Experts: The FBI's iPhone-unlocking plan for Apple is risky

February 22 2016, by Brandon Bailey

This Feb. 17, 2016 file photo shows an iPhone in Washington. In the searing debate over the FBI's effort to unlock a terrorist's iPhone, federal authorities argue they're seeking only limited help from Apple that won't compromise the privacy of other iPhone users. Security experts say it's not so simple. (AP Photo/Carolyn Kaster)

In its battle with Apple over an extremist's iPhone, the FBI says neither the company nor anyone else has anything to fear. Although they want to compel assistance from Apple to unlock a phone used by San Bernardino mass shooter Syed Farook, officials say the techniques they propose are limited in scope and pose no risk to the privacy of other iPhone users.

Security experts say it's not so simple.

"It's a very dangerous proposition to claim that this capability could not be re-used," said Will Ackerly, chief technology officer at Virtru, a computer security firm he co-founded after working 8 years at the National Security Agency.

Federal prosecutors have asked a court to force Apple to produce special software that would help the FBI guess the passcode to an iPhone found in Farook's car. Federal officials say Apple will be free to destroy that software once the iPhone is open to investigators.

Apple argues it's unrealistic to think that governments, both in the U.S. and overseas, won't ask to use the same program again in other cases. Ackerly and other experts echoed that concern. And on technical grounds, experts say, it may simply be impossible to keep the program from falling into the wrong hands.

True, some experts say Apple CEO Tim Cook is exaggerating when he says the government wants the company to create a "backdoor" into otherwise secure information held on iPhones. It might be closer to say the government wants to require Apple to help pick the lock to the front door. Even that approach, however, could still pose broader dangers.

Essentially, the FBI wants Apple to write a program that disables some iPhone security features so that federal computer experts could guess the phone's passcode by "brute force." Unlocking the phone with the passcode automatically decodes encrypted files. In particular, the FBI wants to disable a "self-destruct" mechanism that could render the phone unreadable after 10 bad guesses, as well as an enforced delay of up to an hour between incorrect passcode attempts.

U.S. officials say their precautions would prevent anyone else—governments and criminal hackers included—from re-using that bypass software on other phones.

First, the government says Apple can design the program to work only when it recognizes Farook's iPhone, by checking the unique identifying code assigned to each device Apple makes. The iPhone won't respond if the program doesn't contain a cryptographic signature that verifies the software was created by Apple, the government said in its court filing.

Authorities say the program can be loaded onto the iPhone's temporary memory, so it will disappear once the iPhone is turned off. As an additional precaution, the government says Apple can design the program to let investigators try different passcodes by submitting them electronically, so that Apple can keep physical control over the iPhone while the special program is deployed.

"Compliance with the order presents no danger to any other phone," prosecutors said Friday in a court document signed by Assistant U.S. Attorney Tracy Wilkinson.

Those measures should prevent anyone from getting their hands on the special software or re-using it on another phone, agreed Chris Eng, vice president of research at Veracode, a computer security firm. "From a technical perspective, I believe what's being described is completely possible."

Eng said he'd be more concerned if the government was seeking a true "backdoor"—a change in Apple's encryption algorithm that would let others break the code. That's not what the FBI is pursuing in this case, he said.

But other experts warned of technical risks in the government's plan. They said it would be difficult, but not impossible, to reverse-engineer the Apple program so it could work with other phones. Software is easy to copy, despite the government's reassurances, said Bruce Schneier, a security expert and chief technology officer for Resilient Systems. "That's the nature of software."

The program wouldn't work on another iPhone unless a hacker modified it to recognize that device, and that would require forging Apple's digital signature, said Steve Bellovin, a computer science and security expert at Columbia University. But he said it's not beyond the realm of possibility that sophisticated hackers or a foreign government could steal Apple's signature code.

Though Apple is known for guarding its secrets closely, a senior executive said recent history shows that no companies are immune to hacking—either by outsiders or an employee who's been bribed to steal secrets. The executive, who spoke on condition of anonymity, also asserted that an outsider wouldn't need Apple's digital signature to modify the program so it works with another phone.

Any risk that the software could be stolen or modified will increase because other law enforcement agencies are likely to ask Apple to re-use that tool in the future, Apple contends. "Law enforcement agents around the country have already said they have hundreds of iPhones they want Apple to unlock if the FBI wins this case," the company said in a statement Monday.

Using the software even once could give authorities or outsiders new clues to how Apple's security features work, potentially exposing vulnerabilities that could be exploited in the future, Ackerly said. If

Apple allows federal investigators to submit passwords through a remote connection, he added, that could open the phone to intrusion—including efforts to copy the program.

The government has promised it won't try to copy Apple's software, of course, and doing so would risk a judge's ire or even legal penalties.

Computer forensics expert Jonathan Zdziarski raised another possibility: If authorities find anything on the iPhone that they use in court—for example, to identify and prosecute any accomplices who aided the San Bernardino shooters—then Apple could be required to explain its software in court. A judge might also permit defense attorneys and their experts to study the program.

There's a strong likelihood "this tool won't be used once, but many times," Zdziarski said in an email, adding that each time could expose the software to copying or misuse.

Citation: Experts: The FBI's iPhone-unlocking plan for Apple is risky (2016, February 22) retrieved 25 April 2024 from
https://phys.org/news/2016-02-experts-fbi-iphone-unlocking-apple-risky.html