Apple closing iPhone security gap used by law enforcement

14 June 2018, by Michael Liedtke

In this July 28, 2016 file photo, the Apple logo is shown on a sign hanging in front of a new Apple Store, in the Williamsburg section in the Brooklyn borough of New York. Apple is closing a security gap that allowed outsiders to pry personal information from locked iPhones without a password, a change that will thwart law enforcement agencies that exploited the vulnerability to collect evidence in criminal investigations. (AP Photo/Mark Lennihan, File)

Apple is closing a security gap that allowed outsiders to pry personal information from locked iPhones without a password, a change that will thwart law enforcement agencies that have been exploiting the vulnerability to collect evidence in criminal investigations.

The loophole will be shut down in a forthcoming update to Apple's iOS software, which powers iPhones.

Once fixed, iPhones will no longer be vulnerable to intrusion via the Lightning port used both to transfer data and to charge iPhones. The port will still function after the update, but will shut off data an hour after a phone is locked if the correct password isn't entered.

The current flaw has provided a point of entry for authorities across the U.S. since the FBI paid an unidentified third party in 2016 to unlock an iPhone used by a mass killer in the San Bernardino shooting a few months earlier. The FBI sought outside help after Apple rebuffed the agency's efforts to make the company create a security backdoor into iPhone technology.

Apple's refusal to cooperate with the FBI at the time became a political hot potato pitting the rights of its customers against the broader interests of public safety. While waging his successful 2016 campaign, President Donald Trump ripped Apple for denying FBI access to the San Bernardino killer's locked iPhone.

In a Wednesday statement, Apple framed its decision to tighten iPhone security even further as part of its crusade to protect the highly personal information that its customers store on their phones.

CEO Tim Cook has hailed privacy as a "fundamental" right of people and skewered both Facebook and one of Apple's biggest rivals, Google, for vacuuming up vast amounts of personal information about users of their free services to sell advertising based on their interests. During Apple's 2016 battle with the FBI, he called the FBI's effort to make the company alter its software a "dangerous precedent" in an open letter .

"We're constantly strengthening the security protections in every Apple product to help customers defend against hackers, identity thieves and intrusions into their personal data," Apple said. "We have the greatest respect for law enforcement, and we don't design our security improvements to frustrate their efforts to do their jobs."

it was first reported by various new outlets, including Reuters and The New York Times.

It's unclear what took Apple so long to close an iPhone entryway that had become well-known among legal authorities and, presumably, criminals as well.

It got to that point that two different firms, Israel-based Cellebrite and U.S. startup Grayshift, began to sell their services to law enforcement agencies trying to hack into locked iPhones, according to media reports. Grayshift, founded by a former Apple engineer, even markets a $15,000 device designed to help police to exploit the security hole in the iPhone's current software.