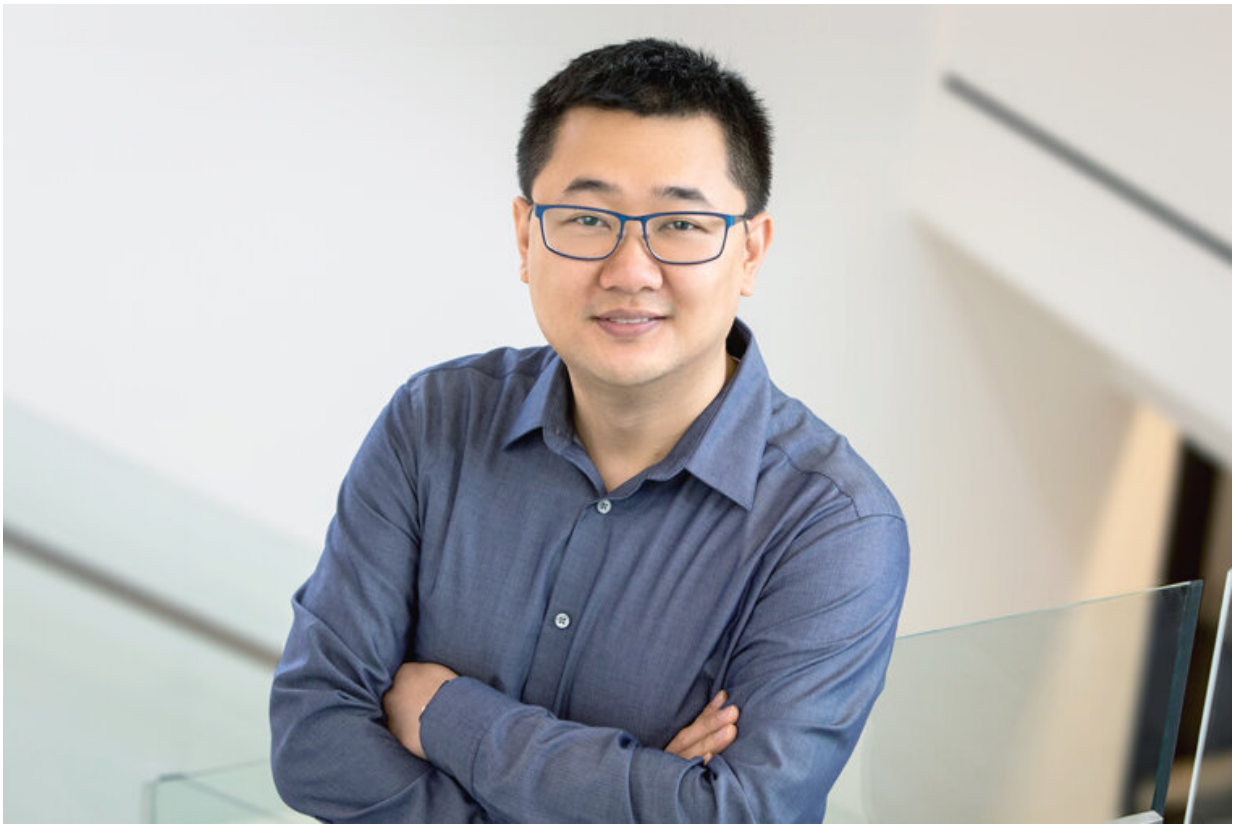
'Surfing attack' hacks Siri, Google with ultrasonic waves

February 27 2020, by Brandie Jefferson



Ning Zhang, assistant professor of computer science and engineering at the McKelvey School of Engineering. Credit: Washington University in St. Louis

Ultrasonic waves don't make a sound, but they can still activate Siri on your cellphone and have it make calls, take images or read the contents

of a text to a stranger. All without the phone owner's knowledge.

Attacks on cell phones aren't new, and researchers have previously shown that ultrasonic waves can be used to deliver a single command through the air.

However, new research from Washington University in St. Louis expands the scope of vulnerability that ultrasonic waves pose to cellphone security. These waves, the researchers found, can propagate through many solid surfaces to activate voice recognition systems and—with the addition of some cheap hardware—the person initiating the attack can also hear the phone's response.

The results were presented Feb. 24 at the Network and Distributed System Security Symposium in San Diego.

"We want to raise awareness of such a threat," said Ning Zhang, assistant professor of computer science and engineering at the McKelvey School of Engineering. "I want everybody in the public to know this."

Zhang and his co-authors were able to send "voice" commands to cellphones as they sat inconspicuously on a table, next to the owner. With the addition of a stealthily placed microphone, the researchers were able to communicate back and forth with the phone, ultimately controlling it from afar.

Ultrasonic waves are sound waves in a frequency that is higher than humans can hear. Cellphone microphones, however, can and do record these higher frequencies. "If you know how to play with the signals, you can get the phone such that when it interprets the incoming sound waves, it will think that you are saying a command," Zhang said.

To test the ability of ultrasonic waves to transmit these "commands"

through solid surfaces, the research team set up a host of experiments that included a phone on a table.

Attached to the bottom of the table was a microphone and a piezoelectric transducer (PZT), which is used to convert electricity into ultrasonic waves. On the other side of the table from the phone, ostensibly hidden from the phone's user, is a waveform generator to generate the correct signals.

The team ran two tests, one to retrieve an SMS (text) passcode and another to make a fraudulent call. The first test relied on the common virtual assistant command "read my messages" and on the use of two-factor authentication, in which a passcode is sent to a user's phone—from a bank, for instance—to verify the user's identity.

The attacker first told the virtual assistant to turn the volume down to Level 3. At this volume, the victim did not notice their phone's responses in an office setting with a moderate noise level.

Then, when a simulated message from a bank arrived, the attack device sent the "read my messages" command to the phone. The response was audible to the microphone under the table, but not to the victim.

In the second test, the attack device sent the message "call Sam with speakerphone," initiating a call. Using the microphone under the table, the attacker was able to carry on a conversation with "Sam."

The team tested 17 different phone models, including popular iPhones, Galaxy and Moto models. All but two were vulnerable to ultrasonic wave attacks.

Ultrasonic waves made it through metal, glass and

wood

They also tested different table surfaces and phone configurations.

"We did it on metal. We did it on glass. We did it on wood," Zhang said. They tried placing the phone in different positions, changing the orientation of the microphone. They placed objects on the table in an attempt to dampen the strength of the waves. "It still worked," he said. Even at distances as far as 30 feet.

Ultrasonic wave attacks also worked on plastic tables, but not as reliably.

Phone cases only slightly affected the attack success rates. Placing water on the table, potentially to absorb the waves, had no effect. Moreover, an attack wave could simultaneously affect more than one phone.

The research team also included researchers from Michigan State University, the University of Nebraska-Lincoln and the Chinese Academy of Sciences.

Zhang said the success of the "surfing attack," as it's called in the paper, highlights the less-often discussed link between the cyber and the physical. Often, media outlets report on ways in which our devices are affecting the world we live in: Are our cellphones ruining our eyesight? Do headphones or earbuds damage our ears? Who is to blame if a self-driving car causes an accident?

"I feel like not enough attention is being given to the physics of our computing systems," he said. "This is going to be one of the keys in understanding attacks that propagate between these two worlds."

The team suggested some defense mechanisms that could protect against such an attack. One idea would be the development of phone software

that analyzes the received signal to discriminate between ultrasonic waves and genuine human voices, Zhang said. Changing the layout of mobile phones, such as the placement of the microphone, to dampen or suppress ultrasound waves could also stop a surfing attack.

But Zhang said there's a simple way to keep a phone out of harm's way of ultrasonic waves: the interlayer-based defense, which uses a soft, woven fabric to increase the "impedance mismatch."

In other words, put the phone on a tablecloth.

More information: Qiben Yan et al, SurfingAttack: Interactive Hidden Attack on Voice Assistants Using Ultrasonic Guided Waves, *Proceedings 2020 Network and Distributed System Security Symposium* (2020). DOI: 10.14722/ndss.2020.24068