In a first, researchers use Bluetooth signals to identify and track smartphones

June 8 2022

Researchers tested their method to track Bluetooth fingerprints on campus. They use an off-the-shelf device to track and identify devices. Credit: University of California San Diego

A team of engineers at the University of California San Diego has demonstrated for the first time that the Bluetooth signals emitted constantly by our mobile phones have a unique fingerprint that can be used to track individuals' movements.

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" lost device tracking service; COVID-19 tracing apps; and connect smartphones to other devices such as wireless earphones.

Prior research has shown that wireless fingerprinting exists in WiFi and other wireless technologies. The critical insight of the UC San Diego team was that this form of tracking can also be done with Bluetooth, in a highly accurate way.

"This is important because in today's world Bluetooth poses a more significant threat as it is a frequent and constant wireless signal emitted from all our personal mobile devices," said Nishant Bhaskar, a Ph.D. student in the UC San Diego Department of Computer Science and Engineering and one of the paper's lead authors.

The team, which includes researchers from the Departments of Computer Science and Engineering and Electrical and Computer Engineering, presented its findings at the IEEE Security & Privacy conference in Oakland, Calif., on May 24, 2022.

All wireless devices have small manufacturing imperfections in the hardware 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. For Bluetooth, this would allow an attacker to circumvent anti-tracking techniques such as constantly changing the address a mobile device uses to connect to Internet networks.

Tracking individual devices via Bluetooth is not straightforward. Prior fingerprinting techniques built for WiFi rely on the fact that WiFi

signals include a long known sequence, called the preamble. But preambles for Bluetooth beacon signals are extremely short.

"The short duration gives an inaccurate fingerprint, making prior techniques not useful for Bluetooth tracking," said Hadi Givehchian, also a UC San Diego computer science Ph.D. student and a lead author on the paper.

Instead, the researchers designed a new method that doesn't rely on the preamble but looks at the whole Bluetooth signal. They developed an algorithm that estimates two different values found in Bluetooth signals. These values vary based on the defects in the Bluetooth hardware, giving researchers the device's unique fingerprint.

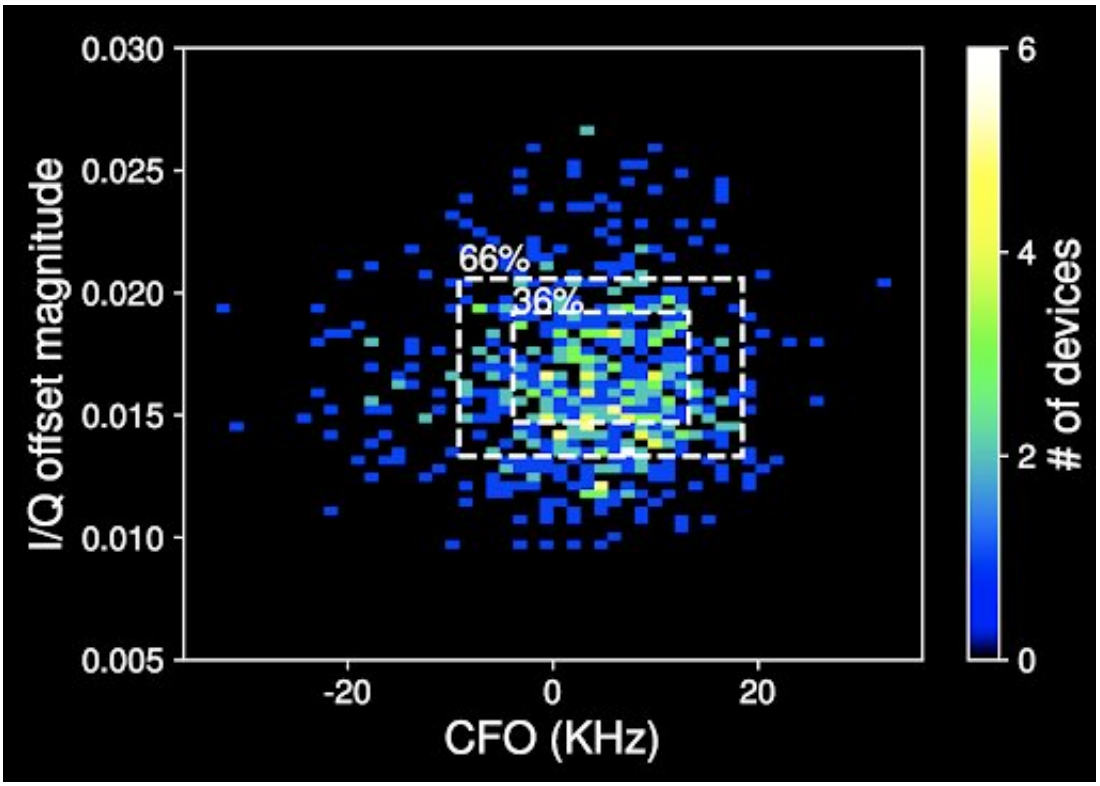
Real-world experiments

The researchers evaluated their tracking method through several real-world experiments. In the first experiment, they found 40% of 162 mobile devices seen in public areas, for example coffee shops, were uniquely identifiable. Next, they scaled up the experiment and observed 647 mobile devices in a public hallway across two days. The team found that 47% of these devices had unique fingerprints. Finally, the researchers demonstrated an actual tracking attack by fingerprinting and following a mobile device owned by a study volunteer as they walked in and out of their house.

Challenges

Although their finding is concerning, the researchers also discovered several challenges that an attacker will face in practice. Changes in ambient temperature for example, can alter the Bluetooth fingerprint. Certain devices also send Bluetooth signals with different degrees of

power, and this affects the distance at which these devices can be tracked.



Researcher were able to detect unique fingerprints for 47% of 647 devices. Credit: University of California San Diego

Researchers also note that their method requires an attacker to have a high degree of expertise, so it is unlikely to be a widespread threat to the public today.

Despite the challenges, the researchers found that Bluetooth tracking is likely feasible for a large number of devices. It also does not require sophisticated equipment: the attack can be performed with equipment that costs less than $200.

Solutions and next steps

So how can the problem be fixed? Fundamentally, Bluetooth hardware would have to be redesigned and replaced. But the researchers believe that other, easier solutions can be found. The team is currently working on a way to hide the Bluetooth fingerprints via digital signal processing in the Bluetooth device firmware.

Researchers are also exploring whether the method they developed could be applied to other types of devices. "Every form of communication today is wireless, and at risk," said Dinesh Bharadia, a professor in the UC San Diego Department of Electrical and Computer Engineering and one of the paper's senior authors. "We are working to build hardware-level defenses to potential attacks."

Researchers noticed that just disabling Bluetooth may not necessarily stop all phones from emitting Bluetooth beacons. For example, beacons are still emitted when turning off Bluetooth from the control center on the home screen of some Apple devices. "As far as we know, the only thing that definitely stops Bluetooth beacons is turning off your phone," Bhaskar said.

Researchers are careful to say that even though they can track individual devices, they are not able to obtain any information about the devices' owners. The study was reviewed by the campus' Internal Review Board and campus counsel.

"It's really the devices that are under scrutiny," said Aaron Schulman, a UC San Diego computer science professor and one of the paper's senior authors.

More information: Evaluating physical-layer BLE location tracking attacks on mobile devices, IEEE Security & Privacy conference in

Oakland, Calif., May 24, 2022. PDF: cseweb.ucsd.edu/~schulman/docs … nd22-bletracking.pdf

Provided by University of California - San Diego