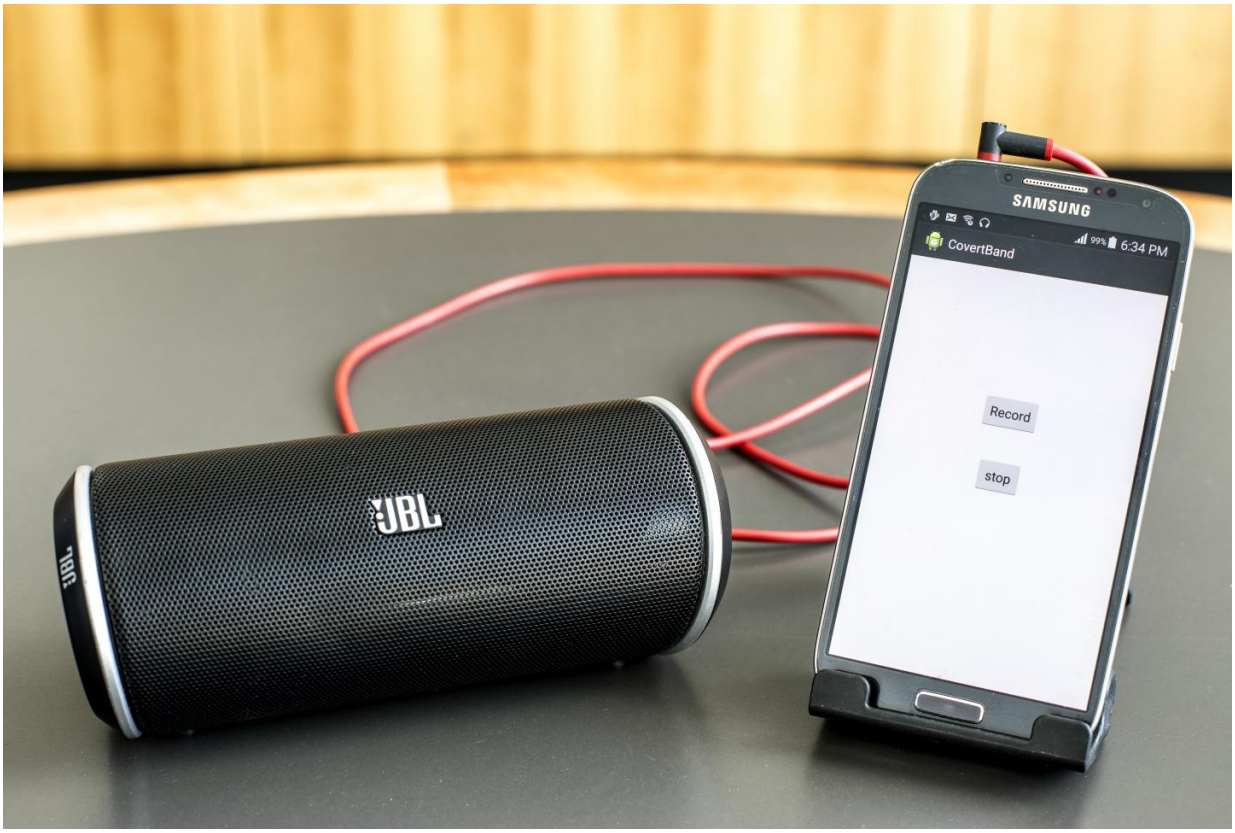
Computer scientists use music to covertly track body movements, activity

August 16 2017



The researchers tested CovertBand using a Samsung Galaxy S4 smartphone hooked up to a portable speaker. Credit: Dennis Wise/University of Washington

As smartphones, tablets, smart TVs and other smart devices become more prevalent in our lives, computer scientists have raised concerns that

these network-enabled devices, if not properly secured, could be co-opted to steal data or invade user privacy.

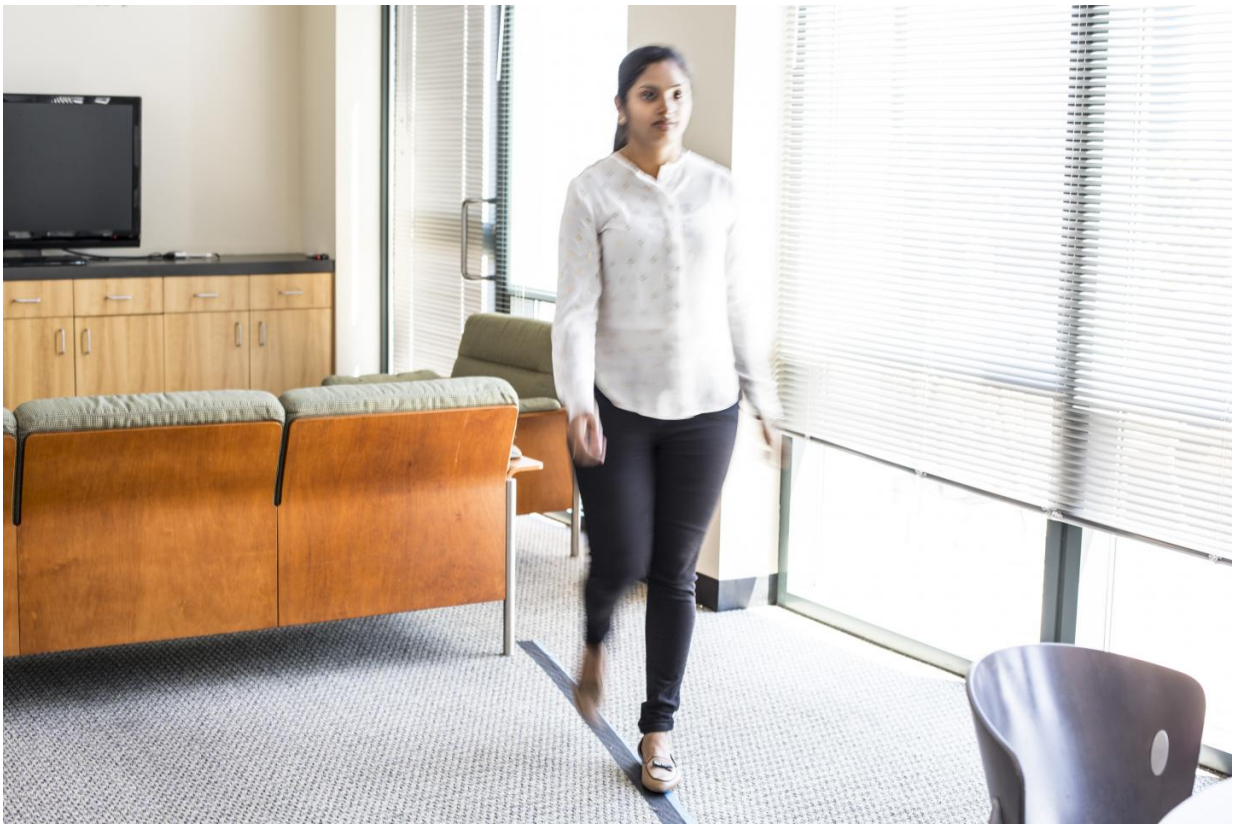
Now researchers at the University of Washington have demonstrated how it is possible to transform a smart device into a surveillance tool that can collect information about the body position and movements of the user, as well as other people in the device's immediate vicinity. Their approach involves remotely hijacking smart devices to play music embedded with repeating pulses that track a person's position, body movements, and activities both in the vicinity of the device as well as through walls.

The team, from the UW's Paul G. Allen School of Computer Science & Engineering, showed how it is possible to collect such detailed data on personal activity using CovertBand, software code they created to turn smart devices into active sonar systems. As the researchers will report at the Ubicomp 2017 conference in September, CovertBand can utilize built-in microphones and speakers in a smart device—and can be controlled remotely.

"To our knowledge, this is the first time anyone has demonstrated that it is possible to convert smart commodity devices—like smartphones and smart TVs—into active sonar systems using music," said senior author Shyam Gollakota, a UW associate professor of computer science and engineering. "And the physical information CovertBand can gather—even through walls—is sufficiently detailed for an attacker to know what the user is doing, as well as other people nearby."

CovertBand utilizes the principles of active sonar to gather this information. Active sonar systems, such as on submarines, determine the position of objects by sending out an acoustic pulse. Those sound waves bounce off objects in their path, and the deflected waves can be picked up by a receiver to determine the object's position, distance and shape.

Through the speaker of a smartphone or other device, CovertBand sends out a repeating pulse of sound waves in the 18 to 20 kHz range. Much like sonar on a submarine, these sound waves are reflected when they encounter objects in their path. CovertBand uses the device's built-in microphones as a receiver to pick up these reflected sound waves. The smart device then transmits this information to the attacker, who could be a few feet away or halfway across the globe.



UW doctoral student and co-lead author Rajalakshmi Nandakumar demonstrates the simple walking motion that CovertBand can detect. Credit: Dennis Wise/University of Washington

"Most of today's smart devices including smart TVs, Google Home,

Amazon Echo and smartphones come with built-in microphones and speaker systems—which lets us use them to play music, record video and audio tracks, have phone conversations or participate in videoconferencing," said co-lead author Rajalakshmi Nandakumar, a UW doctoral student in computer science and engineering. "But that also means that these devices have the basic components in place to make them vulnerable to attack in this manner."

"Other surveillance approaches require specialized hardware, from the 'classic' hidden camera to an ultrasound-like device that must be placed on the wall of a neighboring room," said co-lead author Alex Takakuwa, a UW doctoral student in computer science and engineering. "CovertBand shows for the first time that through-barrier surveillance is possible using no hardware beyond what smart devices already have."

The team tested CovertBand's effectiveness using a smartphone hooked up to either a portable speaker or a standard flat-screen TV. In both cases, CovertBand's data could be used to decipher repetitive movements such as arm-pumping, walking or pelvic tilts to a range of up to 6 meters from the smartphone, with a positional error of only 8 to 18 centimeters. Researchers also discovered that, with the portable speaker, CovertBand's pulses can transmit through thin, interior walls—though the range drops to 2 to 3 meters.

Currently, CovertBand can automatically identify and infer repetitive motions. More detailed inferences require manual analyses of data—or additional tools.

"Our initial goal was to demonstrate that it is possible to use passive acoustics to gather even basic—but still highly sensitive—information using CovertBand," said Gollakota. "But if you have enough data from CovertBand, you could run it through machine-learning algorithms to help classify more movements for faster identification."

The 18 to 20 kHz repeating pulses employed by CovertBand are on the low range of what many people can hear accurately, though children, younger adults and even pets might be able to hear it well, said Nandakumar. But to increase the range of surveillance and work through walls, the authors increased the volume of these repeating pulses, which made them audible. To mask the sound, they "covered" Covertband's pulses by playing songs or other audio clips over them. Some songs work better than others—particularly compositions with repetitive, percussive beats. When they played the CovertBand pulses beneath 20 popular songs—including Lenny Kravitz's "American Woman" and Michael Jackson's "Bad"—listeners could identify the "hacked" version of the song 58 percent of the time, just slightly above the 50 percent accuracy expected by guessing randomly.

"Since Covertband enables through-the-wall surveillance, anyone can play music on their smart devices to track people through walls," said Takakuwa. "This is concerning because, if a neighbor is playing music, it could either be a benign act or an act of surveillance to determine if anyone is in the adjacent apartment, track their movements or infer their activities."

The researchers said that soundproofing a room would prevent attacks through walls. Emitting a jamming signal at the same 18 to 20 kHz frequency range would also prevent hacked devices or attackers in the next room from gathering information. But currently, those are also impractical defenses for most people. Soundproofed rooms have no windows, for example, and jamming signals would have to be sent the moment an attack is detected. Another potential—though partial—defense could be to allow users to deactivate the speakers or microphones on their smart devices. But such a move would go against industry trends for some of these devices.

"In many cases, when the device is on, then its speakers and

microphones are also on," said Nandakumar.

The team hopes that knowledge of what is possible will help develop awareness of privacy dangers and prompt scientists to develop practical countermeasures.

"We always want to stay one step ahead of the bad guys—of attackers who are trying to collect this information about users," said co-author Tadayoshi Kohno, a UW professor of computer science and engineering. "We're providing education about what is possible and what capabilities the general public might not know about, so that people can be aware and can build defenses against this."

More information: musicattacks.cs.washington.edu … ormation-leakage.pdf

Provided by University of Washington