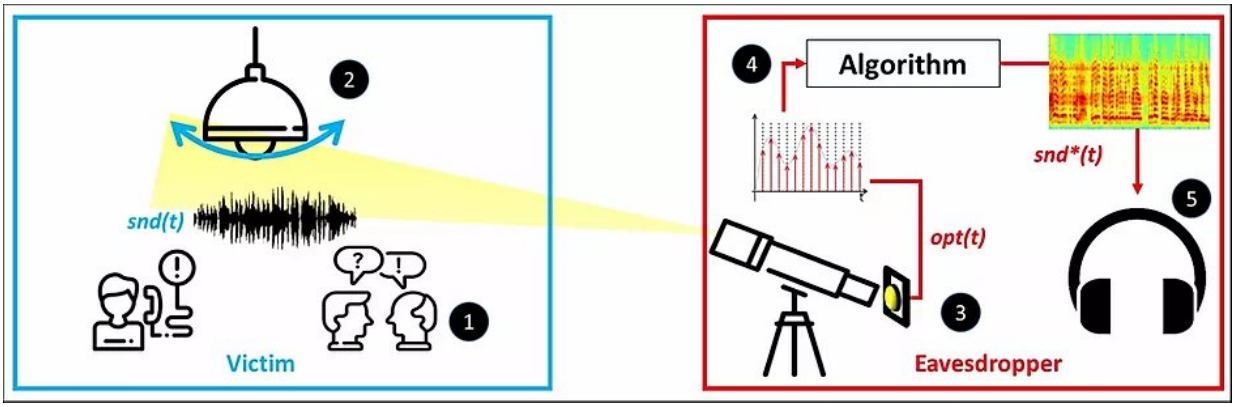
Light bulb vibrations yield eavesdropping data

June 15 2020, by Peter Grad



In an era of digital eavesdropping where hackers employ a variety of means to take over built-in video cameras, peruse personal digital data and snoop on cellular conversations, researchers have finally seen the light.

Literally.

Israeli researchers report that they successfully tapped into speech and music inside an apartment simply by focusing on a light bulb.

In a paper published over the weekend, the researchers said all they

needed were a telescope and a $400 optical sensor, which they used to measure barely perceptible light bulb vibrations triggered by either voices or music in the room.

The research team conducted the test by pointing a telescope situated in a bridge towards a light bulb in an apartment building 27 yards away. Capturing the vibrations from the bulb, they were able to reconstruct, with a fair degree of fidelity, "Let It Be" by the Beatles, "Clocks" by Coldplay and a snippet of a speech by President Trump.

"We show how fluctuations in the air pressure on the surface of the hanging bulb (in response to sound), which cause the bulb to vibrate very slightly (a millidegree vibration), can be exploited by eavesdroppers to recover speech and singing, passively, externally, and in real time," the researchers said.

They noted that a direct line of sight to the bulb is required; lampshades or window curtains will prevent it from working. Also, the test sounds were played at maximum volume.

The approach, called "lamphone," is an improvement over recent developments in eavesdropping technology.

"Any sound in the room can be recovered from the room with no requirement to hack anything and no device in the room," explained Ben Nassi, a developer of the program and researcher at Ben-Gurion University of the Negev. "You just need line of sight to a hanging bulb, and this is it."

Previous comparable approaches include the memorable 2014 "visual microphone" developed by MIT, Microsoft and Adobe that reconstructed speech and music from a room by analyzing micro-vibrations from a bag of potato chips sitting on a table. While

impressive, the device required massive computational power and much time to analyze recorded vibrations. Lamphone can be conducted in real time.

Similarly, Stanford University researchers also in 2014 discovered they could tap into vibrations stemming from pressure plates in Android device gyroscopes and determine at least some of what is said in its vicinity. But Nassi said that approach required first obtaining and infecting the target's hardware. The lamphone requires no manipulation of the target's device and no entry into the target's office.

"When you actually use it in real time you can respond in real time rather than losing the opportunity," Nassi said in an interview with Wired magazine.

He was quick to remind observers that he's not interested in providing a roadmap for future hackers.

"We want to raise the awareness of this kind of attack vector," he said. "We're not in the game of providing tools."

Eavesdropping has a long and colorful history. Miniature cameras that could fit in a buttonhole were devised as early as 1885. Carrier pigeons were equipped with mini-cameras in World War I. Years later, an American ambassador in Moscow was housed in an office found to have a dollar-sized commemorative display with no battery or wires that used radio waves to secretly transmit conversations. U.S. officials never determined precisely how it worked.

In a precursor to lamphone, the Soviets decades ago used infrared waves reflected off certain points on windows to decipher speech.

And exactly 60 years ago this August, the United States launched and

then recovered in mid-air a satellite holding 20 pounds of film capable of closeup photography over enemy territories. The satellite's name, coincidentally, was Corona.

And finally, there is always old-fashioned sex. Russian KGB spies attempting to blackmail Indonesian President Ahmed Sukarno, known for his great fondness of sexual pleasures, lured him to a plane where a party filled with young girls was held. Sukarno ultimately invited the girls to his hotel room, where two hidden cameras recorded everything. But when the film was played for him in a private showing where it was expected he would capitulate to blackmail, he instead was so impressed with his performance in the sex tapes that he asked for additional copies to play in Indonesian theaters.

Lamphone probably would have worked better.

More information: Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations (PDF)

www.nassiben.com/lamphone

Citation: Light bulb vibrations yield eavesdropping data (2020, June 15) retrieved 27 April 2024 from https://techxplore.com/news/2020-06-bulb-vibrations-yield-eavesdropping.html