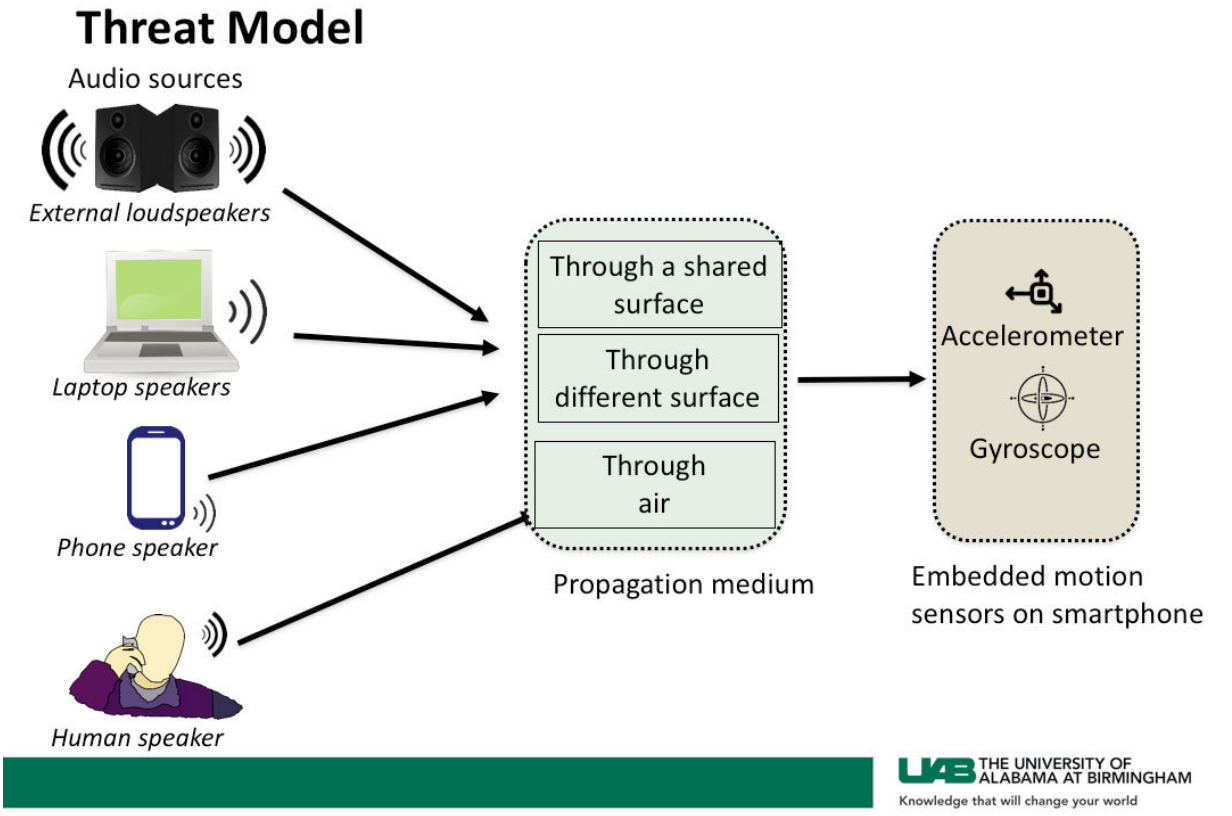
Researchers investigate potential threat to speech privacy via smartphone motion sensors

June 15 2018, by Tiffany Westry Womack



Credit: University of Alabama at Birmingham

Could smartphone motion sensors be used by cybercriminals to record speech? It is a question that many academic and industry researchers are working to answer in order to ward off this kind of malicious use before it happens.

Recent studies suggest security flaws and sensitivities to low-frequency audio signals, such as human speech, in accelerometers and gyroscopes could allow cybercriminals to collect confidential information such as credit card numbers and Social Security numbers as users speak into or near a mobile device.

While some studies have revealed the ability to use motion sensor data and algorithms to decipher passwords and PINs entered on touchscreens, researchers at the University of Alabama at Birmingham have found that motion sensors may pose a threat to speech privacy only in limited scenarios.

"These motion sensors are readily available in smartphones and other smart wearable devices that have become a predominant feature in everyone's life," Nitesh Saxena, Ph.D., associate professor in the UAB College of Arts and SciencesDepartment of Computer Science. "Unlike with microphones, users do not have to give newly installed applications permission to use them, making these sensors prime tools for malicious activity. This body of research is incredibly important to help protect users from myriad real and hypothetical privacy invasions."

In a paper published at the 2018 IEEE Symposium on Security and Privacy in May, doctoral student Abhishek Anand and Saxena analyze how speech signals traveling through the air and solid surfaces affect smartphone motion sensor readings.

In their threat analysis, Anand and Saxena used stereo speakers, laptop speakers, smartphone speakers and live human speech at different

volume levels to test the effect audio signals had on a smartphone placed on the same surface as the speaker, on a different surface and through the air.

They found that built-in laptop speakers were able to affect the accelerometer only when the laptop and the motion sensor shared a surface. Motion sensors could possibly be affected by speech signals from a stereo speaker when both objects are on the same surface. Smartphone speakers were not found to be powerful enough to invoke a response in the motion sensors through aerial vibrations. Human speech was not powerful enough to register a response.

"In light of recent research and resulting news articles about the potential threat of smartphone motion sensors, the public perception is that this threat is very serious and motion sensors could record in the same way that a microphone does," Anand said. "Our research indicates that this is not the case. Motion sensors are very much limited in their capability of picking up speech characteristics. It is not possible for an accelerometer or gyroscope to act in the same capacity that a microphone does."

They conclude human speech traveling through the air is incapable of triggering motion sensors such as an accelerometer or gyroscope, and the impact of loudspeakers and other machine-rendered speech on motion sensors is primarily through shared conductive surfaces.

More information: Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors. IEEE Computer Society. doi.ieeecomputersociety.org/10.1109/SP.2018.00004

Provided by University of Alabama at Birmingham