Sensors can tap into mobile vibrations to eavesdrop remotely, researchers find

October 10 2022, by Ashley WennersHerron

Credit: Unsplash/CC0 Public Domain

Using an off-the-shelf automotive radar sensor and a novel processing approach, Penn State researchers demonstrated they could detect the vibrations of a cell phone's earpiece and decipher what the person on the

other side of the call was saying with up to 83% accuracy.

The demonstration, available in the *2022 IEEE Symposium on Security and Privacy (SP)*, reveals a significant security concern, according to Mahanth Gowda, assistant professor of computer science and engineering, and Suryoday Basak, doctoral candidate pursuing a degree in computer science and advised by Gowda.

"As technology becomes more reliable and robust over time, the misuse of such sensing technologies by adversaries becomes probable," Basak said. "Our demonstration of this kind of exploitation contributes to the pool of scientific literature that broadly says, 'Hey! Automotive radars can be used to eavesdrop audio. We need to do something about this.'"

The radar operates in the millimeter-wave (mmWave) spectrum, specifically in the bands of 60 to 64 gigahertz and 77 to 81 gigahertz, which inspired the researchers to name their approach "mmSpy." This is a subset of the radio spectrum used for 5G, the fifth-generation standard for communication systems across the globe.

In the mmSpy demonstration, the researchers simulated people speaking through the earpiece of a smartphone. The brand is irrelevant, Basak said, but the researchers tested their approach on both a Google Pixel 4a and a Samsung Galaxy S20. The phone's earpiece vibrates from the speech, and that vibration permeates across the body of the phone.

"We use the radar to sense this vibration and reconstruct what was said by the person on the other side of the line," Basak said, noting that their approach works even when the audio is completely inaudible to both humans and microphones nearby. "This isn't the first time similar vulnerabilities or attack modalities have been found, but this particular aspect—detecting and reconstructing speech from the other side of a smartphone line—was not yet explored."

The radar sensor data is pre-processed via MATLAB and Python modules, which are computing platform-language interfaces used in this research to remove hardware-related and artifact noise from the data. The researchers then feed that to machine learning modules trained to classify speech and reconstruct audio. When the radar senses vibrations from a foot away, the processed speech is 83% accuracy. That drops the farther the radar moves from the phone, down to 43% accurate at six feet.

Once the speech is reconstructed, the researchers can then filter, enhance or classify keywords as needed, Basak said. The team is continuing to refine their approach to better understand not only how to protect against this security vulnerability, but also how to exploit it for good.

"The methodology that we developed can also be used for sensing vibrations in industrial machinery, smart home systems and building-monitoring systems," Basak said. "Vibration tracking over time can help assess wear and tear—using our approach could help identify when machinery needs maintenance before it would traditionally be obvious, for example."

According to Basak, there are similar home maintenance or even health monitoring systems that could benefit from such sensitive tracking.

"Imagine a radar that could track a user and call for help if some health parameter changes in a dangerous way," Basak said. "With the right set of target actions, radars in smart homes and industry can enable a faster turnaround when problems and issues are detected."

The researchers are now working to scale their eavesdropping attack with mmSpy to both strengthen their approach and to translate it to these more constructive applications.

"Compared to how our world was about a decade ago, today we are much better connected and use sensor systems to monitor our breathing, physical activity and even make our homes more secure," Basak said. "As a research group, we are extremely excited to be working in this area as the world is increasingly relying on wireless sensor systems. We enjoy overcoming complex technological challenges and design methods that can be used in real-world systems of the future."

More information: Suryoday Basak et al, mmSpy: Spying Phone Calls using mmWave Radars, *2022 IEEE Symposium on Security and Privacy (SP)* (2022). DOI: 10.1109/SP46214.2022.9833568

Provided by Pennsylvania State University