Is your smartphone spying on you?

6 July 2018, by Bill Ibelle

Credit: CC0 Public Domain

Some popular apps on your phone may be secretly taking screenshots of your activity and sending them to third parties, according to a new study by a team of Northeastern researchers.

The researchers said this is particularly disturbing because these screenshots—and videos of your activity on the screen—could include usernames, passwords, credit card numbers, and other important personal information.

"We found that thousands of popular apps have the ability to record your screen and anything you type," said David Choffnes, one of two computer science professors who supervised the study. "That includes your username and password, because it can record the characters you type before they turn into those little black dots."

The study, which was conducted largely by two students—undergraduate Elleen Pan and doctoral candidate Jingjing Ren—was designed to investigate a persistent urban legend that phones are secretly recording our conversations and then selling that information to companies so they can pepper you with targeted advertisements.

While the researchers found no evidence of recorded conversations, they discovered activity that could be even more dangerous.

"We knew we were looking for a needle in a haystack," said Choffnes, "and we were surprised to find several needles."

What they found is that some companies were sending screenshots and videos of user phone activities to third parties. Although these privacy breaches appeared to be benign, they emphasized how easily a phone's privacy window could be exploited for profit.

"This opening will almost certainly be used for malicious purposes," said Christo Wilson, another computer science professor on the research team. "It's simple to install and collect this information. And what's most disturbing is that this occurs with no notification to or permission by users.

"In the case we caught, the information sent to a third party was zip codes, but it could just as easily have been credit card numbers," he added.

The study

The researchers analyzed more than 17,000 of the most popular apps on the Android operating system, using an automated test program written by the students. Although the study was conducted on Android phones, both Wilson and Choffnes said there is no reason to believe that other phone operating systems would be less vulnerable.

Pan started the project as a research co-op in the fall of 2017 and continued to work on it until she graduated in May. She will present the paper in Barcelona later this month at the Privacy Enhancing Technology Symposium Conference.

"Coming into this project, I didn't think much about phone privacy and neither did my friends," said Pan, who is the first author on the paper. "This has definitely sparked my interest in research, and I will

consider going back to graduate school."

But for the time being, Pan is preparing for the Barcelona conference and starting a job in August as a software engineer for Square, a mobile payments company.

While conducting the research, Wilson said the team was quite surprised as the results came in.

"There were no audio leaks at all—not a single app activated the microphone," he said. "Then we started seeing things we didn't expect. Apps were automatically taking screenshots of themselves and sending them to third parties."

In all, 9,000 of the 17,000 apps had the potential to take screenshots.

"In one case, the app took video of the screen activity and sent that information to a third party," said Wilson.

That app was GoPuff, a fast-food delivery service, which sent the screenshots to Appsee, a data analytics firm for mobile devices. All this was done without the awareness of app users.

Both Wilson and Choffnes emphasized that neither company appeared to have any nefarious intent. They said that web developers commonly use this type of information to debug their apps and improve the user experience.

But that doesn't mean a malicious company couldn't use this privacy window to steal personal information for profit.

"That has the potential to be much worse than having the camera taking pictures of the ceiling or the microphone recording pointless conversations," said Choffnes. "There is no easy way to close this privacy opening."

GoPuff has changed its terms of service agreement to alert users that the company may take screenshots of their use patterns. Google issued a statement emphasizing that its policy requires developers to disclose to users how their information will be collected.

But Wilson said this shields the companies from lawsuits while doing little to protect the privacy of users, who rarely read these long, legalistic agreements.

Both said the privacy window will not be closed until the phone companies redesign their operating systems, which isn't likely to happen anytime soon.

Provided by Northeastern University