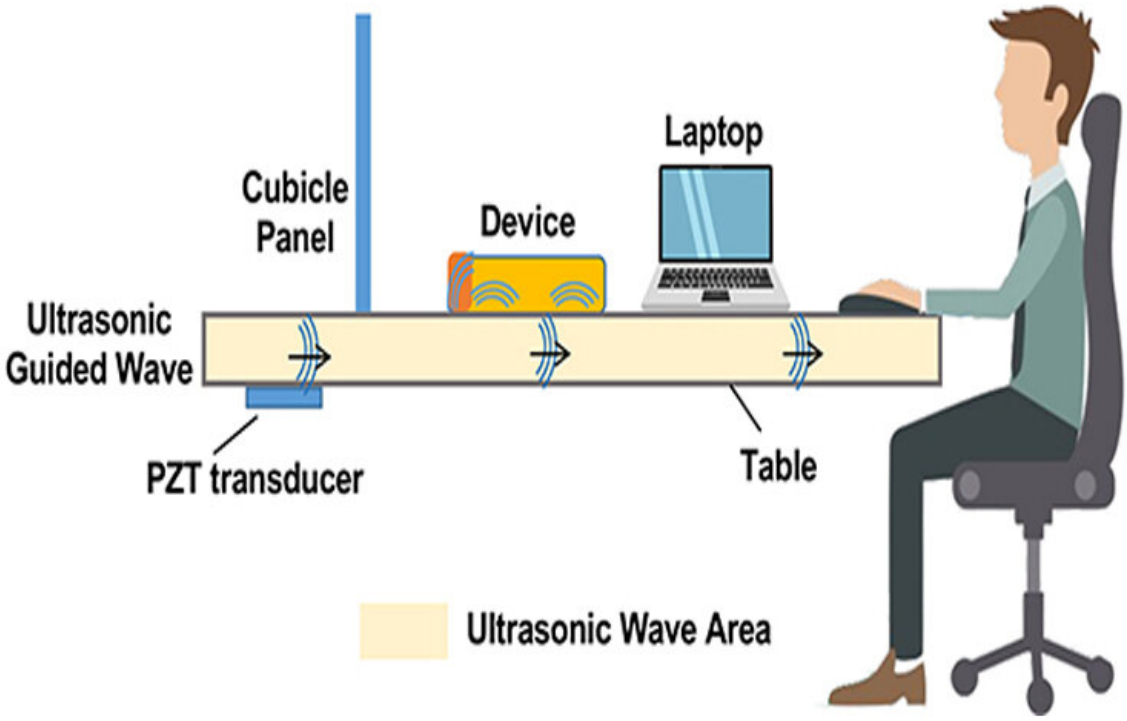
Research finds a new way to hack Siri and Google Assistant with ultrasonic waves

March 12 2020, by Patricia Mroczek, Caroline Brooks



Credit: Michigan State University

Think twice before recharging an iPhone on tabletops in public places like airports and coffee shops.

Researchers at the Michigan State University College of Engineering have discovered a new way for hackers to inexpensively target personal devices and put Apple's Siri and Google Assistant to work against smartphone owners.

Qiben Yan, assistant professor in the Department of Computer Science and Engineering and lead author of the research, said the research team discovered a new attack factor—inaudible vibrations that can be sent through wood, metal and glass tabletops to command voice assistant devices up to 30 feet away.

The research, SurfingAttack, was presented Feb. 24 at the Network and Distributed System Security Symposium in San Diego.

Yan advises smartphone owners to be wary of public charging stations. "Hackers could use malicious ultrasonic waves to secretly control the voice assistants in your smart devices," he said. "It can be activated using phrases like, "OK Google' or "Hey Siri," as wake-up words. Then, attack commands can be generated to control your voice assistants, like 'read my messages," or make a fraud call using text-to-speech technology.

"In other words," Yan said, "they can call your friends, family and colleagues and do all sorts of things—from canceling plans to asking for money. If you are tech-savvy and own voice controllable smart home gadgets, hackers may even use your smartphones to control your smart gadgets, for example, setting home temperature or opening the garage door."

Yan said hackers attach a low-cost piezoelectric transducer under a table or charging station, making it possible for an attacker to inconspicuously hijack two-factor authentication codes and even place fraudulent calls

Hanqing Guo, an MSU graduate student in the Department of Computer

Science and Engineering and co-author of the study, said "It's pretty scary to see my phone being activated and controlled in public spaces without my knowledge. Our research exposes the insecurity of smartphone voice assistants, which everyone needs to be aware of."

SurfingAttack worked on 15 out of 17 phone models tested, including four iPhones; the 5, 5s, 6 and X; the first three Google Pixels; three Xiaomis; Mi 5, Mi 8 and Mi 8 Lite; the Samsung Galaxy S7 and S9 and the Huawei Honor View 8.

"Our research exposes the insecurity of smartphone voice assistants,"said Guo.

Yan, who directs MSU's Secure Intelligent Things Lab, worked in collaboration with researchers from MSU, Washington University in St. Louis, Chinese Academy of Sciences and the University of Nebraska-Lincoln.

"Our best advice is if you are going to place your unattended phone on a table to recharge, make sure it's not flat," he said. "SurfingAttack can be made less effective by simply lifting your phone up or using a soft woven tablecloth. Lean your phone on something to disrupt the ultrasonic guided waves. The fix is simple and adds a layer of security."

More information: For additional videos, see surfingattack.github.io/

Provided by Michigan State University