MOTHERBOARD

Why the FBI's Order to Apple Is So Technically Clever

Lorenzo Franceschi-Bicchierai and Joshua Kopstein

18 February 2016

On Tuesday, the US government dropped what might be the biggest bombshell yet in its ongoing war on encryption: A court order compelling Apple to help the FBI unlock the iPhone of one of the San Bernardino shooters who killed 14 people and injured 22 last December.

This is the latest chapter in the FBI's fight against Apple and encryption, which started when Apple implemented new security and encryption features with the launch of the iPhone 6 and iOS 9 in September of 2014. At the time, Apple said it wouldn’t be able to unlock phones anymore—even if the authorities came knocking at their door with a warrant—because it just didn’t have the technical means. But the US government has since been testing the legal boundaries of what it can force Apple, and by extension any other tech company, to do, mainly using the questionable legal authorities granted by a 227-year-old law.

And this time, it might have devised a way to prove that Apple does have the technical means to help cops and feds when they have to access data on a locked device.

At stake is whether a company can be legally compelled to sabotage the security of its own software

In the case of the San Bernardino shooter, rather than telling Apple to break the encryption protecting the device, which is an older iPhone 5C running iOS 9, the order would force the company to build a special version of its software that removes protections against anyone guessing your passcode millions of times until it gets it right—what’s technically known as a “brute-force” attack.

Apple immediately contested the order, calling it an “unprecedented step” where the government is essentially asking the company to “hack” its own users and create a “backdoor” that could be used any other time in the future.

For the US government, on the other hand, this is simply “writing software code,” which is not an “unreasonable burden for a company that writes software code as part of its regular business,” as an FBI agent argued in the case. This code, moreover, will only be targeted for this specific phone, according to the feds. In other words, they’re claiming this is just a one-time solution and doesn't constitute a backdoor.

But given what is known about how the iPhone protects users’ data with encryption, and what the feds are asking in this case, that is likely untrue—not just according to Apple, but also security experts who have studied the company’s software.

The government’s demands, the experts argue, ultimately have very little to do with unlocking a single phone, and everything to do with establishing far-reaching powers, and a technical way for the US government—and presumably, any government—to force companies to hack their own products.

Can Apple Comply With The Government’s Demand In This Case?

The answer, according to experts, is yes. Dan Guido, the CEO of cybersecurity firm Trail Of Bits, explained it in detail in a lengthy post on Tuesday.

Essentially, the US government is asking Apple to create a custom version of its operating system—Guido jokingly calls it “FBiOS”—which it can then load onto any iOS device to bypass its protections against rapidly guessing passcodes. On iOS 9, a security mechanism wipes the device clean if the wrong passcode is entered 10 times, and guesses are delayed for every wrong attempt. These were measures put in place to avoid forensic tools that could brute-force passcodes on previous iOS versions.

But the special OS version the court is ordering Apple to create (which court documents call a Software Image File, or SIF, and which some compare to a “forensic tool” developed by Apple itself) would remove those restrictions when loaded onto the device, leaving investigators free to try every possible passcode combination until the device is unlocked. The investigators wouldn’t even need to input the passcodes manually on the phone because they could connect the phone to an external computer or device and just run password-cracking software on it.

At that point, unlocking the phone depends on how long the passcode is. If it’s made of just six numbers—which is what people normally use given that it’s what Apple suggests by default—it would require less than a day, given that the iPhone’s hardware allows roughly 12 guesses per second (one every 80 milliseconds).

Could Apple Do The Same With Other iPhones?

What makes this case particularly interesting is that the phone in question is an older iPhone, the 5C. So the natural question is, could the FBI force Apple to help unlock other iPhones such as the 6 or 6S too? Could the FBI use the software specifically created by Apple to unlock the iPhone of the San Bernardino shooter and easily use it on other iPhones?

The answer then becomes much more complicated, thanks to the Secure Enclave, which became available on iPhones starting from the iPhone 5S, launched in 2013, but was not available on its cheaper brother, the 5C.

The Secure Enclave is not just a new feature, it’s an entirely separate computer within the iPhone which has control over the most sensitive parts of the iPhone, such as Apple Pay, TouchID, and, most importantly, the keys that encrypt the data on the phone, as well as those that encrypt iMessages.

Starting with iOS9, the Secure Enclave also enforces all those restrictions against brute-forcing mentioned before. It makes sure the phone gets wiped if the passcode gets guessed more than 10 times, and forces delays for every incorrect try.

Moreover, the Secure Enclave adds another layer of security. When you unlock the phone, your passcode gets mixed up with another key that’s physically embedded and fused in the Secure Enclave. This makes it extremely hard for anyone to get this embedded key, known as the “Class Key,” on their own.

That, however, doesn’t mean it’s impossible. In theory, the FBI could open up the phone and try to extract the keys using lasers, chemicals, or X-rays. But that, according to Guido, is “really uncharted territory” given that “the exact methods required are kind of unknown and the FBI would actually be making some new science here.”

That would also likely be expensive, and, most importantly, risky because it could destroy the data that the FBI is actually after.

“We’re only talking about one shot to take apart the phone and read out the hardware key, and if they screw up there is no way to turn back the dial,” Guido told Motherboard.

“It should be completely possible to apply this attack even on the newer phones.”

There’s one big catch, however. None of this matters if Apple can alter the firmware running the Secure Enclave. So if the feds ever get Apple to write that custom forensic tool to disable restrictions against brute-forcing passcodes on a 5C, there might be nothing preventing them to ask Apple to do the same for newer phones. (In that case, they would need two custom forensic tools, but the underlying workaround would be the same.)

Apple declined to comment, and did not answer a specific question asking whether it’s possible for Apple to alter the firmware on the Security Enclave. But experts, while saying only Apple knows the real answer, agree that it likely is.

“It should be completely possible to apply this attack even on the newer phones,” Ryan Stortz, a senior security researcher at Trail of Bits, who has studied how the Security Enclave works, told me. “Apple will still be creating a solution for the FBI that can be trivially re-used” [...] It’d be pretty generically applicable in the future.”

Stortz explained that at this point, the only difference would be that the brute-forcing would have to be done on the device itself, so the investigators wouldn’t be able to use an external computer. But Apple could still allow the same brute-forcing process to work via some sort of API, and at that point, the only restriction would still be the 80 millisecond limit between guesses, which is enforced at the hardware level, according to Stortz.

Could The Feds Do It Without Apple's Help?

Crucially, the SIF or "FBiOS" would need to be signed by Apple's developer key in order for the device to accept it. That's why Apple is being ordered to code the special software itself. But if the US government, or anyone else, could force Apple to surrender that master developer key, or stole it, then Apple wouldn't be needed anymore.

The order says that the action taken must be "proportionate," so legally compelling Apple to surrender its master development key would be a stretch. But accomplishing this would still be technically possible, though much harder, without Apple's help, if the FBI or NSA somehow managed to get Apple's signing key—say, by stealing it. (And we know from documents leaked by Edward Snowden that the CIA has been workingon ways to hack the iPhone without Apple's help for years.)

Once the key in their possession, investigators would be able to write the customized software image themselves and disable the auto-wipe feature without Apple's cooperation. Even further, it would empower the FBI to make software updates stamped with Apple's digital signature. In that case, it would essentially be game over.

Forcing a company to surrender encryption keys through legal means isn't completely without precedent, either. Edward Snowden's former email provider Lavabit was infamously compelled to hand over all of its SSL keys during a protracted legal fight with the US government, which resulted in the site being permanently shuttered by its owner, Ladar Levison.

In either case, security and legal experts point out that this would raise troublingconstitutional issues, since Apple would either be forced to create software to hack its own products or forced to surrender keys, which it would likely argue are protected under several regulations, including intellectual property laws, including as "trade secrets."

"'Give us your dev key' is probably on firmer ground legally than 'write custom code for us' but arguably way, way scarier," the CATO Institute's Julian Sanchez wrote on Twitter.

Give an FBI a key and he can fish for a day, but teach an FBI how to replace firmware and he can SPY FOREVER.

What's Really At Stake

Snowden called the case "the most important tech case in a decade," and it might very well be. At stake is whether a company can be legally compelled to sabotage the security of its own software, and the potential consequences are numerous and far-reaching.

Apple believes this is not about whether the company is technically able to comply with this particular order, but about the legal precedent this request would set, according to a source with knowledge of the matter. If the government wins in this case, the source said, it will compel Apple to weaken any other technical protections in the future, no matter the phone.

Furthermore, if the US government can compel Apple to write software that helps it crack passcodes, what's to stop other countries from demanding the same?

Despite the government's narrow framing on a single iPhone used by a dead mass murderer, one thing that's clear is that whatever technical solution results from the case will be used on countless other devices for years to come.

"We knew Apple could hack their own phones, the real question is, will the FBI get the precedent they want to be able to force Apple to hack their own phones?" Jonathan Zdziarski, a well-known iOS forensic expert, told Motherboard. "I have no doubt that if Apple wants to get into an iPhone 6 it can get into an iPhone 6. The bigger question is whether or not we're gonna let the courts decide that."