TechXplore

Researchers hacked a robotic vacuum cleaner to record speech and music remotely

November 18 2020

Researchers repurposed the laser-based navigation system on a vacuum robot (right) to pick up sound vibrations and capture human speech bouncing off objects like a trash can placed near a computer speaker on the floor. Credit: Sriram Sami

A team of researchers demonstrated that popular robotic household vacuum cleaners can be remotely hacked to act as microphones.

The researchers—including Nirupam Roy, an assistant professor in the University of Maryland's Department of Computer Science—collected information from the laser-based navigation system in a popular vacuum robot and applied signal processing and deep learning techniques to recover speech and identify television programs playing in the same room as the device.

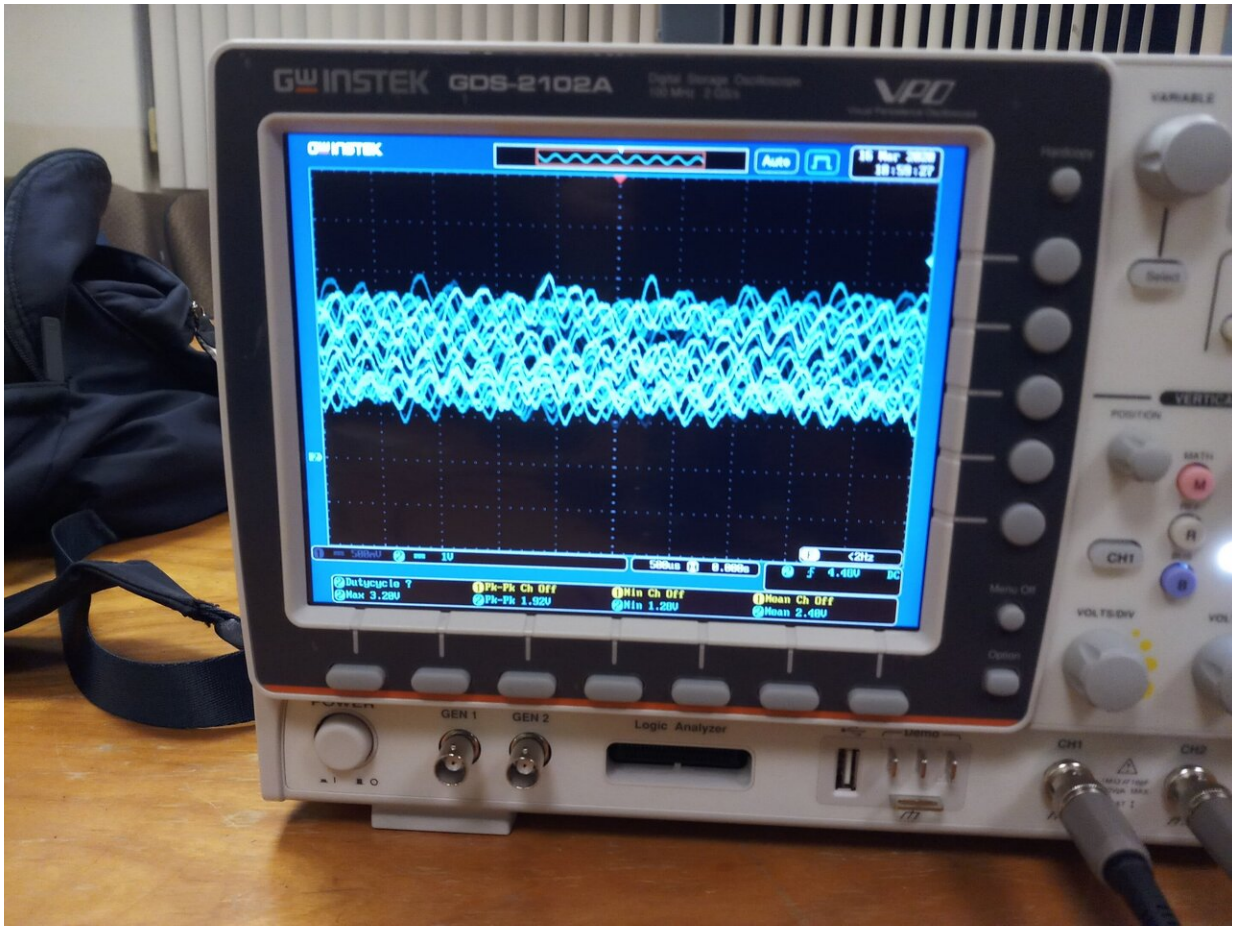
The research demonstrates the potential for any device that uses light detection and ranging (Lidar) technology to be manipulated for collecting sound, despite not having a microphone. This work, which is a collaboration with assistant professor Jun Han at the University of Singapore was presented at the Association for Computing Machinery's Conference on Embedded Networked Sensor Systems (SenSys 2020) on November 18, 2020.

"We welcome these devices into our homes, and we don't think anything about it," said Roy, who holds a joint appointment in the University of Maryland Institute for Advanced Computer Studies (UMIACS). "But we have shown that even though these devices don't have microphones, we can repurpose the systems they use for navigation to spy on conversations and potentially reveal private information."

The Lidar navigation systems in household vacuum bots shine a laser beam around a room and sense the reflection of the laser as it bounces off nearby objects. The robot uses the reflected signals to map the room and avoid collisions as it moves through the house.

Privacy experts have suggested that the maps made by vacuum bots, which are often stored in the cloud, pose potential privacy breaches that could give advertisers access to information about such things as home size, which suggests income level, and other lifestyle-related information. Roy and his team wondered if the Lidar in these robots could also pose potential security risks as sound recording devices in users' homes or businesses.

Sound waves cause objects to vibrate, and these vibrations cause slight variations in the light bouncing off an object. Laser microphones, used in espionage since the 1940s, are capable of converting those variations back into sound waves. But laser microphones rely on a targeted laser beam reflecting off very smooth surfaces, such as glass windows.



Deep learning algorithms were able to interpret scattered sound waves, such those above that were captured by a robot vacuum, to identify numbers and musical sequences. Credit: Sriram Sami

A vacuum Lidar, on the other hand, scans the environment with a laser and senses the light scattered back by objects that are irregular in shape and density. The scattered signal received by the vacuum's sensor provides only a fraction of the information needed to recover sound waves. The researchers were unsure if a vacuum bot's Lidar system could be manipulated to function as a microphone and if the signal could be interpreted into meaningful sound signals.

First, the researchers hacked a robot vacuum to show they could control the position of the laser beam and send the sensed data to their laptops through Wi-Fi without interfering with the device's navigation.

Next, they conducted experiments with two sound sources. One source was a human voice reciting numbers played over computer speakers and the other was audio from a variety of television shows played through a TV sound bar. Roy and his colleagues then captured the laser signal sensed by the vacuum's navigation system as it bounced off a variety of objects placed near the sound source. Objects included a trash can, cardboard box, takeout container and polypropylene bag—items that might normally be found on a typical floor.

The researchers passed the signals they received through deep learning algorithms that were trained to either match human voices or to identify musical sequences from television shows. Their computer system, which they call LidarPhone, identified and matched spoken numbers with 90% accuracy. It also identified television shows from a minute's worth of recording with more than 90% accuracy.

"This type of threat may be more important now than ever, when you consider that we are all ordering food over the phone and having meetings over the computer, and we are often speaking our credit card or bank information," Roy said. "But what is even more concerning for me is that it can reveal much more personal information. This kind of information can tell you about my living style, how many hours I'm working, other things that I am doing. And what we watch on TV can reveal our political orientations. That is crucial for someone who might want to manipulate the political elections or target very specific messages to me."

The researchers emphasize that vacuum cleaners are just one example of potential vulnerability to Lidar-based spying. Many other devices could be open to similar attacks such as smartphone infrared sensors used for face recognition or passive infrared sensors used for motion detection.

"I believe this is significant work that will make the manufacturers aware of these possibilities and trigger the security and privacy community to come up with solutions to prevent these kinds of attacks," Roy said.

More information: The research paper, "Spying with Your Robot Vacuum Cleaner: Eavesdropping via Lidar Sensors," Sriram Sami, Yimin Dai, Sean Rui Xiang Tan, Nirupam Roy and Jun Han, was presented on November 18, 2020, at the Association for Computing Machinery, SenSys 2020.

Provided by University of Maryland

Citation: Researchers hacked a robotic vacuum cleaner to record speech and music remotely (2020, November 18) retrieved 25 April 2024 from
https://techxplore.com/news/2020-11-hacked-robotic-vacuum-cleaner-speech.html