Phone snooping via gyroscope to be detailed at Usenix

August 15 2014, by Nancy Owano

Experimental setup

Put aside fears of phone microphones and cameras doing eavesdropping mischief for a moment, because there is another sensor that has been

flagged. Researchers from Stanford and defense research group at Rafael will present their findings on the smartphones' gyroscopes to measure acoustic signals in the vicinity of the phone at the Usenix Security on Friday, August 22. Translation: Your smartphone could eavesdrop on conversations. They found that the gyroscopes were sensitive enough to allow them to pick up some sound waves, turning them into crude microphones, said a detailed report by Andy Greenberg this week about their work, in Wired. The team themselves said their work demonstrated "an unexpected threat resulting from the unmitigated access to the gyro: applications and active web content running on the phone can eavesdrop sound signals, including speech, in the vicinity of the phone."

What is more, in a video the researchers prepared for the upcoming Usenix event, Recognizing Speech from Gyroscope Signals, they said, gyroscopes are present in most of the modern smartphones. They measure angular velocity. Every application and website can access them without the user's consent. "We show that we can use gyroscopes to eavesdrop on speech without using the microphone at all, which can potentially risk private information such as identity, social security and credit card numbers."

But how well does the researchers' snooping technique work? "It works just well enough to pick up a fraction of the words spoken near a phone," said Greenberg.

The team, in their paper, "Gyrophone: Recognizing Speech From Gyroscope Signals," wrote, "We show that the acoustic signal measured by the gyroscope can reveal private information about the phone's environment such as who is speaking in the room and, to some extent, what is being said. We use signal processing and machine learning to analyze speech from very low frequency samples. With further work on low-frequency signal processing of this type it should be possible to

further increase the quality of the information extracted from the gyro." As one cannot fully reconstruct a comprehensible speech from measurements of a single gyroscope, they stated, they resorted to automatic speech recognition. They extracted features from the gyroscope measurements using various signal processing methods and train machine learning algorithms for recognition.

"We achieve about 50% success rate for speaker identification from a set of 10 speakers. We also show that while limiting ourselves to a small vocabulary consisting solely of digit pronunciations ("one","two", "three", ...) and achieve speech recognition success rate of 65% for the speaker dependent case and up to 26% recognition rate for the speaker independent case."

According to Wired, Dan Boneh, computer security professor at Stanford and part of the team, said, "Whenever you grant anyone access to sensors on a device, you're going to have unintended consequences." The authors wrote in their paper, "A general conclusion we suggest following this work is that access to all sensors should be controlled by the permissions framework, possibly differentiating between low and high sampling rates."

More information: — crypto.stanford.edu/gyrophone/ — crypto.stanford.edu/gyrophone/files/gyromic.pdf