Issued 9/5/17

A Simple Design Flaw Makes It Astoundingly Easy To Hack Siri and Alexa

Using a technique called the DolphinAttack, a team from Zhejiang University translated typical vocal commands into ultrasonic frequencies that are too high for the human ear to hear, but perfectly decipherable by the microphones and software powering our always-on voice assistants. This relatively simple translation process lets them take control of gadgets with just a few words uttered in frequencies none of us can hear.

The researchers didn't just activate basic commands like "Hey Siri" or "Okay Google," though. They could also tell an iPhone to "call. 123.456.7890" or tell an iPad to FaceTime the number. They could force a Macbook or a Nexus 7 to open a malicious website. They could order an Amazon Echo to "open the backdoor." Even an Audi Q3 could have its navigation system redirected to a new location. "Inaudible voice commands question the common design assumption that adversaries may at most try to manipulate a [voice assistant] vocally and can be detected by an alert user," the research team writes in a paper just accepted to the ACM Conference on Computer and Communications Security.

To hack each voice assistant, the researchers used a smartphone with about $3 of additional hardware, including a tiny speaker and amp. In

theory, their methods, which are now public, are duplicatable by anyone with a bit of technical know-how and just a few bucks in their pocket.

The exploit is enabled by a combination of hardware and software problems, the researchers explain in their paper. The microphones and software that power voice assistants like Siri, Alexa, and Google Home can pick up inaudible frequencies–specifically, frequencies above the 20KhZ limits of human ears. (How high is 20kHz? It's just above the mosquito ringtone that went viral a few years ago, which allowed young students who hadn't damaged their hearing yet to text message friends without their teachers hearing.)