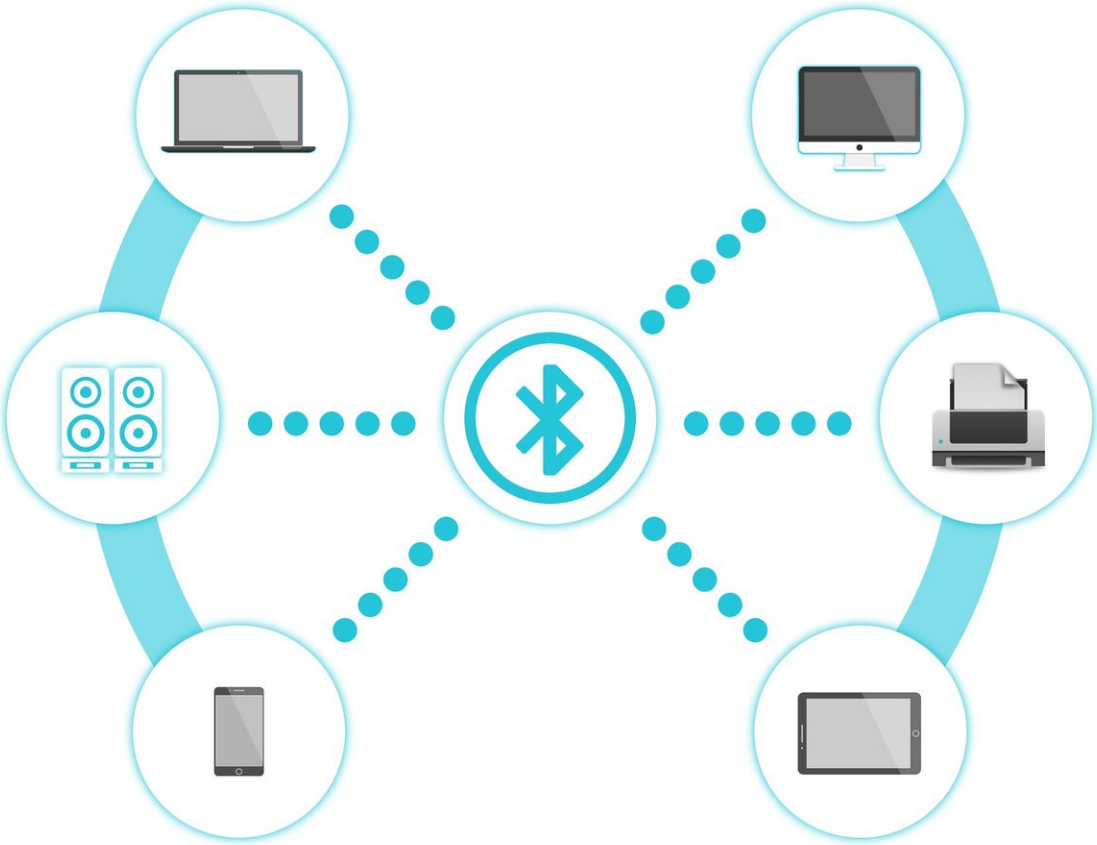
Design flaw could open Bluetooth devices to hacking

November 14 2019, by Laura Arenschield



Credit: CC0 Public Domain

Mobile apps that work with Bluetooth devices have an inherent design

flaw that makes them vulnerable to hacking, new research has found.

The problem lies in the way Bluetooth Low Energy devices—a type of Bluetooth used by most modern gadgets—communicate with the mobile apps that control them, said Zhiqiang Lin, associate professor of computer science and engineering at The Ohio State University. Lin presented the findings this week at the Association for Computing Machinery's Conference on Computer and Communications Security (ACM CCS 2019).

"There is a fundamental flaw that leaves these devices vulnerable—first when they are initially paired to a mobile app, and then again when they are operating," Lin said. "And while the magnitude of that vulnerability varies, we found it to be a consistent problem among Bluetooth low energy devices when communicating with mobile apps."

Consider a wearable health and fitness tracker, smart thermostat, smart speaker or smart home assistant. Each first communicates with the apps on your mobile device by broadcasting something called a UUID—a universally unique identifier. That identifier allows the corresponding apps on your phone to recognize the Bluetooth device, creating a connection that allows your phone and device to talk to one another.

But that identifier itself is also embedded into the mobile app code. Otherwise, mobile apps would not be able to recognize the device. However, such UUIDs in the mobile apps make the devices vulnerable to a fingerprinting attack, Lin and his research team found.

"At a minimum, a hacker could determine whether you have a particular Bluetooth device, such as a smart speaker, at your home, by identifying whether or not your smart device is broadcasting the particular UUIDs identified from the corresponding mobile apps," Lin said. "But in some cases in which no encryption is involved or encryption is used

improperly between mobile apps and devices, the attacker would be able to 'listen in' on your conversation and collect that data."

Still, that doesn't mean you should throw your smartwatch away.

"We think the problem should be relatively easy to fix, and we've made recommendations to app developers and to Bluetooth industry groups," he said.

After Lin and his team realized Bluetooth devices had this built-in vulnerability, they wanted to see how widespread it might be in the real world. They built a "sniffer"—a hacking device that can identify Bluetooth devices based on the broadcasting messages sent by the devices.

"The typical understanding is that Bluetooth Low Energy devices have signals that can only travel up to 100 meters," he said. "But we found that with a simple receiver adapter and amplifier, the signal can be 'sniffed' (or electronically found) much farther—up to 1,000 meters away."

They then drove the "sniffer" around a 1.28-square-mile area near Ohio State's campus to field-test the vulnerability. They found more than 5,800 Bluetooth Low Energy devices. Of those, about 5,500—94.6 percent—were able to be "fingerprinted" (or identified) by an attack and 431—7.4 percent—were vulnerable to unauthorized access or eavesdropping attacks.

Those that were vulnerable to unauthorized access had issues with the initial "fingerprinting" between device and phone app that put them at risk of hacking. "It was in the initial app-level authentication, the initial pairing of the phone app with the device, where that vulnerability existed," Lin said. If app developers tightened defenses in that initial

authentication, he said, the problem could be resolved.

The team reported their findings to developers of vulnerable apps and to the Bluetooth Special Interest Group, and created an automated tool to evaluate all of the Bluetooth Low Energy apps in the Google Play Store—18,166 at the time of their research. In addition to building the databases directly from mobile apps of the Bluetooth devices in the market, the team's evaluation also identified 1,434 vulnerable apps that allow unauthorized access, a number that surprised Lin. Their analysis did not include apps in the Apple Store.

"It was alarming," he said. "The potential for privacy invasion is high."

These devices know a lot about us—they are the wearable technologies that track our steps and our heart rates; the speakers that "hear" us and play songs we want to hear, or give us an easy way to order new things off the internet.

Lin's research focuses on vulnerabilities in tech, trying to identify those potential security gaps before they become true security problems. Earlier this summer, he and researchers at the Georgia Institute of Technology found more than 1,600 vulnerabilities in the support ecosystem behind the top 5,000 free apps in the Google Play Store.

Provided by The Ohio State University