Written by **Joe Wolverton, II, J.D.** on August 16, 2014

Snoops Could Hack Smartphone Gyros to Record Ambient Conversation

Just when you thought there was no other way the snoops could hack your smartphone, along comes a story in *Wired U.K.* that adds another entry on the list of leaks in the technologically advanced telephones.

In an article published online on August 15, Andy Greenberg reports that spies can take control of a smartphone and use it to record sound completely without the consent or cognizance of the user. Greenberg writes:

> In a presentation at the Usenix security conference next week, researchers from Stanford University and Israel's defence [sic] research group Rafael plan to present a technique for using a smartphone to surreptitiously eavesdrop on conversations in a room — not with a gadget's microphone, but with its gyroscopes, the sensors designed to measure the phone's orientation. Those sensors enable everything from motion-based games like DoodleJump to cameras' image stabilisation [sic] to the phones' displays toggling between vertical and horizontal orientations. But with a piece of software the researchers built called Gyrophone, they found that the gyroscopes were also sensitive enough to allow them to pick up some sound waves, turning them into crude microphones. And unlike the actual mics built into phones, there's no way for users of the Android phones they tested to deny an app or website access to those sensors' data.

Scientists working with the Israeli military have developed a way to turn the phone's gyroscope into a makeshift microphone sensitive enough to record ambient conversations.

Although certainly very clever, the hack isn't perfect yet. Greenberg reports that the gyroscope-turned-microphone "could identify as many as 65 percent of digits spoken in the same room as the device by a single speaker" and "could also identify the speaker's gender with as much as 84 percent certainty."

That level of accuracy is unsuitable for complex covert eavesdropping, but it demonstrates the potential of the procedure.

Citing information provided by Dan Boneh, a Stanford University computer security professor, Greenberg reports:

> But Boneh argues that more work on speech recognition algorithms could refine the technique into a far more real eavesdropping threat. And he says that a demonstration of even a small amount of audio pickup through the phones' gyroscopes should serve as a warning to Google to change how easily rogue Android apps could exploit the sensors' audio sensitivity.

Although the experiment has been conducted so far only on phones running Google's Android mobile operating system, similar devices manufactured by Apple use gyroscopes for a variety of functions, as well, and are thus susceptible to the surreptitious recording of sounds.

The big difference between the Google approach to this information and that taken by Apple is that the latter limits the number of times an application can access data provided by the gyroscope, whereas

Google has thus far failed to do so. Regarding this potentially privacy-invading access, Boneh reported told *Wired U.K.*, "There's no reason a video game needs to access it 200 times a second."

Of the lack of need for such constant communication between an app and the phone's gyroscope, *Slate* magazine writes,

> Downloading an untrusted app is one thing, but *Wired* points out that you could even be at risk by navigating to unsecure webpages in Firefox's mobile browser. Safari and Chrome for Android limit gyroscope readings to 20 hertz, but Firefox allows the whole 200 hertz.

Over the years, *The New American* has chronicled the discovery of various nefarious manipulations of a smartphone that could be made by government or others wanting to listen in to otherwise private cellphone conversations.

In May, this reporter highlighted the "improvement" of the Facebook mobile app that allowed the social media giant to access the built-in microphone and record and store ambient sounds. I wrote:

> In the "coming weeks," the social media behemoth will roll out a service that, according to an announcement on its blog, will give users:
>
> > the option to use your phone's microphone to identify what song is playing or what show or movie is on TV.
>
> That means if you want to share that you're listening to your favorite Beyoncé track or watching the season premiere of *Game of Thrones*, you can do it quickly and easily, without typing.

Certainly, as the company claims, that is a handy little tool for recording the sounds entering into a smartphone's microphone with nearly no human interaction required.

There is something disturbing in the potential uses of this option, however. The frightening application of the app is, accidentally it seems, explained in a *Huffington Post* article promoting the technology: "Facebook Can Now Listen To Everything You Listen To."

In 2012, *The New American* reported on a federal appeals court decision that upheld the government's remote activation of a cellphone's microphone, converting the device into a "roving bug."

> In its decision, the Ninth Circuit upheld a lower court's ruling, essentially allowing the federal government to convert cellphones into "roving bugs" so long as the government makes it clear that it will be using the target's cellphone in that manner. Notice, the Ninth Circuit — a court created under the authority granted to Congress in Article III of the Constitution — did not throw out the matter as a violation of the defendant's Fourth Amendment right against "unreasonable searches and seizures." Instead, it simply informed the government that it needs to get permission before doing so.

Given the ubiquity of smartphones, it seems there will come a day when these technologies will combine and enable nonstop monitoring of every phone and face-to-face conversation. This information, stored on some government computer, could then potentially be used to blackmail or embarrass people who dare defy the decrees of an increasingly autocratic federal authority.

Joe A. Wolverton, II, J.D. is a correspondent for The New American*. Follow him on Twitter @TNAJoeWolverton.*