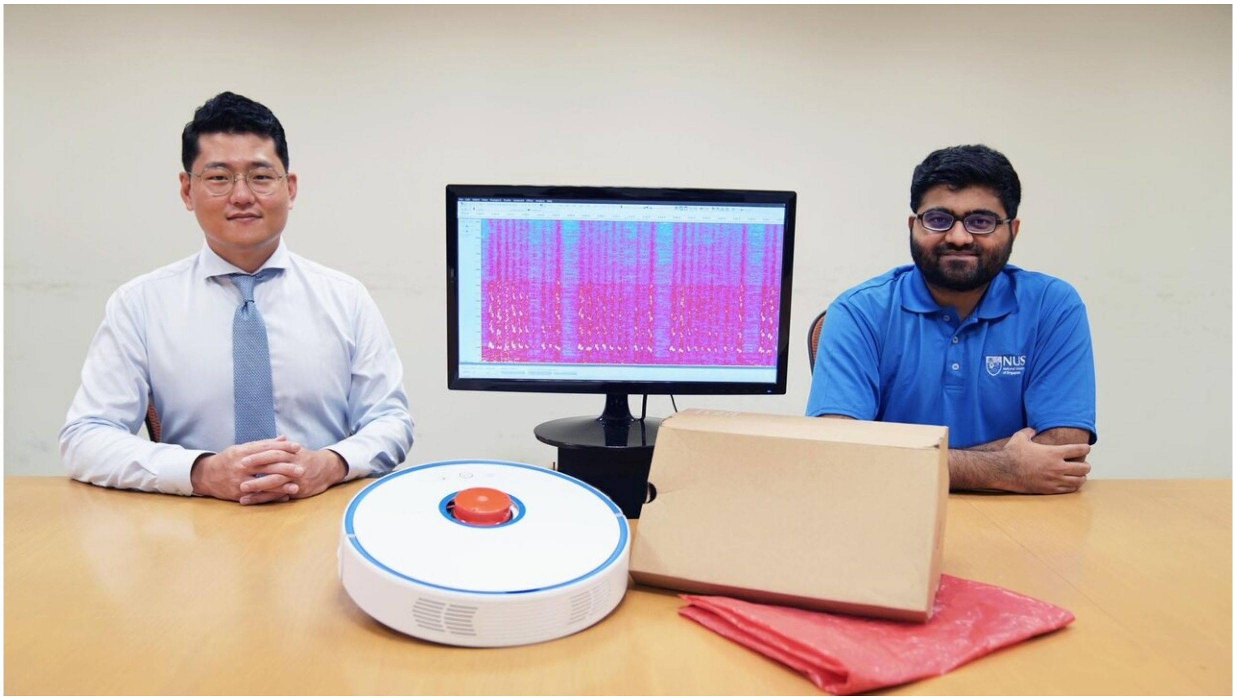
Robot vacuum cleaners can spy on private conversations

December 8 2020



Asst Prof Jun Han (left) and doctoral student Mr Sriram Sami (right) from NUS Computing with a robot vacuum cleaner, a monitor showing recovered sound waves, and common household items made from materials that can reflect sound. Credit: National University of Singapore

When your robot vacuum cleaner does its work around the house, beware that it could pick up private conversations along with the dust and dirt. Computer scientists from NUS have demonstrated that it is indeed possible to spy on private conversations using a common robot vacuum cleaner and its built-in Light Detection and Ranging (Lidar) sensor.

The novel method, called LidarPhone, repurposes the Lidar sensor that a robot vacuum cleaner normally uses for navigating around a home into a laser-based microphone to eavesdrop on private conversations.

The research team, led by Assistant Professor Jun Han from NUS Computer Science, and his doctoral student Mr Sriram Sami, managed to recover speech data with high accuracy. NUS students, Mr Dai Yimin and Mr Sean Tan Rui Xiang, as well as Assistant Professor Nirupam Roy from the University of Maryland, also contributed to this work.

Mr Sami shared, "The proliferation of smart devices—including smart speakers and smart security cameras—has increased the avenues for hackers to snoop on our private moments. Our method shows it is now possible to gather sensitive data just by using something as innocuous as a household robot vacuum cleaner. Our work demonstrates the urgent need to find practical solutions to prevent such malicious attacks."

The work was presented at the Association for Computing Machinery's Conference on Embedded Networked Sensor Systems (SenSys 2020) on 18 November 2020, where the team clinched the Best Poster Runner Up Award.

How the attack works

The core of the LidarPhone attack method is the Lidar sensor, a device which fires out an invisible scanning laser, and creates a map of its surroundings. By reflecting lasers off common objects such as a dustbin or a takeaway bag located near a person's computer speaker or television soundbar, the attacker could obtain information about the original sound that made the objects' surfaces vibrate. Using applied signal processing and deep learning algorithms, speech could be recovered from the audio data, and sensitive information could potentially be obtained.

In their experiments, the researchers used a common robot vacuum cleaner with two sources of sound. One was the voice of a person reading out numbers played from a computer speaker, while the other source was music clips from television shows played through a television soundbar.

The team collected more than 19 hours of recorded audio files and passed them through deep learning algorithms that were trained to either match human voices or identify musical sequences. The system was able to detect the digits being spoken aloud, which could constitute a victim's credit card or bank account numbers. Music clips from television shows could potentially disclose the victim's viewing preferences or political orientation. The system achieved a classification accuracy rate of 91 percent when recovering spoken digits, and a 90 percent accuracy rate when classifying music clips. These results are significantly higher than a random guess of 10 percent.

The researchers also experimented with common household materials to test how well they reflected the Lidar laser beam and found that the accuracy of audio recovery varied between different materials. They discovered the best material for reflecting the laser beam was a glossy polypropylene bag, while the worst was glossy cardboard.

Preventing such attacks

To prevent Lidars from being misused, the researchers recommend users to consider not connecting their robot vacuum cleaners to the Internet. The team also recommends that Lidar sensor manufacturers incorporate a mechanism that cannot be overridden, to prevent the internal laser from firing when the Lidar is not rotating.

"In the long term, we should consider whether our desire to have increasingly 'smart' homes is worth the potential privacy implications. We might have to accept that each new Internet-connected sensing device brought into our homes poses an additional risk to our privacy, and make our choices carefully," shared Asst Prof Han.

Future work

The team is working on applying ideas learnt from LidarPhone to autonomous vehicles—which also use Lidar sensors—as they could also be used to eavesdrop on conversations happening in nearby cars through minute vibrations of the car windows. They are also looking at the vulnerability of active laser sensors found on the latest smartphones, which could reveal further privacy issues.

More information: Sriram Sami et al. LidarPhone: acoustic eavesdropping using a lidar sensor, *Proceedings of the 18th Conference on Embedded Networked Sensor Systems* (2020). DOI: 10.1145/3384419.3430430

Provided by National University of Singapore

Citation: Robot vacuum cleaners can spy on private conversations (2020, December 8) retrieved 30 April 2024 from https://techxplore.com/news/2020-12-robot-vacuum-cleaners-spy-private.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.