BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

Siri, Google Assistant, and Amazon Alexa can be Hijacked with Light
By Mohsin Saleem Ullah, LLM Candidate 2020 | 19 November 2019

Researchers have recently found that voice assistant technology is vulnerable to hijacking by cheap lasers.

Researchers from Tokyo's University of Electro-Communications and the University of Michigan have almost bested inbuilt security mechanism in voice-controlled devices, including popular smartphones. A mere shining of a bright laser at the devices' microphone is interpreted as a sound by their system.

Researchers have concluded that by producing electrical signals in the light beam on microphones hijackers may control a device because the system will interpret it as a genuine command. For this test, the cheap laser pointers used was around $13.99 to $17.99. This was coupled with a sound amplifier to direct speakers with a specific instruction cost of $27.99. A laser device was also connected to control the Lasers intensity. This was the most expensive tool of all, costing $339.

The team ran a test on voice control speakers and smartphones of renowned major tech firms, such as Google's Assistant, Amazon's Alexa, and Apple's Siri. The list is not exhaustive, but includes Google Home, various Amazon Echo models, the Apple Home Pod, and Facebook's Portal speaker, which runs Alexa. They also tested an iPhone XR, a Samsung Galaxy S9, and a Google Pixel 2.

Relying on inbuilt security layers in the gadgets is now in question. The varying degree of vulnerability in tablets, phones, and speakers is another issue discovered by the researchers after shining the laser from some distance, including through windows. Out of all devices tested, Google Home was hijacked from 110 meters away.

But it may relieve anxieties to consumers using iPhone, iPad, and a few Android smartphones that these devices require extra layers of authentication or a "Wake Word" to activate a device before the hijackers trick the system. This additional authentication of preventing a system against an invasion requires a system hacker to use a wake-up a command such as "Hey Siri" or "OK Google. Unfortunately, these additional security measures are missing in the smart speakers.

Researchers went to great lengths to explain in their paper the prospective chance that lasers could also be used to unlock smartphones and devices connected with it. This could expose consumers credit card information and even result in the ability to unlock tech-driven cars which are connected to a victim's Google account.

Since the paper's publication, it is clear that tech giants such as Amazon need to update their gadgets security software to protect against any foreign invasion. Unfortunately, the research has already shaken consumers trust.