Researchers find a new way to snoop with smartphones. But should you be worried?

August 14 2019, by Jordan Wilkerson, The Dallas Morning News

Credit: CC0 Public Domain

Smartphones are like living things. With their cameras and microphones, they can see and hear. They can detect the amount of ambient lighting, the air pressure and the temperature—among a host of other aspects

about the environment they're in.

Six years ago, less than half of Americans owned a smartphone. Four out of five own one now, says the Pew Research Center. There are millions of people walking around every day with a vast array of these sensors in their pockets.

And smartphones can record all of it.

This has created major concern about how easily one's privacy can be invaded by these sensor-rich devices, with particular focus on the cameras and microphones. SMU professors Eric Larson and Mitchell Thornton recently looked into how a more eccentric sensor could be used to eavesdrop on you: the phone's motion sensors.

The researchers created an app laced with aspects of artificial intelligence, which an attacker could use to figure out some of what you're typing. The attacker would just need to place a few smartphones with the app on the same table as your computer.

A couple of smartphones can correctly guess almost half of all the keystrokes you type, according to the SMU researchers. Around a fourth of the words can be "perfectly translated" even when people are talking around you, says Dr. Larson, an expert in mobile computing.

And the smartphones can determine these words just seconds after you type it. The researchers' study was published earlier this summer in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*.

You're probably not typing up classified information at Starbucks. But even typed conversations you consider benign could provide an attacker unnerving insight about you. "For example, if you're at a coffee shop,

and you answer an email from your child. If anyone were to be listening, you've just divulged the fact that you have a child that's not with you," says Thornton.

The cluster of smartphones, however, doesn't do a particularly good job of picking up passcodes. The app, in its current configuration, is trained to pick up conversation. Passwords, often being a nonsensical collection of numbers and letters, go under the radar.

But by using the app to narrow down which characters are typed, "instead of taking years to decode someone's password, it may take days," Larson says.

Before this study, scientists had already examined this issue but in a much more controlled way. In previous studies, no noise other than typing was permitted. The person had to type at a constant, steady rate. They had a restricted vocabulary.

That's cute, but it's not the most realistic set-up. For the SMU study, a person sat in a conference room, typing at whatever pace they wanted and use whatever words they wanted. The person could even chat with other people in the conference room as they typed.

"This study explored a more real-world scenario for this attack," says Dr. Nitesh Saxena, a computer science professor at the University of Alabama at Auburn who was not involved with the study.

So how can someone use a couple smartphones to snoop on what you're typing, anyway? The app uses two of the smartphone's sensors in ways they were not intended: the microphone and the accelerometer. The microphone detects the sounds made by your keystrokes.

In general, an accelerometer indicates how quickly an object is moving.

Smartphone makers put this in the phone to help give its orientation. But the SMU researchers use the sensors to pick up much subtler motion. They detect faint vibrations that reverberate through the table when someone types.

"The internal dynamics of a keyboard behaves more like a drum," says Saxena. The tap of each specific key creates a slightly different sound and slightly different vibration in the table. Because of this, every keystroke is potentially unique. The app's aim is to use highly capable sensors in the nearby phones to detect that.

Any time a new snooping attack like this is announced, "the tendency is that people think, "Hey, this attack is too good. My devices are really vulnerable. I should throw my phones out of the window,"" says Saxena.

But a major challenge for this attack is that each type of keyboard is like a different drum. Each table vibrates differently, too.

The researchers' app must be taught the different sounds and vibrations from that specific keyboard/table combination before the smartphones can figure out much of anything.

Most people likely do not know how to create an app like this, let alone optimize it for a specific computer and tabletop. "It's not like some teenager is going to come up here and use this technology and infer what anybody's typing. It's going to require people that have some training," Larson says.

The researchers tested a few different types of keyboards and tables. Though more thorough research awaits, they found that the accuracy of word-guessing falls drastically if you try to apply what the app learned about one table to another.

This means you also don't need to worry about accidentally downloading malware on your own phone that snoops on you like this, says Larson. At least not yet. "With enough training data," he says, "this could be at the level to where you don't need to understand something in the room. That's a possibility."

Tech companies like Google currently require that apps request user permission to access the microphone and camera. They don't need permission to tap into your phone's motion sensors.

"I don't know if the designers thought about, "Hey, we can also use this to pick up vibrations of keyboard typing." I don't think they did," Thornton says.

Should tech companies change their policy now before these kinds of attacks become more feasible? "They should do it," Saxena says. "There's no harm in letting the user know which app is accessing these sensors even though the threat may not be practical at this point in time."

But there's perhaps a better question about the malicious use of motion sensors in smartphones: should the public be worried about this?

"They should not be concerned," Saxena says, "but they should be aware."