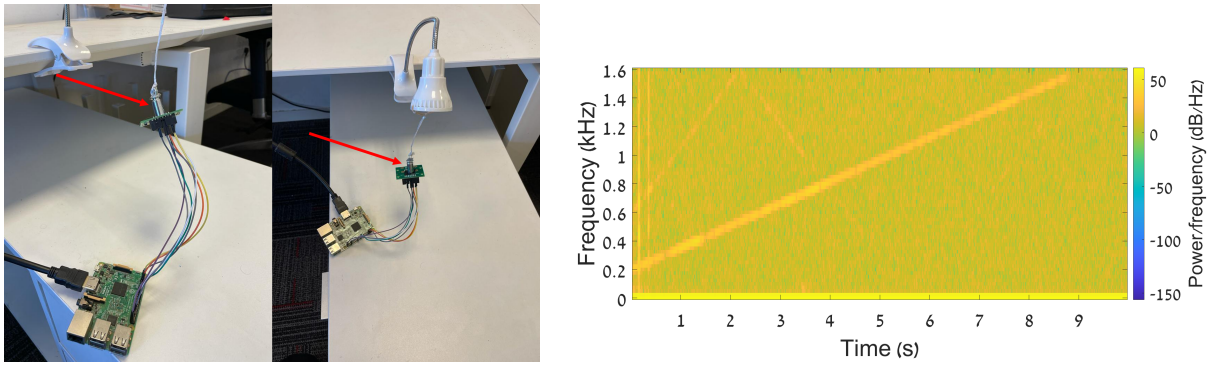

Fig. 2. Left: the gyroscope attached to the weight (indicated by the red arrow). The gyroscope is sampled by a Raspberry Pi 3. Right: The spectrogram extracted from the gyroscope measurements during a frequency scan that was played by nearby speakers.

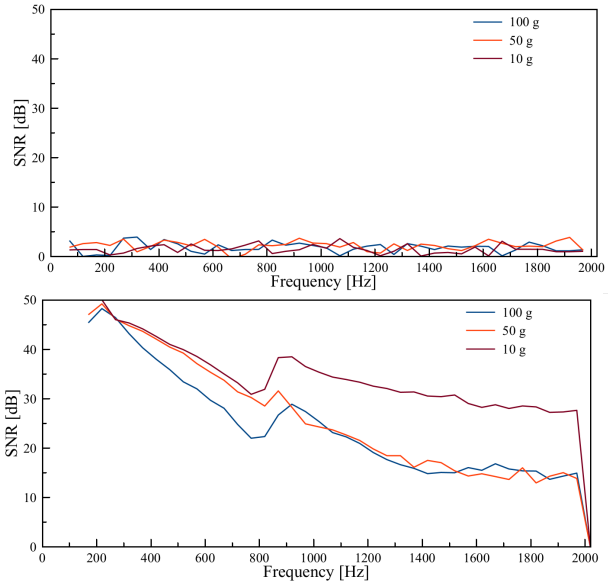

Fig. 3. The SNR obtained from the weights when the lights in the room were off (top) and on (bottom).

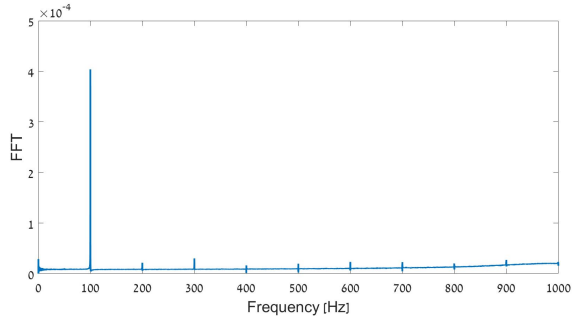

Fig. 4. The FFT of the optical signal when no sound is played (the baseline).

obtained by analyzing the SNR values: (1) When the lights are off, the weights' vibrations cannot be identified in the optical measurements, however when the lights are on, the vibrations of the weights can be spotted in the optical measurements. (2) The SNR increases with lighter weights, but the unique behavior of the SNR is maintained across all of the weights tested. (3) The response is not the same across the spectrum and decreases as a function of the frequency.

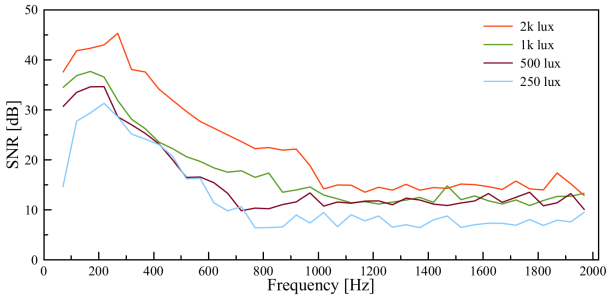

Fig. 5. The SNR as a function of the light reflected from the weight.

Based on these experiments, we made the following conclusions: (1) When light hits a reflective object, the reflection of the light from the object modulates the object's vibration, which is associated with the sound played nearby; this fact can be exploited by an eavesdropper to recover sound from a passive lightweight shiny object located near a victim during a virtual or physical conversation. (2) In some cases, the physical movement of the reflective object required the use of an equalizer to balance an unequal response across the spectrum. (3) The zero SNR value obtained in the dark rules out another reasonable explanation for this phenomenon, which is that the measurements obtained by the photodiode were affected by EMR emitted from the speakers; clearly, the optical measurements were not affected by any possible side effects; if they were, the SNR in the dark would not be zero.

B. Characterizing the Optical Signal

In this experiment, we examine the characteristics of the optical signal when no sound is played, with the aim of profiling the optical signal in order to filter out any side effects that are not associated with sound from the recovered audio signal.

Experimental Setup: We obtained five seconds of optical measurements from the photodiode when no sound was played near the weights when the lights were turned on.

Results: The FFT graph extracted from the optical measurements when no sound was played is presented in Fig. 4. As can be seen in the FFT graph, peaks appear around 100 Hz, 200 Hz, etc. Since the optical measurements were obtained via a photodiode directed at an object that reflected the light in

the office, the light frequency (100 Hz) and its harmonics are added to the optical measurements. The optical phenomenon that occurs at 100 Hz (which was captured by the photodiode) is the result of power net harmonics. The LED bulb in the office uses DC voltage which is converted from AC. A diode bridge is integrated into the electrical device, which flips the negative half of the sinus, doubling the base frequency from 50 Hz to 100 Hz. As a result, the LED changes its intensity 100 times a second which creates a periodic phenomenon of 100 Hz, 200 Hz, 300 Hz, etc.

Conclusions: Based on this experiment, we concluded that bandstop filtering would be required to eliminate side effects which are not the result of the sound that we want to recover yet greatly impact the optical signal.

Next, we examine how the SNR of the optical signal that was obtained from a weight is affected by the intensity of the light reflected from the weight.

Experimental Setup: In this case, we made one change to the experimental setup used to obtain optical measurements in the experiments described in this section: we measured the amount of light reflected on the surface of the shiny object using a professional lux meter (this corresponds to the amount of light reflected back from the object to the photodiode). We played a frequency scan via the speakers near a 50 gram weight in four experiments, varying the intensity of the light reflected on the object in each experiment (250, 500, 1000, 2000 lux).

Results & Conclusions: Fig. 5 presents the signal-to-noise ratio (SNR) obtained from the optical measurements in the four experiments. As can be seen, the intensity of the light reflected from the weight has a strong effect on the SNR of the optical measurements. Unsurprisingly, the SNR improves when greater intensity light hits the surface of the weight.

The experiments described in this section demonstrate that the vibrations of the weights correlate to nearby sound. As a result, the optical measurements of the photodiode are affected by the weight's vibrations (which correlate to the sound) when light is reflected from the weight. This fact can be exploited by eavesdroppers to recover sound; eavesdroppers can accomplish this by using a remote photodiode to analyze the optical measurements obtained from a lightweight shiny object. In the series of experiments described in this section, we chose to use a simple shiny object (a weight) as the lightweight reflective object; the use of such a generic object allowed us to investigate whether a photodiode can be used to successfully recover sound from shiny objects. In the sections that follow, we show that while reflective objects can be exploited for the purpose of sound recovery, their optical response to sound can change depending on their physical structure.

V. Optical Acoustical Transformation

In this section, we leverage the findings presented in Section IV and present an optical-acoustic transformation (OAT), which is used to recover audio from measurements obtained from a photodiode directed at a shiny object.

Throughout this section, we consider $snd(t)$ as the sound played inside the victim's room, $opt(t)$ as the optical signal obtained via a photodiode directed at a shiny object, and $snd^*(t)$ as the audio signal recovered from $opt(t)$ using the OAT. The OAT consists of the following steps:

Filtering Side Effects. As discussed in Section IV and seen in Fig. 4, 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.

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

Noise Reduction. Noise reduction is the process of removing noise from a signal in order to optimize its quality. 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 [24].

Equalizer. Equalization is the process of adjusting the balance between frequency components within an electronic signal. We use an equalizer to amplify the response of weak frequencies.

The techniques used in this study to recover speech are commonly used in the area of speech processing; we used them for the following reasons: (1) the techniques rely on a speech signal that is obtained from a single channel; if eavesdroppers have the capability of sampling using additional sensors, thereby obtaining several signals via multiple channels, other methods can also be applied to recover an optimized signal; (2) the techniques do not require any prior data collection to create a model; other novel speech processing methods use neural networks that are used to characterize/profile the noise in order to optimize the speech quality, however such neural networks require a large amount of data for the training phase in order to create robust models, a requirement that may be offputting to eavesdroppers; and (3) the techniques are adaptive and can be applied to recover sound from various shiny objects which may behave differently (e.g., require different equalizers) or produce different noise levels and distributions.

VI. Evaluation

In this section, we evaluate the performance of the little seal bug attack in terms of its ability to recover sound from light reflected from various objects. We compare the little seal bug attack's performance to three state-of-the-art sound recovery methods by replicating their experimental setup: the visual microphone [14], the hard drive of hearing [8], and Lamphone [15].

A. Metrics & Experimental Setup

The reader can assess the quality of the recovered sound visually by analyzing the extracted graphs (spectrograms), qualitatively by listening to the recovered audio signals online,[4,5] and quantitatively based on metrics used by the audio processing community to compare a recovered signal to its original signal: (1) Intelligibility - a measure of how comprehensible speech is in given conditions; the intelligibility is

[4] https://www.youtube.com/watch?v=DmWXcPUXpMA
[5] https://www.youtube.com/watch?v=XarrgwYsfT0

Fig. 6. The lightweight reflective objects used to recover sound: (1) decorative bucket, (2) smartphone stand, (3) iced coffee can, (4) Venetian blinds, (5) bird statuette, (6) Rubik's Cube.

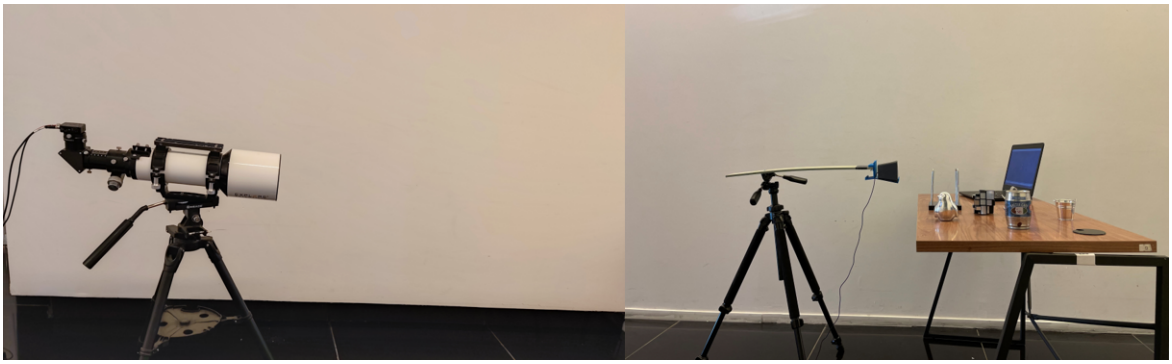

Fig. 7. The experimental setup - the telescope is directed at the reflective objects (see Fig. 6) which are placed on a desk.

affected by the level and quality of the speech signal and the type and level of the background noise and reverberation [25]. To measure the intelligibility, we used the metric suggested by [26], which results in values between [0,1]. A higher intelligibility value indicates higher sound quality. (2) NIST Speech SNR (NIST-SNR) - the speech-to-noise ratio, which is defined as the logarithmic ratio between the speech power and the noise power estimated over 20 consecutive milliseconds [27]. A higher NIST-SNR indicates higher sound quality.

We used the following equipment, setup, and configurations to recover sound in all of the experiments conducted and described in this section: a telescope (with a lens diameter of 25 cm) was directed at various lightweight reflective objects. We mounted a photodiode (Thorlabs PDA100A2 [22]), which was configured for the highest gain level before saturation, to the telescope. The output of the photodiode (the voltage associated with the light intensity) was sampled with a 24-bit ADC NI-9234 card. The sampling frequency of the ADC was configured at 2 KHz. We used Logitech Z200 speakers, which were placed on a dedicated stand, to produce the sound; the sound level was measured with a professional decibel meter. The data was processed in a LabVIEW script that we wrote. In the rest of this section, we refer to this setup, which can be seen in Fig. 7, as the eavesdropping equipment.

In our evaluation we recovered speech from a variety of lightweight reflective objects. We used three decorative ornaments that an individual might place on a desk: a Rubik's Cube, decorative bucket, and a hollow bird statuette. We also included two objects typically purchased by individuals for consumption or daily use: a smartphone stand and an iced coffee can (which was empty in our experiments), as well as an item often used in offices to protect the privacy of individuals: Venetian blinds. The objects are presented in Fig. 6.

B. A Comparison of the Little Seal Bug Attack to the Visual Microphone

The authors proposing the visual microphone [14] demonstrated the recovery of six sentences from the TIMIT repository [28] by playing the sentences via speakers and analyzing the resulting vibrations of a bag of chips via a high-frequency video camera (2200 FPS) from a distance of two meters. Here, we compare the performance of the little seal bug attack, when recovering the same sentences, to that of the visual microphone.

Experimental Setup: We replicated the experimental setup used in the visual microphone study [14] as follows: We placed the speakers on a dedicated stand five centimeters from various shiny objects, which is the same distance that the bag of chips was placed from the speakers in the visual microphone study). We played the same six sentences from the TIMIT repository

TABLE I
COMPARISON OF THE INTELLIGIBILITY OF THE RECOVERED SPEECH USING THE LITTLE SEAL BUG ATTACK (BIRD STATUTE, ROBIK'S CUBE, SMARTPHONE, ICED COFFEE CAN, VENETIAN BLINDS) AND VISUAL MICROPHONE [14] BASED ON SENTENCES FROM THE TIMIT REPOSITORY.

	Speech Recovered	Bird Statuette	Rubik's Cube	Decorative Bucket	Smartphone Stand	Iced Coffee Can	Venetian Blinds	Visual Microphone
Female speaker-fadg0, sa1	SShe had your dark suit in greasy wash water all year"	0.52	0.73	0.79	0.64	0.64	0.51	0.72
Female speaker-fadg0, sa2	"Don't ask me to carry an oily rag like that"	0.47	0.59	0.62	0.52	0.51	0.39	0.65
Male speaker-mabw0, sa1	SShe had your dark suit in greasy wash water all year"	0.47	0.65	0.74	0.61	0.59	0.495	0.59
Male speaker-mabw0, sa1	"Don't ask me to carry an oily rag like that	0.45	0.59	0.69	0.49	0.49	0.41	0.67
Male speaker-mccs0, sa1	SShe had your dark suit in greasy wash water all year"	0.59	0.72	0.77	0.63	0.63	0.51	0.77
Male speaker-mccs0, sa1	"Don't ask me to carry an oily rag like that"	0.51	0.63	0.71	0.54	0.53	0.41	0.72
	Average	0.51	0.65	0.72	0.57	0.56	0.45	0.68
	STD	0.05	0.05	0.06	0.06	0.06	0.05	0.06

TABLE II
COMPARISON OF THE NIST-SNR OF THE RECOVERED SPEECH USING THE LITTLE SEAL BUG ATTACK (BIRD STATUTE, ROBIK'S CUBE, SMARTPHONE, ICED COFFEE CAN, VENETIAN BLINDS) AND VISUAL MICROPHONE [14] BASED ON SENTENCES FROM THE TIMIT REPOSITORY.

	Speech	Bird Statuette	Rubik's Cube	Decorative Bucket	Smartphone Stand	Iced Coffee Can	Venetian Blinds	Visual Microphone
Female speaker-fadg0, sa1	"She had your dark suit in greasy wash water all year"	7	7.5	4.25	20.75	17.25	4.3	26.8
Female speaker-fadg0, sa2	"Don't ask me to carry an oily rag like that"	3	4	3.75	4.75	7.25	3.5	43.3
Male speaker-mabw0, sa1	"She had your dark suit in greasy wash water all year"	5.5	5.25	2.25	6.75	8.5	6.5	27.3
Male speaker-mabw0, sa1	"Don't ask me to carry an oily rag like that"	2	5	3.25	15	5.5	27.5	18
Male speaker-mccs0, sa1	"She had your dark suit in greasy wash water all year"	3.75	6.25	12.25	12	16.25	10.8	6
Male speaker-mccs0, sa1	"Don't ask me to carry an oily rag like that"	1.25	3	14.25	3.75	5.25	25.5	25.8
	Average	3.75	5.17	6.67	10.5	10	13.02	24.53
	STD	1.98	1.46	4.73	6.06	4.90	9.83	12.27

recovered by the visual microphone via the speakers at the same volume level used in the visual microphone study (95 dB). We placed the eavesdropping equipment 2.5 meters from the lightweight reflective object (the same distance that the video camera was placed in the visual microphone study). Our experimental setup is presented in Fig. 7. We recovered speech from the six objects presented in Fig. 6.

Results & Conclusions: We used the OAT to recover speech from the optical measurements (see Section V). The recovered audio signals are available online[4] where they can be heard. The spectrograms extracted from the optical measurements for three of the sentences recovered when using various objects to recover sound are presented in Figs. 8-10. We evaluated the intelligibility and NIST-SNR of the recovered signals and reported the results in Tables I and II. We also downloaded the same six audio signals that were recovered and published in the study presenting the visual microphone and evaluated their performance based on the same metrics. The following interesting observations can be made from the results presented in the tables: The average intelligibility of the speech recovered depends, to a large extent, on the shiny object used to implement the attack. In some cases, the average intelligibility of the object is considered good (the Rubik's Cube and decorative bucket) according to [25]; in the case of other objects (the smartphone stand, bird statuette, iced coffee can, and Venetian blinds), the average intelligibility is considered fair. A similar conclusion can also be made by analyzing the NIST-SNR of the speech recovered, which ranges from 3.75-13 for the six objects examined.

TABLE III
COMPARISON OF THE NIST-SNR RESULTS OF THE HARD DRIVE OF HEARING [8] AND THE LITTLE SEAL BUG ATTACK FOR THE RECOVERY OF SPEECH.

	Hard Drive of Hearing	Rubik's Cube	Iced Coffee Can	Smartphone Stand
Male (List 57)	11.2	23.5	22.8	25.8
Female (List 1)	7.8	18.5	23.5	26.3
Average	9.5	21	23.15	26.05
STD	1.7	2.5	0.35	0.25

Based on our analysis of the results of the experiments conducted to compare the performance of the little seal bug to

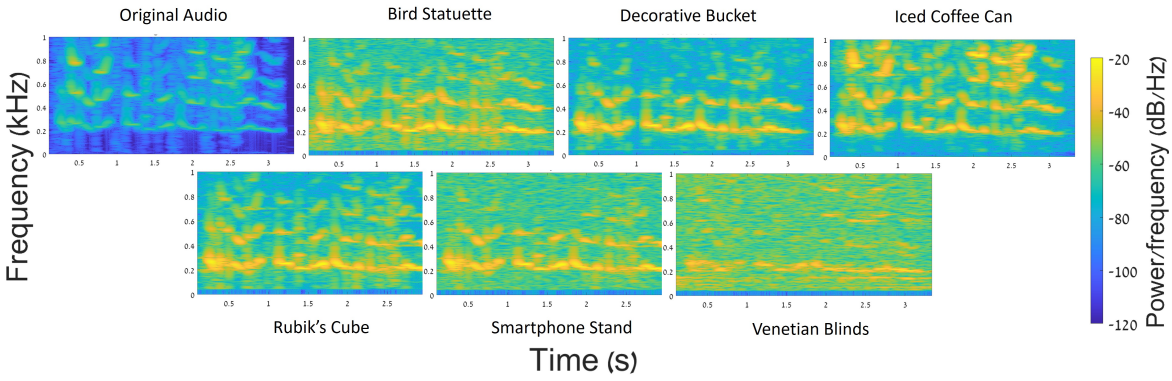

Fig. 8. Recovery of the sentence "She had your dark suit in greasy wash water all year" by fadg0,sa1 from various objects.

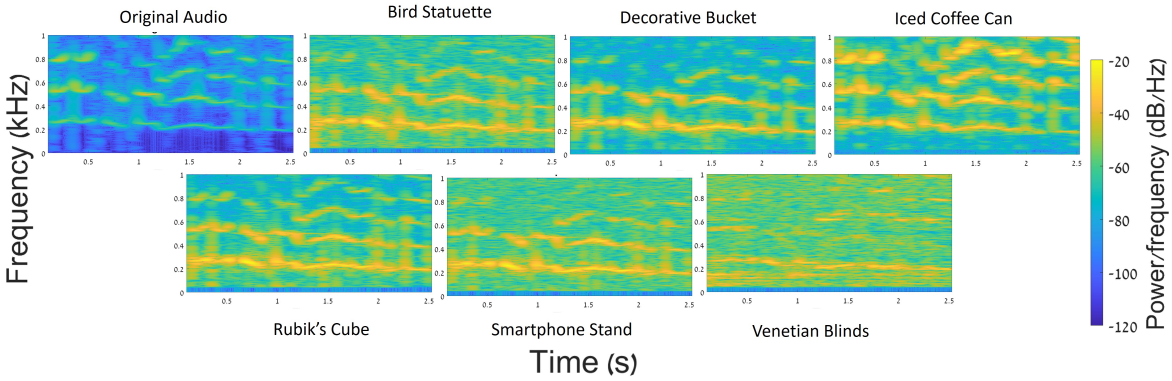

Fig. 9. Recovery of the sentence "Don't ask me to carry an oily rag like that" by fadg0,sa2 from various objects.

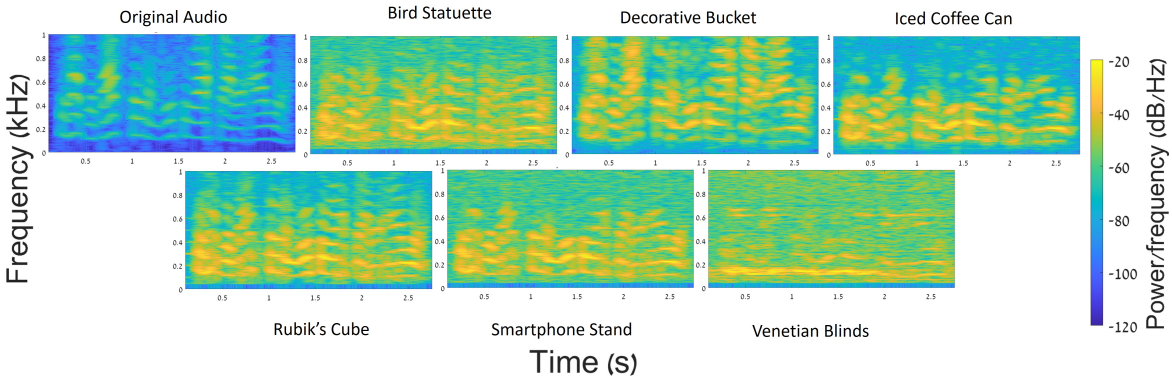

Fig. 10. Recovery of the sentence "She had your dark suit in greasy wash water all year" by mabw0,sa1 from various objects.

that of the visual microphone, we concluded that the answer to the question of which of the two methods is better depends on the metric used to evaluate the methods and the object used to recover speech.

C. A Comparison of the Little Seal Bug Attack to the Hard Drive of Hearing

The authors proposing the hard drive of hearing [8] demonstrated the recovery of two recordings from the Harvard sentences database: a female sample (list 1) and a male sample (list 57). The specific audio samples were obtained from the Open Speech Repository [29]. Here, we compare the performance of the little seal bug attack, when recovering the same sentences, from three objects: an iced coffee can, a Rubik's Cube, and a smartphone stand.

Experimental Setup: We followed the experimental setup used in the hard drive of hearing [8] study as follows: We placed speakers on a dedicated stand at a distance of 25 cm from the three objects used in this experiment, which is the same distance that was used in the hard drive of hearing study. We played the two audio samples from the Open Speech Repository recovered by the hard drive of hearing via the speakers at the same volume level used in the hard drive of hearing study (85 dB). In our experiment the eavesdropping equipment was placed 2.5 meters from the objects.

Results & Conclusions: We used the OAT to recover speech from the optical measurements. Since we were unable to ob-

TABLE IV
COMPARISON OF THE INTELLIGIBILITY AND NIST-SNR RESULTS OF LAMPHONE [15] AND THE LITTLE SEAL BUG ATTACK FOR THE RECOVERY OF SPEECH FROM VARIOUS DISTANCES.

	Intelligibility				NIST-STNR			
	Rubik's Cube	Bird Statuette	Decorative Bucket	Lamphone	Rubik's Cube	Bird Statuette	Decorative Bucket	Lamphone
	15m							
25 cm	0.61	0.34	0.34	0.52	16.3	2	1.8	21
50 cm	0.35	0.36	0.34	0.46	2	3.8	1.8	12.3
	25m							
25 cm	0.55	0.32	0.3	0.49	14.5	8.8	4	21.8
50 cm	0.32	0.35	0.32	0.4	6	2	1.5	21
	35m							
25 cm	0.5	0.32	0.31	0.45	14.5	4	8	17.5
50 cm	0.38	0.33	0.32	0.36	12.8	4	0.3	11.5

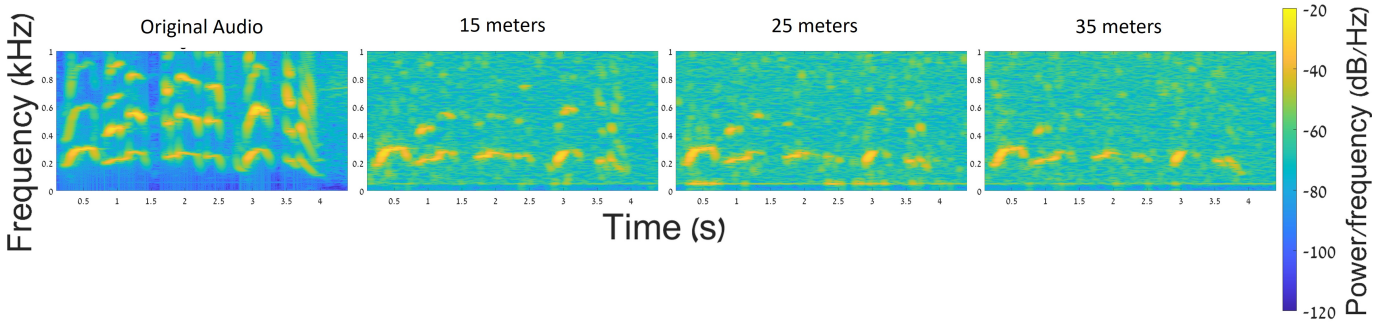

Fig. 11. Recovery of the sentence "We Will Make America Great Again" from various distances (15, 25, 35 meters) from light reflected from a Rubik's Cube when the speakers were located 25 cm from the object.

tain the recovered audio samples from the hard drive of hearing study, we compared the little seal bug attack's performance to the results reported in that paper. The authors of that study evaluated their recovered signals using the NIST-SNR, so here we compare the sentences recovered by the little seal bug attack and the hard drive of hearing based on the NIST-SNR. The results of our comparison are presented in Table III. The following interesting observations can be made from the results presented in the table: (1) The average NIST-SNR of the speech recovered by the little seal bug attack (which ranges from 21-26 for the examined objects) is higher (better) than the average NIST-SNR of the recovered speech reported in the hard drive of hearing paper (9.5). (2) Moreover, the STD of the NIST-SNR obtained by the little seal bug is lower (better) than the STD of the NIST-SNR reported in the hard drive of hearing paper for two of the three objects (the iced coffee can and smartphone stand) examined in this study.

After analyzing the results of the experiments conducted to compare the performance of the little seal bug attack to that of the hard drive of hearing, we concluded that the quality of the speech recovered by the little seal bug attack is higher than that of the hard drive of hearing.

D. A Comparison of the Little Seal Bug Attack to Lamphone

The authors proposing Lamphone [15] demonstrated the recovery of the statement "We Will Make America Great Again" made by former US president Donald Trump from various distances. We compare the little seal bug attack's performance when recovering the same sentence from three objects: an iced coffee can, Rubik's Cube, and smartphone stand.

Experimental Setup: We followed the experimental setup used in the Lamphone [15] study as follows: We placed the eavesdropping equipment at various distances (15, 25, 35 meters) from the three objects used in this experiment, and the speakers were placed two distances (25 cm and 50 cm) away from the reflective objects. Then, we played the sentence via the speakers at the volume level of a virtual meeting (75 dB) while obtaining the optical measurements.

Results & Conclusions: We used the OAT to recover speech from the optical measurements. The recovered audio signals are available online.[5] The spectrograms of the speech extracted from the Rubuik's cube from various distances (15, 25, 35 meters) when objects were located 25 meters from the speakers are presented in Fig. 11. The intelligibility and NIST-SNR of the recovered signals are reported in Table IV. The following observations can be made from the results presented in the table: Although the intelligibility of the audio signals recovered from the Rublik's Cube decreases (from 0.61 to 0.5) with distance when the object is placed 25 cm from the speakers, fair intelligibility (according to [25]) is achieved from all three distances examined.

The experiments show that the little seal bug attack can be used by eavesdroppers to recover the content of a phone call or virtual meeting held by a victim seated at a desk from reflective objects (e.g., Rubik's Cube) placed on the desk a reasonable distance away from the victim (25 cm is half of the depth of a standard desk).

VII. Limitations, Discussion, and Future Work

The primary objective of this research was to raise awareness regarding the fact that shiny lightweight objects can serve as optical implants that can be exploited by eavesdroppers to recover sound. The secondary objective of this research was to demonstrate that the issues associated with speech recovery from light are more serious and widespread than initially thought based on prior research focused on recovering speech directly from objects/devices that emit light (e.g., a light bulb and the power LED of speakers). This research shows that light can also be used to recover speech indirectly by using its reflections from nearby objects.

We also note that optical sound eavesdropping has progressed significantly in the past seven years: a few studies have presented innovative methods to recover speech using data acquired from a high frequency video camera [14], LiDAR [9], and a photodiode [13, 15]. Our attack continues the trend of recovering sound by exploiting optical side effects, and we believe that other studies will address this topic in the next few years. Over the years, smartphone manufacturers have continuously increased the sampling rate of the integrated sensors of the smartphone . According to [3], the manufacturers of Android smartphones have doubled the sampling rate of accelerometers from 200 Hz in 2014 to 500 Hz in 2018 (e.g., for the Huawei P20 Pro and Mate 20). Given the extent of this improvement in the sampling rate, we raise a concern about a new problem which may arise: the sampling rate of smartphones may enable eavesdroppers to recover compressible speech from the smartphone's integrated light sensor (which is used to balance the smartphone's screen lighting). Such a development will allow eavesdroppers to obtain optical measurements via a compromised application without any permission from the user.

In future work, we plan to investigate how the sound recovery model can be improved by integrating advanced algorithms for speech processing (e.g., [30–34]) and denoising. We also suggest investigating the use of a transcription light-to-text model which can be implemented by training a neural network that receives optical signals and outputs transcription/text.

References

[1] J. Landt, "The history of rfid," *IEEE potentials*, vol. 24, no. 4, pp. 8–11, 2005.

[2] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing speech from gyroscope signals," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, 2014, pp. 1053–1067. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/michalevsky

[3] Z. Ba, T. Zheng, X. Zhang, Z. Qin, B. Li, X. Liu, and K. Ren, "Learning-based practical smartphone eavesdropping with built-in accelerometer," in *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium*, 2020, pp. 23–26.

[4] S. A. Anand and N. Saxena, "Speechless: Analyzing the threat to speech privacy from smartphone motion sensors," in *2018 IEEE Symposium on Security and Privacy (SP)*, vol. 00, pp. 116–133. [Online]. Available: doi.ieeecomputersociety.org/10.1109/SP.2018.00004

[5] L. Zhang, P. H. Pathak, M. Wu, Y. Zhao, and P. Mohapatra, "Accelword: Energy efficient hotword detection through accelerometer," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2015, pp. 301–315.

[6] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Speake(a)r: Turn speakers to microphones for fun and profit," in *11th USENIX Workshop on Offensive Technologies (WOOT 17)*. Vancouver, BC: USENIX Association, 2017. [Online]. Available: https://www.usenix.org/conference/woot17/workshop-program/presentation/guri

[7] N. Roy and R. Roy Choudhury, "Listening through a vibration motor," in *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '16. New York, NY, USA: ACM, 2016, pp. 57–69. [Online]. Available: http://doi.acm.org/10.1145/2906388.2906415

[8] A. Kwong, W. Xu, and K. Fu, "Hard drive of hearing: Disks that eavesdrop with a synthesized microphone," in *2019 2019 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2019. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP.2019.00008

[9] S. Sami, Y. Dai, S. R. X. Tan, N. Roy, and J. Han, "Spying with your robot vacuum cleaner: Eavesdropping via lidar sensors," in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, ser. SenSys '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 354–367. [Online]. Available: https://doi.org/10.1145/3384419.3430781

[10] G. Wang, Y. Zou, Z. Zhou, K. Wu, and L. M. Ni, "We can hear you with wi-fi!" *IEEE Transactions on Mobile Computing*, vol. 15, no. 11, pp. 2907–2920, Nov 2016.

[11] T. Wei, S. Wang, A. Zhou, and X. Zhang, "Acoustic eavesdropping through wireless vibrometry," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '15. New York, NY, USA: ACM, 2015, pp. 130–141. [Online]. Available: http://doi.acm.org/10.1145/2789168.2790119

[12] J. Choi, H.-Y. Yang, and D.-H. Cho, "Tempest comeback: A realistic audio eavesdropping threat on mixed-signal socs," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1085–1101. [Online]. Available: https://doi.org/10.1145/3372297.3417241

[13] B. Nassi, Y. Pirutin, T. C. Galor, Y. Elovici, and B. Zadov, "Glowworm attack: Optical tempest sound recovery via a device's power indicator led," *Cryptology ePrint Archive*, 2021.

[14] A. Davis, M. Rubinstein, N. Wadhwa, G. J. Mysore, F. Durand, and W. T. Freeman, "The visual microphone: passive recovery of sound from video," 2014.

[15] B. Nassi, Y. Pirutin, A. Shamir, Y. Elovici, and B. Zadov, "Lamphone: Real-time passive sound recovery from light bulb vibrations," Cryptology ePrint Archive, Tech. Rep.
[16] R. P. Muscatell, "Laser microphone," Oct. 25 1983, uS Patent 4,412,105.
[17] P. Walker and N. Saxena, "Sok: assessing the threat potential of vibration-based attacks against live speech using mobile sensors," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021, pp. 273–287.
[18] C. V. Wright, L. Ballard, F. Monrose, and G. M. Masson, "Language identification of encrypted voip traffic: Alejandra y roberto or alice and bob?" in *USENIX Security Symposium*, vol. 3, 2007, pp. 43–54.
[19] A. M. White, A. R. Matthews, K. Z. Snow, and F. Monrose, "Phonotactic reconstruction of encrypted voip conversations: Hookt on fon-iks," in *Security and Privacy (SP), 2011 IEEE Symposium on*. IEEE, 2011, pp. 3–18.
[20] C. V. Wright, L. Ballard, S. E. Coull, F. Monrose, and G. M. Masson, "Spot me if you can: Uncovering spoken phrases in encrypted voip conversations," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. IEEE, 2008, pp. 35–49.
[21] "Mpu-6000," https://invensense.tdk.com/wp-content/uploads/2015/02/MPU-6000-Datasheet1.pdf.
[22] "Pda100a2." [Online]. Available: https://www.thorlabs.com/thorproduct.cfm?partnumber=PDA100A2
[23] "Ni 9234 datasheet." [Online]. Available: https://www.ni.com/pdf/manuals/374238a_02.pdf
[24] N. Upadhyay and A. Karmakar, "Speech enhancement using spectral subtraction-type algorithms: A comparison and simulation study," *Procedia Computer Science*, vol. 54, pp. 574–584, 2015.
[25] "Intelligibility," https://en.wikipedia.org/wiki/Intelligibility_(communication).
[26] C. H. Taal, R. C. Hendriks, R. Heusdens, and J. Jensen, "An algorithm for intelligibility prediction of time–frequency weighted noisy speech," vol. 19, no. 7. IEEE, 2011, pp. 2125–2136.
[27] "Nist-snr," https://www.nist.gov/itl/iad/mig/nist-speech-signal-noise-ratio-measurements.
[28] J. S. Garofolo, L. F. Lamel, W. M. Fisher, J. G. Fiscus, and D. S. Pallett, "Darpa timit acoustic-phonetic continous speech corpus cd-rom. nist speech disc 1-1.1," *STIN*, vol. 93, p. 27403, 1993.
[29] "The open speech repository," http://www.voiptroubleshooter.com/open_speech/american.html.
[30] P. Jax and P. Vary, "On artificial bandwidth extension of telephone speech," *Signal Processing*, vol. 83, no. 8, pp. 1707–1719, 2003.
[31] H. Pulakka, U. Remes, S. Yrttiaho, K. Palomaki, M. Kurimo, and P. Alku, "Bandwidth extension of telephone speech to low frequencies using sinusoidal synthesis and a gaussian mixture model," *IEEE transactions on audio, speech, and language processing*, vol. 20, no. 8, pp. 2219–2231, 2012.
[32] V. Iyengar, R. Rabipour, P. Mermelstein, and B. R. Shelton, "Speech bandwidth extension method and apparatus," Oct. 3 1995, uS Patent 5,455,888.
[33] S. Li, S. Villette, P. Ramadas, and D. J. Sinder, "Speech bandwidth extension using generative adversarial networks," in *2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2018, pp. 5029–5033.
[34] H. Pulakka and P. Alku, "Bandwidth extension of telephone speech using a neural network and a filter bank implementation for highband mel spectrum," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 19, no. 7, pp. 2170–2183, 2011.

Ben Nassi is a postdoctoral researcher at Ben-Gurion University of the Negev (BGU) and a former Google employee. He has a B.Sc. degree in Computer Science and M.Sc. and Ph.D. degrees in Software and Information Systems Engineering from BGU. His research interests are side-channel attacks, applied crypto, TEMPEST attacks, AI security, and IoT security. His papers have been published at prestigious venues.

Raz Swissa is a security researcher at Ben-Gurion University of the Negev's Cyber Security Research Center. He has a B.Sc. degree in Computer Engineering from Ben-Gurion University of the Negev. His primary research interests are side-channel attacks and cyber security.

Yuval Elovici is the director of the Telekom Innovation Laboratories at Ben-Gurion University of the Negev (BGU), head of BGU's Cyber Security Research Center, and a professor in the Department of Software and Information Systems Engineering at BGU. He holds B.Sc. and M.Sc. degrees in Computer and Electrical Engineering from BGU and a Ph.D. in Information Systems from Tel Aviv University. Prof. Elovici has published numerous articles in leading peer-reviewed journals and at various peer-reviewed conferences. In addition, he has co-authored books on social network security and information leakage detection and prevention. His primary research interests are computer and network security, cyber security, web intelligence, information warfare, social network analysis, and machine learning.

Boris Zadov is postdoctoral researcher in the Department of Software and Information Systems Engineering at Ben-Gurion University of the Negev. He holds a B.Sc. degree in Electrical and Electronics Engineering from the Sami Shamoon College of Engineering, Israel, an M.Sc. in Electrical and Computer Engineering from Ben-Gurion University of the Negev, and a Ph.D in Electrical and Computer Engineering in Ben-Gurion University of the Negev.