GlobalResearch
Center for Research on Globalization

Ultrasonic Attacks Can Trigger Alexa & Siri with Hidden Commands, Raise Serious Security Risks

By Zero Hedge
Global Research, May 17, 2018
Zero Hedge 16 May 2018

Region: USA
Theme: Intelligence

Over the last two years, academic researchers have identified various methods that they can transmit hidden commands that are undetectable by the human ear to Apple's Siri, Amazon's Alexa, and Google's Assistant.

According to a new report from The New York Times, scientific researchers have been able "to secretly activate the artificial intelligence systems on smartphones and smart speakers, making them dial phone numbers or open websites." This could, perhaps, allow cybercriminals to unlock smart-home doors, control a Tesla car via the App, access users' online bank accounts, load malicious browser-based cryptocurrency mining websites, and or access all sort of personal information.

In 2017, Statista projected around 223 million people in the U.S. would be using a smartphone device, which accounts for roughly 84 percent of all mobile users. Of these 223 million smartphones users, around 108 million Americans are using the Android Operating System, and some 90 million are using Apple's iOS (operating system). A new Gallup poll showed that 22 percent of Americans are actively using Amazon Echo or Google Assistant in their homes.

With much of the country using artificial intelligence systems on smartphones and smart speakers, a new research document published from the University of California, Berkeley indicates inaudible commands could be embedded "directly into recordings of music or spoken text," said The New York Times.

For instance, a millennial could be listening to their favorite song: 'The Middle' by Zedd, Maren Morris & Grey. Embedded into the audio file could have several inaudible commands triggering Apple's Siri or Amazon's Alexa to complete a task that the user did not instruct — such as, buying merchandise from the music performer on Amazon.

> "We wanted to see if we could make it even more stealthy," said Nicholas Carlini, a fifth-year Ph.D. student in computer security at U.C. Berkeley and one of the paper's authors.

At the moment, Carlini said this is only an academic experiment, as it is only a matter of time before cybercriminals figure out this technology.

> "My assumption is that the malicious people already employ people to do what I do," he added.

The New York Times said Amazon "does not disclose specific security measure" to thwart a device from an ultrasonic attack, but the company has taken precautionary measures to protect users from unauthorized human use. Google told The New York Times that security development is ongoing and has developed features to mitigate undetectable audio commands.

> Both companies' [Amazon and Google] assistants employ voice recognition technology to prevent devices from acting on certain commands unless they recognize the user's voice.
>
> Apple said its smart speaker, HomePod, is designed to prevent commands from doing things like unlocking doors, and it noted that iPhones and iPads must be unlocked before Siri will act on commands that access sensitive data or open apps and websites, among other measures.
>
> Yet many people leave their smartphones unlocked, and, at least for now, voice recognition systems are notoriously easy to fool.
>
> There is already a history of smart devices being exploited for commercial gains through spoken commands," said The New York Times.

Last year, there were several examples of companies and even cartoons taking advantage of weaknesses in voice recognition systems, including Burger King's Google Home commercial to South Park's episode with Alexa.

While there are currently no American laws against broadcasting subliminal or ultrasonic messages to humans, let alone artificial intelligence systems on smartphones and smart speakers. The Federal Communications Commission (FCC) warns against the practice, calling it a *"counter to the public interest,"* and the Television Code of the National Association of Broadcasters bans *"transmitting messages below the threshold of normal awareness."* However, The New York Times points out that *"neither says anything about subliminal stimuli for smart devices."*

Recently, the ultrasonic attack technology showed up in the hands of the Chinese. Researchers at Princeton University and China's Zhejiang University conducted several experiments showing that inaudible commands can, in fact, trigger voice-recognition systems in an iPhone.

> "The technique, which the Chinese researchers called DolphinAttack, can instruct smart devices to visit malicious websites, initiate phone calls, take a picture or send text messages. While DolphinAttack has its limitations — the transmitter must be close to the receiving device — experts warned that more powerful ultrasonic systems were possible," said The New York Times.

DolphinAttack could inject covert voice commands at 7 state-of-the-art speech recognition systems (e.g., Siri, Alexa) to activate always-on system and achieve various attacks, which include activating Siri to initiate a FaceTime call on iPhone, activating Google Now to switch the phone to the airplane mode, and even manipulating the navigation system in an Audi automobile. (Source: guoming zhang)

DolphinAttack Demonstration Video

While the number of smart devices in consumers' pockets and at their homes is on the rise, it is only a matter of time before the technology falls into the wrong hands, and unleashed against them. Imagine, cybercriminals accessing your Audi or Tesla via ultrasonic attacks against voice recognition technology on a smart device. Maybe these so-called smart devices are not smart after all, as the dangers of these devices are starting to be realized. Millennials will soon be panicking.

Articles by: Zero Hedge