THE CONVERSATION
Academic rigour, journalistic flair

Shutterstock

The next cyberattack could come from sound waves

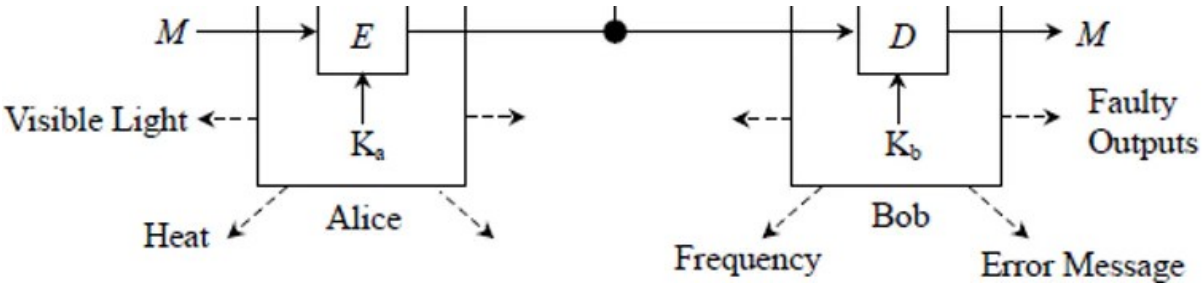
March 27, 2017 3.53pm BST

Author

Bill Buchanan
Head, The Cyber Academy, Edinburgh
Napier University

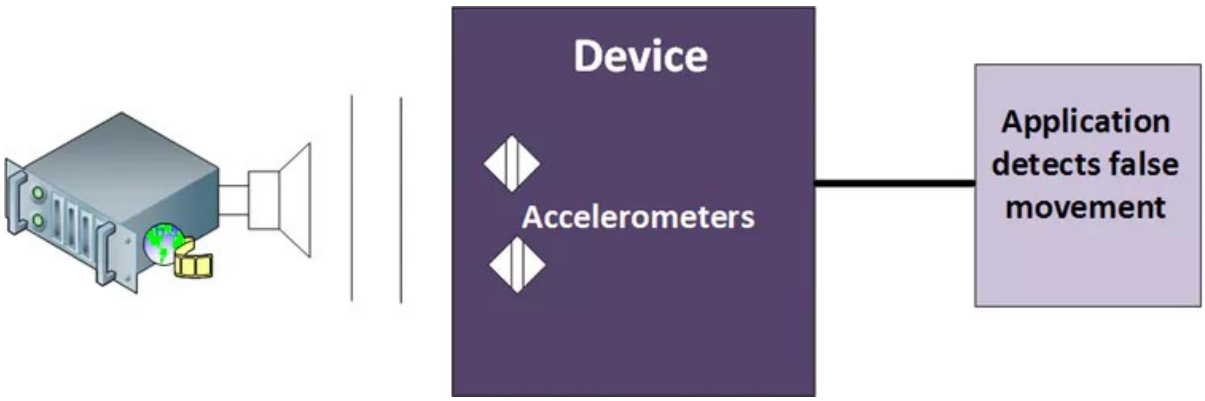
You might think your smartphone or laptop is relatively safe from cyber attacks thanks to anti-virus and encryption software. But your devices are increasingly at risk from "side-channel" attacks, where an intruder can bypass traditional network entry points and use another way to compromise the device.

These side channels can involve measuring several of the device's characteristics, including its power consumption, the time it takes to perform certain functions, or the amount of light or other electromagnetic radiation it emits. These outputs have long been used as a way of spying on communications. But now there is an increasing risk that they could also be used to disrupt the operation of electronic devices. This is a particular worry as more and more objects are equipped with miniature computers to connect them to the internet.



Side-channel methods.

In the latest example of this, researchers from the University of Michigan have found a new way of using sound to interfere with devices containing accelerometers, a device for measuring acceleration that is found in things such as navigation systems. Smartphones use them to detect movement and calculate things like which way up the phone is being held, and even how many steps it has been carried. The researchers found that the vibrations from music playing on a smartphone could affect its accelerometer in a way that made it seem as if the user was moving. Overall, they found the flaw in more than half of the devices they tested.



Interference of sensors.

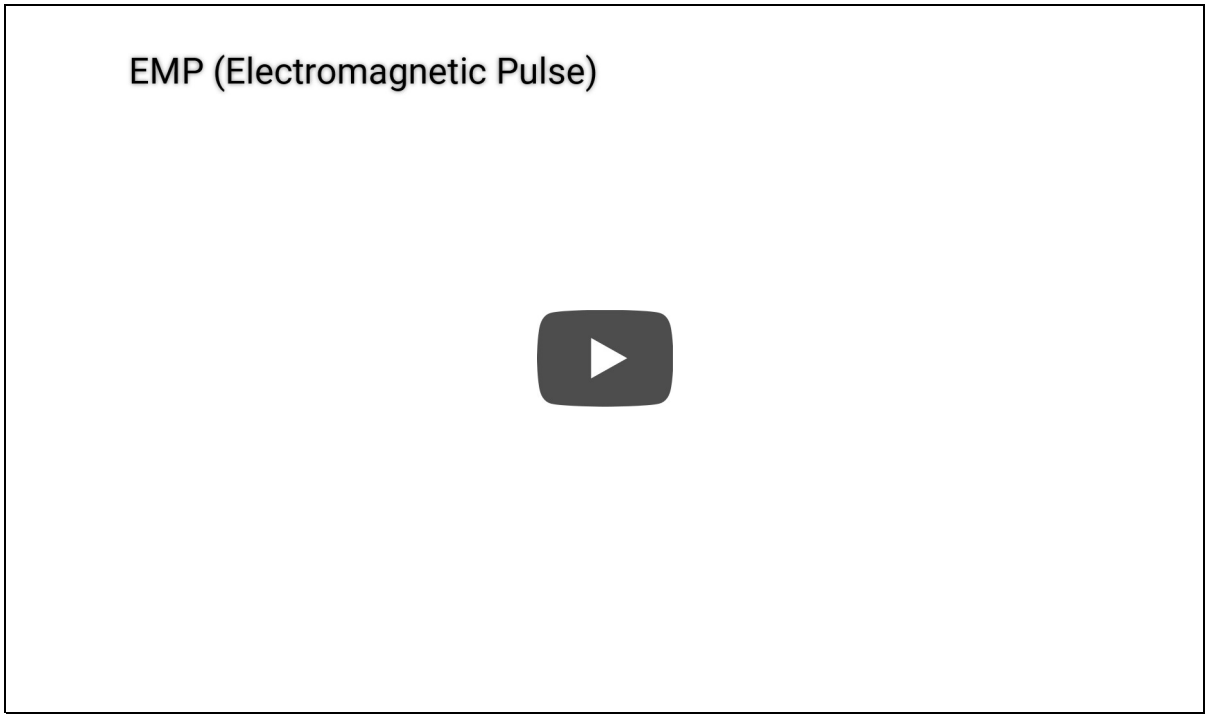
Simply increasing the number of steps a user thinks they've taken isn't likely to cause much damage other than to their exercise plan. But this flaw shows there is a more serious risk of intruders confusing the motion sensors within the control systems of other devices, such as the computers that run modern cars or drones. Previous research has also shown that accelerometers can be used for spying by effectively turning them into microphone or using them to monitor what keys a user is pressing on their smartphone.

Risks to devices

There is a general risk, too, around medical equipment, as accelerometers are often used to measure things such as the flow of medicine to a patient. So if medical devices can be affected by music, they could lead to incorrect flow measurements and so incorrect doses. The Michigan researchers outline that accelerometers are also used in healthcare applications, such as in pacemakers, and which could be affected by external sounds.

There is a similar potential problem in industrial plants, where accelerometers are again used to measure things like flow rates of chemicals or fuel. A high-powered sound wave could be used to confuse a plant's control system and cause its equipment to shut down. If used against power plants, this could lead to the nightmare scenario of an attack on the energy supply network.

Imagine if a drone army was flown over an area emitting high-powered sound waves. This could interfere with all local accelerometers in a way that interrupted the equipment they were part of, effectively causing a mass denial of service attack. This is already a known risk for radio interference, and where high-powered electromagnetic (EM) radio waves can be used to compromise the operation of electronic equipment as part of military operations. Further research would be required to find out the exact frequencies that affect the device and if they could be heard by humans.



Ocean's Eleven EM Power Blast.

The movie Ocean's Eleven even outlined an attack using EM pulses to cause a black-out in Las Vegas. And while disaster planners have looked to the threats of EM blasts, little work has been done on the effects of sound waves on modern electronic systems.

Other risks

Sound waves can be used to do more than just disrupt equipment. By analysing the noise coming from an electronic device, it is possible to extract data from it. Researchers at the University of Alabama at Birmingham in the US also found that they could determine user passwords by listening to the sounds that the keyboard made.

To the human ear, each keystroke sounds the same but it actually gives off a unique sound frequency

pattern. By using a number of suitably placed microphones to measure time differences and amplitudes of the received sound pulses, and with knowledge of the geometry of the keyboard, the researchers could identify which keys were being pressed.

Similarly, data can be obtained by analysing the radio signals or even the power variations from a device. A group of researchers recently demonstrated that it is possible to detect the movement of a user's hand on their device and so reveal their password by examining how it alters the reflection of local wi-fi signals.

Another researcher was able to analyse electrical power variations from eight of the most popular SIM cards for mobile phones and recover the keys that encrypt them within 40 minutes.

How to prevent it?

It is possible to protect a device against these side-channel attack, usually with a physical shield that protects them from leaking information or becoming compromised. A simple metal shield can stop radio signals but to stop sound waves affecting an accelerometer you would need a more complex acoustic shield to absorb the noise and minimise the vibrations causing the sensor to move. This would need to involve filtering out noise such as audio and speech signals, so the sensor only detected the movement it was designed to capture.

The findings that accelerometers can be affected by sound will come as a shock to many instrumental manufacturers, especially within the devices used in critical national infrastructure. More sensitive devices, such as medical equipment and those used in critical infrastructure, also need more rigorous testing to see how they respond in the face of a range of side-channel attacks.

Hacking **Cyber security** **Internet of Things** **Cyber-attack** **Sound waves**