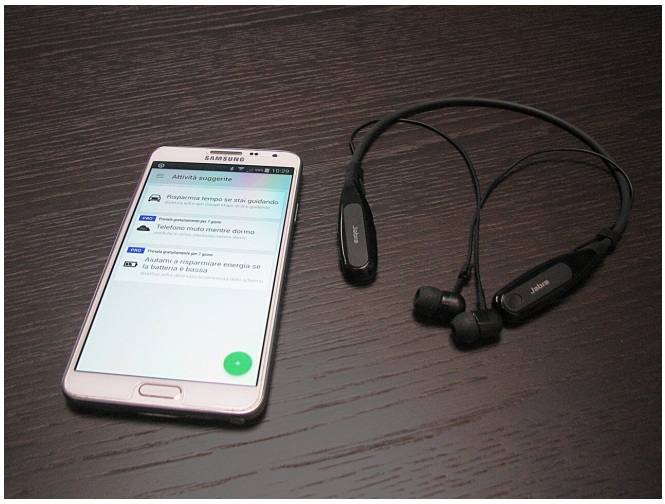
Bluetooth implementation issue raised by team exploring tracking

21 July 2019, by Nancy Cohen



Credit: CC0 Public Domain

Bluetooth devices could be giving away your location. That is what Boston University researchers discovered in their explorations, which are detailed in their paper, "Tracking Anonymized Bluetooth Devices" by Johannes Becker, David Li and David Starobinski, in *Proceedings on Privacy Enhancing Technologies*.

The authors reported that they devised a method for tracking Bluetooth devices despite built-in protections.

They were at the Privacy Enhancing Technologies Symposium in Stockholm, where they made their work known: a third-party algorithm could track the location of some Bluetooth devices.

The Brink, a site focused on research from Boston University, discussed the team's findings on July 17. Team member Becker was asked what made them chase this topic. "We were looking into different IoT protocols in general and trying to find privacy issues with those products," Becker told *The Brink*. "Basically everybody is carrying around a Bluetooth device nowadays in some way, shape, or form, and that makes it very relevant."

The Brink said that since the payload information updates at a different rate than the address information, the communication blips between Bluetooth devices paint an identifiable pattern. Having discovered this vulnerability, the researchers decided to test out how well it could be used by a third party to track individual devices.

PCMag India: When you connect two devices through Bluetooth, one of them acts as the main part of the connection and the other the peripheral, sending out data associated with the connection including a randomized address, which is like the IP address on your laptop or PC, to the main device.

A sniffer algorithm can be used to decode the randomized. address even though this randomized address gets reconfigured regularly.

"While this doesn't divulge personal information, it can allow third-parties to locate active Bluetooth devices and thereby the people using those devices. Theoretically, this issue can be leveraged to track the location of any Bluetooth-enabled device, be it a phone, smartband or a headphone," said *PCMag India*.

Also discussing this Bluetooth research was Ravie Lakshmanan in *TNW*:

To make device pairing easy, BLE (stands for Bluetooth Low Energy) uses public non-encrypted advertising channels to announce presence to nearby devices. The protocol originally attracted privacy concerns for broadcasting permanent Bluetooth MAC (Media Access Control) addresses of devices—a unique 48-bit identifier—on these channels.

However, BLE tried to solve the problem by letting

device manufacturers use a periodically changing, randomized address instead of a permanent MAC address.

So, devices may use a periodically changing, randomized address and not their permanent Media Access Control (MAC) address. And there's the rub: The authors showed how many devices implementing such anonymization measures could actually be vulnerable to passive tracking.

Perth-based *iLounge* on Friday translated what that might mean: "A recent flaw in Bluetooth technology allows individuals to track Apple Watches, Macs, iPads and iPhones. Tablets and laptops running Windows 10 and Fitbit wearables are also vulnerable, but for some reason Android devices are unaffected."

Android was found to be unaffected by all this. The researchers stated in their paper that "We describe a tracking vulnerability that affects Windows 10, iOS, and macOS devices as long as they are continuously observed by the adversary." Android devices do not appear to be vulnerable to our passive sniffing algorithm, as they typically do not send advertising messages containing suitable identifying tokens."

What to do?

Samantha Wiley in *iLounge* said the solution was not complicated, just "shut off your Bluetooth off and back on if you're worried about being tracked. This can be done via System Settings on the macOS' menu bar or in the Settings of your iPhone."*The Brink* similarly said thwarting this security gap "can be as simple as turning off and back on your device's Bluetooth connection, at least in the case of Windows 10 and iOS devices."

More information: Johannes K Becker*, David Li, and David Starobinski, "Tracking Anonymized Bluetooth Devices," *Proceedings on Privacy Enhancing Technologies* ; 2019 (3):50–65. petsymposium.org/2019/files/pa … popets-2019-0036.pdf