wiley

NEWSLETTER

An Acoustic Hack – The Next Botnet Breach?

April 2017

Researchers at the University of Michigan and the University of South Carolina claim to have discovered that music could be used to disable or, to a certain extent, even control some Internet of Things (IoT) devices. The researchers say they were able, through sound waves, to add steps to a Fitbit tracker and interfere with a cell phone app's ability to steer a remote-controlled toy car.

To do so, the researchers used varying acoustic frequencies to exploit a claimed vulnerability in certain accelerometers – a hardware component that measures the amount of static acceleration due to gravity. These sensors serve a variety of purposes, ranging from those as basic as ensuring that your tablet computer screen is displayed upright to determining precisely when to deploy airbags in the event of a car accident. Manufacturers often build accelerometers within chip-based devices known as microelectromechanical systems (MEMs), which are used in a variety of products including cell phones, wearable devices, and drones and automobiles. The software components of connected devices frequently rely on the information provided by MEMs to determine the appropriate response. By creating an acoustic disturbance, the researchers affected the MEMs output.

This latest announcement emphasizes the role that academics and industry researchers can play in examining, discussing, and enhancing cybersecurity. Third-party research efforts can have various impacts and companies continue to grapple with how to address claims about their services and devices. Threats to IoT security are complex and constantly evolving, making cybersecurity research and information sharing key to enhancing the safety and reliability of connected devices. The University of Michigan and University of South Carolina researchers who discovered this potential vulnerability have

Authors

Madeleine M. Lottenbach
Associate
202.719.4193
mlottenbach@wiley.law

Practice Areas

Connected & Autonomous Vehicles
Internet of Things
Privacy, Cyber & Data Governance
Telecom, Media & Technology

also developed hardware and software solutions that can defend against acoustic attacks. The researchers are already working with chip manufacturers to improve the MEMs' design, as well as enhance the security of products already in the hands of consumers.

As connectivity explodes and more "things" interact with each other and the human environment, innovators can expect to continue reading about such "discoveries" – and having to address them.