New app reveals how your smartphone can spy on you without permission (VIDEO)

Published time: August 17, 2014 15:07
Reuters / Eddie Keogh

Your Android phone can be turned into a microphone without your permission or knowledge. All that's needed are the gyros in your phone that measure orientation. Stanford researchers have shown how to rewire them to pick up sound waves.

Together with the defense firm Rafael, they created an Android app called Gyrophone, which shows just how easy it is to get the vibrating pressure plates used by the gyroscope to pick up vibrations of sound at frequencies in the 80-250Hz range – the base frequencies of the human voice.

"We show that the MEMS gyroscopes found on modern smartphones are sufficiently sensitive to measure acoustic signals in the vicinity of the phone. The resulting signals contain only very low-frequency information (< 200 Hz). Nevertheless we show, using signal processing and machine learning, that this information is sufficient to identify speaker information and even parse speech. Since iOS and Android require no special permissions to access the gyro, our results show that apps and active web content that cannot access the microphone can nevertheless eavesdrop on speech in the vicinity of the phone," the scientists say on the Stanford Security Research website, where they also offer the Android application as a free download.

They also provide a link to a webpage that can be browsed via a mobile phone to demonstrate the efficacy of the method. The resulting data isn't recorded anywhere, although it can be saved as a file, if the user wishes.

What the researchers have shown is that the big array of sensors on a smartphone can be used for a variety of purposes. In another, related paper, they *"demonstrate how the multitude of sensors on a smartphone can be used to construct a reliable hardware fingerprint of the phone. Such a fingerprint can be used to de-anonymize mobile devices as they connect to web sites, and as a second factor in identifying legitimate users to a remote server. We present two implementations: one based on analyzing the frequency response of the speakerphone-microphone system, and another based on analyzing device-specific accelerometer calibration errors."*

Although currently the trick only works on Android devices, researchers say it's only a matter of time until the technology is rigged to work with an iPhone (whose own gyro sensor works only with frequencies below 100Hz). The discovery is just another chapter in the already controversial scandalous saga of communications surveillance with tools as simple as the smartphone's microphone being turned on remotely. It became more pertinent with the recent revelations offered by former US government intelligence contractor Edward Snowden, who is now resident in Russia after having his US passport invalidated a year ago and US prosecutors demanding his return to the States.

In late June, Russia's Kaspersky Lab, one of the world's top information security firms, reported on legal malware produced by an Italian company, Hacking Team, which since 2001 has offered its clients the opportunity to snoop on their targets. Their product is said to be the first Remote Control Systems (RCS) malware with a positive link to mobile phones, opening them up to new potential security threats.

However, internet companies have also been said to store information on users …

To read this article in its entirety, go to:
http://rt.com/usa/180884-phone-gyros-voice-microphone/