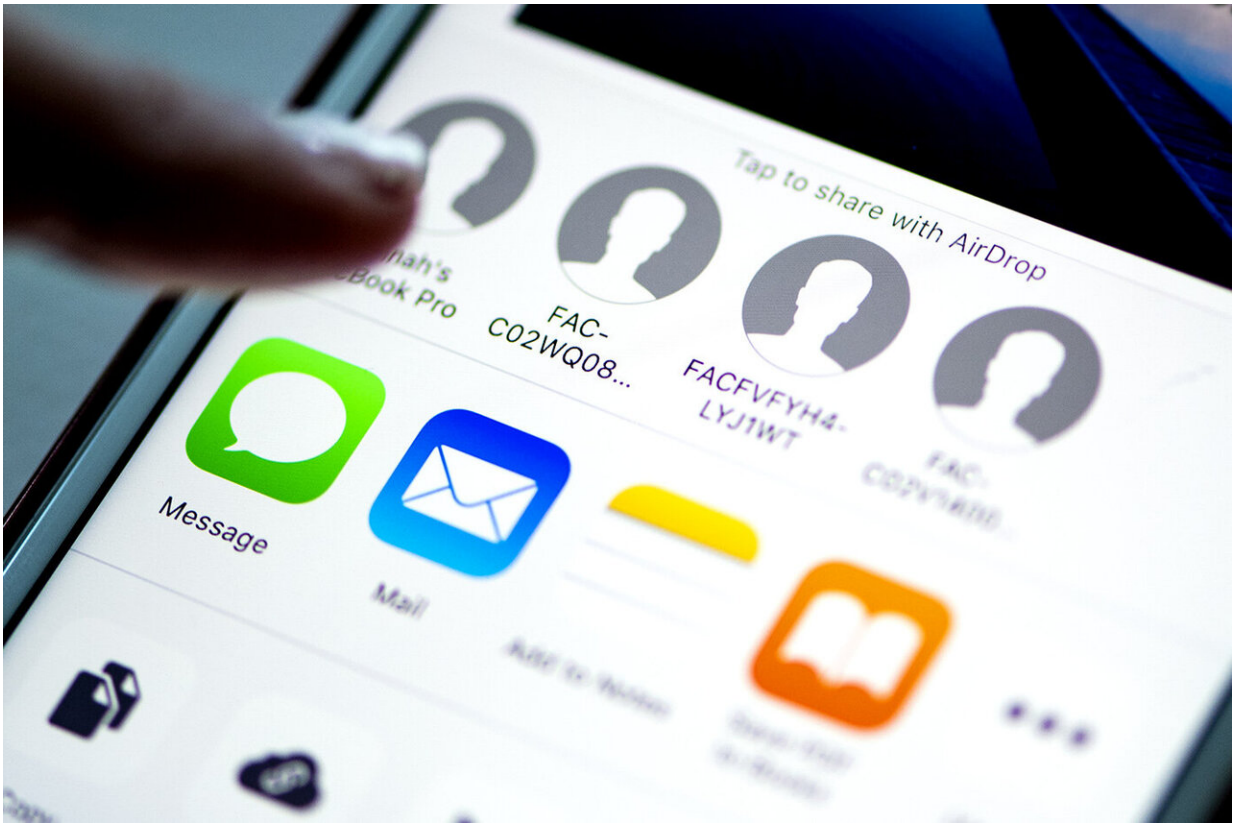
AirDrop is making your iPhone vulnerable to attackers

August 20 2019, by Laura Castañón



Credit: Ruby Wallau/Northeastern University

Whether you're checking text messages on your smartwatch or sharing selfies with a friend at a concert, it's becoming easier and easier to send files and information between devices. But this connectivity may come

at the expense of security.

A team of researchers from Northeastern University and the Technical University of Darmstadt in Germany recently uncovered a series of flaws that make Apple's AirDrop and similar services vulnerable to attack. Their work was presented at the Usenix Security Symposium last week.

"The worst aspect is that these attacks could happen anywhere," says Guevara Noubir, a professor of computer sciences and director of Northeastern's cybersecurity graduate program, who was part of the research team. "The attacker does not have to be connected to a network."

AirDrop uses Apple Wireless Direct Link, a protocol that allows nearby devices to communicate with one another through a combination of Bluetooth and Wi-Fi technologies. The researchers found design flaws and implementation bugs that would allow an attacker to crash devices, track users, and intercept files.

"All Apple devices rely on Apple Wireless Direct Link to discover neighboring devices," Noubir says. "Your phone to your laptop or to your smartwatch or Apple TV. They all use it."

In their first attack, Noubir and his collaborators showed that they could use Apple Wireless Direct Link to track a particular device and, in many cases, acquire personal information about it's owner.

Imagine you're using AirDrop to send a photo to your friend (we'll call him Gary). When you tap the "share" icon, your phone sends out a signal to wake up any nearby devices. If Gary has his iPhone's AirDrop set to receive data from anyone, his phone will automatically share identifying information. If he has AirDrop set to "contacts only," his device will

only wake up and send this information if it thinks you are in his contacts.

Every time you add a contact to your phone, it is assigned a condensed, identifying set of numbers. If a nearby device sends a signal with these numbers, your phone will assume the device is in your contacts and reply with more information. Gary's phone will recognize yours and respond.

But there is not an infinite number of identifiers. In fact, there are only 65,536 possibilities.

"Which means that if someone sends these 65,536 possible messages, every device would wake up and say, "This is me,"" Noubir says. "And then you can track them."

As long as an attacker sends a message that matches one of your contacts, your phone will respond automatically. The more contacts that you have in your phone, the less time it will take for an attacker to hit on a matching identifier. But even when they attacked a phone with just one contact, the researchers found they were able to send all 65,536 messages in about 30 seconds.

In a separate attack, Noubir and his colleagues were able to disrupt the communication between two devices, intercept the files being transferred, and pass on their own files instead.

Picture this: You and Gary both keep your AirDrop in "contacts only" mode. You try to send Gary a file, but your phone can't seem to detect his. Weird. Gary switches his phone to receive files from anyone, to see if that helps. It works! You see "Gary's iPhone" show up on your screen. You send Gary the file, and he accepts it.

But it wasn't you who sent him that file.

By keeping the two phones from detecting one another, the researchers created an opportunity to masquerade as the expected sender and receiver.

"We can interpose ourselves," Noubir says. "There will be a secure connection from one phone to us and a secure connection from us to the other phone, but they think they are talking to each other."

And now the attacker has the file you were trying to send and poor Gary has a virus on his phone.

The researchers also demonstrated that they could cause a series of devices to crash simultaneously. This last attack exploited a bug in Apple Wireless Direct Link, which Apple was able to patch after the team reported it. Noubir's collaborators included Sashank Narain, a postdoctoral researcher at Northeastern; Milan Stute, a doctoral student at the Technical University of Darmstadt who was a visiting scholar at Northeastern; and several other students and faculty from the Technical University of Darmstadt (Alex Mariotto, Alexander Heinrich, David Kreischmann, and Matthias Hollick).

The other vulnerabilities the researchers have discovered (and reported to Apple) will be more of a challenge to solve, because they are built into the design of the technology.

"They could redesign it more carefully, with different mechanisms to protect against these attacks," Noubir says. "It's just that it's difficult once all these devices are deployed. You need it to be compatible."

So what can Apple users do in the meantime? Install any updates that come out, Noubir says, and consider turning AirDrop off, or at least restrict it to your contacts.

"Unfortunately, the design of many mobile and wireless systems prioritizes user convenience and resource efficiency, until attacks are practically demonstrated and can no longer be ignored," Noubir says.

More information: Milan Stute, et al. A Billion Open Interfaces for Eve and Mallory: MitM, DoS, and Tracking Attacks on iOS and macOS Through Apple Wireless Direct Link. www.usenix.org/conference/usen … 9/presentation/stute

Provided by Northeastern University