# Research hack reveals call security risk in smartphones

August 22 2023, by Nancy Luedke


Smartphone manufacturers listen up; malware created by academic researchers showed how call security can be compromised in three areas. Credit: Texas A&M Engineering

Advanced smartphone features attract users who want more from their devices, especially in health and entertainment areas, but do these features create a security risk when making or receiving actual calls? A team of academic researchers from Texas A&M University and four other institutions created malicious software, or malware, to answer that

question.

The researchers' malware, called EarSpy, used machine learning algorithms to filter a surprising amount of caller information from ear speaker vibration data recorded by an Android smartphone's own motion sensors—and did so without overcoming any safeguards or needing user permissions.

"A standard attack on a cell phone taps the microphone and records the voices," said Ahmed Tanvir Mahdad, a doctoral student in the Department of Computer Science and Engineering at Texas A&M. "We are recording motion sensor data, which is not directly related to speech, and detecting caller information from that in a side-channel attack."

Mahdad was the primary author of "EarSpy: Spying Caller Speech and Identity through Tiny Vibrations of Smartphone Ear Speakers," a paper published in December 2022, on the pre-print server *arXiv*, that explained the project's results.

Ear speakers at the top of smartphones are traditionally small and produce low sound pressures during conversations. These vibrations improve clarity when the phone is pressed against the user's ear.

The speakers are not considered a good source for audible eavesdropping because of their size and how they function. Yet some manufacturers are replacing these small speakers with bigger ones to create the stereo sounds needed for videos and streaming without considering how much vibration data the bigger ear speakers emit. Since smartphones are equipped with motion sensors called accelerometers to record vibration data tracking user exercises and locations, this has led to a situation where ear speaker vibrations can also be recorded and potentially compromised.

The researchers chose two recent smartphones similar in design, used Android operating systems, and had powerful ear speakers. They played recorded voices only through the ear speakers at a volume comfortable for a user's hearing. The researchers then used EarSpy to analyze the phones' accelerometers' data.

They found EarSpy could identify if the speaker was a repeat caller with 91.6% accuracy and determine the gender of the speaker with 98.6% accuracy. The malware also recognized spoken digits, specifically numbers from zero to nine, with 56% accuracy, which is five times higher than a random guess.

"Say you are talking to a health care provider or bank's customer service agent, and they asked you to provide your identification or credit card numbers," said Mahdad. "If the EarSpy malware was on your phone, the attacker could access your phone's accelerometer data and pull it from your phone through an internet connection for processing so that they can extract this information."

The research focused on Android smartphones because motion sensor data can be retrieved from them without any explicit permission from the user.

Previous research indicated it was difficult to extract speech features from accelerometer data induced by tiny ear speakers on older Android smartphones. The two newer phones the researchers chose had larger speakers that gave progressively more information; the algorithm could detect 45–90% of the word regions from their accelerometer data to use for further analysis. The researchers concluded that moving the accelerometer to a different location in the phone might reduce the amount of data recorded, but it wouldn't stop the recordings entirely.

Future tests on other phones might be warranted, since results suggested

all smartphone manufacturers should be aware of the security risks.

Mahdad pointed out the hack could only happen if the attacker concealed malware in an application the user downloaded.

"Any benign-looking app with malware in it can extract this information, but only if the user approves the app," said Mahdad. "Once installed, it could run in the background without notifying the user."

**More information:** Ahmed Tanvir Mahdad et al, EarSpy: Spying Caller Speech and Identity through Tiny Vibrations of Smartphone Ear Speakers, *arXiv* (2022). DOI: 10.48550/arxiv.2212.12151

Provided by Texas A&M University College of Engineering