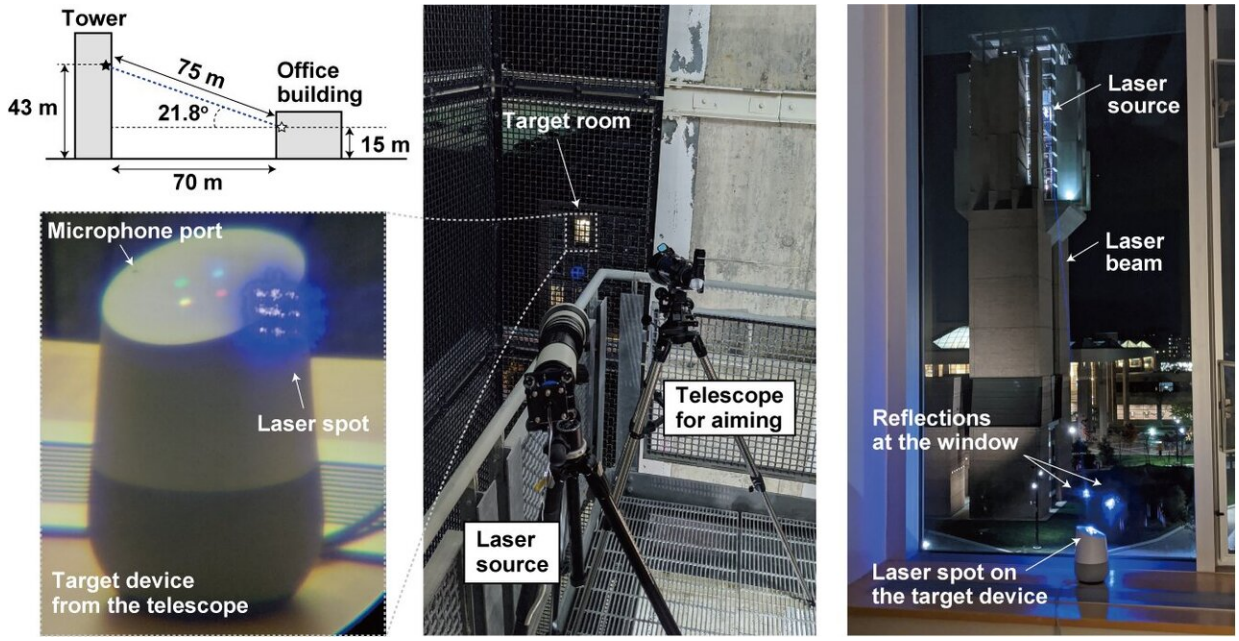
When a light is a thief that tells your garage door to open

November 6 2019, by Nancy Cohen



Credit: lightcommands.com

Shining lasers at voice assistants like Alexa and Siri, researchers from Michigan and Japan achieved a hack where lasers had the power of commands from the human voice.

By shining the laser through the window at microphones inside devices like tablets, or phones, a far away attacker can remotely send inaudible and potentially invisible commands acted on by Alexa, Portal, Google

assistant or Siri.

Simply put, an attacker can hijack the voice assistant and send commands.

How did the team carry out light as sound? A vulnerability in microphones using micro-electro-mechanical systems (MEMS) is exploited. The MEMS components unintentionally respond to light as if it were sound, said *Ars Technica*.

What's the worst that can happen? A lot. *Ars Technica* described the lasers injecting inaudible commands into the devices and surreptitiously causing them "to unlock doors, visit websites, and locate, unlock, and start vehicles."

The researchers discussed their work in their paper published on Monday. "Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems" is by five authors with affiliations from the University of Michigan (four) and from The University of Electro-Communications, Japan (one).

"In our paper," they said, "we demonstrate this effect, successfully using light to inject malicious commands into several voice controlled devices such as smart speakers, tablets, and phones across large distances and through glass windows."

How easy was it to carry out?

For thwarting authentication, fairly easy.

"Voice-controlled systems often don't require users to authenticate themselves," wrote *Ars Technica*'s Dan Goodin. The attack in those instances could be frequently carried out with no need for passwords or

PINs. Frequently. "Even when the systems require authentication for certain actions," he added, "it may be feasible to brute force the PIN, since many devices don't limit the number of guesses a user can make."

Also, the attack was not expensive to carry out. Light commands can be mounted cheaply, said a video presenter, using regular laser pointers. This could even be done between two buildings.

The team said they tried their attack on popular voice recognition systems, namely Amazon Alexa, Apple Siri, Facebook Portal, and Google Assistant. Actually, though, "any system that uses MEMS microphones and acts on this data without additional user confirmation might be vulnerable," according to their own light commands site.

What's the danger with Light Commands?

Alexa, what's the weather? That's harmless. The attacker can control smart-home switches. Open smart garage doors. Remotely start vehicles. In fact, you can watch a video injecting "OK Google, open the garage door" to a Google Home just by shining a cheap laser pointer.

What can be done to protect against the vulnerability? The video presenter said the basic vulnerability cannot be addressed without expensive microphone redesign.

"We are collaborating with Amazon, Google, Apple, as well as other vendors on defensive measures." They have more information and demonstrations at lightcommands.com.

"An additional layer of authentication can be effective at somewhat mitigating the attack. Alternatively, in case the attacker cannot eavesdrop on the device's response, having the device ask the user a simple randomized question before command execution can be an

effective way at preventing the attacker from obtaining successful command execution.

"Manufacturers can also attempt to use sensor fusion techniques, such as acquire audio from multiple microphones. When the attacker uses a single laser, only a single microphone receives a signal while the others receive nothing...

Another approach consists in reducing the amount of light reaching the microphone's diaphragm using a barrier that physically blocks straight light beams for eliminating the line of sight to the diaphragm, or implement a non-transparent cover on top of the microphone hole for attenuating the amount of light hitting the microphone. However, we note that such physical barriers are only effective to a certain point, as an attacker can always increase the laser power in an attempt to compensate for the cover-induced attenuation or for burning through the barriers, creating a new light path."

The above appeared on their light commands site, while the paper also discussed mitigation approaches and limitations.

Meanwhile, Mariella Moon in *Engadget* reminded her readers that this would not be the first time researchers found vulnerabilities in digital assistants. "Researchers from China's Zheijiang University found that Siri, Alexa and other voice assistants can be manipulated with commands sent in ultrasonic frequencies."

More information: lightcommands.com/
Paper (PDF): lightcommands.com/20191104-Light-Commands.pdf