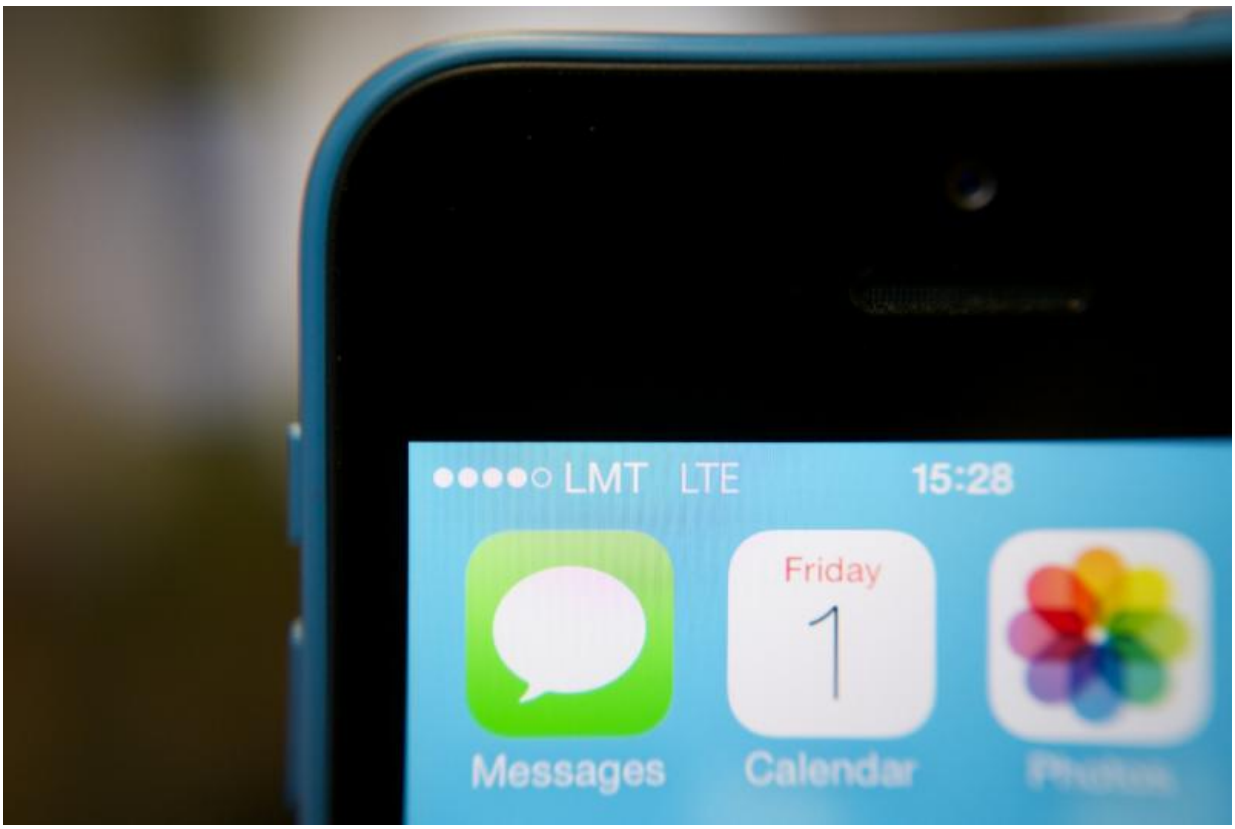
Passwords, privacy and protection—can Apple meet FBI's demand without creating a 'backdoor'?

February 24 2016, by H V Jagadish, University Of Michigan



Apple's security will erase a phone's contents after a certain number of failed attempts – something the FBI wants to avoid. Credit: janitors/flickr, CC BY

The San Bernardino terrorist suspect Syed Rizwan Farook used an

iPhone 5c, which is now in the possession of the FBI. The iPhone is locked. The FBI wants Apple to help unlock it, presumably so they can glean additional evidence or information about other possible attacks. Apple has declined, and appears to ready to defy a court order. Its response is due February 26. So what's the technology they're fighting over?

The code to unlock the phone is known only to Farook, who is dead, and any confidants he may have shared it with. Even if he were alive, it would probably be difficult to get him to reveal it.

But phones are typically locked with a very simple personal identification number (PIN) of only four to six digits. That means, at most, there are a million possible PIN values. It's straightforward to write a computer program that would methodically walk through all these possible values, trying each in turn until the correct one is found. Indeed, there even are products on the market that will do just this. Given that modern computers can execute over one billion instructions every second, even a conservative estimate says testing all one million PIN possibilities would take only about a second.

Ways to ward off attack

One way to defend against this kind of break-in attempt is to do something drastic after multiple failures. For example, Apple deletes all data on the iPhone after 10 incorrect unlocking attempts in succession, if the user has turned on this feature. We don't know if this defense is activated on Farook's phone – but the FBI doesn't want to gamble that it isn't, turn out to be wrong, and watch the phone be wiped clean after 10 incorrect guesses.

A second approach is to force a delay after each failed attempt. If the real authorized user accidentally types in the wrong code, she won't mind

waiting 60 seconds before the phone will let her try again. But for a computer that wants to try a million possibilities, the time required to try all possibilities has gone up by a factor of a million or more.

The FBI, of course, should have no difficulty programming a computer to try all possible passwords. It simply wants Apple to turn off the defenses.

What the FBI is and isn't asking for

The feds *aren't* demanding Apple create a "backdoor." In encryption, a backdoor is when someone has a means to access protected content outside of the normal (frontdoor) process. For example, there could be a skeleton key built into the encryption mechanism. The National Institute for Standards and Technology is reputed to have built such a facility into a random number generator, a function used in the heart of most encryption techniques.

Encryption with a backdoor is technology explicitly designed so that a third party – in most cases, law enforcement – can gain access to the protected data when the need arises. But it's very hard to build a backdoor into encryption, while still making it hard for an attacker to defeat. I don't believe anyone is calling for such encryption anymore.

Rather than tinker with its encryption, the FBI says it has asked Apple only to modify the defense mechanism built into iOS, its operating system. It's presumably easy for Apple to create a version of iOS where the delay and data erase features are turned off. This would be a new, less secure version of the standard operating system.

This less secure operating system could be loaded on to the Farook phone, which the FBI could then access more easily. Other iPhones would not be affected.

Software piracy is a major challenge here. Apple has to worry that copies of this insecure operating system may get out and become easily available – and not just to the good guys, but also the bad guys. It's common practice for software to require that a license be verified explicitly with the software vendor. If the license is not verified, the software will not function. This mechanism can block the insecure operating system from normal use.

But if the insecure operating system is installed for the purpose of data theft, then this normal license protection may not help – even if it doesn't allow normal use, it may not stop data access. In other words, it could be problematic if copies of this insecure operating system proliferate. However, it doesn't seem that hard to make sure that a one-time use operating system never leaks out.

It therefore appears there are no major technical barriers, or even immediate consequent difficulties, that prevent Apple from complying with the court order. Furthermore, it is hard to imagine a stronger case for law enforcement to gain access to encrypted data. In fact, a survey finds only 38 percent of Americans side with Apple and agree that they shouldn't unlock the terror suspect's phone. Nevertheless, there remain issues.

Our secure systems already fail all the time

It's not easy to build a secure system. We have so many breaches reported every day, in spite of the best efforts of so many. And the defenses that Apple has been asked to remove have already been violated, at least for some versions of Apple's products. Every additional wrinkle in the system design makes it more likely that new exploits will be found.

There is little question that this particular request from FBI will not be

the last one. In all likelihood, Apple would be asked to use the desired insecure iOS in other future situations. With every use, the possibility increases of the software being leaked.

It's also worth noting law enforcement does have access to the data in encrypted form without any help from Apple. These encrypted data look like gobbledygook and must be decrypted before they make sense. (In contrast, if they had, or could guess, the PIN, they would directly have access to the data in the convenient form ordinary users see.)

The point of encryption is to make decryption hard. However, hard does not mean impossible. The FBI could decrypt this data, with sufficient effort and computational power, and they could do this with no help from Apple. However, this route would be expensive, and would take some time. In effect, what they're requesting of Apple is to make their job easier, cheaper and faster.

Ultimately, how this matter gets resolved may depend more on the big-picture question of what privacy rights we as a society want for the data we record on our personal devices. Understanding the technical questions can inform this discussion.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: Passwords, privacy and protection—can Apple meet FBI's demand without creating a 'backdoor'? (2016, February 24) retrieved 26 April 2024 from https://phys.org/news/2016-02-passwords-privacy-protectioncan-apple-fbi.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.