The clever cryptography behind Apple's "Find My" feature



Enlarge / The 2018 15-inch Apple MacBook Pro with Touch Bar.
Samuel Axon

reader comments

125 with 69 posters participating

Share this story

When Apple executive Craig Federighi described a new location-tracking feature for Apple devices at the company's Worldwide Developer Conference keynote on Monday, it sounded—to the sufficiently paranoid, at least—like both a physical security innovation and a potential privacy disaster. But while security experts immediately wondered whether Find My would

also offer a new opportunity to track unwitting users, Apple says it built the feature on a unique encryption system carefully designed to prevent exactly that sort of tracking—even by Apple itself.

In upcoming versions of iOS and macOS, the new Find My feature will broadcast Bluetooth signals from Apple devices even when they're offline, allowing nearby Apple devices to relay their location to the cloud. That should help you locate your stolen laptop even when it's sleeping in a thief's bag. And it turns out that Apple's elaborate encryption scheme is also designed not only to prevent interlopers from identifying or tracking an iDevice from its Bluetooth signal, but also to keep Apple itself from learning device locations, even as it allows you to pinpoint yours.

"Now what's amazing is that this whole interaction is end-to-end encrypted and anonymous," Federighi said at the WWDC keynote. "It uses just tiny bits of data that piggyback on existing network traffic so there's no need to worry about your battery life, your data usage, or your privacy."



In a background phone call with WIRED following its keynote, Apple broke down that privacy element, explaining how its "encrypted and anonymous" system avoids leaking your location data willy nilly, even as your devices broadcast a Bluetooth signal explicitly designed to let you track your device. The solution to that paradox, it turns out, is a trick that requires you to own at least two Apple devices. Each one emits a constantly changing key that nearby Apple devices use to encrypt and upload your geolocation data, such that only the other Apple device you own possesses the key to decrypt those locations.

That system would obviate the threat of marketers or other

snoops tracking Apple device Bluetooth signals, allowing them to build their own histories of every user's location. "If Apple did things right, and there are a lot of ifs here, it sounds like this could be done in a private way," says Matthew Green, a cryptographer at Johns Hopkins University. "Even if I tracked you walking around, I wouldn't be able to recognize you were the same person from one hour to the next."

In fact, Find My's cryptography goes one step further than that, denying even Apple itself the ability to learn a user's locations based on their Bluetooth beacons. That would represent a privacy improvement over Apple's older tools like Find My iPhone and Find Friends, which don't offer such safeguards against Apple learning your location.

Here's how the new system works, as Apple describes it, step by step:

- When you first set up Find My on your Apple devices—and Apple confirmed you do need at least two devices for this feature to work—it generates an unguessable private key that's shared on all those devices via end-to-end encrypted communication so that only those machines possess the key.
- Each device also generates a *public* key. As in other public key encryption setups, this public key can be used to encrypt data such that no one can decrypt it without the corresponding private key, in this case the one stored on all your Apple devices. This is the "beacon" that your devices will broadcast out via Bluetooth to nearby devices.
- That public key frequently changes, "rotating" periodically to a new number. Thanks to some mathematical magic, that new number doesn't correlate with previous versions of the public key, but it still retains its ability to encrypt data such that only your devices can decrypt it. Apple refused to say just how often the key rotates. But every time it does, the

change makes it that much harder for anyone to use your Bluetooth beacons to track your movements.

- Say someone steals your MacBook. Even if the thief carries it around closed and disconnected from the internet, your laptop will emit its rotating public key via Bluetooth. A nearby stranger's iPhone, with no interaction from its owner, will pick up the signal, check its own location, and encrypt that location data using the public key it picked up from the laptop. The public key doesn't contain any identifying information, and since it frequently rotates, the stranger's iPhone can't link the laptop to its prior locations, either.
- The stranger's iPhone then uploads two things to Apple's server: the encrypted location, and a hash of the laptop's public key, which will serve as an identifier. Since Apple doesn't have the private key, it can't decrypt the location.
- When you want to find your stolen laptop, you turn to your second Apple device—let's say an iPad—which contains both the same private key as the laptop and has generated the same series of rotating public keys. When you tap a button to find your laptop, the iPad uploads the same hash of the public key to Apple as an identifier so that Apple can search through its millions upon millions of stored encrypted locations and find the matching hash. One complicating factor is that iPad's hash of the public key won't be the same as the one from your stolen laptop, since the public key has likely rotated many times since the stranger's iPhone picked it up. Apple didn't quite explain how this works. But Johns Hopkins' Green points out that the iPad could upload a series of hashes of all its previous public keys so that Apple could sort through them to pull out the previous location where the laptop was spotted.
- Apple returns the encrypted location of the laptop to your iPad, which can use its private key to decrypt it and tell you the laptop's last known location.

> Meanwhile, Apple has never seen the decrypted location, and since hashing functions are designed to be irreversible, it can't even use the hashed public keys to collect any information about where the device has been.

As staggeringly complex as that might sound, Apple warns that it's still a somewhat simplified version of the Find My protocol, and that the system is still subject to change before it's actually released in MacOS Catalina and iOS 13 later this year. The true security of the system will depend on the details of its implementation, warns Johns Hopkins' Green. But he also says that if it works as Apple described to Wired, it might indeed offer all the privacy guarantees Apple has promised.

"I give them nine out of 10 chance of getting it right," Green says. "I have not seen anyone actually deploy anything like this to a billion people. The actual techniques are pretty well known in the scientific sense. But actually implementing this will be pretty impressive."

This story originally appeared on wired.com.

https://arstechnica.com/?p=1517721