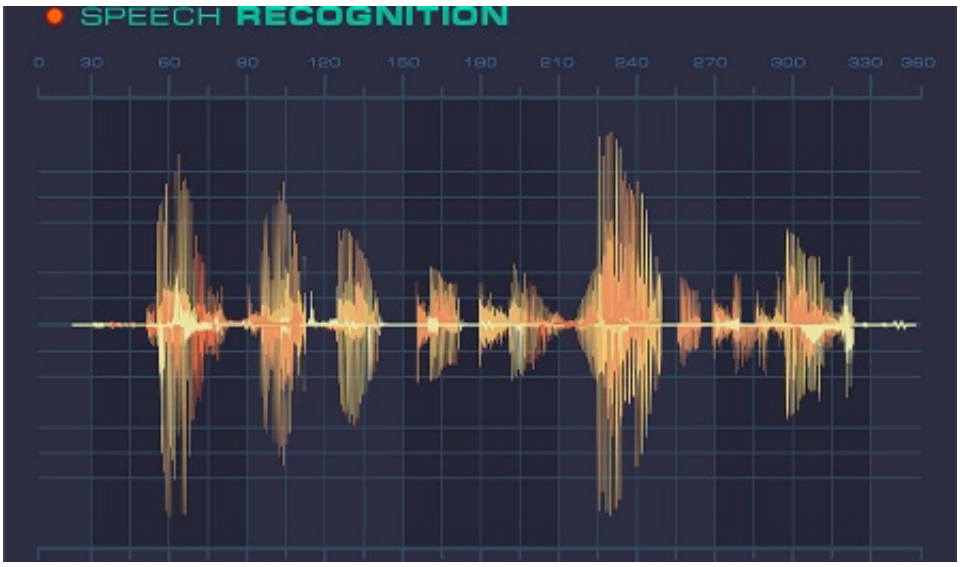
App uses smartphone compass to stop voice hacking

June 5 2017, by Grove Potter



The app uses uses the magnetometer in a phone, which is there for the phone's compass, to detect a magnetic field. Credit: University at Buffalo

While convenient, Siri, WeChat and other voice-based smartphone apps can expose you to a growing security threat: voice hacking.

With just a few minutes of audio samples, attackers can replay your voice convincingly enough to trick people as well as top digital security systems. The consequences, from impersonating you with your friends to dipping into your bank account, are terrifying.

Using only tools already on smartphones, including the compass, a University at Buffalo-led team of engineers is creating an app to stop voice hacking. Described in a study to be presented this week in Atlanta at the 37th International Conference on Distributed Computing Systems, a prototype proved highly accurate in stopping machine-based voice impersonation attacks.

"Every aspect of your life is now on your phone," said Kui Ren, PhD, director of the Ubiquitous Security and Privacy Research Laboratory (UbiSeC) at UB, and one of the study's lead authors. "That is your security hub. It is really critical now."

Ren, a professor of computer science and engineering in UB's School of Engineering and Applied Sciences, doesn't mince words when discussing the importance of better cellphone security.

"Hackers are out there, more than you can imagine. There is a whole underground grey market to sell your password and your personal information," he said.

The best way to protect your cellphone, he said, is to use several security methods.

"Technology is advancing so fast; we have to think of different ways. The strategy is using multiple lines of defense. We call that defense in depth," he said.

Voice recognition could become a more common security tool because more Internet-connected devices are being developed that do not have keypads, he said.

"With the Internet of things, what is a security interface? It is not like the phone. There is often no touch screen or keypad so voice

authentication may be useful." he said.

The study, which Ren co-authored with former PhD student Si Chen (now an assistant professor at West Chester University of Pennsylvania), has been awarded the Best Student Paper Award at the conference, which is organized by the Institute of Electrical and Electronic Engineers.

Voice recognition attacks can come in various forms. Attacks can synthesize your voice, but these are detectable by existing algorithms. A human can imitate your voice, but again, existing technology can detect this.

A third method is replaying someone's actual voice, and here is where Ren's invention comes in. Any replay must be broadcast on a speaker, and speakers have magnetic fields. Ren's system uses the magnetometer in a phone, which is there for the phone's compass, to detect a magnetic field.

In addition, the system uses the phone's trajectory mapping algorithm to measure the distance between the speaker and the phone. It requires a phone user to be close to the phone when speaking to guarantee that anyone using a replay of a voice over a mechanical speaker is close enough that the magnetic field can be detected.

Finally, the system requires that the phone be moving—swung in front of the mouth—when the voice recognition is being used. When a replayed voice is moved, the magnetic field changes and the phone can detect this.

Several of Ren's former and current PhD students are co-authors of the study, including Chen, Sixu Piao, Cong Wang, and Qian Wang, in addition to Lu Su and Aziz Mohaisen, both assistant professors in UB's

Department of Computer Science and Engineering, and Jian Weng from Jinan University, China.

The team plans to refine the system and soon make it downloadable as an app.

"We cannot decide if voice authentication will be pervasive in the future. It might be. We're already seeing the increasing trend," Ren said. "And if that is the case, we have to defend against voice replay attacks. Otherwise, voice authentication cannot be secure."

Provided by University at Buffalo