

Researchers hack Siri, Alexa, and Google Home by shining lasers at them

Sugawara et al.

reader comments

104 with 80 posters participating, including story author

Share this story

Siri, Alexa, and Google Assistant are vulnerable to attacks that use lasers to inject inaudible—and sometimes invisible—commands into the devices and surreptitiously cause them to unlock doors, visit websites, and locate, unlock, and start vehicles, researchers report in a research paper published on Monday. Dubbed Light Commands, the attack works against Facebook Portal and a variety of phones.

Shining a low-powered laser into these voice-activated systems allows attackers to inject commands of their choice from as far away as 360 feet (110m). Because voice-controlled systems often don't require users to authenticate themselves, the attack can frequently be carried out without the need of a password or PIN. Even when the systems require authentication for certain actions, it may be feasible to brute force the PIN, since many devices don't limit the number of guesses a user can make. Among other things, light-based commands can be sent from one building to another and penetrate glass when a vulnerable device is kept near a closed window.

The attack exploits a vulnerability in microphones that use

micro-electro-mechanical systems, or MEMS. The microscopic MEMS components of these microphones unintentionally respond to light as if it were sound. While the researchers tested only Siri, Alexa, Google Assistant, Facebook Portal, and a small number of tablets and phones, the researchers believe all devices that use MEMS microphones are susceptible to Light Commands attacks.

A novel mode of attack

The laser-based attacks have several limitations. For one, the attacker must have direct line of sight to the targeted device. And for another, the light in many cases must be precisely aimed at a very specific part of the microphone. Except in cases where an attacker uses an infrared laser, the lights are also easy to see by someone who is close by and has line of sight of the device. What's more, devices typically respond with voice and visual cues when executing a command, a feature that would alert users within earshot of the device.

Despite those constraints, the findings are important for a host of reasons. Not only does the research present a novel mode of attack against voice-controllable, or VC, systems, it also shows how to carry out the attacks in semi-realistic environments. Additionally, the researchers still don't fully understand the physics behind their exploit. A better understanding in the coming years may yield more effective attacks. Last, the research highlights the risks that result when VC devices, and the peripherals they connect to, carry out sensitive commands without requiring a password or PIN.

"We find that VC systems are often lacking user authentication mechanisms, or if the mechanisms are present, they are incorrectly implemented (e.g., allowing for PIN bruteforcing)," the researchers wrote in a paper titled Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems. "We show how an attacker can use light-

injected voice commands to unlock the target's smart-lock protected front door, open garage doors, shop on e-commerce websites at the target's expense, or even locate, unlock and start various vehicles (e.g., Tesla and Ford) if the vehicles are connected to the target's Google account."

Below is a video explaining the Light Commands attack:

[embedded content]
LightCommands v3 2

Low cost, low power requirements

The paper describes different setups used to carry out the attacks. One is composed of a simple laser pointer (price \$18 for three), a Wavelength Electronics LD5CHA laser driver (\$339), and a Neoteck NTK059 audio amplifier (\$27.99). The setup can use an optional Opteka 650-1300mm telephoto lens (\$199.95) to focus the laser for long-range attacks. The laser driver and diodes are intended for lab use, a condition that requires an attacker to experience with lasers to successfully assemble and test the setups.

[embedded content]
Light Commands demo with inexpensive setup.
Another setup used an infrared laser that's invisible to the human eye for more stealthy attacks. A third setup relied on an Acebeam W30 500 lumens laser-excited phosphor flashlight to eliminate the requirement to precisely aim a light on a specific part of a MEMS microphone.

One of the researchers' attacks successfully injected a command through a glass window 230 feet away. In that experiment, a VC device was positioned next to a window on the fourth floor of a building, or about 50 feet above the ground. The attacker's laser was placed on a platform inside a nearby bell tower, located about 141 feet above ground level. The laser then shined a light onto the Google Home device, which

has only top-facing microphones.

Enlarge / A diagram of the building-to-building attack using Light Commands.

Sugawara et al.

[embedded content]

Building-to-building Light Commands attack.

In a different experiment, the researchers used a telephoto lens to focus the laser to successfully attack a VC device 360 feet away. The distance was the maximum allowed in the test environment, raising the possibility that longer distances are possible.

[embedded content]

Light Commands in a corridor.

<https://arstechnica.com/?p=1595561>