# How the FBI might hack into an iPhone without Apple's help

March 22 2016, by Bree Fowler And Brandon Bailey

In this Friday, Sept. 25, 2015, file photo, a customer tries out a new Apple iPhone 6S at an Apple store in Chicago. The FBI now says that it may have a way to crack into an iPhone used by one of the San Bernardino shooters, despite previous claims that it could only achieve that with Apple's help, but it remains unclear exactly how it plans to do that. (AP Photo/Kiichiro Sato, File)

For more than a month, federal investigators have insisted they have no alternative but to force Apple to help them open up a phone used by one

of the San Bernardino shooters.

That changed Monday when the Justice Department said an "outside party" recently showed the FBI a different way to access the data on the phone used by Syed Farook, who with his wife killed 14 people in the Dec. 2 attack.

The magistrate judge in the case postponed a hearing scheduled for Tuesday and gave the government two weeks to test its method. But federal officials have been mum about who came forward and what method they've proposed. Here are some of the leading options outside experts think the FBI might be exploring.

—

BACK UP AND ATTACK

One likely scenario involves making multiple copies of the iPhone's flash memory, which investigators could use to restore the phone's data should they inadvertently trigger the phone's "self-destruct" feature by making too many wrong guesses at the passcode.

That feature doesn't actually erase all the files on the iPhone. Instead, it erases a section of the iPhone's memory that contains one of the keys necessary to unlock the data on the phone. This section, known as the "effaceable storage," sits in a memory chip that theoretically could be removed and plugged into a reader device that's capable of electronically copying what's stored on the chip—and then replacing the data if it's been erased.

While the technique hasn't been proven for this purpose, forensic expert Jonathan Zdziarski said it was demonstrated in a widely circulated video that shows a Chinese smartphone vendor using a similar procedure to

install more memory capacity on an iPhone. FBI Director James Comey was asked about the technique during a congressional hearing on March 1, but Comey didn't say directly whether the FBI had considered the approach.

---

RESET THE COUNT

A more nuanced approach would involve isolating the portion of the phone's memory where the count of how many passcode attempts have been made is stored, said Ajay Arora, CEO and co-founder of Vera, an encryption software company.

In theory, the person working on the phone would then be able to reset the count each time it approached 10, allowing investigators to make an infinite number of guesses.

"This is more technical and a little more difficult, because you'd have to isolate the section," he said. Apple hasn't provided any maps to show where that data is stored. The main problem: The FBI would run the risk of losing information if something went wrong.

Shane McGee, chief privacy officer at the FireEye cybersecurity firm, agreed that this kind of approach could potentially work. "All the government really needs is the opportunity to do a very simple, brute-force attack," he said.

---

DE-CAPPING

Another approach, sometimes known as "chip de-capping," calls for

physically removing the casing of the iPhone's processor chip, using acid or a laser drill. In theory, investigators could then connect electronic probes capable of reading the phone's unique identification code bit by bit from the location where it is "fused" into the phone's hardware. This method would also have to read the algorithm that combines that code with the user passcode to unlock the phone.

Once they get that information, investigators could then load it onto another computer, where they can run thousands of attempts at guessing the passcode without worrying about triggering the auto-erase function on the phone itself.

Forensic investigators have used similar procedures to read other kinds of data from computer chips, according to McGee. But experts say the process of physically dismantling a chip is technically demanding and has a high risk of causing damage that would make the data unreadable.

—

A BRAND NEW 'ZERO DAY'

Even a tiny flaw unknown to the software's creator—known as a zero-day vulnerability—could potentially give the government, or someone else, a way in, said Jay Kaplan, CEO of Synack and an a former NSA counterterrorism researcher.

Those exploits are considered valuable to hackers, who often sell them to others, and to intelligence agencies that use them for gathering data. It isn't clear if the government would share the information with Apple—which might then try to fix the vulnerability—or if the government would try to keep the information "in its back pocket" so it can be used for future cases, Kaplan said.

While in theory it's possible that investigators could go with some kind of brute-force attack, Kaplan thinks it's more likely that the FBI's mystery assistant found a zero day instead.

"There's plenty of them out there that vendors don't know about," Kaplan said. "Regardless of the method, it's going to be a pretty complex process, whether it involves a zero day or not. I'm sure a lot of really smart people are working on the problem."



Citation: How the FBI might hack into an iPhone without Apple's help (2016, March 22) retrieved 6 May 2024 from https://phys.org/news/2016-03-fbi-hack-iphone-apple.html