Subject: Apple, Americans, and Security vs. FBI
Posted by Azrael on Wed, 24 Feb 2016 21:45:05 GMT
View Forum Message <> Reply to Message

This week's order by a federal magistrate judge requiring Apple to engineer new security flaws in its iPhone software operating system has prompted widespread and escalating controversy. Legitimate concerns about its implications have driven users around the country to raise their voices in defense of not only their privacy, but also the security of their online platforms threatened by the FBI's demands.

Beyond a single phone

While the FBI has framed its demand as addressing a single phone, it has failed to address concerns that the implementation of the order--which was issued on the same day the FBI submitted its motion, without changes--would necessarily place at risk the security of millions of other devices and the people who use them.

This week's order requires the development of a new software vulnerability that, as explained by the device's manufacturer, "[i]n the wrong hands...would have the potential to unlock any iPhone in someone's physical possession."

This tool would be dangerous, whether used by a black hat hacker who might infiltrate Apple systems, a future FBI investigation emboldened by this week's order to apply the precedent in other less compelling settings, or a dictatorship looking for new ways to oppress people that might cite the company's compliance with this FBI demand as a reason to comply with those of its own intelligence agencies. As my colleague Nate Cardozo explained on the PBS News Hour:

Authoritarian regimes around the world are salivating at the prospect of the FBI winning this order. If Apple creates the master key that the FBI has demanded that they created, governments around the world are going to be demanding the same access.

Beyond a single case

In that respect, the FBI's demands reflect a familiar pattern of security agencies leveraging the most seemingly compelling situations--usually the aftermath of terror attacks--to create powers that are later used more widely and eventually abused. The government programs monitoring the telephone system and Internet, for example, were created in the wake of the 9/11 attacks. Those programs came to undermine the rights of billions of people, doing more damage to our security than the tragic events that prompted their creation.

The power to force a company to undermine security protections for its customers may seem compelling in a particular case, but this week's order has very significant implications both for technology and the law. Not only would it require a company to create a new vulnerability potentially affecting millions of device users, the order would also create a dangerous legal precedent. The next time an intelligence agency tries to undermine consumer device security by forcing a company to develop new flaws in its own security protocols, the government will find a supportive case to cite where before there were none.

What is worse, we fear the government will not use this precedent carefully given that agency officials have a disturbing habit of twisting the facts even under oath, misleading judges and legislators on the rare occasion that they are forced to answer tough questions.

Yes, we are talking about creating a backdoor

Ultimately, this week's order risks undermining the interests of millions of iPhone users whose device security would be undermined by the development of a new backdoor.

"Backdoors" in security parlance refer to vulnerabilities used to access an otherwise closed system, like the vulnerabilities on Cisco routers that the NSA surreptitiously placed after intercepting that company's hardware shipments. While Judge Pym's order does not require the creation of a back door per se, it does require Apple to disable core security features that will allow the FBI to quickly and easily hack the phone.

Some people have suggested that this is not a backdoor, since implementing the order would not, in itself, give the FBI access to the phone (which it would still need to brute force in order to access). But the order removes important security features, leaving the phone vulnerable to the same extent that removing the security gate in front of a door might leave it vulnerable to someone inclined to break it down.

This is functionally a backdoor, one that the court has required Apple to create, to allow the FBI to then open using brute force. If any black hat hacker, foreign intelligence agency, or criminal syndicate got their hands on this tool, they could exploit it for their own nefarious purposes.

Don't take this sitting down

Resistance to this half-baked and ill-advised judicial command has already taken many forms, and will continue to escalate over the next week, when Apple is scheduled to file its objections to the magistrate's order just a few days before EFF will file an amicus brief supporting Apple.

The day after the order was issued, users congregated at the Apple store in San Francisco to voice their support of the company's stance against FBI demands to undermine security for everyone. Next week, similar gatherings are planned in cities across the country, and at the FBI headquarters in Washington, DC, organized by our friends at Fight For The Future with transpartisan support from numerous organizations including CREDO, Demand Progress, the Bill of Rights Defense Committee / Defending Dissent Foundation, Downsize DC, and others.

While we help defend Apple in the courts, we invite you to participate in the defense of your own privacy & security by joining these actions and raising your voice through every channel available. If you do participate in an action next week responding to these FBI demands, please join us to share your experience with others.

https://www.eff.org/deeplinks/2016/02/apple-americans-and-se curity-vs-fbi