HOW ENCRYPTION WORKS ON PHONES

BY GARY ROBBINS The San Diego Union Tribune Thursday, February 18, 2016

What's the technology underlying the escalating showdown between Apple and the FBI?

The company is challenging a federal judge's order to help the agency "unlock" an iPhone that was used by Syed Rizwan Farook, who along with his wife killed 14 people and injured about two dozen others in San Bernardino in December. Here is a primer about the encryption standards in question, based on statements by Apple, the FBI, UC San Diego computer scientist Stefan Savage, cybersecurity expert Murray Jennex at San Diego State University and Rajesh Gupta, chair of the computer science and engineering department at UC San Diego. Their information has been edited for continuity and clarity.

Q:

Why does the FBI need Apple's help to decrypt the iPhone 5C used by one of the shooters in the San Bernardino terrorist attack?

A:

The FBI doesn't know the four-digit passcode for the iPhone. Its agents can type in guesses. But if they guess wrong 10 times, it could trigger the phone's autoerase feature, which would destroy the encrypted data the agency is trying to recover.

Besides wanting Apple to help it avoid wrong guesses, the government seeks a way to disable the auto-erase feature. It's essentially trying to bypass or disable the phone's security system.

This would require Apple to write a software program, a "back door" of sorts, to safely access the phone. Apple has created such "back doors" in years past, but said it no longer does so because it's concerned that they would be used to unlawfully access people's private information.

"Technically, I don't think Apple is arguing (that unlocking) cannot be done," Gupta said. "It's just that a customized version — like a virus— has a potential to 'escape' and do more harm."

It's also possible that Farook or his accomplices modified the phone to thwart counter-hacking efforts.

Q:

If the auto-erase program is triggered, would it immediately erase all data on the phone?

A:

When you erase a file, it doesn't go away immediately. It frees up space. The data goes away after the file has been overwritten a number of times. And it's not like the phone will burn up or start smoking or physically destroy itself.

Q:

Is there a way to reconstruct data that has been erased from an iPhone?

A:

It's a possibility. An agency might have advanced abilities that we don't know about. But the FBI suspects that Farook's phone might contain details involving the militant group Islamic State, so it doesn't want to risk doing something that might wipe out key information.

Q:

Couldn't Apple create a one-time "back door" that would unlock Farook's phone and then destroy that "back door"?

A:

That's a possibility, but Apple is concerned about the prospect. In a letter it sent to customers Wednesday, the company said in part: "Some would argue that building a 'back door' for just one iPhone is a simple, clean-cut solution. But it ignores both the basics of digital security and the significance of what the government is demanding in this case."

In today's digital world, the "key" to an encrypted system is a piece of information that unlocks the data, and that "key" is only as secure as the protections around it. Once the information is known or a way to bypass the code is revealed, the encryption can be defeated by anyone with such knowledge.

"The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again on any number of devices," Apple said in its letter. "In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks— from restaurants and banks to stores and homes. No reasonable person would find that acceptable."

UC San Diego's Gupta said how the battle between personal privacy and crime-fighting plays out will be most consequential.

"This story is interesting not for what is, but what could be in the future," he said. "Unfortunately, it is a future still unknown."

gary.robbins@sduniontribune.com

"The government suggests this tool could only be used once, on one phone. But that's simply not true." Apple's letter sent to customers on Wednesday