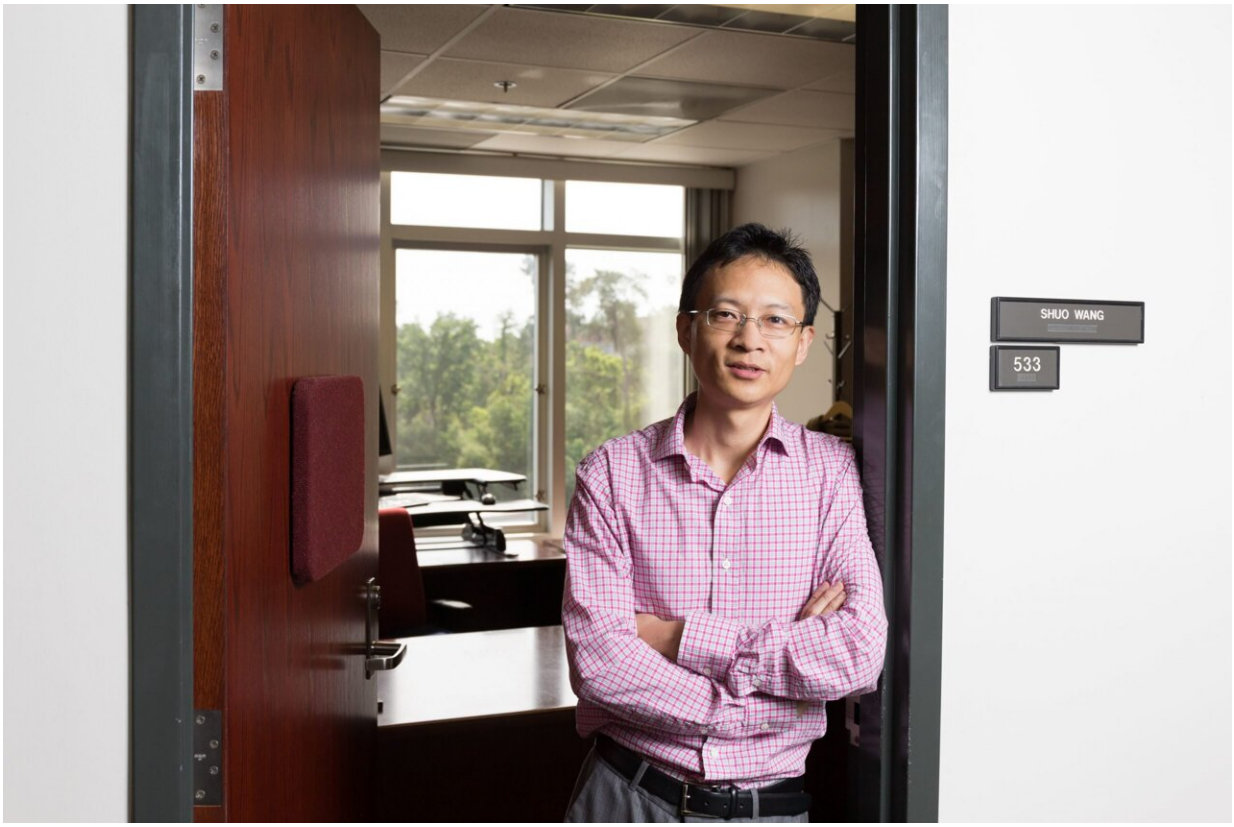
New 'invisible finger' technology poses potential phone-hacking threats, researchers say

February 9 2023, by Karen Dooley



Shuo Wang. Credit: University of Florida

When a team of researchers from the University of Florida unveiled new technology that allows someone to hack into a nearby touchscreen-

enabled device using what they call an "invisible finger," those in the field of cybersecurity took notice.

The discovery, publicly recognized by the Institute of Electrical and Computer Engineering during its 2022 Symposium on Security and Privacy, was reported in dozens of trade publications, including PC Magazine and Digital Information World. And leading device manufacturers quickly reached out to the researchers, inviting input on how they could get ahead of the potential security threat.

"Our research is designed to help the industry identify vulnerabilities, so they can improve the security of their products for the customers and reduce the potential for phone-hacking," said Shuo Wang, the UF electrical and computer engineering professor who led the team. "In other words, we're looking for the weaknesses."

So what is the invisible finger?

The hacking technique uses a set of multiple connected antennas, known as an antenna array, to remotely tap and swipe a touchscreen through electromagnetic signals. Once controllers gain access, they can perform a variety of criminal acts—for example, download malware or send themselves money through the victim's account on a payment platform.

"An attack like this is possible because most modern touchscreens work by using electrodes placed underneath the screen to detect the small electrical charge released by a finger when it comes into contact with the screen," Wang said. "The pressure from the finger is not a factor."

The team became involved with this line of research after working on an earlier project with Google in which they investigated whether touchscreens are susceptible to the noise around them, including electrical and magnetic noise. The team's findings prompted them to

explore other ways in which touchscreens might be vulnerable.

"We learned the basic fundamentals behind the touchscreen and how they can react to the noise," Wang said. "We then used that knowledge to develop another technology to reduce the immunity of the touchscreen and compromise the security of the device."

As researchers demonstrate the invisible finger, they note that the new type of hacking has a few key limitations and is a proof-of-concept at this point—far from being a threat to the public. Wang explained that the invisible finger's false touch works only when the victim's phone is unlocked, or the attacker knows the password and the phone is placed face down on a surface. And the antenna array must be no more than four centimeters away.

While the threat isn't realized just yet, Wang's goal is to stay ahead of any would-be hackers and help manufacturers prevent the problem before it starts.

"Our task now is to continue to improve on the technology, make it more powerful and increase the distance of its effectiveness," he said. "We have a comprehensive team with varied backgrounds, including hardware and software security, electromagnetic interference and power electronics. That kind of collaboration is why we've been successful in developing this technology."

Provided by University of Florida