A simple firmware update completely hides a device's Bluetooth fingerprint

July 10 2024, by Ioana Patringenaru

Researchers developed a firmware update that hides a device's Bluetooth fingerprint. Credit: University of California - San Diego

A smartphone's unique Bluetooth fingerprint could be used to track the device's user–until now. A team of researchers have developed a simple firmware update that can completely hide the Bluetooth fingerprint, eliminating the vulnerability.

The method was developed by a team of researchers at the University of California San Diego. The team discovered the vulnerability caused by Bluetooth fingerprints in a study they presented at the 2022 IEEE Security & Privacy conference. They presented the fix to this vulnerability two years later at the 2024 IEEE Security & Privacy conference. The math behind the update itself is complex but the implementation is not.

"We assumed the strongest possible attack, a nation-state type of attacker that would know which algorithm we are using. They still failed," said Aaron Schulman, one of the paper's senior authors and a faculty member in the UC San Diego Department of Computer Science and Engineering.

Mobile devices, including phones, smartwatches and fitness trackers, constantly transmit signals, known as Bluetooth beacons, at the rate of roughly 500 beacons per minute. These beacons enable features like Apple's "Find My"—a tracking service to find a lost device as well as COVID-19 tracing apps; and connect smartphones to other devices such as wireless earphones.

The current approach taken by smartphone companies to make the devices hard to track by their Bluetooth signals is to randomly change the phone's identity, its MAC address. However, that doesn't address the physical-layer fingerprints inherent in each device's transmissions due to unique hardware imperfections.

All wireless devices have small manufacturing imperfections in the hardware used to emit these beacons that are unique to each device. These fingerprints are an accidental byproduct of the manufacturing process. These imperfections in Bluetooth hardware result in unique distortions, which can be used as a fingerprint to track a specific device.

The method the researchers developed uses several layers of randomization. The nature of the method is complex, but it's a bit like using several layers of contact lenses to mask a person's original eye color–and switching those layers repeatedly and randomly. This method would make it difficult to infer the person's true eye color–regardless of what the original color actually was.

The UC San Diego researchers implemented a prototype of this new defense on the Texas Instruments CC2640 chipset currently used in a number of smart devices, such as fitness trackers, tags and lighting systems. They analyzed the impact of different parameters that affect the success of attacks to track and fingerprint a device in practical scenarios. The result of their tests shows that the adversary has to observe a device continuously for more than 10 days to achieve the same level of tracking accuracy as they could achieve within a minute without the firmware update.

"This means that the fingerprints are no longer useful for the attacker to infer the identity of the device and the optimal attacker can barely do better than a random guess," said Professor Dinesh Bharadia, one of the paper's senior authors and a faculty member in the UC San Diego Department of Electrical and Computer Engineering.

"You can't track the phone's fingerprint even if you're sitting right next to it, because both MAC and PHY identities keep changing," he added.

Researchers are now looking for industry partners that can build this technology into their chipsets.

"This defense can be rolled out incrementally, requiring only software modification on at least one widely-used Bluetooth Low Energy chipset," said Hadi Givehchian, the paper's first author and a Ph.D. student in the UC San Diego Department of Computer Science and Engineering. "But

in order to deploy this defense widely, we need to partner with Bluetooth chip manufacturers."

The team also believes that the method would work to obfuscate WiFi fingerprints.

More information: Givehchian et al. Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices. *IEEE Symposium on Security and Privacy* (2022). DOI: 10.1109/SP46214.2022.00030, ieeexplore.ieee.org/stamp/stam … IPnOiQA7iRjYUtqPbUB4

Provided by University of California - San Diego