Spies can eavesdrop by watching a light bulb’s variations

Michael Blann | Getty Images

reader comments

21 with 19 posters participating

Share this story

The list of sophisticated eavesdropping techniques has grown steadily over years: wiretaps, hacked phones, bugs in the wall—even bouncing lasers off of a building’s glass to pick up conversations inside. Now add another tool for audio spies: Any light bulb in a room that might be visible from a window.

Researchers from Israeli’s Ben-Gurion University of the Negev and the Weizmann Institute of Science today revealed a new technique for long-distance eavesdropping they call “lamphone.” They say it allows anyone with a laptop and less than a thousand dollars of equipment—just a telescope and a $400 electro-optical sensor—to listen in on any sounds in a room that’s hundreds of feet away in real-time, simply by observing the minuscule vibrations those sounds create on the glass surface of a light bulb inside. By measuring the tiny changes in light output from the bulb that those vibrations cause, the researchers show that a spy can pick up sound clearly enough to discern the contents of conversations or even recognize a piece of music.

“Any sound in the room can be recovered from the room with no

requirement to hack anything and no device in the room," says Ben Nassi, a security researcher at Ben-Gurion who developed the technique with fellow researchers Yaron Pirutin and Boris Zadov, and who plans to present their findings at the Black Hat security conference in August. "You just need line of sight to a hanging bulb, and this is it."

In their experiments, the researchers placed a series of telescopes around 80 feet away from a target office's light bulb, and put each telescope's eyepiece in front of a Thorlabs PDA100A2 electro-optical sensor. They then used an analog-to-digital converter to convert the electrical signals from that sensor to digital information. While they played music and speech recordings in the faraway room, they fed the information picked up by their set-up to a laptop, which analyzed the readings.

The researchers found that the tiny vibrations of the light bulb in response to sound—movements that they measured at as little as a few hundred microns—registered as measurable changes in the light their sensor picked up through each telescope. After processing the signal through software to filter out noise, they were able to reconstruct recordings of the sounds inside the room with remarkable fidelity: They showed, for instance, that they could reproduce an audible snippet of a speech from President Donald Trump well enough for it to be transcribed by Google's Cloud Speech API. They also generated a recording of the Beatles' "Let It Be" clear enough that the name-that-tune app Shazam could instantly recognize it.

The technique nonetheless has some limitations. In their tests, the researchers used a hanging bulb, and it's not clear if a bulb mounted in a fixed lamp or a ceiling fixture would vibrate enough to derive the same sort of audio signal. The

voice and music recordings they used in their demonstrations were also louder than the average human conversation, with speakers turned to their maximum volume. But the team points out that they also used a relatively cheap electro-optical sensor and analog-to-digital converter, and could have upgraded to a more expensive one to pick up quieter conversations. LED bulbs also offer a signal-to-noise ratio that's about 6.3 times that of an incandescent bulb and 70 times a fluorescent one.

Regardless of those caveats, Stanford computer scientist and cryptographer Dan Boneh argues that the researchers' technique still represents a significant and potentially practical new form of what he calls a "side channel" attack—one that takes advantage of unintended leakage of information to steal secrets. "It's a beautiful application of side channels," Boneh says. "Even if this requires a hanging bulb and high decibels, it's still super interesting. And it's still just the first time this has been shown to be possible. Attacks only get better, and future research will only improve this over time."

The research team, which was advised by BGU's Yuval Elovici and Adi Shamir, the coinventor of the ubiquitous RSA encryption system, isn't the first to show that unexpected sonic phenomena can enable eavesdropping. Researchers have known for years that a laser bounced off a target's window can allow spies to pick up the sounds inside. Another group of researchers showed in 2014 that the gyroscope of a compromised smartphone can pick up sounds even if the malware can't access its microphone. The closest previous technique to lamphone is what MIT, Microsoft, and Adobe researchers in 2014 called a "visual microphone": By analyzing video recorded via telescope of an object in a room that picks up vibrations—a bag of potato chips or a houseplant, for instance—those researchers were able to reconstruct speech and music.

[embedded content]

But Nassi points out that the video-based technique, while far more versatile since it doesn’t require a bulb to be visible in the room, requires analysis of the video with software after it’s recorded to convert the subtle vibrations observed in an object into the sounds it picked up. Lamphone, by contrast, enables real-time spying. Since the vibrating object is itself a light source, the electro-optical sensor can pick up vibrations in far simpler visual data.

That could make lamphone significantly more practical for use in espionage than previous techniques, Nassi argues. “When you actually use it in real time you can respond in real time rather than losing the opportunity,” he says.

Still, Nassi says the researchers are publishing their findings not to enable spies or law enforcement, but to make clear to those on both sides of surveillance what’s possible. “We want to raise the awareness of this kind of attack vector,” he says. “We’re not in the game of providing tools.”

As unlikely as being targeted by this technique is, it’s also easy to forestall. Just cover any hanging bulbs, or better yet, close the curtains. And if you’re paranoid enough to be concerned about this sort of spy game, hopefully you’ve already used anti-vibration devices on those windows to prevent eavesdropping with a laser microphone. And swept your house for bugs. And removed the microphones from your phone and computer. After all, in an era when even the light bulbs have ears, a paranoiac’s work is never done.

This story originally appeared on wired.com.

https://arstechnica.com/?p=1683598