An iPhone-hacking tool likely wouldn't stay secret for long

March 18 2016, by Bree Fowler

In this Friday, Sept. 25, 2015 file photo, people wait in front of an Apple store in Munich, Germany before the worldwide launch of the iPhone 6s. Tech and legal experts say if Apple were to create the iPhone-hacking software demanded by the FBI, it would have a tough time staying secret, given the "potentially unlimited" number of people that would likely get a look at its inner workings. (AP Photo/Matthias Schrader, File)

Suppose Apple loses its court fight with the FBI and has to produce a software tool that would help agents hack into an iPhone—specifically, a

device used by one of the San Bernardino mass shooters. Could that tool really remain secret and locked away from potential misuse?

Not very likely, according to security and legal experts, who say a "potentially unlimited" number of people could end up getting a close at the tool's inner workings. Apple's tool would have to run a gauntlet of tests and challenges before any information it helps produce can be used in court, exposing the company's work to additional scrutiny by forensics experts and defense lawyers—and increasing the likelihood of leaks with every step.

True, the Justice Department says it only wants a tool that would only work on the San Bernardino phone and that would be useless to anyone who steals it without Apple's closely guarded digital signature.

But widespread disclosure of the software's underlying code could allow government agents, private companies and hackers across the world to dissect Apple's methods and incorporate them into their own device-cracking software. That work might also point to previously unknown vulnerabilities in iPhone software that hackers and spies could exploit.

Cases in which prosecutors have signaled interest in the Apple tool, or one like it, continue to pile up. In Manhattan, for instance, the district attorney's office says it holds 205 encrypted iPhones that neither it nor Apple can currently unlock, up from 111 in November. Such pent-up demand for the tool spells danger, says Andrea Matwyshyn, a professor of law and computer science at Northeastern University, since its widespread dissemination presents a clear threat to the security of innocent iPhone users.

"That's when people get uncomfortable with a potentially unlimited number of people being able to use this in a potentially unlimited number of cases," Matwyshyn says.

—

THE CREATION PROCESS

The concerns raised by experts mirror those in Apple's own court filings, where the company argues that the tool would be "used repeatedly and poses grave security risks." Outside experts note that nothing would prevent other prosecutors from asking Apple to rewrite the tool for the phones they want to unlock, or hackers from reverse engineering it for their own purposes.

Apple's long history of corporate secrecy suggests it could keep the tool secure during development and testing, says John Dickson, principal at Denim Group, a San Antonio, Texas-based software security firm. But after that, "the genie is out of the bottle," he says.

Even if the software is destroyed after use in the San Bernardino case, government authorities—in the U.S. or elsewhere—could always compel them to recreate it.

—

TESTING THE TOOL

Apple argues that the tool, which is essentially a new version of its iOS phone operating software, would need rigorous testing. That would include installing it on multiple test devices to ensure it won't alter data on the San Bernardino iPhone.

Similarly, the company would need to log and record the entire software creation and testing process in case its methods were ever questioned, such as by a defense attorney. That detailed record itself could be a tempting target for hackers.

Before information extracted by the Apple tool could be introduced in court, the tool would most likely require validation by an outside laboratory, say forensics experts such as Jonathan Zdziarski, who described the process in a post on his personal blog . For instance, Apple might submit it to the National Institute of Standards and Technology, an arm of the Commerce Department, exposing its underlying code and functions to another outside group of experts.

The likelihood of someone stealing the tool grows with every copy made, says Will Ackerly, a former National Security Agency employee who's now chief technology officer at Virtru, a computer security startup. And while Apple may be known for its security, the federal government isn't.

Lance Cottrell, chief scientist at Ntrepid, a Herndon, Virginia-based provider of secured Internet browsers, pointed to last year's hacking of the Office of Personnel Management, which compromised the personal information of 21 million Americans, including his own.

Once such a tool exists, "it will become a huge target for hackers, particularly nation-state hackers," Cottrell predicted. "If I was a hacker and I knew this software had been created, I'd be really trying really hard to get it."

___

SCRUTINY IN COURT

Then there's court, where defense experts would want a close look at the tool to ensure it wasn't tainting evidence, says Jeffrey Vagle, a lecturer in law at the University of Pennsylvania Law School. "It could get quite tangled from a technical standpoint," he says.

One very likely consequence: More eyes on the tool and its underlying

code. And as more jurisdictions face the issue of iPhones they can't unlock, it's impossible to calculate where that would end.

The Manhattan DA's office, for instance, says it expects the number of locked phones to rise over time. The vast majority of iPhones now run iOS 8 or more recent versions, all of which supports the high level of encryption in question.

Elsewhere in the country, the Harris County DA's office in Texas encountered more than 100 encrypted iPhones last year. And the Cook County State Attorney's Cyber Lab received 30 encrypted devices in the first two months of this year, according to the Manhattan DA's office.