Contact Monifa Thomas-Nguyen at 773-619-4693 (cell) or 214-768-7640 (office)

ATTACKERS COULD SOON BE LISTENING TO WHAT YOU TYPE

SMU researchers were able to detect what is typed with remarkable accuracy using just a smartphone

DALLAS (SMU) – You likely know to avoid suspicious emails to keep hackers from gleaning personal information from your computer. But a new study from SMU (Southern Methodist University) suggests that it's possible to access your information in a much subtler way: by using a nearby smart phone to intercept the sound of your typing.

Researchers from SMU's Darwin Deason Institute for Cybersecurity found that acoustic signals, or sound waves, produced when we type on a computer keyboard can successfully be picked up by a smartphone. The sounds intercepted by the phone can then be processed, allowing a skilled hacker to decipher which keys were struck and what they were typing.

The researchers were able to decode much of what was being typed using common keyboards and smartphones – even in a noisy conference room filled with the sounds of other people typing and having conversations.

"We were able to pick up what people are typing at a 41 percent word accuracy rate. And we can extend that out – above 41 percent – if we look at, say, the top 10 words of what we think it might be," said Eric C. Larson, one of the two lead authors and an assistant professor in SMU Lyle School's Department of Computer Science.

The study was published in the June edition of the journal *Interactive, Mobile, Wearable and Ubiquitous Technologies*. Co-authors of the study are Tyler Giallanza, Travis Siems, Elena Sharp, Erik Gabrielsen and Ian Johnson – all current or former students at the Deason Institute.

It might take only a couple of seconds to obtain information on what you're typing, noted lead author Mitch Thornton, director of SMU's Deason Institute and professor of electrical and computer engineering.

"Based on what we found, I think smartphone makers are going to have to go back to the drawing board and make sure they are enhancing the privacy with which people have access to these sensors in a smartphone," Larson said.

SMU Simulated a Noisy Conference Room, But Typing Could Still Be Intercepted

The researchers wanted to create a scenario that would mimic what might happen in real life. So they arranged several people in a conference room, talking to each other and taking notes on a laptop. Placed on the same table as their laptop or computer, were as many as eight mobile phones, kept anywhere from three inches to several feet feet away from the computer, Thornton said.

Study participants were not given a script of what to say when they were talking, and were allowed to use shorthand or full sentences when typing. They were also allowed to either correct typewritten errors or leave them, as they saw fit.

“We were looking at security holes that might exist when you have these ‘always-on’ sensing devices – that being your smartphone,” Larson said. “We wanted to understand if what you’re typing on your laptop, or any keyboard for that matter, could be sensed by just those mobile phones that are sitting on the same table.”

The answer was a definite, “Yes.”

But just how does it work?

“There are many kinds of sensors in smartphones that cause the phone to know its orientation and to detect when it is sitting still on a table or being carried in someone’s pocket. Some sensors require the user to give permission to turn them on, but many of them are always turned on,” Thornton explained. “We used sensors that are always turned on, so all we had to do was develop a new app that processed the sensor output to predict the key that was pressed by a typist.”

There are some caveats, though.

“An attacker would need to know the material type of the table,” Larson said, because different tables create different sound waves when you type. For instance, a wooden table like the kind used in this study sounds different than someone typing on a metal tabletop.

Larson said, “An attacker would also need a way of knowing there are multiple phones on the table and how to sample from them.”

A successful interception of this sort could potentially be very scary, Thornton noted, because “there’s no way to know if you’re being hacked this way.”

The Deason Institute is part of SMU’s Lyle School of Engineering, and its mission is to to advance the science, policy, application and education of cyber security through basic and problem-driven, interdisciplinary research.

About SMU

SMU is the nationally ranked global research university in the dynamic city of Dallas. SMU’s alumni, faculty and nearly 12,000 students in seven degree-granting schools demonstrate an entrepreneurial spirit as they lead change in their professions, communities and the world.