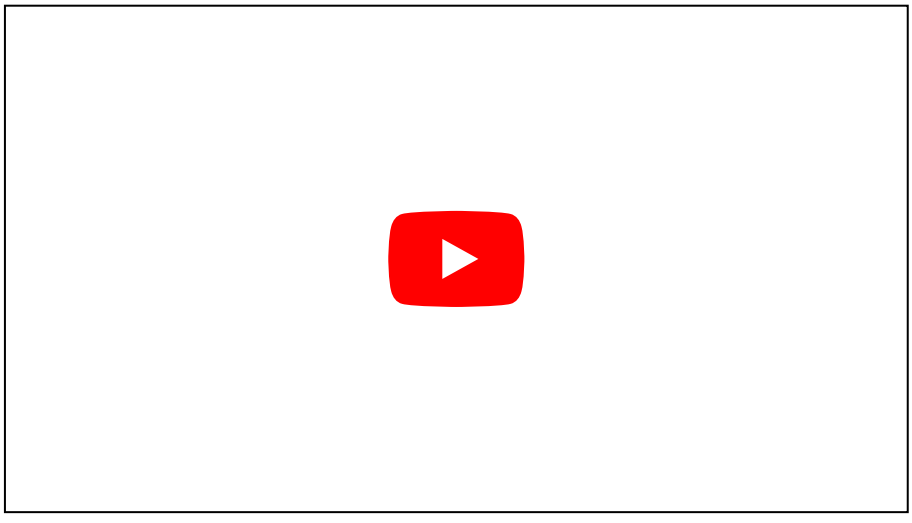
Ben Nassi

Glowworm Attack

Optical TEMPEST Sound Recovery via a Device's Power Indicator LED

Ben Nassi Yaron Pirutin Tomer Cohen Galor Yuval Elovici Boris Zadov

Ben-Gurion University of the Negev



DOWNLOAD PAPER DOWNLOAD PICTURES

Abstract

Two main classes of optical TEMPEST attacks against the confidentiality of information processed/delivered by devices have been demonstrated in the past two decades; the first class includes methods for recovering content from monitors, and the second class includes methods for recovering keystrokes from physical and virtual keyboards.
In this paper, we identify a new class of optical TEMPEST attacks: recovering sound by analyzing optical emanations from a device's power indicator LED.
We analyze the response of the power indicator LED of various devices to sound and show that there is an optical correlation between the sound that is played by connected speakers and the intensity of their power indicator LED due to the facts that: (1) the power indicator LED of various devices is connected directly to the power line, (2) the intensity of a device's power indicator LED is correlative to the power consumption, and (3) many devices lack a dedicated means of countering this phenomenon.
Based on our findings, we present the Glowworm attack, an optical TEMPEST attack that can be used by eavesdroppers to recover sound by analyzing optical measurements obtained via an electro-optical sensor directed at the power indicator LED of various devices (e.g., speakers, USB hub splitters, and microcontrollers).
We propose an optical-audio transformation (OAT) to recover sound by isolating the speech from the optical measurements obtained by directing an electro-optical sensor at a device's power indicator LED.
Finally, we test the performance of the Glowworm attack in various experimental setups and show that an eavesdropper can apply the attack to recover speech from a speaker's power indicator LED with good intelligibility from a distance of 15 meters and with fair intelligibility from 35 meters.

Results

"Don't Ask Me To Carry An Oily Rag Like That"

Original speech played by speakers

Speech recovered from the power indicator LED of Winner speakers

Speech recovered from the power indicator LED of Logitech S120 speakers

Speech recovered from the power indicator LED of TP-Link USB hub

"We Will Make America Great Again!"

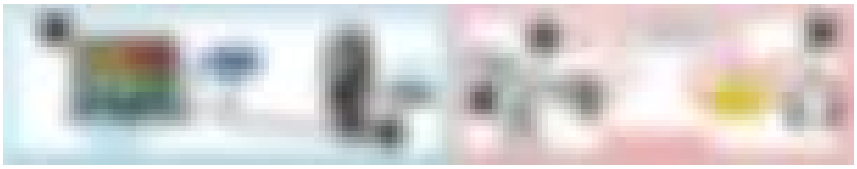
Speech recovered from speakers from 5 meters away

Speech recovered from speakers from 15 meters away

Speech recovered from speakers from 25 meters away

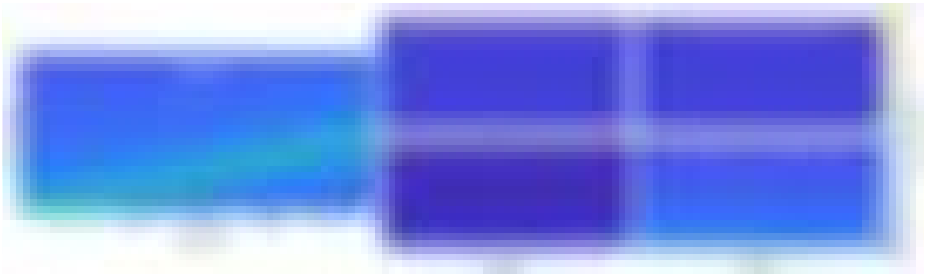
Speech recovered from speakers from 35 meters away

Threat Model



The sound $snd\ (t\ )$ of the virtual meeting (1) which is played by the connected speakers creates changes in the power consumption of the power indicator LED of a (2) connected peripheral (e.g., the speakers themselves, a USB hub splitter). The eavesdropper directs an electro-optical sensor at the power indicator LED of a connected peripheral using a telescope (3). The optical signal $opt\ (t\ )$ is sampled from the electro-optical sensor via an ADC (4) and processed, using an algorithm to recover the acoustic signal $snd*\ (t\ )$ (5).

Analysis



The four spectrograms on the right were obtained from the power (upper row) and optical (bottom row) measurements of Logitech speakers (middle) and TP-Link USB hub (right) when the speakers played the frequency scan (0-4 KHz) on the left.

Which manufacturers are vulnerable to this attack?

In one word, many.

About 50% of the devices we analyzed are vulnerable to the Glowworm Attack.

Some of the vulnerable manufacturers and devices are presented below.

Google - Google Home Mini, Google Nest Audio

Logitech - Z120 Speakers, S120 speakers

JBL - JBL Go 2

Sony - SRS-XB33, SRS-XB43

CREATIVE - Pebble speakers

TP-Link - TP-Link UE330 USB splitter

Miracase - Miracase USB splitter model MHUB500

Raspberry Pi - 3, 4

Frequently Asked Questions

Q1: Why do devices leak information from their power indicator LED?

In many devices, the power indicator LED is connected directly to the power line.
As a result, the intensity of a device's power indicator LED is correlative to the power

consumption.
In addition, many devices lack dedicated means of countering this phenomenon.

Q2: Why did you call attack the Glowworm attack?

Both the attack and the insect develop from a bug that emits light.

Q3: What is the difference between the Lamphone and Glowworm attacks?

Both methods recover sound from light via an electro-optical sensor.
The Lamphone attack is a side-channel attack that exploits a light bulb's miniscule vibrations, which are the result of sound waves hitting the bulb.
The Glowworm attack is a TEMPEST attack that exploits the way that electrical circuits were designed. It can recover sound from devices like USB hub splitters that do not move in response to the acoustic information played by the speakers.

Q4: Did you disclose the details of the attack with the manufacturers?

Yes.

Q5: Can attackers apply the Glowworm Attack using a video camera?

No.