NSE News

Lasers Can Hack Voice Assistant Systems, Research Finds

Pointing a laser or flashlight into the microphone of a Google Home, Siri or Alexa system, allowed researchers to control the devices and the systems connected to them.

In a paper published by the University of Michigan on Monday, cybersecurity researchers shared their findings of how they were able to manipulate Amazon, Google and Apple digital assistants from hundreds of feet away. In some cases, some were able to take over the devices from over 300 feet away and through glass windows. Researchers describe this vulnerability as manipulation by "Light Commands." Laser Pointers and Flashlights were utilized to shine light into the microphone of the voice assistant devices. From there they were able to inject inaudible and invisible commands into smart speakers, tablets and phones.

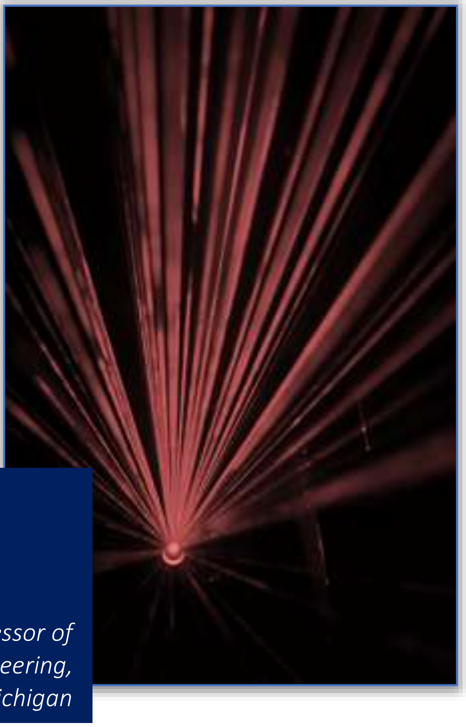
> "Just five milliwatts of laser power—the equivalent of a laser pointer—was enough to obtain full control over many popular Alexa and Google smart home devices, while about 60 milliwatts was sufficient in phones and tablets."
>
> *– Michigan News, University of Michigan*

The threats associated with the attacks tested range from minor, to quite concerning depending on how much a user has connected to their assistant device. Successful Light Command attacks from the study were able to accomplish a number of takeovers.

- *Unlock a smart-lock enabled front door*
- *Open a Garage Door connected to the assistant*
- *Shop on websites*
- *Locate, unlock & start a car connected to the account*

17 different devices were tested, representing a range of the most popular assistants in the market.

Companies affected by the issue, including Tesla, Ford, Amazon, Apple and Google, were notified of the light vulnerability prior to the release of the paper by Michigan University. Each corporation stated they were studying the issues detailed in the research.



How Can You Take Action?

"One suggestion is to simply avoid putting smart speakers near windows, or otherwise attacker-visible places," said Sara Rampazzi, a researcher in computer science and engineering at the university. "While this is not always possible, it will certainly make the attacker's window of opportunity smaller. Another option is to turn on user personalization, which will require the attacker to match some features of the owner's voice in order to successfully inject the command."

> "This is the tip of the iceburg."
>
> *– Kevin Fu, associate professor of computer science and engineering, University of Michigan*