Johns Hopkins researchers find bug in iMessage encryption

22 March 2016, by Nancy Owano

(Tech Xplore)—On the one side, you have the U.S. government sounding an alarm to Silicon Valley that encryption, as it's being deployed, hampers law enforcement in reaching the communications of terrorists and criminals.

On the other side, you have encryption capabilities unleashed by Apple —shielding data on devices, video calls and instant messages to protect their customers' privacy.

This week a third actor jumped on stage, with important news: Johns Hopkins University researchers found a bug in Apple's encryption, enough to allow an attacker to decrypt photos and videos sent as secure instant messages.

The Washington Post reporter Ellen Nakashima along with numerous other sites came out with the story on Monday. The specific flaw is in Apple's iMessage program, which is utilized to send text messages. Robert McMillan, reporter, *The Wall Street Journal*, however, pointed out: The researchers' findings have no direct bearing on the iPhone of interest to the government. "The iMessage flaw could be used to decrypt attachments only as they were sent over the Internet, not to read stored messages from a locked and encrypted iPhone …."

The security hole in the iMessage program may not help the FBI in the San Bernardino quest but it had its own teachable moment, according to *The Washington Post*.

It shatters the notion that strong commercial encryption has left no opening for law enforcement and hackers, said Matthew D. Green, a computer science professor at Johns Hopkins University. Green led the research team.

Apple, meanwhile, praised the Johns Hopkins team who found the bug. *The Washington Post* article reported on Apple's statement: "Apple works hard to make our software more secure with every release," the company said. "We appreciate the team of researchers that identified this bug and brought it to our attention so we could patch the vulnerability." The response from Apple also said the company was grateful to have a community of developers and researchers who help them stay ahead.

Apple said it will address the problem through security improvements in its latest operating system, iOS 9.3.

As for the bigger picture, here is an excerpt from Matthew Green's blog post on Monday, which sat under the umbrella title, "A Few Thoughts on Cryptographic Engineering."

"So what does it all mean? As much as I wish I had more to say, fundamentally, security is just plain hard. Over time we get better at this, but for the foreseeable future we'll never be ahead. The only outcome I can hope for is that people realize how hard this process is—and stop asking technologists to add unacceptable complexity to systems that already have too much of it."

APA citation: Johns Hopkins researchers find bug in iMessage encryption (2016, March 22) retrieved 28 June 2022 from https://techxplore.com/news/2016-03-johns-hopkins-bug-imessage-encryption.html